## Large sets of block designs

## Citation for published version (APA):

Kang, Q. (1989). Large sets of block designs. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Mathematics and Computer Science]. Technische Universiteit Eindhoven. https://doi.org/10.6100/IR314990

## DOI:

10.6100/IR314990

## Document status and date:

Published: 01/01/1989

## Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

## Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.
Link to publication


## General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

## Take down policy

If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.

关于区组设计的大集问题
Large Sets of Block Designs

Kang Qingde

LARGE SETS OF BLOCK DESIGNS

# Large Sets of Block Designs 

## PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, Prof. ir. M. Tels, voor een commissie aangewezen door het College van Dekanen in het openbaar te verdedigen op vrijdag 18 augustus 1989 te 16:00 uur

> door

## KANG QINGDE

geboren op 22 oktober 1942 te Shanghai, China

Dit proefschrift is goedgekeurd door de promotoren:
prof. dr. A.E. Brouwer
prof. dr. J.H. van Lint

To my motherland， my parents and my dear wife．

献给我的祖国
我的父母
我的受絜

## Acknowledgements

I want to thank prof. A.E. Brouwer and prof. J.H. van Lint for their help and inspiration. They gave me a lot of stimulation and support during my stay in the Netherlands.

I am very grateful to dr. J.W. Nienhuys who helped me with TEX and many other things. He is always very kind and finds it a pleasure to help others.

Many thanks go to mrs. J. van Amsterdam for her care and her patience. She helped me with many things and created a pleasant working atmosphere.

I wish to express my gratitude to the Department of Mathematics and Computer Science of the Eindhoven University of Technology for inviting me and providing the opportunity and environment to write this thesis.

## Contents

1. Preliminaries ..... 2
1.1 Introduction ..... 2
1.2 Some background about algebra ..... 3
1.3 Block designs and large sets of block designs ..... 5
2. Mendelsohn triple systems ..... 8
2.1 Introduction ..... 8
2.2 The odd order case ..... 8
2.3 A recursive construction ..... 10
2.4 LMTS $\left(2^{n}+2\right), n \neq 2$ ..... 13
2.5 Correction of an error ..... 23
2.6 Nonisomorphic large sets ..... 28
3. Mendelsohn systems ..... 33
3.1 A generalization of MTS ..... 33
3.2 The construction of some $L M(2, k, v)$ ..... 35
3.3 Another method for the prime case ..... 38
3.4 Examples ..... 41
4. Transitive triple systems ..... 44
4.1 Introduction ..... 44
4.2 An analysis for order $2^{n}+2$ ..... 44
4.3 A way to construct $\operatorname{LTTS}\left(2^{2 n}+2\right)$ ..... 50
4.4 Two sufficient conditions and examples ..... 53
5. Steiner triple systems ..... 58
5.1 Introduction ..... 58
5.2 A way to construct $L S T S\left(p^{n}+2\right)$ ..... 58
5.3 A sufficient condition and examples ..... 65
5.4 About $L D$ designs ..... 69
5.5 A recursive construction for $L D(3 n)$ ..... 72
References ..... 82
Curriculum vitae ..... 85

## I. Preliminaries

### 1.1 Introduction.

Given a collection $\mathcal{G}$ of directed graphs, a $\mathcal{G}$-design $(X, \mathcal{B})$ is a set $X$ together with a family $\mathcal{B}$ of directed graphs, each isomorphic to some member of $\mathcal{G}$, such that for some constant $\lambda$ each ordered pair of elements of $X$ (i.e., each directed edge of the complete directed graph on $X$ ) is covered by precisely $\lambda$ members of $\mathcal{B}$. In this thesis we shall always assume $\lambda=1$. $\mathcal{G}$-designs are studied widely. E.g., when $\mathcal{G}$ is a collection of complete directed graphs then the $\mathcal{G}$-designs are the pairwise balanced designs with corresponding block sizes. In particular, when $\mathcal{G}$ consists of a single complete graph the corresponding designs are the Balanced Incomplete Block Designs used in statistics. When $\mathcal{G}$ consists of matchings then $\mathcal{G}$-designs can be regarded as tournament schedules for two-player games, maybe with a constraint on the number of simultaneous games. Similarly, for complete bridge tournaments one may use $\mathcal{G}$-designs where $\mathcal{G}=\left\{C_{4}\right\}$ or $\mathcal{G}=\left\{2 K_{2}\right\}$. Work has been done on the case where $\mathcal{G}$ consists of trees or paths or cycles, and in most cases where $\mathcal{G}$ consists entirely of small graphs (say, on not more than five vertices) the spectrum (i.e., the collection of values $v=|X|$ for which a $\mathcal{G}$-design ( $X, \mathcal{B}$ ) exists) has been determined completely.

A large set of $\mathcal{G}$-designs is a collection $\left\{\mathcal{D}_{i} \mid i \in I\right\}$ of $\mathcal{G}$-designs $\mathcal{D}_{i}=$ $\left(X, B_{i}\right)$ on the same point set $X$, such that every subgraph of (the complete directed graph on) $X$ that is isomorphic to a member of $\mathcal{G}$ is element of precisely one family $\mathcal{B}_{i}$. Maybe the first to investigate large sets of designs was Cayley[Ca](1850) who showed that a large set of Steiner triple systems of order 7 does not exist. Probably 7 is the only bad order; at least it is known now by the work of Schreiber[Sch], Wilson[Wi2], Denniston[De], Teirlinck[Tei1,2] and Lu Jiaxi[Lu] that large sets of Steiner triple systems of order $v \neq 7$ do exist for all admissible orders $v$ except perhaps $v=141,283,501,789,1501,2365$. In Chapter 5 of this thesis we show how to reduce the existence problem for these six values of $v$ to the construction of two relatively small structures. So far about the undirected case. There are two ways to orient a triangle, giving a directed 3 -cycle and a transitive triple, respectively. Corresponding large sets have been studied by C.J. Colbourn, M.J. Colbourn[CoCo], Wu Lisheng[Wu], L.Teirlinck[TeiLin], C.C.Lindner[Lin1,2] and A.P. Street[LinSt]; in Chapters 2 and 4 we describe our progress. As a generalization of the directed 3-cycle we consider in Chapter 3 the case of the directed $k$-cycle. Of course much less complete results can be expected in this case, for $k \geq 15$ not even the existence problem for $\mathcal{G}$-designs has been settled, let alone that of large sets of $\mathcal{G}$-designs. Here
we do the first steps towards the beginnings of a theory by considering the cases $k=v$ and $k=v-1$. Unfortunately, it has been necessary in a few cases (in Chapters 4 and 5) to just give a detailed suggestion of how we think a solution can most likely be obtained. Indeed, since our stay at Eindhoven University of Technology lasted only one year, and scarcely eight months were available for research and writing and typesetting of this thesis, it was impossible to do more. (However, I hope to return to these questions on some future occasion.)

### 1.2 Some background about algebra.

This section contains some definitions that most readers will be acquainted with already- we add it for completeness only.

Let $S$ and $T$ be two sets. We denote by $S \times T$ the set of all ordered pairs $(x, y)$ with $x \in S$ and $y \in T$. This set is called the Cartesian product of $S$ and $T$. Any subset of $S \times T$ is called a correspondence between $S$ and $T$. A mapping from $S$ to $T$ is a correspondence between $S$ and $T$ such that to each $s \in S$ there corresponds exactly one $t \in T$. If $f$ is the mapping, usually one writes

$$
f: S \longrightarrow T \quad \text { and } \quad s \longmapsto t
$$

An important special case of a mapping is that of a one-to-one mapping, also called a bijection. Here there corresponds to each $t \in T$ just one $s \in S$. Given a mapping $f: S \longrightarrow T$ we shall denote the mapping from the power set of $S$ to the power set of $T$ defined by

$$
A \longmapsto\{f(a) ; a \in A\}
$$

by the same symbol $f$.
By a monoid we understand a set $S$ with an element $e$ and a mapping $f: S \times S \longrightarrow S$ such that if $f(x, y)$ is the result of applying $f$ to the pair $(x, y) \in S \times S$ then

$$
\left\{\begin{array}{c}
f(x, f(y, z))=f(f(x, y), z), \forall x, y, z \in S \\
f(e, x)=x=f(x, e), \quad \forall x \in S
\end{array}\right.
$$

The mapping $f$ is called a (binary) operation on $S$ and denoted by $x y$ (instead of $f(x, y)$ ). The element $e$ is called its unity element. An element $x$ of a monoid $S$ is said to be invertible if there exists $x^{\prime} \in S$ such that $x x^{\prime}=x^{\prime} x=e$. If $x$ is invertible, the corresponding $x^{\prime}$ is unique and is denoted by $x^{-1}$. By a group one understands a monoid in which every element is invertible. If the operation of a group is commutative (i.e. $x y=y x \forall x, y$ ) then the group is called abelian. A subgroup of the
group $G$ is a subset of $G$, which is a group relative to the operation in $G$. Given a group $G$ and a subgroup $H$, for any $x \in G$ the subset of $G: x H=\{x h \mid h \in H\}$ (resp. $H x=\{h x \mid h \in H\}$ ) is called a left (resp. right) coset of $H$ in $G$. Clearly,

$$
x H=y H(\text { or } H x=H y) \quad \text { iff } \quad x^{-1} y\left(\text { or } x y^{-1}\right) \in H .
$$

There is a partition of the group $G$ in the form

$$
G=\bigcup_{x} x H \quad\left(\text { or } \quad G=\bigcup_{x} H x\right)
$$

For a finite group $G$ containing $n$ elements, and any $x \in G$, there exists a positive integer $m$ with $m \mid n$ such that $x^{m}=e$ and $x^{k} \neq e$ $(\forall k<m)$, where $e$ is the unity element of $G$. Call the integer $m$ the order of the element $x$. Let $S$ be an arbitrary subset of a group $G$. Then there exists a unique smallest subgroup of $G$ containing $S$. We shall denote this subgroup by $\langle S\rangle$ and call it the subgroup generated by $S$. In case $S=\left\{x_{1}, \ldots, x_{t}\right\}$ we also write $\left.<x_{1}, \ldots, x_{i}\right\rangle$ for this subgroup. A cyclic group is a group generated by a single element.

Let $X$ be a finite set containing $n$ elements $1,2, \ldots, n$. A permutation $\xi$ of $X$ is a bijection from $X$ to $X$, and is usually denoted by

$$
\xi=\left(\begin{array}{cccc}
1 & 2 & \ldots & n \\
i_{1} & i_{2} & \ldots & i_{n}
\end{array}\right)
$$

where $i_{k}=\xi(k), 1 \leq k \leq n$. All such permutations of $X$ form a group, which is called the symmetric group on $X$ and is denoted by $\operatorname{Sym}(X)$, brief $S_{n}$, It is well known that $S_{n}$ (or $\operatorname{Sym}(X)$, if $X$ contains $n$ elements) contains just $n$ ! elements. The permutation which maps $i_{j}$ to $i_{j+1}(0 \leq j \leq k-1$, subscript $\bmod k$ ) and fixes each element in $X \backslash\left\{i_{0}, i_{1}, \ldots, i_{k-1}\right\}$ is called a cyclic permutation of length $k$ and is denoted by $\left(i_{0}, i_{1}, \ldots, i_{k-1}\right)$.

A ring (with identity) is a set $R$ with two binary operations, $(x, y) \mapsto$ $x+y$, called addition, and $(x, y) \mapsto x y$, called multiplication, such that (i) $R$ is an abelian group under the addition; (ii) $R$ is a monoid under the multiplication; (iii) The addition and the multiplication are related by the distributive laws:

$$
(x+y) z=x z+y z \quad \text { and } \quad z(x+y)=z x+z y, \forall x, y, z \in R .
$$

The unity element of the additive group is called the zero element of the ring and is usually denoted by 0 .

For a given positive integer $n$, all integers are separated into $n$ classes: $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, where

$$
\bar{k}=\{i n+k ; \quad i \in Z\}, \quad k=0,1, \ldots, n-1,
$$

and $Z$ is the set containing all integers. Provided with the two operations defined by

$$
\overline{k_{1}}+\overline{k_{2}}=\overline{k_{1}+k_{2}} \text { and } \overline{k_{1}} \cdot \overline{k_{2}}=\overline{k_{1} k_{2}},
$$

the set $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ forms a ring, which is called the residue class ring modulo $n$ and is denoted by $Z_{n}$.

A ring is called a field, if its non-zero elements (for its multiplication) form a commutative group. The unity element of the multiplicative group is usually denoted by 1 . It is well known that if a finite field contains $v$ elements, then $v$ must be a prime power, and conversely, if $v$ is a prime power then up to isomorphism there is a unique field with $v$ elements. A finite field is usually denoted $G F\left(p^{n}\right)$ or $F_{p^{n}}$ where $p$ is a prime and $n$ is a positive integer. The multiplicative group of a finite field $F$ is a cyclic group, a generator $g$ of which is called a primitive element of $F^{*}=F \backslash\{0\}$. So the set of non-zero elements of $F_{p^{n}}$ can be written as $\left\{1, g, g^{2}, \ldots, g^{p^{n}-2}\right\}$.
A so-called quasigroup is a set $Q$ with a binary operation, multiplication 0 , such that both maps

$$
l_{Q}: x \longmapsto a \circ x \text { and } r_{Q}: x \longmapsto x \circ a
$$

are permutations of $Q$ for each $a \in Q$. It is denoted by ( $Q, \circ$ ). A quasigroup ( $Q, \circ$ ) is called idempotent if $a \circ a=a$ for each $a \in Q$.

### 1.3 Block designs and large sets of block designs.

Starting with two famous recreational problems, Kirkman's schoolgirl problem and Euler's problem of the 36 officers, and inspired by the needs of statisticians, the subject of design theory has grown into a large branch of combinatorial mathematics.
In Combinatorics the subject of design theory, roughly speaking, is the study of incidence structures satisfying certain numerical requirements. It contains many sub-branches such as block designs, magic squares, Latin squares, difference sets, Hadamard matrices and so on.
In general, a block design is a pair ( $X, \mathcal{B}$ ), where $X$ is a set and $\mathcal{B}$ is a collection of subsets of $X$, called blocks, such that some conditions are satistied. A design $(X, \mathcal{B})$ is called resolvable when $\mathcal{B}$ can be partitioned into partitions of $X$. The classical type of block designs is the so-called BIBD (balanced incomplete block design): $X$ is a set of $v$
elements and $\mathcal{B}$ is a collection of $k$-subsets of $X$ such that each 2-subset of $X$ appears exactly in $\lambda$ blocks. So-called $t$-designs and $P B D$ designs are generalizations of $B I B D$ 's in two senses (" 2 -subset" $\longrightarrow$ " $t$-subset" and " $k$ " $\longrightarrow k_{1}, k_{2}, \ldots, k_{s}$ "). A $B I B D$, with some additional conditions (such as the resolvability" of $\mathcal{B}$, a fixed order on each block, etc.), will become some new type of block design (such as a $R B I B D$, a Mendelsohn system, a transitive system and so on). Of course, there are still other block designs.

A $B I B D$ is also called a $(v, k, \lambda)$-design. The simplest nontrivial $B I B D$ 's are the ( $v, 3,1$ )-designs; these are called Steiner triple systems $(S T S(v))$. A resolvable $S T S(v)$ is called a Kirkman triple system $(K T S(v))$. In general, a block design with block size $k=3$ is called a triple system, and below we shall meet Mendelsohn triple systems (MTS) and transitive triple systems (TTS). The main topics of our thesis will be the three kinds of triple systems and a generalization of $M T S ' s$. We will devote attention to the problem of so-called large sets of such designs.

In general, a large set of a certain kind of block design is a collection of $\left(X, \mathcal{B}_{i}\right)$ such that each $\left(X, \mathcal{B}_{i}\right)$ is one of this kind of block designs, and all $\mathcal{B}_{i}$ are pairwise disjoint (two block systems are disjoint if there are no common blocks) and together they contain all subsets of $X$ with the stipulated size.

In this thesis, the problem of the isomorphism of the block designs also will be touched upon. Two block designs $(X, \mathcal{B})$ and $\left(X^{\prime}, \mathcal{B}^{\prime}\right)$ of the same type and with the same parameters are called isomorphic if there exists a bijection $f$ from $X$ to $X^{\prime}$ such that all blocks in $\mathcal{B}$ are just mapped by $f$ to all blocks of $\mathcal{B}^{\prime}$ (Here the image of a block $B=\left(x_{1}, x_{2}, \ldots, x_{k}\right)$ under $f$ is the block $\left.f(B)=\left(f\left(x_{1}\right), f\left(x_{2}\right), \ldots, f\left(x_{k}\right)\right)\right)$. Two large sets $\left\{\left(X, \mathcal{B}_{i}\right)\right\}$ and $\left\{\left(X^{\prime}, \mathcal{B}_{i}^{\prime}\right)\right\}$ are called isomorphic if there exists a bijection $f$ from $X$ to $X^{\prime}$ such that all $\mathcal{B}_{i}$ are just mapped by $f$ to all $\mathcal{B}_{i}^{\prime}$. (The image of a block system $\mathcal{B}$ under $f$ is the block system $f(\mathcal{B})=\{f(B) ; b \in B\}$.)

A Latin square of order $n$ is defined to be a $n$-by- $n$ array made out of $n$ distinct symbols (for example $1,2, \ldots, n$ ) with the property that each of the $n$ symbols occurs exactly once in each row of the array and exactly once in each column. Let $A=\left(a_{i j}\right)_{1}^{n}$ and $B=\left(b_{i j}\right)_{1}^{n}$ be two Latin squares of order $n\left(a_{i j}, b_{i j} \in\{1,2, \ldots, n\}\right)$. If the $n^{2}$ ordered pairs $\left(a_{i j}, b_{i j}\right)$ for $1 \leq i, j \leq n$ are distinct, then $A$ and $B$ are called orthogonal (and $B$ is called an orthogonal mate of $A$ ). Obviously, for given $k \in\{1,2, \ldots, n\}$, there are exactly $n$ pairs ( $a_{i j}, k$ ) among the $n^{2}$ ordered pairs $\left(a_{i j}, b_{i j}\right), 1 \leq i, j \leq n$, and these $a_{i j}$ are distinct and lie in distinct rows and distinct columns of $A$. We call these positions of $A$ a transversal of $A$. For a Latin square $A$ of order $n$, there exists an
orthogonal mate of $A$ if and only if $A$ has $n$ disjoint transversals. A Latin square $A=\left(a_{i j}\right)_{1}^{n}, 1 \leq a_{i j} \leq n$, is called idempotent if $a_{i i}=i$, $\forall i$. It is easy to see that an (idempotent) Latin square of order $v$ is equivalent to an (idempotent) quasigroup containing $v$ elements.

A transversal design $T(k, n)$ is a $\operatorname{triad}(X, \mathcal{G}, \mathcal{A})$, where $X$ is a set of $k n$ elements, $\mathcal{G}=\left\{G_{i} \mid i \in I\right\}$ ( $I$ is an indexing set of cardinality $k$ ) is a partition of $X$ into $k n$-subsets $G_{i}$ (called groups), and $\mathcal{A}$ is a class of $k$-subsets of $X$ (called blocks) such that $\left|A \cap G_{i}\right|=1$ for each block $A$ and each group $G_{i}$, and for any pair of distinct elements which belong to different groups, there is a unique block $A$ containing this pair.

We now mention some concepts from graph theory, that occur in some of our proofs. A graph $G$ consists of a finite set $V$ of objects called vertices, along with a set $E$ of unordered pairs of vertices, which are called edges. A directed graph (or digraph) is a graph in which each edge has been assigned a direction. In a directed graph, for a given vertex, there are two kinds of edges (called arcs for a digraph): in-arcs and out-arcs. A path in a digraph $D$ is a sequence $x_{0}, x_{1}, \ldots, x_{k}$ of $k+1$ different vertices of $D$ such that $\left(x_{0}, x_{1}\right),\left(x_{1}, x_{2}\right), \ldots,\left(x_{k-1}, x_{k}\right)$ are arcs of $D$ with no arc repeated. A circuit is defined like a path except that the vertex $x_{0}$ is the same as the vertex $x_{k}$. The length of a circuit is the number of vertices it contains. If the length of a circuit is $k$, then we call it a $k$-circuit. A Hamilton circuit in $D$ is a circuit containing all the vertices of $D$. If each vertex of $D$ has just one in-arc and one out-arc, then $D$ is the union of pairwise disjoint circuits. A complete symmetric digraph $K_{n}^{*}$ is a graph with $n$ vertices in which for any two distinct vertices $x, y$ there are arcs $x \rightarrow y$ and $y \rightarrow x$.

## II. Mendelsohn triple systems

### 2.1 Introduction.

Let $X$ be a set of $v$ elements $(v \geq 3)$. A cyclic triple from $X$ is a collection of three ordered pairs $(x, y),(y, z),(z, x)$, where $x, y$, and $z$ are distinct elements of $X$. We will denote the cyclic triple $\{(x, y),(y, z),(z, x)\}$ by $\langle x, y, z\rangle$, or $\langle y, z, x\rangle$ or $\langle z, x, y\rangle$. A Mendelsohn triple system on $X$ is a pair $(X, \mathcal{B})$ where $\mathcal{B}$ is a collection of cyclic triples from $X$ such that each ordered pair of distinct elements of $X$ is covered by a unique cyclic triple from $\mathcal{B}$. The number $|X|=v$ is called the order of the Mendelsohn triple system $(X, \mathcal{B})$. For brevity, one denotes such a system by $M T S(v)$. It is easy to see that if $(X, \mathcal{B})$ is a $M T S(v)$, then $|\mathcal{B}|=\frac{v(v-1)}{3}$. Thus, a necessary condition for the existence of a $M T S(v)$ is $v \equiv 0$ or 1 $(\bmod 3)$.

This kind of design was studied first by N.S. Mendelsohn [Men]. He called such a design a generalized triple system and proved that the necessary condition for the existence of a $M T S(v)$ is also sufficient except if $v=6$. (J.C. Bermond [Berl] independently studied the same design and obtained the same result for this question, i.e., the decomposition of the symmetric oriented complete graph into 3 -circuits.)

Let $C(X)$ be the set of all cyclic triples from the set $X$ of $v$ elements. Then $|C(X)|=\frac{1}{3} v(v-1)(v-2)$. The following problem arises quite naturally. Given a set $X$ with size $v \equiv 0$ or $1(\bmod 3)$ and $v \geq 3, v \neq 6$, is it always possible to partition $C(X)$ into $v-2$ subsets $\mathcal{B}_{1}, \mathcal{B}_{2}, \ldots, \mathcal{B}_{v-2}$ so that each of $\left(X, \mathcal{B}_{1}\right),\left(X, \mathcal{B}_{2}\right), \ldots,\left(X, \mathcal{B}_{v-2}\right)$ is a $M T S(v)$ ? Such a collection of $M T S(v)$ 's is called a large set of pairwise disjoint $M T S(v)$ 's, we denote it by $L M T S(v)$. The research work on this problem started in 1981. By 1987 there already were some results on this problem (for details see $\S 2.5$ ). However, all known results are obtained recursively and the problem was very far from a complete solution.

In this chapter a number of results of our research, started in 1987, will be stated. It contains one recursive construction (Theorem 2.3.3, $v+2 \longrightarrow u v+2$ for $u \equiv \pm 1(\bmod 6)$ ), two direct constructions (Theorem 2.2 .1 for all odd orders and Theorem 2.4 .6 for order $2^{n}+2, n \geq 3$ ), a few corrections of errors in other papers (in §2.5) and a discussion about nonisomorphic large sets of pairwise disjoint Mendelsohn triple systems. Through §2.2-2.4 we affirm the existence of $L M T S(v)$ for the great majority of orders $v$. All that remains for a complete solution of the problem is $v \equiv 6$ or $22(\bmod 72)$.

### 2.2 The odd order case.

For the odd order case, i.e. $v \equiv 1$ or $3(\bmod 6), v \geq 3$, if there is a $L S T S(v)$ (a large set of disjoint Steiner triple systems of order $v$ ), then
we can get $\operatorname{LMTS}(v)$ by replacing each triple $\{x, y, z\}$ by the cyclic triples $\langle x, y, z\rangle$ and $\langle x, z, y\rangle$. It is well known that there exist $\operatorname{LSTS}(v)$ for all $v \equiv 1$ or $3(\bmod 6), v \neq 7$ except for six possible orders: 141, 283, $501,789,1501$ and 2365 [ Lu$]$. In the following we do not use the results on $\operatorname{LSTS}(v)$ 's but construct directly $L M T S(v)$ for all admissible odd order $v$.

In the following construction, each $M T S(v)=(X, \mathcal{B})$ has the property: there exist $a \neq b \in X$ such that

$$
\begin{align*}
& \langle a, b, x\rangle \in \mathcal{B} \Longleftrightarrow\langle b, a, x\rangle \in \mathcal{B}  \tag{*}\\
& \langle a, x, y\rangle \in \mathcal{B} \Longleftrightarrow\langle b, y, x\rangle \in \mathcal{B}
\end{align*}
$$

where $x, y \in X \backslash\{a, b\}$. In [Ka1], we called such a MTS a Symmetric Mendelsohn triple system and denoted it by SMTS.
Theorem 2.2.1. For $v \equiv 1$ or $3(\bmod 6)$ and $v \geq 3$, there exists an LMTS(v).
Proof. We use the following construction.
Let $u \equiv \pm 1(\bmod 6)$ and $X=\{a, b\} \cup Z_{u}$, where $Z_{u}=\{0,1, \ldots, u-1\}$ is the residue class ring modulo $u, a, b \notin Z_{u}$ and $v=u+2=|X|$. We can construct $u$ cyclic triple systems $\mathcal{B}_{i}\left(i \in Z_{u}\right)$ on X as follows.

There are three types of cyclic triples in $\mathcal{B}_{i}$ :
(1) $(a, b, i),(b, a, i) ;$ this gives two cyclic triples.
(2) $\langle a, x+i,-2 x+i\rangle,\langle b,-2 x+i, x+i\rangle$, where $x \in Z_{u} \backslash\{0\}$; this gives $2(u-1)$ cyclic triples.
(3) $\langle x, y, z\rangle,\langle x, z, y\rangle$, where $x<y<z$ and $\{x, y, z\}$ is a 3 -subset of $Z_{u}$ such that $x+y+z \equiv 3 i(\bmod u)$; this gives $\frac{1}{3}(u-1)(u-2)$ cyclic triples.

We now prove that this indeed defines an $\operatorname{LMTS}(v)$.
Firstly, for $u=1$ (i.e. $v=3$ ), $\operatorname{LMTS}(3)=\{\{(a, b, 0\rangle,\langle b, a, 0\rangle\}\}$ is trivial. Next, let $u \geq 5$; notice $u \not \equiv 0(\bmod 2)$ and $u \not \equiv 0(\bmod 3)$; it is easy to see that 2 and 3 are invertible in $Z_{u}$ and $x+i \neq-2 x+i$ ( $x \in Z_{u} \backslash\{0\}$ ).
$1^{\circ}$ Each of the $\mathcal{B}_{i}$ 's is a $M T S(v)$ :
Direct calculation shows that $\mathcal{B}_{i}$ contains $\frac{1}{3}(u+1)(u+2)$ cyclic triples, just the number we expected. Therefore, we only need to show that no ordered pair of distinct elements of X is covered by more than one cyclic triple in $\mathcal{B}_{i}$, but that is immediately clear.
$2^{\circ}\left\{\mathcal{B}_{i} \mid i \in Z_{u}\right\}$ is an $\operatorname{LMTS}(v)$ :
Again it suffices to verify that no cyclic triple is in more than one $\mathcal{B}_{i}$ (since we have the right total number of triples). This is obvious for the triples of types (1) and (3) and easy to see for those of type (2):

$$
\langle a, x, y\rangle \in \mathcal{B}_{(y+2 x) / 3} \text { and }\langle b, x, y\rangle \in \mathcal{B}_{(x+2 y) / 3} .
$$

This completes the proof.
This theorem establishes the existence of an $L M T S(v)$ for all admissible odd orders $v$, including the six orders, for which an $L S T S(v)$ is unknown and the single order for which there does not exist an $L S T S(v)$.

### 2.3 A recursive construction.

We now establish a recursive construction.
Lemma 2.3.1. For $u \equiv \pm 1(\bmod 6)$ and $v \geq 3$, if there exists an $L M T S(v+2)$ then there also exists an LMTS $(u v+2)$.

Proof. Again, we give a construction and show that it works.
Let $\left\{\left(\{a, b\} \cup Z_{u}, \mathcal{B}_{i}\right) \mid i \in Z_{u}\right\}$ be an $\operatorname{LMTS}(u+2)$, where the $\mathcal{B}_{i}$ are indexed such that $\langle a, b, i\rangle \in \mathcal{B}_{i}$. By Theorem 2.2.1, there exists such an $L M T S(u+2)$ satisfying the so-called symmetry condition (see $\S 2.2\left(^{*}\right)$ ). Let $\left\{\left(\{a, b\} \cup S_{v}, C_{j}\right) ; j \in S_{v}\right\}$ be an $\operatorname{LMTS}(v+2)$, where $S_{v}=$ $\{0,1, \ldots, v-1\}$ is a set containing $v$ elements, $a, b \notin Z_{u} \cup S_{v}$ and ( $\left.S_{v}, 0\right)$ is an idempotent quasigroup of order $v$ over $S_{v}$. Let $\alpha=(0,1, \ldots, v-1)$ be a cyclic permutation of length $v$ on the set $S_{v}$. Now we can construct $u v$ cyclic triple systems $\mathcal{T}_{i j}\left(i \in Z_{u}, j \in S_{v}\right)$ on the set $\{a, b\} \cup\left(Z_{u} \times S_{v}\right)$ as follows:
(1) $\left((x, m),(y, n),\left(z,(m \circ n) \alpha^{j}\right)\right\rangle$ with $\langle x, y, z\rangle \in \mathcal{B}_{i}, x, y, z \in Z_{u}$, $m, n \in S_{v}$; this gives $\frac{1}{3} v^{2}(u-1)(u-2)$ cyclic triples.
(2) $\left\langle(x, m),(x, n),\left(y,(m \circ n) \alpha^{j}\right)\right\rangle$ with $\langle a, x, y\rangle \in \mathcal{B}_{i}, x, y \in Z_{u}, m \neq$ $n \in S_{v}$; this gives $\left(v^{2}-v\right)(u-1)$ cyclic triples.
(3) $\left\langle a,(x, m),\left(y, m \alpha^{j}\right)\right\rangle$ and $\left\langle b,\left(y, m \alpha^{j}\right),(x, m)\right\rangle$ with $\langle a, x, y\rangle \in \mathcal{B}_{i}$, $x, y \in Z_{u}, m \in S_{v}$; this gives $2 v(u-1)$ cyclic triples.
(4) $\langle(i, m),(i, n),(i, l)\rangle$ with $\langle m, n, l\rangle \in \mathcal{C}_{j}$ (whenever $a$ or $b$ appears for $m, n, l$, omit the first coordinate $i$; this gives $\frac{1}{3}(v+2)(v+1)$ cyclic triples.

We prove that the construction works.
By the symmetry condition $\left(^{*}\right)$ of $\mathcal{B}_{i}$ and $\langle a, b, i\rangle \in \mathcal{B}_{i}$, it is easy to see that the conditions in (2) and (3) imply $x, y \in Z_{u} \backslash\{i\}$ and both $\langle a, x, y\rangle$ and $(b, y, x)$ belong to $B_{i}$.
$1^{\circ}$ Each $\mathcal{T}_{i j}$ is a $M T S(u v+2)$.
Direct calculation shows that each $T_{i j}$ contains $\frac{1}{3}(u v+2)(u v+1)$ cyclic triples, just the number we expected. Therefore we only need to show that every ordered pair $P$ of distinct elements of the set $\{a, b\} \cup\left(Z_{u} \times\right.$ $S_{v}$ ) is contained in some cyclic triple in $\mathcal{T}_{i j}$. All the possibilities are exhausted as follows:
i) $P=(a, b) \in\langle a, b,(i, m)\rangle$ in (4), where $m \in S_{v}$ such that $\langle a, b, m\rangle \in$ $\mathcal{C}_{j} ; P=(b, a) \in(b, a,(i, n)\rangle$ in (4), where $n \in S_{v}$ such that $\langle b, a, n\rangle \in \mathcal{C}_{j}$.
ii) For $x \in Z_{u}$ and $m \in S_{v}, P=(a,(x, m))$ belongs to the cyclic triple
$\langle b, a,(i, m)\rangle$ in (4), if $x=i$ and $\langle a, m, b\rangle \in \mathcal{C}_{j} ;$
$\langle a,(i, m),(i, n)\rangle$ in (4), if $x=i$ and $\langle a, m, n\rangle \in \mathcal{C}_{j}, n \in S_{v} ;$
$\left\langle a,(x, m),\left(y, m \alpha^{j}\right)\right\rangle$ in (3) if $x \neq i$ and $\langle a, x, y\rangle \in \mathcal{B}_{i}$.
Similarly, for $P=(b,(x, m)),((x, m), a)$ and $((x, m), b)$.
iii) For $x \in Z_{u}$ and $m \neq n \in S_{v}, P=((x, m),(x, n))$ belongs to the cyclic triple
$\left\langle(x, m),(x, n),\left(y,(m \circ n) \alpha^{j}\right)\right\rangle$ in (2), if $x \neq i$ and $\langle a, x, y\rangle \in \mathcal{B}_{i} ;$
$\langle(i, m),(i, n),(i, l)\rangle$ in (4), if $x=i$ and $\langle m, n, l\rangle \in \mathcal{C}_{j}$.
iv) For $x \neq y \in Z_{u}$ and $m, n \in S_{v}, P=((x, m),(y, n))$ belongs to the cyclic triple
$\left\langle(x, m),(y, n),\left(z,(m \circ n) \alpha^{j}\right)\right\rangle$ in $(1)$, if $\langle x, y, z\rangle \in \mathcal{B}_{i}$ and $z \in Z_{u} ;$
$\left\langle a,(x, m),\left(y, m \alpha^{j}\right)\right\rangle$ in (3), if $\langle x, y, a\rangle \in \mathcal{B}_{i}$ and $m \alpha^{j}=n$;
$\left\langle\left(x, n^{\prime}\right),(x, m),\left(y,\left(n^{\prime} \circ m\right) \alpha^{j}\right)\right\rangle$ in $(2)$, if $\langle x, y, a\rangle \in \mathcal{B}_{i}$ and $\left(n^{\prime} \circ\right.$ $m) \alpha^{j}=n ;$
$\left\langle b,\left(x, n \alpha^{j}\right),(y, n)\right\rangle$ in (3), if $\langle x, y, b\rangle \in \mathcal{B}_{i}$ and $n \alpha^{j}=m ;$
$\left\langle(y, n),\left(y, m^{\prime}\right),\left(x,\left(n \circ m^{\prime}\right) \alpha^{j}\right)\right\rangle$ in (2), if $\langle x, y, b\rangle \in \mathcal{B}_{i}$ and ( $n \circ$ $\left.m^{\prime}\right) \alpha^{j}=m$.
$2^{\circ}\left\{\mathcal{T}_{i j} \mid i \in Z_{u}, j \in S_{v}\right\}$ is an $\operatorname{LMTS}(u v+2)$
We only need to show that every cyclic triple $T$ from the set $\{a, b\} \cup$ $\left(Z_{u} \times S_{v}\right)$ is contained in some $\mathcal{T}_{i j}$ above. All the possibilities are exhausted as follows:
i) $T=\langle a, b,(i, m)\rangle$, where $i \in Z_{u}, m \in S_{v}$, is contained in (4) of $\mathcal{T}_{i j}$, where $j \in S_{v}$ such that $\langle a, b, m\rangle \in \mathcal{C}_{j}$. Similarly, for $T=\langle b, a,(i, m)\rangle$.
ii) $T=\langle a,(i, m),(i, n)\rangle$, where $i \in Z_{u}, m \neq n \in S_{v}$, is contained in (4) of $\mathcal{T}_{i j}$, where $j \in S_{v}$ such that $\langle a, m, n\rangle \in \mathcal{C}_{j}$. Similarly, for $T=\langle b,(i, m),(i, n)\rangle$.
iii) $T=\langle a,(x, m),(y, n)\rangle$, where $x \neq y \in Z_{u}, m, n \in S_{v}$, is contained in (3) of $\mathcal{T}_{i j}$, where $i \in Z_{u}, j \in S_{v}$ such that $\langle a, x, y\rangle \in \mathcal{B}_{i}$ and $n=m \alpha^{j}$. Similarly, for $T=\langle b,(x, m),(y, n)\rangle$.
iv) $T=\langle(i, m),(i, n),(i, l)\rangle$, where $i \in Z_{u}$ and $m, n, l \in S_{v}$ are pairwise distinct, is contained in (4) of $\mathcal{T}_{i j}$, where $\langle m, n, l\rangle \in \mathcal{C}_{j}$.
v) $T=\langle(x, m),(x, n),(y, l)\rangle\left(x \neq y \in Z_{u}, m, n, l \in S_{v}, m \neq n\right)$ is contained in (2) of $\mathcal{T}_{i j}$, where $i \in Z_{u}, j \in S_{v}$ such that $\langle a, x, y\rangle \in \mathcal{B}_{i}$ and $(m \circ n) \alpha^{j}=l$.
vi) $T=\langle(x, m),(y, n),(z, l)\rangle\left(x, y, z \in Z_{u}, x \neq y \neq z \neq x\right.$ and $m, n, l \in$ $S_{v}$ ) is contained in (1) of $\mathcal{T}_{i j}$, where $i \in Z_{u}, j \in S_{v}$ such that $\langle x, y, z\rangle \in \mathcal{B}_{i}$ and $(m \circ n) \alpha^{j}=l$.

This completes the proof.
Lemma 2.3.2. For $u \equiv \pm 1(\bmod 6)$, there exists an $L M T S(2 u+2)$.

## Proof.

Let $\left\{\left(\{a, b\} \cup Z_{u}, \mathcal{C}_{i}\right) ; i \in Z_{u}\right\}$ be an $\operatorname{LMTS}(u+2)$, where the $\mathcal{C}_{i}$ are indexed such that $\langle a, b, i\rangle \in \mathcal{C}_{i}$. By Theorem 2.2 .1 there exists such an $L M T S(u+2)$ satisfying the so-called symmetry condition (see $\S 2.2\left(^{*}\right)$ ), Let $I_{2}=\{0,1\}$. We can construct $2 u$ cyclic triple systems $\mathcal{B}_{i j}\left(i \in Z_{u}, j \in\right.$ $I_{2}$ ) on the set $\{a, b\} \cup\left(Z_{u} \times I_{2}\right)$, where the elements $(x, 0)$ and $(x, 1)$ of $Z_{u} \times I_{2}$ are briefly denoted by $x_{0}$ and $x_{1}$.
$\mathcal{B}_{i, 0}\left(i \in Z_{u}\right)$ consists of the following four types of triples
(1) $\left\langle a, b, i_{0}\right\rangle,\left\langle b, a, i_{1}\right\rangle,\left\langle a, i_{0}, i_{1}\right\rangle$ and $\left\langle b, i_{1}, i_{0}\right\rangle$; this gives four cyclic triples.
(2) $\left\langle a, x_{0}, y_{0}\right\rangle,\left\langle a, x_{1}, y_{1}\right\rangle,\left\langle b, y_{0}, x_{1}\right\rangle$ and $\left\langle b, y_{1}, x_{0}\right\rangle$ with $\langle a, x, y\rangle \in$ $\mathcal{C}_{i}, x, y \in Z_{u}$; this gives $4(u-1)$ cyclic triples.
(3) $\left\langle x_{0}, x_{1}, y_{0}\right\rangle$ and $\left\langle x_{1}, x_{0}, y_{1}\right\rangle$ with $\langle a, x, y\rangle \in \mathcal{C}_{i}, x, y \in Z_{u}$; this gives $2(u-1)$ cyclic triples.
(4) $\left\langle x_{0}, y_{0}, z_{0}\right\rangle,\left\langle x_{0}, y_{1}, z_{1}\right\rangle,\left\langle x_{1}, y_{0}, z_{1}\right\rangle$ and $\left\langle x_{1}, y_{1}, z_{0}\right\rangle$ with $\langle x, y, z\rangle \in$ $\mathcal{C}_{i}, x, y, z \in Z_{u} ;$ this gives $\frac{4}{3}(u-1)(u-2)$ cyclic triples.
$\mathcal{B}_{i, 1}\left(i \in Z_{u}\right)$ consists of the following four types of triples
(1) $\left\langle a, b, i_{1}\right\rangle,\left\langle b, a, i_{0}\right\rangle,\left\langle a, i_{1}, i_{0}\right\rangle$ and $\left\langle b, i_{0}, i_{1}\right\rangle$.
(2) $\left\langle a, x_{0}, y_{1}\right\rangle,\left\langle a, x_{1}, y_{0}\right\rangle,\left\langle b, y_{0}, x_{0}\right\rangle$ and $\left\langle b, y_{1}, x_{1}\right\rangle$ with $\langle a, x, y\rangle \in$ $\mathcal{C}_{i}, x, y \in Z_{u}$.
(3) $\left\langle x_{0}, x_{1}, y_{1}\right\rangle$ and $\left\langle x_{1}, x_{0}, y_{0}\right\rangle$ with $\langle a, x, y\rangle \in \mathcal{C}_{i}, x, y \in Z_{u}$.
(4) $\left\langle x_{1}, y_{1}, z_{1}\right\rangle,\left\langle x_{1}, y_{0}, z_{0}\right\rangle,\left\langle x_{0}, y_{1}, z_{0}\right\rangle$ and $\left\langle x_{0}, y_{0}, z_{1}\right\rangle$ with $\langle x, y, z\rangle \in$ $\mathcal{C}_{i}, x, y, z \in Z_{u}$.

The proof that the method works follows.
Firstly, since each $\mathcal{C}_{i}$ has the so-called symmetry property, both $\langle a, b, i\rangle$ and $\langle b, a, i\rangle$ belong to $\mathcal{C}_{i}$, and the condition in (2), (3) implies that $x, y \in$ $Z_{u} \backslash\{i\}$ and both $(a, x, y)$ and $(b, x, y)$ belong to $\mathcal{C}_{i}$.
$1^{\circ}$ Each of $\mathcal{B}_{i j}$ is a $\operatorname{MTS}(2 u+2)$.
Direct calculation shows that $\mathcal{B}_{i j}$ contains $\frac{1}{3}(2 u+1)(2 u+2)$ cyclic triples, just the number we expected. So, we only need to show that every ordered pair $P$ of distinct elements of the set $\{a, b\} \cup\left(Z_{u} \times I_{2}\right)$ is contained in some cyclic triple of $\mathcal{B}_{i j}$. All the possibilities are exhausted as follows (We only give the proof for $\mathcal{B}_{i, 0}$, the proof for $B_{i, 1}$ is similar to it.):
i) $P=(a, b)$ and ( $b, a)$ are contained in part (1).
ii) $P=\left(a, i_{j}\right),\left(b, i_{j}\right),\left(i_{j}, a\right)$ and $\left(i_{j}, b\right)$ are contained in part (1).
iii) $P=\left(a, x_{j}\right),\left(b, x_{j}\right),\left(x_{j}, a\right)$ and $\left(x_{j}, b\right)(x \neq i)$ are contained in part (2).
iv) $P=\left(x_{j}, x_{1-j}\right)\left(x \in Z_{u}, j \in I_{2}\right)$ belongs to part (1), if $x=i$; or part (2), if $x \neq i$.
v) $P=\left(x_{j}, y_{k}\right)\left(x \neq y \in Z_{w}, j \in I_{2}\right)$ belongs to
part (2)(or (3)), if $\langle x, y, a\rangle \in \mathcal{C}_{i}$ and $j=k$ (or $j \neq k$ );
part (3)(or (2)), if $\langle x, y, b\rangle \in \mathcal{C}_{i}$ and $j=k($ or $j \neq k) ;$
part (4), if $\langle x, y, z\rangle \in \mathcal{C}_{i}$ and $z \in Z_{u}$.
$2^{\circ}\left\{\mathcal{B}_{i j} ; i \in Z_{u}, j \in I_{2}\right\}$ is an $\operatorname{LMTS}(2 u+2)$.
We only need to show that every cyclic triple $T$ from $\{a, b\} \cup\left(Z_{u} \times I_{2}\right)$ is contained in some $\mathcal{B}_{i j}$ above. All the possibilities are exhausted as follows:
i) $T=\left\langle a, b, i_{j}\right\rangle$ and $\left\langle a, i_{j}, i_{1-j}\right\rangle\left(i \in Z_{u}, j \in I_{2}\right)$ are contained in (1) of $\mathcal{B}_{i j} ; T=\left\langle b, a, i_{j}\right\rangle$ and $\left\langle b, i_{j}, i_{1-j}\right\rangle\left(i \in Z_{u}, j \in I_{2}\right)$ are contained in (1) of $\mathcal{B}_{i, 1-j}$.
ii) $T=\left\langle a, x_{j}, y_{k}\right\rangle\left(\right.$ or $\left.\left\langle b, x_{j}, y_{k}\right\rangle\right)\left(x \neq y \in Z_{u}, j, k \in I_{2}\right)$ is contained in (2) of $\mathcal{B}_{i, s}\left(\right.$ or $\left.\mathcal{B}_{i, 1-s}\right)$, where $\langle a, x, y\rangle \in \mathcal{C}_{i}$ and $s \equiv j+k(\bmod 2)$.
iii) $T=\left\langle x_{j}, x_{1-j}, y_{k}\right\rangle\left(x \neq y \in Z_{u}, j, k \in I_{2}\right)$ is contained in (3) of $\mathcal{B}_{i, 0}$ or $\mathcal{B}_{i, 1}$, where $\langle a, x, y\rangle \in \mathcal{C}_{i}$.
iv) $T=\left\langle x_{j}, y_{k}, z_{k}\right\rangle\left(x, y, z \in Z_{u}\right.$ are pairwise distinct, $\left.j, k \in I_{2}\right)$ is contained in (4) of $\mathcal{B}_{i j}$, where $\langle x, y, z\rangle \in \mathcal{C}_{i}$.

This completes the proof.
Theorem 2.3.3. For $u \equiv \pm 1(\bmod 6)$ and $v \geq 2$, if there exists an $L M T S(v+2)$ then there also exists an $L M T S(u v+2)$.

Proof. This is a consequence of Lemma 2.3.1 and 2.3.2.

### 2.4 LMTS $\left(2^{n}+2\right), n \neq 2$.

We have already discussed the designs $\operatorname{LMTS}(v)$ for all odd orders $v$ $($ of course, $v \not \equiv 2(\bmod 3))$. For even order $v($ also $v \not \equiv 2(\bmod 3))$, we can express $v$ in the form $v=2^{n} u+2$, where $n$ is a positive integer and $u \equiv \pm 1(\bmod 6)$. By Theorem 2.3.3, if we can construct $L M T S\left(2^{n}+2\right)$ for each positive integer $n$, then the existence problem of $L M T S(v)$ for all $v$ will be solved completely.

For $n=1$, it is very easy to give the following $\operatorname{LMTS}(2+2)=$ $\left\{\left(\{a, b\} \cup I_{2}, \mathcal{B}_{i}\right) ; i \in I_{2}\right\}:$

$$
\begin{aligned}
& \mathcal{B}_{0}=\{\langle a, b, 0\rangle,\langle b, a, 1\rangle,\langle a, 0,1\rangle,\langle b, 1,0\rangle\} \\
& \mathcal{B}_{1}=\{\langle a, b, 1\rangle,\langle b, a, 0\rangle,\langle a, 1,0\rangle,\langle b, 0,1\rangle\}
\end{aligned}
$$

But for $n=2$ there does not exist an $\operatorname{LMTS}\left(2^{2}+2\right)$, since there does not exist an $M T S(6)$. Now we will devote attention to the construction of an $L M T S\left(2^{n}+2\right)$ for every positive integer $n \geq 3$.

### 2.4.1 The pair class and triple class.

Let $\mathbf{F}$ be a finite field containing $2^{n}$ elements ( $n \geq 3$ ). Its zero and unit elements are denoted by 0 and 1 , respectively. Let $g$ be a primitive element of $\mathbf{F}^{*}=\mathbf{F} \backslash\{0\}$. We define two elements $\infty_{1}, \infty_{2} \notin \mathrm{~F}$. Let $\mathbf{R}=\mathbf{Z}_{2^{n}-1}=\left\{0,1, \ldots, 2^{n}-2\right\}$ be a residue class ring modulo $2^{n}-1$. Below, all operations are over $\mathbf{F}$ or $\mathbf{R}$, respectively.

For $\alpha, \beta \in \mathbf{R}^{*}=\mathbf{R} \backslash\{0\}$, if $g^{\alpha}+g^{\beta}=1$ then call $\alpha, \beta$ a couple and denote this by $\alpha C \beta$. We point out that
(C1) If $\alpha C \beta$ then $\alpha \neq \beta$ and $\beta C \alpha,(-\beta) C(\alpha-\beta),(-\alpha) C(\beta-\alpha)$, $\left(2^{t} \alpha\right) C\left(2^{t} \beta\right)$ for an arbitrary positive integer $t$.
(C2) If $\alpha C \beta$ and $\gamma C \delta$ then $\operatorname{ind}(\alpha+\delta, \beta+\gamma)-\beta) C(\delta-\beta)$ and (ind $(\alpha+$ $\delta, \beta+\gamma)-\gamma) C(\alpha-\gamma)$,where $\varepsilon=\operatorname{ind}(\lambda, \mu)$ means $g^{\lambda}+g^{\mu}=g^{\epsilon}$.

Let $x \in \mathbf{F}$ be given. For an ordered pair $(y, z)$ of distinct elements in $\mathbf{F} \backslash\{x\}$, we have $\frac{x-y}{x-y} \in \mathbf{F} \backslash\{0,1\}$. So we can let $\frac{z-y}{x-y}=g^{\alpha}$, where $\alpha \in \mathbf{R}^{*}$, and write $z=g^{\alpha} x+g^{\beta} y$, where $\beta \in \mathbf{R}^{*}, \alpha C \beta$. Then we say that the ordered pair $(y, z)=\left(y, g^{\alpha} x+g^{\beta} y\right)$ in $\mathbf{F} \backslash\{x\}$ belongs to the pair class $\langle\alpha, \beta>$ (briefly $\mathrm{PC}\langle\alpha, \beta\rangle$ or $\langle\alpha\rangle$ ).
Lemma 2.4.1. For a given element $x \in \mathbf{F}$,
(1) Each ordered pair of distinct elements of $\mathbf{F} \backslash\{x\}$ belongs to a uniquely determined PC. The total number of pair classes is $2^{n}-2$. Each $P C$ contains $2^{n}-1$ distinct ordered pairs.
(2) For the cyclic triple $\left\langle g^{\gamma} x+g^{\delta} y, y, g^{\alpha} x+g^{\beta} y\right\rangle$, where $y \in \mathcal{F} \backslash\{x\}$, $\alpha, \beta, \gamma, \delta \in \mathbf{R}^{*}, \alpha C \beta, \gamma C \delta$ and $\alpha \neq \gamma$, its three ordered pairs belong to the pair classes $\langle\alpha, \beta\rangle,\langle\operatorname{ind}(\alpha+\delta, \beta+\gamma)-\beta, \delta-\beta\rangle$ and $\langle\gamma-\delta,-\delta\rangle$, respectively.
(3) For the cyclic triple $\left\langle u, y, g^{\alpha} x+g^{\beta} y\right)$, where $u=x$ (or $\infty_{1}$, or $\infty_{2}$ ), $\alpha, \beta \in \mathbf{R}^{*}$ and $\alpha C \beta$, only one among its three ordered pairs, namely ( $y, g^{\alpha} x+g^{\beta} y$ ), belongs to $P C\langle\alpha, \beta\rangle$.

## Proof.

(1) is trivial by definition.
(2) Let $X=g^{\gamma} x+g^{\delta} y, Y=y$ and $Z=g^{\alpha} x+g^{\beta} y$, then $Y=g^{\gamma-\delta} x+$ $g^{-\delta} X$ and $g^{\beta} X+g^{\delta} Z=\left(g^{\gamma+\beta}+g^{\alpha+\delta}\right) x$. And the latter implies

$$
X=\frac{g^{\alpha+\delta}+g^{\beta+\gamma}}{g^{\beta}} x+g^{\delta-\beta} Z
$$

(3) is trivial.

For an ordered triple $\langle\langle u, v, w\rangle\rangle$ of distinct elements in $\mathbf{F}$, similar to the above process, we can also write $v=g^{\alpha} u+g^{\beta} w$, where $\alpha, \beta \in \mathbf{R}$ and $\alpha C \beta$. We say that the ordered triple $\langle(u, v, w)\rangle$ belongs to $[\alpha, \beta]$. Since a cyclic triple $\langle u, v, w\rangle$ is equivalent to three ordered triples $\langle\langle u, v, w\rangle\rangle$, $\langle\langle v, w, u\rangle\rangle$ and $\langle\langle w, u, v\rangle\rangle$, and $v=g^{\alpha} u+g^{\beta} w$ implies $w=g^{-\beta} v+g^{\alpha-\beta} u$ and $u=g^{\beta-\alpha} w+g^{-\alpha} v$, we shall say that the cyclic triple $\langle u, v, w\rangle$ belongs to the triple class $\{[\alpha, \beta],[-\beta, \alpha-\beta],[\beta-\alpha,-\alpha]\}$ (brief TC $\{\alpha,-\beta, \beta-\alpha\})$. Note that the three couples in a TC have the following property:
(T) The first coordinate of each couple equals the negative of the second coordinate of another couple.

For convenience below, we call three such couples having property (T) a trio, and denote them by $\{\alpha,-\beta, \beta-\alpha\}$ (only write down their first coordinates). We point out that, if $A=\{\alpha,-\beta, \beta-\alpha\}$ is a trio, then $-A=\{-\alpha, \beta, \alpha-\beta\}, 2 A=\{2 \alpha,-2 \beta, 2 \beta-2 \alpha\}$ and $(-2) A=$ $\{-2 \alpha, 2 \beta, 2 \alpha-2 \beta\}$ also are.

## Lemma 2.4.2.

(1) The total number of trios (in $\mathbf{R}^{*}$ ) is $\frac{2^{n}-2}{3}$ if $n$ is odd, or $\frac{2^{n}-4}{3}+2$ if $n$ is even. When $n$ is cven, there are two so-called small trios: $\{\theta, \theta, \theta\}$ and $\{2 \theta, 2 \theta, 2 \theta\}$, where $\theta=\frac{2^{n}-1}{3}$. In all other cases each trio consists of three different numbers.
(2) Each cyclic triple of distinct elements in F belongs to a uniquely determined TC. Each small TC (corresponding to a small trio) contains $\frac{2^{n}\left(2^{n}-1\right)}{3}$ pairwise distinct cyclic triples, and each of the other TC's contains $2^{n}\left(2^{n}-1\right)$ pairwise distinct cyclic triples.
(3) The cyclic triple $\left\langle g^{\gamma} x+g^{\delta} y, y, g^{\alpha} x+g^{\beta} y\right\rangle$ belongs to the $T C\{[\alpha-$ $\varepsilon, \gamma-\varepsilon],[\varepsilon-\gamma, \alpha-\gamma],[\gamma-\alpha, \varepsilon-\alpha]\}$, where $\alpha, \beta, \gamma, \delta \in \mathbf{R}^{*}, \alpha C \beta, \gamma C \delta$ and $\varepsilon=$ ind $(\alpha+\delta, \beta+\gamma)$. The cyclic triple $\left\langle x, y, g^{\alpha} x+g^{\beta} y\right\rangle$ belongs to the $T C\{[\alpha-\beta,-\beta],[\beta, \alpha],[-\alpha, \beta-\alpha]\}$.

## Proof.

(1) First, we analyze the possibilities of equality between three numbers in a trio. Suppose the trio is $\{\alpha,-\beta, \beta-\alpha\}$, where $\alpha, \beta \in \mathbf{R}^{*}$ and $\alpha C \beta$. We have the following three possibilities:

$$
\left\{\begin{aligned}
\alpha & =-\beta, \text { then } \alpha C(2 \alpha) \text { since }(-\beta) C(\alpha-\beta) \\
\alpha & =\beta-\alpha, \text { then } 2 \alpha=\beta, \text { i.e., } \alpha C(2 \alpha) \\
-\beta & =\beta-\alpha, \text { then } \alpha=2 \beta, \text { but }(2 \alpha) C(2 \beta) \text { so }(2 \alpha) C \alpha
\end{aligned}\right.
$$

All cases give $g^{2 \alpha}+g^{\alpha}+1=0$, so $g^{3 \alpha}=1$. This implies $\left(2^{n}-1\right) \mid 3 \alpha$, since $g$ is a primitive element in $\mathbf{F}^{*}$. But $0<\alpha<2^{n}-1\left(\alpha \in \mathbf{R}^{*}\right)$, so $3 \mid\left(2^{n}-1\right)$. For odd $n$ this is impossible, but when $n$ is even this gives $\alpha=\frac{2^{n}-1}{3}$ or $\frac{2\left(2^{n}-1\right)}{3}$. Then, the corresponding trio will be $\{\theta, \theta, \theta\}$ or $\{2 \theta, 2 \theta, 2 \theta\}$, i.e. a small trio.

By this analysis, when $n$ is odd all numbers in $\mathbf{R}^{*}$ are partitioned into $\frac{2^{n}-2}{3}$ trios; when $n$ is even all numbers in $\mathbf{R}^{*} \backslash\{\theta, 2 \theta\}$ are partitioned into $\frac{2^{n}-4}{3}$ trios.
(2) The cyclic triples belonging to different TC's are different. In fact, suppose $\left\langle u, g^{\alpha} u+g^{\beta} w, w\right\rangle=\left\langle u^{\prime}, g^{\gamma} u^{\prime}+g^{\delta} w^{\prime}, w^{\prime}\right\rangle$ (of course $u \neq w, u^{\prime} \neq$ $w^{\prime}$ and $\alpha \boldsymbol{C \beta}, \gamma \boldsymbol{\gamma} \delta$ ), but $\{\alpha,-\beta, \beta-\alpha\}$ and $\{\gamma,-\delta, \delta-\gamma\}$ are different

TC's. Then, there are the following three possibilities (but they are all impossible):
i) $u=u^{\prime}, g^{\alpha} u+g^{\beta} w=g^{\gamma} u^{\prime}+g^{6} w^{\prime}$ and $w=w^{\prime}$. Then $\left(g^{\alpha}+g^{\gamma}\right) u=$ $\left(g^{\beta}+g^{\delta}\right) w$, but $g^{\alpha}+g^{\gamma}=g^{\beta}+g^{6} \neq 0$, so $u=w$, a contradiction.
ii) $u=g^{\gamma} u^{\prime}+g^{\delta} w^{\prime}, g^{\alpha} u+g^{\beta} w=w^{\prime}$ and $w=u^{\prime}$. Then $g^{\beta} u+g^{\gamma} w^{\prime}=$ $g^{\beta+\delta} w^{\prime}+g^{\alpha+\gamma} u$, so $\left(g^{\beta}+g^{\alpha+\gamma}\right) u=\left(g^{\gamma}+g^{\beta+\delta}\right) w^{\prime}$. But $g^{\beta}\left(1+g^{\delta}\right)=$ $g^{\beta} g^{\gamma}=\left(1+g^{\alpha}\right) g^{\gamma}$ and $g^{\beta}+g^{\alpha+\gamma} \neq 0$ (else $\gamma=\beta-\alpha$, two TC will be the same), so $u=w^{\prime}$. This implies $u=g^{\alpha} u+g^{\beta} w$, so $g^{\beta}(u-w)=0$, i.e. $u=w$, again a contradiction.
iii) $u=w^{\prime}, g^{\alpha} u+g^{\beta} w=u^{\prime}$ and $w=g^{\gamma} u^{\prime}+g^{\delta} w^{\prime}$. This case is similar to ii).

Futhermore, suppose $\left\langle u, g^{\alpha} u+g^{\beta} w, w\right\rangle=\left\langle u^{\prime}, g^{\alpha} u^{\prime}+g^{\beta} w^{\prime}, w^{\prime}\right\rangle(u \neq$ $w, u^{\prime} \neq w^{\prime}, \alpha C \beta$ ). There are the following three cases:
i) $u=u^{\prime}, g^{\alpha} u+g^{\beta} w=g^{\alpha} u^{\prime}+g^{\beta} w^{\prime}$ and $w=w^{\prime}$. Then $(u, w)=\left(u^{\prime}, w^{\prime}\right)$.
ii) $u=g^{\alpha} u^{\prime}+g^{\beta} w^{\prime}, g^{\alpha} u+g^{\beta} w=w^{\prime}$ and $w=u^{\prime}$. Then $g^{\beta} u+g^{\alpha} w^{\prime}=$ $g^{2 \beta} w^{\prime}+g^{2 \alpha} u$, so $\left(g^{2 \alpha}+g^{\beta}\right) u=\left(g^{2 \beta}+g^{\alpha}\right) w^{\prime}$. But $g^{\alpha}+g^{\beta}=1=g^{2 \alpha}+g^{2 \beta}$, so $\left(g^{2 \alpha}+g^{\beta}\right)\left(u-w^{\prime}\right)=0$. Since $u \neq w^{\prime}$ (or else $g^{\alpha} u+g^{\beta} w=u$, then $g^{\beta}(u-w)=0$, so $u=w$, a contradiction), so $g^{2 \alpha}+g^{\beta}=0$. Thus $2 \alpha=\beta$ and $2 \beta=\alpha\left(\bmod 2^{n}-1\right)$, i.e. $3 \alpha=0\left(\bmod 2^{n}-1\right)$. This is equivalent to stating that $\{\alpha,-\beta, \beta-\alpha\}$ is a small trio (or a small TC).
iii) $u=w^{\prime}, g^{\alpha} u+g^{\beta} w=u^{\prime}, w=g^{\alpha} u+g^{\beta} w^{\prime}$. This case is similar to ii).

Since there are $2^{n}\left(2^{n}-1\right)$ ordered pairs $(u, w)$ of distinct elements in $F$, if a TC is not a small TC, it contains exactly $2^{n}\left(2^{n}-1\right)$ pairwise distinct cyclic triples, and each small TC (by ii) and iii)) only contains $\frac{2^{n}\left(2^{n}-1\right)}{3}$ pairwise distinct cyclic triples.
(3) For the cyclic triple $\langle u, v, w\rangle$, where $u=g^{\gamma} x+g^{6} y, v=y, w=$ $g^{\alpha} x+g^{\beta} y$ with a given $x \in F$, we have $g^{\alpha} u+g^{\gamma} w=\left(g^{\alpha+\delta}+g^{\beta+\gamma}\right) v$. So

$$
\begin{aligned}
& v=\frac{g^{\alpha}}{g^{\alpha+\delta}+g^{\beta+\gamma}} u+\frac{g^{\gamma}}{g^{\alpha+\delta}+g^{\beta+\gamma}} w ; \\
& w=\frac{g^{\alpha+\delta}+g^{\beta+\gamma}}{g^{\gamma}} v+g^{\alpha-\gamma} u ; \\
& u=g^{\gamma-\alpha} w+\frac{g^{\alpha+\delta}+g^{\beta+\gamma}}{g^{\alpha}} v .
\end{aligned}
$$

Similarly, for the cyclic triple $\left\langle x, y, g^{\alpha} x+g^{\beta} y\right\rangle$.
Later, in §2.4.3, the $2^{n}$ disjoint Mendelsohn triple systems of the $\operatorname{LMTS}\left(2^{n}+2\right)$ over the set $X=\left\{\infty_{1}, \infty_{2}\right\} \cup F$ that we shall construct, are indexed with elements $x \in F$. The Mendelsohn triple system ( $X, \mathcal{B}_{x}$ ) will contain the following four types of cyclic triples ( $y \in F \backslash\{x\}$ )
besides $\left\langle\infty_{1}, \infty_{2}, x\right\rangle$ and $\left\langle\infty_{2}, \infty_{1}, x\right\rangle$

| name | form of cyclic triple | PC | TC |
| :---: | :---: | :---: | :---: |
| $\infty_{1}$-triple | $\left\langle\infty_{1}, y, g^{\alpha_{1}} x+g^{\beta_{1}} y\right\rangle$ | $\left\langle\alpha_{1}, \beta_{1}\right\rangle$ |  |
| $\infty_{2}$-triple | $\left\langle\infty_{2}, y, g^{\alpha_{2}} x+g^{\beta_{2}} y\right\rangle$ | $\left(\alpha_{2}, \beta_{2}\right\rangle$ |  |
| $x$-triple | $\left\langle x, y, g^{\lambda} x+g^{\mu} y\right\rangle$ | $\langle\lambda, \mu\rangle$ | $\#$ |
| $y$-triple | $\left\langle g^{\gamma} x+g^{\delta} y, y, g^{\alpha} x+g^{\beta} y\right\rangle$ | $* *$ | $*$ |

where $\#=\{[\lambda, \mu],[-\mu, \lambda-\mu],[\mu-\lambda,-\lambda]\}, * *$ represents $\langle\alpha, \beta\rangle\langle\epsilon-\beta, \delta-$ $\beta\rangle\langle\gamma-\delta,-\delta\rangle$ and $*=\{[\alpha-\epsilon, \gamma-\epsilon],[\epsilon-\gamma, \alpha-\gamma],[\gamma-\alpha, \epsilon-\alpha]\}$; and the parameters $\alpha_{1}, \beta_{1}, \alpha_{2}, \alpha_{2}, \lambda, \mu, \alpha, \beta, \gamma, \delta \in R^{*}$ and $\lambda C \mu, \alpha C \beta, \gamma C \delta$, $\alpha_{1} C \beta_{1}, \alpha_{2} C \beta_{2}, \varepsilon=\operatorname{ind}(\alpha+\delta, \beta+\gamma)$. By Lemma 2.4.1 and 2.4.2, our main task will be to choose suitable parameters such that the PC and TC listed in the table exactly are all posible PC and TC. Note that all $y$-triples will occupy $\frac{2^{n}-5}{3} \mathrm{TC}$ if $n$ is odd, or $\frac{2^{n}-7}{3}+2 \mathrm{TC}$ if $n$ is even (including two small TC).

### 2.4.2 The choice of parameters.

For a given TC, one can give $3\left(2^{n}-3\right)$ pairs $(\alpha, \gamma)$ such that the corresponding $y$-triples $\left\langle g^{\gamma} x+g^{\delta} y, y, g^{\alpha} x+g^{\beta} y\right\rangle$ all belong to the given TC's (of course $\alpha C \beta$ and $\gamma C \delta$ ). But the PC's given by these pairs usually are rather chaotic, which gave us much difficulties. However, luckily, we have found the following

Lemma 2.4.3. The three $P C^{\prime}$ 's of a $y$-triple $\left\langle g^{\gamma} x+g^{\delta} y, y, g^{\alpha} x+g^{\beta} y\right\rangle$ can form a trio (i.e. they meet the property (T) in §2.4.1) if and only if one of the following holds:
(1) $\delta=\alpha$ (and $\gamma=\beta$ ). In this case the PC's and TC consist of the same couples: $\langle\alpha, \beta\rangle,\langle-\beta, \alpha-\beta\rangle$ and $\langle\beta-\alpha,-\alpha\rangle$.
(2) $\delta=\beta-\alpha$ (and $\gamma=-\alpha$ ). In this case the PC's are $<\alpha, \beta>,<$ $\beta-\alpha,-\alpha>$ and $<-\beta, \alpha-\beta>$, but its $T C$ is $\{[-2 \alpha, 2 \beta-2 \alpha],[2 \alpha-$ $2 \beta, 2 \beta],[2 \beta, 2 \alpha]\}$.

Proof. By the property (T) and the forms of the three PC's given by Lemma 2.4.1(2), we only have the following two possibilities:
$1^{\circ}-\delta=-\alpha$ and $\delta-\beta=-(\gamma-\delta)$. This implies $\delta=\alpha$ and $\gamma=\beta$. Futhermore, $\varepsilon=\operatorname{ind}(\alpha+\delta, \beta+\gamma)=\operatorname{ind}(2 \alpha, 2 \beta)=0$, and by Lemma 2.4.1(2) and 2.4.2(3) we get the case (1).
$2^{\circ} \beta=-(\gamma-\delta)$ and $\delta-\beta=-\alpha$. This implies $\delta=\beta-\alpha$ and $\gamma=-\alpha$. Futhermore, $\varepsilon=\operatorname{ind}(\alpha+\delta, \beta+\gamma)=\operatorname{ind}(\beta, \beta-\alpha)=2 \beta-\alpha$, and for the same reason we get the case (2). $\square$

This lemma is very useful. It can help us to choose the parameters in the table of $\S 2.4 .1$. The lemma gives two transformations between the
trios: case (1) gives the transformation from trio $\alpha,-\beta, \beta-\alpha$ to itself; case (2) gives the transformation from trio $A=\{\alpha,-\beta, \beta-\alpha\}$ to trio $B=\{-2 \alpha, 2 \beta, 2(\alpha-\beta)\}$, i.e. each number in the second trio is $(-2)$ times as large as each number in the first trio (we write $B=(-2) A$ ).

Now we construct a directed graph $G\left(R^{*}\right)$, which is named trioincidence graph. Its vertex set consists of all trios on $R^{*}$. From vertex $A$ to vertex $B$ there is an arc if and only if $B=(-2) A$ (we call $B$ the successor of $A$ ). The graph has $\frac{2^{n}-2}{3}$ (resp. $\frac{2^{n}-4}{3}+2$ ) vertices, when $n$ is odd (resp. even). Obviously, every vertex has exactly one in-arc and one out-arc, by Lemma 2.4 .3 and since (-2) is invertible in $R$. So, in fact, the graph is a union of disjoint directed circuits. Each number $\alpha$ of $R^{*}$ belongs to a unique vertex denoted by $V(\alpha)$. Each vertex $A$ of $G\left(R^{*}\right)$ belongs to a unique circuit denoted by $\sigma(A)$, and the length of the circuit is denoted by $\rho(A)$.
Lemma 2.4.4. Let the vertex $A \in G\left(R^{*}\right)$
(1) If $(-2)^{s} A=A$, then $\rho(A) \mid s$;
(2) $\rho(A)=1$ if and only if $A$ is a small trio;
(3) If $-A \in \sigma(A)=\sigma$, then $\rho(A)$ is even. And for any $B \in \sigma,-B=$ $(-2)^{\frac{\rho(A)}{2}} B \in \sigma\left(\frac{\rho(A)}{2}\right.$ is minimum). If $-A \in \tau \neq \sigma(A)$, then $\tau$ and $\sigma$ have the same length and for any $B \in \sigma,-B \in \tau$.

## Proof.

(1) Obviously, $s \geq k=\rho(A)$. Let $s=p k+t, 0 \leq t<k$. Then

$$
A=(-2)^{s} A=(-2)^{t} \cdot \underbrace{(-2)^{k}(-2)^{k} \ldots(-2)^{k}}_{\rho} A=(-2)^{t} A
$$

So, $t=0$, i.e. $\rho(A) \mid s$.
(2) If $\rho(A)=1$, let $A=\{\alpha,-\beta, \beta-\alpha\}$. Then (-2) $\alpha=\alpha$ (so $3 \alpha=0$ ) or $(-2) \alpha=-\beta$ (so $\beta=2 \alpha$, i.e. $\alpha C(2 \alpha)$ ) or $(-2) \alpha=\beta-\alpha$ (so $-\alpha=\beta$, i.e. $\alpha C(-\alpha)$ ). Thus in each case $A$ is a small trio. The converse is trivial.
(3) Clearly,

$$
(-2)^{s} A=B \text { if and only if }(-2)^{s}(-A)=-B(*)
$$

(for any positive s). Letting $B=A$ we have both $\rho(-A) \leq \rho(A)$ and $\rho(A) \leq \rho(-A)$, thus $\rho(A)=\rho(-A)$. As well as, by the same relationship (*), if $A$ and $B$ are in the same circuit then $-A$ and $-B$ also are. Furthermore, since $B \neq-B$ for any trio $B$, so if $-A \in \sigma(A)$ (thereby $-B \in \sigma(A)$ for any $B \in \sigma(A))$ then $\rho(A)$ must be even. Suppose $(-2)^{t} B=-B(t$ is minimum, so $t<\rho(A)$ ) for $B \in \sigma(A)$, then
$(-2)^{2 t} B=B$. So, by (1), $\rho(A) \mid 2 t$, i.e. $\left.\frac{\rho(A)}{2} \right\rvert\, t$, but $t<\rho(A)$ so we must have $t=\frac{\rho(A)}{2} . \square$

By this lemma (3), for a circuit $\sigma \in G\left(R^{*}\right)$ if there exists a vertex $A \in \sigma$ and a positive integer $s$ such that $(-2)^{s} A=-A$, then call this circuit $\sigma$ self-dual.

Lemma 2.4.5. For any $n \geq 3, G\left(R^{*}\right)$ has a self-dual circuit $\sigma(V(\alpha))$
(1) If there exists an odd $s>1$ with $s \mid n$, then $\alpha=\frac{2^{n}-1}{2^{\circ}-1}$. And $\rho(V(\alpha))=2 s$ (if $3 \dagger s$ ) or 2 (if $s=3$ ).
(2) If $4 \mid n$, then $\alpha=\frac{2^{n}-1}{15}$ and $\rho(V(\alpha))=4$.

## Proof.

(1) First, we have $\left(2^{s}-1\right) \alpha=0\left(\bmod 2^{n}-1\right)$, so $(-2)^{s} \alpha=-2^{s} \alpha=-\alpha$. Thus $(-2)^{s} A=-A(A=V(\alpha))$, i.e. $\sigma(A)$ is self-dual.

Since $(-2)^{2 s} A=A\left(\left[(-2)^{2 s}-1\right] \alpha=\left(2^{2 s}-1\right) \alpha=\left(2^{s}+1\right)\left(2^{n}-1\right) \equiv 0\right.$ $\left(\bmod 2^{n}-1\right)$ ), so $\rho(A) \mid 2 s$ and $\rho(A)$ is even, by Lemma 2.4.4.

When $3 \nmid s$, let $\rho(A)=2 t$. Then $t \mid s$. By $A=(-2)^{2 t} A=2^{2 t} A$ and $\alpha \in A$, we have the following three cases (where $\alpha C \beta$ ):
i) $2^{2 t} \alpha=\alpha$. Then $\frac{2^{2 t}-1}{2^{t}-1}\left(2^{n}-1\right)=\left(2^{2 t}-1\right) \alpha \equiv 0\left(\bmod 2^{n}-1\right)$, so $\left(2^{s}-1\right) \mid\left(2^{2 t}-1\right)$, so $s \mid 2 t$. As $s$ is odd, $s \mid t$, so $t=s$.
ii) $2^{2 t} \alpha=-\beta$. Then $2^{2 t}(-\beta)=\beta-\alpha, 2^{2 t}(\beta-\alpha)=\alpha$ by (C1) in §2.4.1. Thus $\left(2^{6 t}-1\right) \alpha=0$, so $s \mid 6 t$. But $2 \nmid s, 3 \nmid s$, so $s \mid t$, which implies $t=s$.
iii) $2^{2 t} \alpha=\beta-\alpha$. Then $2^{2 t}(-\beta)=\alpha, 2^{2 t}(\beta-\alpha)=-\beta$ by (C1). The argument is the same as in ii). So, when $3 \nmid s$, we always have $p(A)=2 s$.

When $s=3$ we have $g^{8 \alpha}=g^{\alpha}$. Let $x=g^{\alpha}$. Then

$$
x^{8}-x=x(x-1)\left(x^{3}+x+1\right)\left(x^{3}+x^{2}+1\right)=0 .
$$

But $x=g^{\alpha} \neq 0,1$, so $g^{3 \alpha}+g^{\alpha}=1$ (thus $\beta=3 \alpha$, i.e. $\left.(-2) \alpha=-(\beta-\alpha)\right)$ or $g^{3 \alpha}+g^{2 \alpha}=1$ (thus $2 \beta=3 \alpha$, i.e. $\left.(-2)(\beta-\alpha)=-\alpha\right)$. Both cases give $(-2) A=-A$, thus $(-2)^{2} A=A, \rho(A)=2$.
(2) Since $\left(2^{4}-1\right) \alpha \equiv 0\left(\bmod 2^{n}-1\right)$, we have $g^{16 \alpha}=g^{\alpha}$. Let $x=g^{\alpha}$. Then

$$
x^{16}-x=x\left(x^{5}-1\right)\left(x^{2}+x+1\right)\left(x^{4}+x+1\right)\left(x^{4}+x^{3}+1\right)=0 .
$$

But $g^{\alpha} \neq 0, g^{5 \alpha} \neq 1$ and $g^{2 \alpha}=g^{\alpha}+1 \neq 0$ (else $g^{3 \alpha}=1$, but $3 \alpha=$ $\frac{2^{n}-1}{5} \equiv 0\left(\bmod 2^{n}-1\right)$ ), so $g^{4 \alpha}+g^{\alpha}+1=0$ (thus $\beta=4 \alpha$, i.e. $(-2)^{2} \alpha=$ $\beta$ ) or $g^{4 \alpha}+g^{3 \alpha}+1=0$ (thus $4 \beta=3 \alpha$, i.e. $(-2)^{2}(\beta-\alpha)=-\alpha$ ). Both give $(-2)^{2} A=-A$. Obviously, $(-2) A \neq-A$, so $\rho(A)=4$. $\square$

By this lemma we can get a self-dual circuit in $G\left(R^{*}\right)$ for any $n \geq 3$ (if there exists an odd $s>1, s \mid n$, then by (1); else $n=2^{k} \geq 3$ and we must have $4 \mid n$, by (2)). Here, we give a table for $3 \leq n \leq 20$.

| $n$ | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 9 | 10 | 11 | 12 | 12 | 13 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $s$ | 3 | 4 | 5 | 3 | 7 | 4 | 3 | 9 | 5 | 11 | 3 | 4 | 13 |
| $\alpha$ | 1 | 1 | 1 | 9 | 1 | 17 | 7371 | 33 | 1 | 585 | 273 | 1 |  |
| $\rho(V(\alpha))$ | 2 | 4 | 10 | 2 | 14 | 4 | 2 | 18 | 10 | 22 | 2 | 4 | 26 |
| $n$ | 14 | 15 | 15 | 16 | 17 | 18 | 19 | 20 | 20 |  |  |  |  |
| $s$ | 7 | 3 | 5 | 4 | 17 | 3 | 19 | 4 | 5 |  |  |  |  |
| $\alpha$ | 1 | 4681 | 1057 | 4369 | 1 | 37449 | 1 | 69905 | 33825 |  |  |  |  |
| $\rho(V(\alpha))$ | 14 | 2 | 10 | 2 | 34 | 2 | 38 | 4 | 10 |  |  |  |  |

### 2.4.3 The construction and examples.

Let $\alpha$ be given by Lemma 2.4.5, $\rho(V(\alpha))=2 s$. Define $\alpha_{i}=(-2)^{i} \alpha$, $0 \leq i \leq s-1$, and $\lambda=(-2)^{s} \alpha$. Take a number $\gamma_{j}$ from each vertex $A_{j} \in G\left(R^{*}\right) \backslash S$, where

$$
S=\left\{V\left(\alpha_{0}\right), V\left(\alpha_{1}\right), \ldots, V\left(\alpha_{s-1}\right), V(\lambda)\right\} \cup S_{0}, \quad 1 \leq j \leq t
$$

and $S_{0}=\phi$ (if $n$ odd) or $\{\{\theta, \theta, \theta\},\{2 \theta ; 2 \theta, 2 \theta\}\}$ (if $n$ even, $\theta=\frac{1}{3}\left(2^{n}-1\right)$ ); $t=\frac{1}{3}\left(2^{n}-2\right)-s-1$ (if $n$ odd) or $\frac{1}{3}\left(2^{n}-4\right)-s-1$ (if $n$ even). Let $\alpha_{i} C \beta_{i}, \lambda C \mu, \gamma_{j} C \delta_{j}, 0 \leq i \leq s-1,1 \leq j \leq t$. Then, as announced in $\S 2.4 .1, \mathcal{B}_{x}$ will contain the following triples:
(1) $\left\langle\infty_{1}, \infty_{2}, x\right\rangle,\left\langle\infty_{2}, \infty_{1}, x\right\rangle$; this gives two blocks.
(2) $\left\langle\infty_{1}, y, g^{-\mu} x+g^{\lambda-\mu} y\right\rangle,\left\langle\infty_{2}, y, g^{\mu-\lambda} x+g^{-\lambda} y\right\rangle$; this gives $2\left(2^{n}-1\right)$ blocks.
(3) $\left\langle x, y, g^{\lambda} x+g^{\mu} y\right\rangle$; this gives $2^{n}-1$ blocks.
(4) $\left\langle g^{-\alpha_{i}} x+g^{\beta_{i}-\alpha_{i}} y, y, g^{\alpha_{i}} x+g^{\beta_{i}} y\right\rangle, 0 \leq i \leq s-1$; this gives $s\left(2^{n}-1\right)$ blocks.
(5) $\left\langle g^{\delta_{j}} x+g^{\gamma_{j}} y, y, g^{\gamma_{j}} x+g^{\delta_{j}} y\right\rangle, 1 \leq j \leq t$; this gives $t\left(2^{n}-1\right)$ blocks.
(6) $\left\langle g^{2 \theta} x+g^{\theta} y, y, g^{\theta} x+g^{2 \theta} y\right\rangle,\left\langle g^{\theta} x+g^{2 \theta} y, y, g^{2 \theta} x+g^{\theta} y\right\rangle$; this gives $\frac{2}{3}\left(2^{n}-1\right)$ blocks.
where $y$ runs over $F \backslash\{x\}$. Type (6) occurs only if $n$ is even. Letting $y$ run over $F \backslash\{x\}$ produces each element three times but we only retain one copy of each triple.

Theorem 2.4.6. For $n \geq 3$, the above construction $\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup\right.\right.$ $\left.\left.F, \mathcal{B}_{x}\right) ; x \in F\right\}$ gives an $L M T S\left(2^{n}+2\right)$, where $F=G F\left(2^{n}\right)$.

Proof. By $\S 2.4$.1 and 2.4.2, we only need to show the following three points again.
$1^{\circ}$ The total number of cyclic triples in each $\mathcal{B}_{x}$ equals

$$
\left\{\begin{array}{l}
2+3\left(2^{n}-1\right)+s\left(2^{n}-1\right)+\left(\frac{2^{n}-2}{3}-s-1\right)\left(2^{n}-1\right)(n \text { odd }) \\
2+3\left(2^{n}-1\right)+s\left(2^{n}-1\right)+\left(\frac{2^{n}-4}{3}-s-1\right)\left(2^{n}-1\right)+2 \cdot \frac{2^{n}-1}{3} \\
\text { ( } n \text { even })
\end{array}\right.
$$

Both totals are $\frac{1}{3}\left(2^{n}+2\right)\left(2^{n}+1\right)$, exactly as expected.
$2^{\circ}$ The parts (2)-(6) contain all PC's.
Suppose the vertex $V(\alpha)$ in the circuit $\sigma$ as in Figure 1. By Lemma 2.4.5, $\sigma$ is self-dual and $\{\alpha,-\beta, \beta-\alpha\}=$ $-\{\lambda,-\mu, \mu-\lambda\}$. Obviously, the parts (2) and (3) contain the three PC's corresponding to the trio $V(\lambda)$. And, by Lemma 2.4.3(2), each cyclic triple in part (4) contains the three PC's corresponding to the trio $V\left(\alpha_{i}\right), 0 \leq i \leq$ $s-1$. All other PC's consisting of all trios $A_{j}$ and small trios, are covered by parts (5) and (6), by Lemma 2.4.5
 (1).
$3^{\circ}$ The parts (3)-(6) cover all TC's.
By Lemma 2.4.5(2), the cyclic triple in part (4) corresponding to the trio $V\left(\alpha_{i}\right)$ occupies the TC corresponding to the trio $V\left(\alpha_{i+1}\right)$, where $0 \leq i \leq s-1$ and $V\left(\alpha_{s}\right)=V(\lambda)$. And the TC corresponding to $V(\alpha)=V\left(\alpha_{0}\right)$ is occupied by $x$-triple (in part (3)). All other TC's (corresponding to trios $A_{j}$ and to small trios) are occupied by the $y$ triples in part (5) and (6), by Lemma 2.4.5(1).
Example 1. $n=3, g^{3}+g+1=0$
$1 C 3,2 C 6,4 C 5$
$G\left(Z_{7}^{*}\right):$
Take $\alpha=\alpha_{0}=1\left(\beta_{0}=3, s=1\right)$,

$$
\lambda=5(\mu=4)
$$

$\operatorname{LMTS}(10)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F_{8}, \mathcal{B}_{x}\right) ; x \in F_{8}\right\}$, where $\mathcal{B}_{x}$ contains:

$\{3,6,5\}$
(1) $\left\langle\infty_{1}, \infty_{2}, x\right\rangle,\left\langle\infty_{2}, \infty_{1}, x\right\rangle$
$\begin{array}{ccr}\text { (2) } \quad\left\langle\infty_{1}, y, g^{3} x+g y\right\rangle & <3,1> & \\ & \left\langle\infty_{2}, y, g^{6} x+g^{2} y\right\rangle & <6,2> \\ \text { (3) }\left\langle x, y, g^{5} x+g^{4} y\right\rangle & <5,4> & \{3,6,5\} \\ \text { (4) }\left\langle g^{6} x+g^{2} y, y, g x+g^{3} y\right\rangle<1,3><2,6><4,5>\{1,4,2\}\end{array}$

Example 2. $n=4, g^{4}+g+1=0$
$1 C 4,2 C 8,3 C 14,5 C 10$, $6 C 13,7 C 9,11 C 12$
$G\left(Z_{15}^{*}\right):$

$\{5,5,5\} \quad\{10,10,10\}$ $\{1,11,3\}$

Take $\alpha=\alpha_{0}=1\left(\beta_{0}=4, s=2\right)$,

$$
\begin{aligned}
& \alpha_{1}=13\left(\beta_{1}=6\right) \\
& \lambda=4(\mu=1), \gamma_{1}=2\left(\delta_{1}=8\right)
\end{aligned}
$$

$L M T S(18)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F_{16}, \mathcal{B}_{x}\right) ; x \in F_{16}\right\}$, where $\mathcal{B}_{x}$ contains:

(1) $\left\langle\infty_{1}, \infty_{2}, x\right\rangle,\left\langle\infty_{2}, \infty_{1}, x\right\rangle$

(3) $\left\langle x, y, g^{4} x+g y\right\rangle$
$\{3,1,11\}$
(4) $\left\langle g^{14} x+g^{3} y, y, g x+g^{4} y\right\rangle\langle 1,4\rangle\langle 3,14\rangle\langle 11,12\rangle\{9,8,13\}$ $\left\langle g^{2} x+g^{8} y, y, g^{13} x+g^{6} y\right\rangle \quad\{13,6\rangle\langle 8,2\rangle\langle 9,7\rangle \quad\{14,12,4\}$
(5) $\left\langle g^{8} x+g^{2} y, y, g^{2} x+g^{8} y\right\rangle \quad\langle 2,8\rangle\langle 7,9\rangle\langle 6,13\rangle \quad\{2,7,6\}$
(6) $\left\langle g^{10} x+g^{3} y, y, g^{5} x+g^{10} y\right\rangle \quad\langle 5,10\rangle \quad\{5,5,5\}$
$\left\langle g^{5} x+g^{10} y, y, g^{10} x+g^{3} y\right\rangle \quad\langle 10,5\rangle \quad\{10,10,10\}$

Example 3. $n=5, g^{5}+g^{2}+1=0$
$1 C 18,2 C 5,3 C 29,4 C 10,6 C 27,7 C 22$,
$8 C 20,9 C 16,11 C 19,12 C 23,13 C 14$,
$15 C 24,17 C 30,21 C 25,26 C 28 \quad G\left(Z_{31}^{*}\right):$
Take $\alpha=\alpha_{0}=1$

$$
\left(\beta_{0}=18, s=5\right)
$$

$$
\alpha_{1}=29\left(\beta_{1}=3\right)
$$

$$
\alpha_{2}=4\left(\beta_{2}=10\right)
$$

$$
\alpha_{3}=23\left(\beta_{3}=12\right)
$$

$$
\alpha_{4}=16\left(\beta_{4}=9\right)
$$

$$
\gamma_{1}=2\left(\delta_{1}=5\right)
$$

$$
\gamma_{2}=10\left(\delta_{2}=4\right)
$$

$$
\gamma_{3}=8\left(\delta_{3}=20\right)
$$

$$
\gamma_{4}=7\left(\delta_{4}=22\right)
$$

$$
\lambda=30(\mu=17)
$$

$\operatorname{LMTS}(34)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F_{32}, \mathcal{B}_{x}\right) ; x \in F_{32}\right\}$,
where $\mathcal{B}_{\boldsymbol{x}}$ contains:

| (1) $\left\langle\infty_{1}, \infty_{2}, x\right\rangle,\left\langle\infty_{2}, \infty_{1}, x\right\rangle$ |  |
| :---: | :---: |
| (2) $\left\langle\infty_{1}, y, g^{14} x+g^{13} y\right\rangle$ | (14, 13) |
| $\left\langle\infty_{2}, y, g^{18} x+g y\right\rangle$ | $\langle 18,1\rangle$ |
| (3) $\left\langle x, y, g^{30} x+g^{17} y\right\rangle$ | $\langle 30,17) \quad\{13,17,1\}$ |
| (4) $\left\langle g^{30} x+g^{17} y, y, g x+g^{18} y\right\rangle\langle 1,18\rangle\langle 17,30\rangle(13,14\rangle\{28,5,29\}$ |  |
| ( $g^{2} x+g^{5} y, y, g^{29} x+g^{3}$ | $\langle 29,3\rangle\langle 5,2\rangle\langle 28,26\rangle \quad\{21,6,4\}$ |
| $\left\langle g^{27} x+g^{6} y, y, g^{4} x+g^{1}\right.$ | $(4,10\rangle\langle 6,27\rangle\langle 21,25\rangle\{19,20,23\}$ |
| ( $g^{8} x+g^{20} y, y, g^{23} x+g$ | $(23,12\rangle\langle 20,8\rangle\langle 19,11\rangle\{22,24,16\}$ |
| ( $g^{15} x+g^{24} y, y, g^{16} x+g^{\prime}$ | $(16,9\rangle\langle 24,15)\langle 22,7\rangle\{14,18,30\}$ |
| (5) $\left\langle g^{5} x+g^{2} y, y, g^{2} x+g^{5}\right.$ | $\langle 2,5\rangle\langle 26,28\rangle\langle 3,29\rangle \quad\{2,26,3\}$ |
| $\left\langle g^{4} x+g^{10} y, y, g^{10} x+g^{4} y\right\rangle$ | $\langle 10,4\rangle(27,6\rangle(25,31\rangle\{10,27,25\}$ |
| $\left\langle g^{20} x+g^{8} y, y, g^{8} x+g^{20}\right.$ | $\langle 8,20\rangle\langle 11,19\rangle\langle 12,23\rangle\{8,11,12\}$ |
| $\left\langle g^{22} x+g^{7} y, y, g^{7} x+g^{22} y\right\rangle$ | $(7,22\rangle\langle 9,16\rangle\langle 15,24\rangle \quad\{7,9,15\}$ |

The above examples were constructed and checked using a computer. In order to show the complication and usefulness of the trio-incidence graph $G\left(R^{*}\right)$, here we still give the graph $G\left(Z_{63}^{*}\right)$ as follows:

$\{21,21,21\}$

$\{42,42,42\}$


In this graph the shaded circuit is the unique self-dual circuit.

### 2.5 Correction of an error.

Apart from our results mentioned above, there were the following results concerning large sets of disjoint Mendelsohn triple systems (before the end of 1988):
(2.5.1) $\operatorname{LMTS}(v) \longrightarrow \operatorname{LMTS}(3 v)$ (Lindner [Lin1])
(2.5.2) $\operatorname{LMTS}(v+1) \longrightarrow \operatorname{LMTS}(3 v+1), v \geq 3$ (Lindner [Lin1]])
(2.5.3) $G L S(2+m) \longrightarrow L M T S(2+2 m)$ (Wu Lisheng [Wu])
(2.5.4) LMTS $(n+2) \longrightarrow L M T S(n v+2), v \equiv \pm 1(\bmod 6)($ Teirlinck \& Lindner [TeiLin]).

Also, there were some simple direct constructions, for the examples $L M T S(3), L M T S(4)$ and $L M T S(7)$. Here the listed results are all recursive, but our results in $\S 2.2$ and $\S 2.4$ are the only two kinds of direct construction of infinite series of LMTSs. Lemma 2.3.2 is an extension of the above-mentioned (2.5.3), where GLS is a special LSTS defined by Lu Jiaxi in [Lu]. The result (2.5.4) is equivalent to our Theorem 2.3.3, which was published almost at the same time as [TeiLin] and uses a different method as [TeiLin]. For the above-mentioned references (2.5.1) and (2.5.2) we would like to point out some errors and correct them.
In the paper [Lin1] (C.C.Lindner), there are the following mistakes:
i) In the construction (3) of Theorem 2.1 (p. 328, $D(3 v) \geq 2 v+D(v))$ the number of cyclic triples is too small. In this paper, part (i) gives $v(v-1)$ triples and part (ii) gives $2 v(v-1)$ triples, totalling only $3 v(v-1)$, i.e., short by $2 v$ triples.
ii) In the construction ( $3^{\prime}$ ) of Theorem 3.1 (p. 329, $D(3 v+1) \geq 2 v+$ $D(v+1)$ ) the number of cyclic triples is also too small (part ( $i^{\prime}$ ) gives $v(v+1)$ triples and part ( $i i^{\prime}$ ) gives $2 v(v-1)$ triples). Part ( $i i^{\prime}$ ) and ( $\left.i i i^{\prime}\right)$ do not touch upon the case $k=1$, and the case $k=v-1$ is not well handled.
iii) For the symbol $Q$, it is said "a Latin square of order $v$ having $v$ disjoint transversals" in p. 327, but it is again said "any idempotent quasigroup" and "not necessarily related in any way to the Latin square $Q^{\prime \prime}$ in p. 328. This is not correct, the second $Q$ has to relate to the first $Q$ (or the part (i) of $t_{k}$ and $t_{k}^{*}$ will join the part (ii) of $d_{k}$, since $\circ$ is determined by $y_{i k}=i \circ x_{i k}$ ). In fact, the $Q$ should be an idempotent Latin square having an orthogonal mate.
iv) It is enough to keep three cyclic triples from (1)(ii) and (2)(ii) in section 2 (p.328), respectively, because the choice of $i$ and $j$ is unordered.

Below, we give a corrected description of this construction and prove its correctness (there was not any proof in [Lin1]).

Let $v \geq 3, v \neq 6$, and let $Q$ be an idempotent Latin square of order $v$ having $v$ disjoint transversals $T_{1}, T_{2}, \ldots, T_{v}$. The symbols $T_{k}, \alpha_{k}, \alpha_{k}^{*}, \beta_{k}$, $\beta_{k}^{*}, \gamma_{k}$ and $\gamma_{k}^{*}$ are the same as in the paper [Lin1]. The Latin square $Q$ corresponds to a quasigroup $(Q, \circ)$, so $y_{i k}=i \circ x_{i k}$.

## A. The construction of $v \longrightarrow 3 v$.

Define $2 v+D(v) M T S(3 v)_{s}$ ' over the set $Q \times\{1,2,3\}$ as follows:
(1) Define a collection of cyclic triples $t_{k}(1 \leq k \leq v)$ by
(i) $\left\langle(i, 1),\left(x_{i k}, 2\right),\left(y_{i k}, 3\right)\right\rangle,\left\langle\left(x_{i k}, 2\right),(i, 1),\left(y_{i k}, 3\right)\right\rangle, i \in Q$; this gives $2 v$ triples.
(ii) $\left\langle(i, 1),(j, 1),\left((i \circ j) \alpha_{k}, 2\right)\right\rangle,\left\langle(i, 2),(j, 2),\left((i \circ j) \beta_{k}, 3\right)\right\rangle,\langle(i, 3),(j, 3)$ ,$\left.\left((i \circ j) \gamma_{k}, 1\right)\right\rangle, i \neq j \in Q$; this gives $3 v(v-1)$ triples.
(2) define a collection of cyclic triples $t_{k}^{*}(1 \leq k \leq v)$ by
(i) $\left.\left\langle(i, 1),\left(x_{i k}, 2\right),\left(y_{i k}^{*}, 3\right)\right\rangle,\left\langle x_{i k}, 2\right),(i, 1),\left(y_{i k}^{*}, 3\right)\right\rangle, i \in Q$; this gives $2 v$ triples.
(ii) $\left\langle(i, 1),(j, 1),\left((i \circ j) \alpha_{k}^{*}, 3\right)\right\rangle,\left\langle(i, 3),(j, 3),\left((i \circ j) \beta_{k}^{*}, 2\right)\right\rangle,\langle(i, 2),(j, 2$ ), ((ioj) $\left.\left.\gamma_{k}^{*}, 1\right)\right\rangle, i \neq j \in Q$; this gives $3 v(v-1)$ triples.
(3) Let $\left(Q, q_{k}\right) ; 1 \leq k \leq D(v)$ be any collection of $D(v)$ pairwise disjoint $M T S(v)$. Define a collection $d_{k}$ of cyclic triples by
(i) $\langle(x, i),(y, i),(z, i)\rangle$ with $\langle x, y, z\rangle \in q_{k}, i=1,2,3$; this gives $v(v-$ 1) triples.
(ii) $\left\langle(i, 1),(j, 2),\left((i \circ j) \alpha^{k+1}, 3\right)\right\rangle,\left\langle(j, 2),(i, 1),\left((i \circ j) \alpha^{k+1}, 3\right)\right\rangle, i, j \in$ $Q$; this gives $2 v^{2}$ triples.

## Proof.

$1^{\circ}$ Each $t_{k}$ is a $M T S(3 v)$ (Similarly for $t_{k}^{*}$ ).
The total number of triples is $2 v+3 v(v-1)=\frac{3 v(3 v-1)}{3}$, as required. For any ordered pair $P$ of distinct elements of the set $Q \times\{1,2,3\}$, we have the following cases:
$P=((x, i),(y, i))$ with $x \neq y, i=1,2,3$ is contained in part (ii).
$P=((i, 1),(j, 2))$. There exists $s$ such that $(s \circ i) \alpha_{k}=j$. Now $P$ is contained in part (i) if $s=i\left(j=(i \circ i) \alpha_{k}=i \alpha_{k}=x_{i k}\right)$, and otherwise in part (ii).
$P=((i, 1),(j, 3))$. There exists $s$ such that $(j \circ s) \gamma_{k}=i$. Now $P$ is contained in part (i) if $s=j\left(i=(j \circ j) \gamma_{k}=j \gamma_{k}, j=y_{i k}\right)$, and otherwise in part (ii).
$P=((i, 2),(j, 3))$. There exists $s$ such that $(s \circ i) \beta_{k}=j$. Now $P$ is contained in part (i) if $s=i\left(j=(i \circ i) \beta_{k}=i \beta_{k}\right.$, let $i=x_{i^{\prime} k}$ then $j=y_{i^{\prime} k}$ ), and otherwise in part (ii).
$P=((i, 3),(j, 2))$. There exists $s$ such that $(j \circ s) \beta_{k}=i$. Now $P$ is contained in part (i) if $s=j\left(i=(j \circ j) \beta_{k}=j \beta_{k}\right.$, let $j=x_{i^{\prime} k}$ then $i=y_{i^{\prime} k}$ ), and otherwise in part (ii).
$P=((i, 3),(j, 1))$. There exists $s$ such that $(s \circ i) \gamma_{k}=j$. Now $P$ is contained in part (i) if $s=i\left(j=(i \circ i) \gamma_{k}=i \gamma_{k}, i=y_{j k}\right)$, and otherwise in part (ii).
$P=((i, 2),(j, 1))$. There exists $s$ such that $(j \circ s) \alpha_{k}=i$. Now $P$ is contained in part (i) if $s=j\left(i=(j \circ j) \alpha_{k}=j \alpha_{k}=x_{j k}\right)$, and otherwise
in part (ii).
$2^{\circ}$ Each $d_{k}$ is a $M T S(3 v)$ too.
The total number of triples is $v(v-1)+2 v^{2}=\frac{3 v(3 v-1)}{3}$, as just required. For any ordered pair $P$ of distinct elements of the set $Q \times$ $\{1,2,3\}$, we have the following cases:
$P=((x, i),(y, i))$ with $x \neq y, i=1,2,3$ is contained in part (i), since $q_{k}$ is a $M T S(v)$.

$$
P=((i, 1),(j, 2)) \text { and }((i, 2),(j, 1)) \text { are contained in part (ii). }
$$

$P=((i, 1),(j, 3))$. There exists $s$ such that $(i \circ s) \alpha^{k+1}=j$, so $P \in$ part (ii).
$P=((i, 3),(j, 1))$. There exists $s$ such that $(j \circ s) \alpha^{k+1}=i$, so $P \in$ part (ii).
$P=((i, 2),(j, 3))$. There exists $s$ such that $(s \circ i) \alpha^{k+1}=j$, so $P \in$ part (ii).
$P=((i, 3),(j, 2))$. There exists $s$ such that $(s \circ j) \alpha^{k+1}=i$, so $P \in$ part (ii).
$3^{\circ}$ All cyclic triples in all $t_{k}, t_{k}^{*}$ and $d_{k}$ are pairwise different. Instead of this, let us prove that $\left\{t_{k}\right\} \cup\left\{t_{k}^{*}\right\} \cup\left\{d_{k}\right\}$ is a $L M T S(3 v)$ if $D(v)=v-2$. For any cyclic triple $T$ from $Q \times\{1,2,3\}$ we have the following cases.
$T=\langle(x, i),(y, i),(z, i)\rangle$ with $x \neq y \neq z \neq x$. There exists $k$ such that $(x, y, z\rangle \in q_{k}$, so $T \in$ part (i) of $d_{k}$.
$T=\langle(x, i),(y, i),(z, j)\rangle$ with $x \neq y, i \neq j$. There exists $k$ such that
( $x \circ y$ ) $\alpha_{k}=z$ if $(i, j)=(1,2)$, and now $T \in$ part (ii) of $t_{k}$;
( $x \circ y$ ) $\beta_{k}=z$ if $(i, j)=(2,3)$, and now $T \in \operatorname{part}$ (ii) of $t_{k}$;
$(x \circ y) \gamma_{k}=z$ if $(i, j)=(3,1)$, and now $T \in$ part (ii) of $t_{k}$;
( $x \circ y$ ) $\alpha_{k}^{*}=z$ if $(i, j)=(1,3)$, and now $T \in$ part (ii) of $t_{k}^{*}$;
$(x \circ y) \beta_{k}^{*}=z$ if $(i, j)=(3,2)$, and now $T \in \operatorname{part}$ (ii) of $t_{k}^{*}$;
$(x \circ y) \gamma_{k}^{*}=z$ if $(i, j)=(2,1)$, and now $T \in$ part (ii) of $t_{k}^{*}$.
$T=\langle(i, 1),(j, 2),(s, 3)\rangle$. There exists $m(0 \leq m \leq v-1)$ such that $(i \circ j) \alpha^{m}=s$.

If $m=0$, let $j=x_{i k}$, then $i \circ j=s=y_{i k}$, so $T \in$ part (i) of $t_{k}$;
if $m=1$, let $j=x_{i k}$, then $s=(i \circ j) \alpha=y_{i k} \alpha=y_{i k}^{*}$, so $T \in$ part(i) of $t_{k}^{*}$;
if $2 \leq m \leq v-1$, then $T \in \operatorname{part}$ (ii) of $d_{m-1}$.
$T=\langle(i, 2),(j, 1),(s, 3)\rangle$. There exists $m(0 \leq m \leq v-1)$ such that $(j \circ i) \alpha^{m}=s$.

If $m=0$, let $i=x_{j k}$, then $j \circ i=s=y_{j k}$, so $T \in \operatorname{part}$ (i) of $t_{k}$;
if $m=1$, let $i=x_{j k}$, then $s=(j \circ i) \alpha=y_{j k} \alpha=y_{j k}^{*}$, so $T \in$ $\operatorname{part}(\mathrm{i})$ of $t_{k}^{*}$;
if $2 \leq m \leq v-1$, then $T \in \operatorname{part}$ (ii) of $d_{m-1}$.
This completes the proof.

## B. The construction of $v+1 \longrightarrow 3 v+1$.

Define $2 v+D(v+1) M T S(3 v+1) s^{\prime}$ over the set $\{\infty\} \cup(Q \times\{1,2,3\})$ as follows
(1) Define a collection of cyclic triples $t_{k}^{\prime}(1 \leq k \leq v)$ by
(i) $\left\langle\infty,(i, 1),\left(x_{i k}, 2\right)\right\rangle,\left\langle\infty,\left(x_{i k}, 2\right),\left(y_{i k}, 3\right)\right\rangle,\left\langle\infty,\left(y_{i k}, 3\right),(i, 1)\right\rangle, i \in$ $Q$; this gives $3 v$ triples.
(ii) $\left\langle\left(x_{i k}, 2\right),(i, 1),\left(y_{i k}, 3\right)\right\rangle, i \in Q$; this gives $v$ triples.
(iii) Same to $\mathrm{A}(1)$ (ii); this gives $3 v(v-1)$ triples.
(2) Define a collection of cyclic triples $t_{k}^{* *}(1 \leq k \leq v)$ by
(i) $\left\langle\infty,(i, 1),\left(y_{i k}^{*}, 3\right)\right\rangle,\left\langle\infty,\left(x_{i k}, 2\right),(i, 1)\right\rangle,\left\langle\infty,\left(y_{i k}^{*}, 3\right),\left(x_{i k}, 2\right)\right\rangle, i \in$ $Q$; this gives $3 v$ triples.
(ii) $\left\langle(i, 1),\left(x_{i k}, 2\right),\left(y_{i k}^{*}, 3\right)\right\rangle, i \in Q$; this gives $v$ triples.
(iii) Same to A(2) (ii); this gives $3 v(v-1)$ triples.
(3) Let $\left(\{\infty\} \cup Q, q_{k}^{\prime}\right) ; 1 \leq k \leq D(v+1)$ be any collection of $D(v+1)$ pairwise disjoint $M T S(v+1)$. Define a collection $d^{\prime}{ }_{k}$ of cyclic triples by
(i) $\langle(x, i),(y, i),(z, i)\rangle$ with $\langle x, y, z\rangle \in q^{\prime}{ }_{k}, i=1,2,3$ (whenever $\infty$ appears for $x, y, z$, omit the second coordinate $i$ ); this gives $v(v+1)$ triples.
(ii) $\left\langle(i, 1),(j, 2),\left((i \circ j) \alpha^{k+1}, 3\right)\right\rangle,\left((j, 2),(i, 1),\left((i \circ j) \alpha^{k}, 3\right)\right\rangle, i, j \in Q$; this gives $2 v^{2}$ triples. [Note: the two exponents of $\alpha$ are different.]

## Proof.

$1^{\circ}$ Each $t^{\prime}{ }_{k}$ is a $M T S(3 v+1)$ (Similarly for $t_{k}^{\prime *}$ ).
The total number of triples is $3 v+v+3 v(v-1)=\frac{3 v(3 v+1)}{3}$, as required. For any ordered pair $P$ of distinct elements of the set $\{\infty\} \cup(Q \times\{1,2,3\})$, we have the following cases:
$P=(\infty,(x, i))$ and $((x, i), \infty)$ with $x \in Q, i=1,2,3$ is contained in part (i).

For other $P$ the argument is similar to $\mathrm{A} 1^{\circ}$.
$2^{\circ}$ Each $d^{\prime}{ }_{k}$ is a $M T S(3 v+1)$.
The total number of triples is $v(v+1)+2 v^{2}=\frac{3 v(3 v+1)}{3}$, as required. For any ordered pair $P$ of distinct elements of the set $\{\infty\} \cup(Q \times\{1,2,3\})$, we have the following cases:
$P=(\infty,(x, i))$ and $((x, i), \infty)$ with $x \in Q, i=1,2,3$ are contained in part (i).
$P=((x, i),(y, i))$ with $x \neq y \in Q$ is contained in part (i).
$P=((i, 1),(j, 2))$ and ((i,2),(j,1)) are contained in part (ii).
$P=((i, 1),(j, 3))$ is contained in part (ii) (there exists $s$ such that $(i \circ s) \alpha^{k}=j$ ).
$P=((i, 3),(j, 1))$ is contained in part (ii) (there exists $s$ such that $\left.(j \circ s) \alpha^{k+1}=i\right)$.
$P=((i, 2),(j, 3))$ is contained in part (ii) (there exists $s$ such that $\left.(s \circ i) \alpha^{k+1}=j\right)$.
$\boldsymbol{P}=((i, 3),(j, 2))$ is contained in part (ii) (there exists $s$ such that $\left.(s \circ j) \alpha^{k}=i\right)$.
$3^{\circ}$ All cyclic triples in all $t^{\prime}{ }_{k}, t_{k}^{* *}$ and $d^{\prime}{ }_{k}$ are pairwise different. Instead of this let us prove $\left\{t^{\prime}{ }_{k}\right\} \cup\left\{t^{\prime *}\right\} \cup\left\{d^{\prime}{ }_{k}\right\}$ is a $L M T S(3 v+1)$ if $D(v+1)=$ $v-1$. For any cyclic triple $T$ from $\{\infty\} \cup(Q \times\{1,2,3\})$ we have the following cases:

$$
T=\langle\infty,(s, i),(t, j)\rangle \text { with }(s, i) \neq(t, j)
$$

If $i=j$ then $s \neq t \in Q$ and there exists $k(1 \leq k \leq v-1)$ such that $\langle\infty, s, t\rangle \in q^{\prime}{ }_{k}$, so $T \in$ part (i) of $d^{\prime}{ }_{k}$;

If $(i, j)=(1,2),(2,3)$ or (3,1) then $T \in \operatorname{part}(\mathrm{i})$ of $t^{\prime}{ }_{k}$, where $k$ satisfies: $t=x_{a k}$ (if $i=1$ ), $s=y_{t k}$ (if $i=3$ ) or $(s, t)=\left(x_{i k}, y_{i k}\right)$ (if $i=2$ );

If $(i, j)=(1,3),(2,1)$ or $(3,2)$ then $T \in \operatorname{part}(\mathrm{i})$ of $t^{\prime *}$, where $k$ satisfies: $t=y_{s k}^{*}$ (if $i=1$ ), $s=x_{t k}$ (if $i=2$ ) or ( $\left.s, t\right)=\left(y_{i k}^{*}, x_{i k}\right.$ ) (if $i=3$ );
[Remark: Since, for $1 \leq k \leq v$,

$$
T_{k}=\left(\begin{array}{cccc}
1 & 2 & \ldots & v \\
x_{1 k} & x_{2 k} & \ldots & x_{v k} \\
y_{1 k} & y_{2 k} & \ldots & y_{v k}
\end{array}\right)
$$

are $v$ disjoint transversals of $Q$ and $\alpha=(1,2, \ldots, v)$ is a transformation of $Q$, it follows that $\left\{\left(x_{i k}, y_{i k}\right) ; 1 \leq i, k \leq v\right\}=Q \times Q$ and $\left\{\left(x_{i k}, y_{i k}^{*}\right)\right.$; $1 \leq i, k \leq v\}=Q \times Q$, where $\left.y_{i k}^{*}=y_{i k} \alpha\right]$
$T=\langle(x, i),(y, i),(z, i)\rangle$ with $x \neq y \neq z \neq x \in Q$, and $\langle(x, i),(y, i)$, $(z, j)\rangle$ with $x \neq y \in Q, i \neq j, z \in Q$. Similar to $A 3^{\circ}$.
$T=\langle(i, 1),(j, 2),(s, 3)\rangle$ with $i, j, s \in Q$. There exists $m(1 \leq m \leq v)$ such that $(i \circ j) \alpha^{m}=s$
if $m=1$ let $j=x_{i k}$ then $s=(i \circ j) \alpha=y_{i k} \alpha=y_{i k}^{*}$, so $T \in \operatorname{part}($ ii $)$ of $t^{\prime *}$;
else $2 \leq m \leq v$ then $T \in \operatorname{part}$ (ii) of $d^{\prime}{ }_{m-1}$.
$T=\langle(i, 2),(j, 1),(s, 3)\rangle$ with $i, j, s \in Q$. There exists $m(0 \leq m \leq$ $v-1)$ such that $(j \circ i) \alpha^{m}=s$
if $m=0$ let $i=x_{j k}$ then $s=(j \circ i) \alpha=y_{j k} \alpha=y_{j k}^{*}$, so $T \in$ part(ii) of $t^{\prime}{ }_{k}$;
else $1 \leq m \leq v-1$ then $T \in \operatorname{part}$ (ii) of $d^{\prime}{ }_{m-1}$.
This completes the proof.

### 2.6 Nonisomorphic large sets.

Our construction of $\operatorname{LMTS}\left(2^{n}+2\right)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F, \mathcal{B}_{x} ; x \in F\right\}\right.$ in $\S 2.4$ is of such a character that the systems $\mathcal{B}_{x}$ and $\mathcal{B}_{1}$ are isomorphic for any $x \in F^{*}$. In fact, let a bijection $f_{x}$ from the set $S=\left\{\infty_{1}, \infty_{2}\right\} \cup F$ onto $S$ be defined by $f_{x}\left(\infty_{1}\right)=\infty_{1}, f_{x}\left(\infty_{2}\right)=\infty_{2}$, $f_{x}(0)=0$ and $f_{x}(y)=x y$ where $y \in F^{*}$. Then the mapping $f_{x}$ induces a mapping $f_{x}^{*}$ from the cyclic triple system $\mathcal{B}_{1}$ into $\mathcal{B}_{x}: f_{x}^{*}(\langle u, v, w\rangle)=$ $\left\langle f_{x}(u), f_{x}(v), f_{x}(w)\right\rangle$. By the construction in $\S 2.4 .3$, all cases are as follows (for brevity, the power index of $g$ is written $p, q$ or $s, t$ ):
part (1)

$$
f_{x}^{*}\left(\left(\infty_{j}, \infty_{3-j}, 1\right\rangle\right)=\left\langle\infty_{j}, \infty_{3-j}, x\right\rangle(j=1,2)
$$

part (2)
$f_{x}^{*}\left(\left\langle\infty_{j}, y, g^{p} \cdot 1+g^{q} y\right\rangle\right)=\left\langle\infty_{j}, x y, x\left(g^{p} \cdot 1+g^{q} y\right)\right\rangle=\left\langle\infty_{j}, x y, g^{p} x+g^{q}(x y)\right\rangle$ ( $j=1,2, y \in F^{*} \backslash\{1\}$, so $x y \in F^{*} \backslash\{x\}$ );
$f_{x}^{*}\left(\left(\infty_{j}, 0, g^{p} \cdot 1+g^{q} \cdot 0\right\rangle=\left\langle\infty_{j}, 0, x\left(g^{p} \cdot 1+g^{q} \cdot 0\right)\right\rangle=\left\langle\infty_{j}, 0, g^{p} x+g^{q} \cdot 0\right\rangle\right.$ ( $j=1,2$ ).
part (3)
$f_{x}^{*}\left(\left(1, y, g^{p} \cdot 1+g^{q} y\right\rangle\right)=\left\langle x, x y, x\left(g^{p} \cdot 1+g^{q} y\right)\right\rangle=\left\langle x, x y, g^{p} x+g^{q}(x y)\right\rangle$ ( $y \in F^{*} \backslash\{1\}$ );
$f_{x}^{*}\left(\left(1,0, g^{\mathbf{p}} \cdot 1+g^{\boldsymbol{q}} \cdot 0\right\rangle\right)=\left\langle x, 0, x\left(g^{\mathbf{p}} \cdot 1+g^{q} \cdot 0\right)\right\rangle=\left\langle x, 0, g^{\mathbf{p}} x+g^{q} \cdot 0\right\rangle$.
part (4)-(6)
$f_{x}^{*}\left(\left(g^{t} \cdot 1+g^{\boldsymbol{s}} y, y, g^{p} \cdot 1+g^{q} y\right\rangle\right)=\left\langle g^{t} x+g^{g}(x y), x y, g^{p} x+g^{q}(x y)\right\rangle(y \in$ $\left.F^{*} \backslash\{1\}\right) ;$

$$
f_{x}^{*}\left(\left(g^{t} \cdot 1+g^{s} \cdot 0,0, g^{p} \cdot 1+g^{q} \cdot 0\right\rangle\right)=\left(g^{t} x+g^{s} \cdot 0,0, g^{p} x+g^{q} \cdot 0\right\rangle .
$$

Clearly, the induced mapping $f_{x}^{*}$ is a bijection from $\mathcal{B}_{1}$ onto $\mathcal{B}_{x}$. So we can assert that, maybe except for one system $\mathcal{B}_{0}$, all $\mathcal{B}_{x}$ in our construction $\operatorname{LMTS}\left(2^{n}+2\right)=\left\{\left(S, \mathcal{B}_{x}\right) ; x \in F\right\}$ are pairwise isomorphic.

But, the constructions $L M T S(v) \longrightarrow L M T S(3 v)$ and $L M T S(v+$ 1) $\longrightarrow \operatorname{LMTS}(3 v+1)$ in $\S 2.5$ do not have the above-mentioned character. The large set $L M T S(3 v)$ (or $L M T S(3 v+1)$ ) consists of three parts $t_{k}, t_{k}^{*}$ and $d_{k}$ (or $t^{\prime}{ }_{k}, t_{k}^{*}$ and $d^{\prime}{ }_{k}$ ), which are constructed by different methods. And each $d_{k}$ (od $d_{k}^{d}$ ) contains three subsystems LMTS $(v)$ (or LMTS $\left(v+1\right.$ ), but none of the $t_{k}$ and $t_{k}^{*}$ (or $t^{\prime}{ }_{k}$ and $t_{k}^{*}$ ) does contain such subsystems when $v>3$ (when $v=3$, they do contain such ones, since each $t^{\prime}{ }_{k}$ and $t^{\prime *}$ contains $v$ sub-LMTS(4) and each $t_{k}$ and $t_{k}^{*}$ contains $v$ sub-LMTS(3)). So we can assert that, for $v>3$, both the constructions $\operatorname{LMTS}(3 v)$ and $L M T S(3 v+1)$ in $\S 2.5$ have not the character having by our construction $\operatorname{LMTS}\left(2^{n}+2\right)$. Therefore, if we can give the construction of some $\operatorname{LMTS}\left(2^{n}+2\right)$ using recursive methods $v \longrightarrow 3 v$ or $v+1 \longrightarrow 3 v+1$ then we will get nonisomorphic large sets for these orders $2^{n}+2$. This is possible.

Lemma 2.6.1. For $n \equiv 3$ or $5(\bmod 6)$, a large set LMTS $\left(2^{n}+2\right)$ can
be constructed by the recursive methods of Lemma 2.9.2 and (2.5.2).
Proof. Firstly, obviously, we have $2^{6 k}-1 \equiv 0(\bmod 9)$ for any nonnegative integer $k$. So,

$$
\left\{\begin{array}{l}
\frac{2^{6 k+2}-1}{3}=\frac{4\left(2^{6 k}-1\right)}{3}+1 \equiv 1(\bmod 6) \\
\frac{2^{6 k+4}-1}{3}=\frac{16\left(2^{6 k}-1\right)}{3}+5 \equiv 5(\bmod 6)
\end{array}\right.
$$

Thus, by Lemma 2.3.2, there exist $L M T S(v)$ for

$$
\left\{\begin{array}{l}
v=2 \cdot \frac{2^{6 k+2}-1}{3}+2=\frac{2^{6 k+3}+1}{3}+1 \\
v=2 \cdot \frac{2^{6 k+4}-1}{3}+2=\frac{2^{6 k+5}+1}{3}+1
\end{array}\right.
$$

Futhermore, by (2.5.2), we can construct $L M T S\left(2^{6 k+3}+2\right)$ and $L M T S$ $\left(2^{6 k+5}+2\right) . \square$
Lemma 2.6.2. For $n \equiv 10$ or $16(\bmod 18)$, a large set $L M T S\left(2^{n}+2\right)$ can be constructed by the recursive methods of Lemma 2.9.1 and (2.5.1).
Proof. Firstly, since $a^{9}-1=(a-1)\left(a^{2}+a+1\right)\left(a^{6}+a^{3}+1\right)$, if $a \equiv 1$ $(\bmod 3)$ and $a>1$ then each of the factors in the right-hand of the equation contains a factor 3 , so $27 \mid a^{9}-1$. Thus, we have

$$
\left\{\begin{array}{l}
4^{9 k+3}-10=4^{3}\left(4^{9 k}-1\right)+54 \equiv 0(\bmod 54) \\
4^{9 k+6}-46=4^{6}\left(4^{9 k}-1\right)+4050 \equiv 0(\bmod 54)
\end{array}\right.
$$

Hence,

$$
\left\{\begin{array}{l}
\frac{4^{9 k+3}-1}{9}=\frac{4^{9 k+3}-10}{9}+1 \equiv 1(\bmod 6) \\
\frac{4^{9 k+6}-1}{9}=\frac{4^{9 k+6}-46}{9}+5 \equiv 5(\bmod 6)
\end{array}\right.
$$

By Lemma 2.3.1 and Theorem 2.4.6, there exist $L M T S(v)$ for

$$
\left\{\begin{array}{l}
v=2^{4} \cdot \frac{4^{9 k+3}-1}{9}+2=\frac{2^{18 k+10}+2}{9} \\
v=2^{4} \cdot \frac{4^{9 k+6}-1}{9}+2=\frac{2^{18 k+16}+2}{9}
\end{array}\right.
$$

Futhermore, using (2.5.1) twice, we can construct $L M T S\left(2^{18 k+10}+2\right)$ and $\operatorname{LMTS}\left(2^{18 k+16}+2\right)$.

Lemma 2.6.3. For $n \equiv 0$ or $12(\bmod 18)$, a large set $L M T S\left(2^{n}+2\right)$ can be constructed by the recursive methods of Lemma 2.9.2 and (2.5.1), (2.5.2).

Proof. Since $27 \mid a^{9}-1$ when $a \equiv 1(\bmod 3)$ and $a>1$, we have

$$
\left\{\begin{aligned}
4^{9 k}-28 & =4^{9}\left(4^{9(k-1)}-1\right)+262116 \equiv 0(\bmod 108) \\
4^{9 k+6}-100 & =4^{6}\left(4^{9 k}-1\right)+3996 \equiv 0(\bmod 108)
\end{aligned}\right.
$$

Consequently,

$$
\left\{\begin{array}{c}
\frac{4^{9 k}-10}{18}=\frac{4^{9 k}-28}{18}+1 \equiv 1(\bmod 6) \\
\frac{4^{9 k+6}-10}{18}=\frac{4^{9 k+6}-100}{18}+5 \equiv 5(\bmod 6)
\end{array}\right.
$$

By Lemma 2.3.2, there exist $L M T S(u)$ for

$$
\left\{\begin{array}{l}
u=2 \cdot \frac{4^{9 k}-10}{18}+2=\frac{4^{9 k}+8}{9} \\
u=2 \cdot \frac{4^{9 k+6}-10}{18}+2=\frac{4^{9 k+6}+8}{9}
\end{array}\right.
$$

Furthermore, by (2.5.2), there exist $L M T S(v)$ for

$$
\left\{\begin{array}{l}
v=3\left(\frac{4^{9 k}+8}{9}-1\right)+1=\frac{4^{9 k}+2}{3} \\
v=3\left(\frac{4^{9 k+6}+8}{9}-1\right)+1=\frac{4^{9 k+6}+2}{3}
\end{array}\right.
$$

Finally, we can construct $\operatorname{LMTS}\left(2^{18 k}+2\right)$ and $\operatorname{LMTS}\left(2^{18 k+12}+2\right)$, using (2.5.1).

Theorem 2.6.4. For $n \equiv 3,5(\bmod 6)$ and $n \equiv 0,10,12,16(\bmod 18)$ there exist nonisomorphic large sets LMTS $\left(2^{n}+2\right)$ through direct and recursive construction methods.

Proof. By Lemmas 2.6.1, 2.6.2, 2.6.3 and the beginning statements (which exclude the case $v=3$ ), we only need to show that for $L M T S\left(2^{3}\right.$ $+2)$ the direct and recursive construction results are nonisomorphic. In fact, in the recursive construction $L M T S(3+1) \rightarrow L M T S(9+1)$, each of the cyclic triple systems $M T S(10)$ contains three sub-MTS (4), but one may check that no $M T S(10)$ in the direct construction $L M T S(10)$ in $\S 2.4$ has a sub-MTS(4).

Examples. The recursive way for $L M T S\left(2^{n}+2\right)$ :
Lemma 2.6.1

$$
\begin{aligned}
2^{3}+2=10=9+1 \Longleftarrow 3+1=2 \cdot 1+2, & 1 \equiv 1(\bmod 6) \\
2^{5}+2=34=33+1 \Longleftarrow 11+1=2 \cdot 5+2, & 5 \equiv 5(\bmod 6)
\end{aligned}
$$

Lemma 2.6.2

$$
\begin{array}{r}
2^{10}+2=1026 \longleftarrow 342 \longleftarrow 114=2^{4} \cdot 7+2, \quad 7 \equiv 1(\bmod 6) \\
2^{16}+2=65538 \longleftarrow 21846 \longleftarrow 7282=2^{4} \cdot 455+2, \quad 455 \equiv 5(\bmod 6)
\end{array}
$$

Lemma 2.6.3

$$
\begin{array}{r}
2^{12}+2=4098 \longleftarrow 1366=1365+1 \Longleftarrow 455+1=2 \cdot 227+2 \\
227 \equiv 5(\bmod 6) \\
2^{18}+2=262146 \longleftarrow 87382=87381+1 \Longleftarrow 29127+1=2 \cdot 14563+2 \\
14563 \equiv 1(\bmod 6)
\end{array}
$$

where the symbols $\longleftarrow$ and $\Longleftarrow$ denote $v \rightarrow 3 v$ and $v+1 \Rightarrow 3 v+1$.
By the way, for $L M T S\left(2^{n}+2\right), n \equiv 1,2(\bmod 6)$ or $n \equiv 4,6(\bmod 18)$ the above-mentioned recursive way cannot be used, since
(1) $\frac{\left(2^{6 k+1}+2\right)-1}{3}+1=\frac{2\left(2^{6 k}-1\right)}{3}+2 \equiv 2$ and $\frac{2^{8 k+2}+2}{3}=\frac{2^{2}\left(2^{6 k}-1\right)}{3}+2 \equiv 2$ (mod 3), but there do not exist MTS's for such orders.
(2) $v=\frac{2^{18 k+4}+2}{3}=\frac{2\left(8^{6 k}+1\right)}{3} \equiv 0(\bmod 6)$ and for affirming the existence of LMTS $(v)$ there are only two possibilities:
(using (2.5.1)) $\frac{v}{3}=\frac{4^{2}\left(4^{9 k}-1\right)}{9}+2 \equiv 2(\bmod 3)$, this is impossible;
(using Theorem 2.4.6) $v=2^{2}\left(\frac{4^{9 k+1}-1}{3}\right)+2$, this is impossible also.
(3) $v=\frac{2^{18 k+6}+2}{3}=\frac{2\left[2^{2}\left(4^{9 k}-1\right)+3^{3}\right]}{3}+4 \equiv 4(\bmod 18)$ and for affirming the existence of $L M T S(v)$ there are only two posibilities:
(using (2.5.2)) $\frac{y-1}{3}+1=\frac{64\left(4^{2 k}-1\right)+54}{9}+2 \equiv 2(\bmod 3)$ this is impossible.
(using Theorem 2.4.6) $v=2^{2}\left(\frac{4^{9 n+2}-1}{3}\right)+2$, this is impossible too.
Finally, we point out that there is a lot of freedom in our direct construction method for $\operatorname{LMTS}\left(2^{n}+2\right)$. For example, the self-dual circuit maybe not only one, can select any vertex from the self-dual circuit as $\alpha$ (see Lemma 2.4.5), all vertices of every circuit (except the selected selfdual circuit) can take the transformation (1) or (2) (see Lemma 2.4.3), and so on. These different choices will give some different constructions for same $L M T S\left(2^{n}+2\right)$, which may supply more nonisomorphic large sets.

## III Mendelsohn systems

### 3.1 A generalization of MTS's.

Let $X$ be a set of $v$ elements, and $x_{1}, x_{2}, \ldots, x_{k}$ distinct elements of $X$, where $k$ is a positive integer and $v \geq k \geq 3$. A directed $k$-cycle is a collection of $k$ ordered pairs $\left(x_{1}, x_{2}\right),\left(x_{2}, x_{3}\right), \ldots,\left(x_{k-1}, x_{k}\right)$ and ( $x_{k}, x_{1}$ ), which is denoted as $\left\langle x_{1}, x_{2}, \ldots, x_{k}\right\rangle$ or $\left\langle x_{2}, x_{3}, \ldots, x_{k}, x_{1}\right\rangle \ldots$ or ( $x_{k}, x_{1}, \ldots, x_{k-1}$ ). A Mendelsohn system $M(2, k, v)$ on $X$ is a pair $(X, \mathcal{B})$, where $\mathcal{B}$ is a collection of directed $k$-cycles of $X$ such that each ordered pair of distinct elements of $X$ is covered by a unique directed $k$-cycle of $\mathcal{B}$. The numbers $|X|=v$ and $k$ are called the order and the circuit size of the Mendelsohn system $M(2, k, v)$, respectively. The symbol $M(2, k, v)$ and the name Mendelsohn system were chosen by analogy with the Steiner system $S(2, k, v)$. By definition, a Mendelsohn triple system of order $v, M T S(v)$, is just a $M(2,3, v)$. In this sense, the Mendelsohn system $M(2, k, v)$ is a generalization of the Mendelsohn triple system $M T S(v)$.

It is a trivial exercise to see that if $(X, \mathcal{B})$ is a $M(2, k, v)$, then $|\mathcal{B}|=$ $\frac{v(v-1)}{k}$. Thus, a necessary condition for the existence of a $M(2, k, v)$ is

$$
\begin{equation*}
v \geq k \geq 3 \quad \text { and } \quad v(v-1) \equiv 0 \quad(\bmod k) . \tag{*}
\end{equation*}
$$

It is well known that the spectrum for $M(2,3, v)$ is the set of all $v \equiv 0$ or $1(\bmod 3)$, except $v=6[\mathrm{Men}]$. Concerming the existence of $M(2, k, v)$ with circuit size $k>3$, partial results are known. We first discuss the case $k=v$, and then the general case.
(1) Tuscan square.

An Italian square is an $n \times n$ array in which each of the symbols $1,2, \ldots, n$ appears exactly once in each row. A Latin square is an Italian square in which each of the symbols also appears exactly once in each column. A Tuscan square, besides being Italian, has the property:
For any two symbols $a, b$, there is at most one row in which $b$ is the symbol immediately to the right of $a$. It is easy to see that the words "at most" can be replaced by "at least" or "exactly". Sometimes a Tuscan square is also called row complete. By the way, a square is Roman if it is both Tuscan and Latin. The relations between these squares are shown in the figure.


It is well known that the existence of a Tuscan square with size $v \times v$ is equivalent to the existence of a $M(2, v+1, v+1)$. In fact, firstly, it is not difficult to see that the first column and the last column of a Tuscan square consist of pairwise distinct numbers. Suppose $A$ is a $v \times v$ Tuscan square on the set $X=\{1,2, \ldots, v\}$. Then all rows of the extended array ( $0, A$ ) just consist of all directed $(v+1)$-cycles of a $M(2, v+1, v+1)$ on the set $X \cup\{0\}$, where 0 is a column vector (consisting of $v$ numbers 0 ). Conversely, if there exists a $M(2, v+1, v+1)$ on the set $X \cup\{0\}$, then there are $v$ directed $(v+1)$-cycles in the system and each block contains all of the numbers of $X \cup\{0\}$. Denote these blocks $\left(0, a_{i 1}, a_{i 2}, \ldots, a_{i v}\right)$, $1 \leq i \leq v$. Then the array $A=\left(a_{i j}\right)_{1}^{v}$ is just a Tuscan square on the set X.
(2) Decomposition of $K_{v}^{*}$ into circuits.

A complete symmetric directed graph $K_{v}^{*}$ is a simple directed graph with $v$ vertices in which for any two distinct vertices $x, y$ there are arcs $x \rightarrow y$ and $y \rightarrow x$. In Graph Theory, what is called the problem of the decomposition of $K_{v}^{*}$ into circuits is: for what values of $v$ is it possible to partition the arcs of $K_{v}^{*}$ into $k$-circuits (i.e. directed circuits with length $k$ ). Obviously, the existence of the decomposition is equivalent to the existence of a $M(2, k, v)$. In particular, the existence of a Tuscan square with size $v \times v$ is equivalent to the existence of a Hamilton decomposition of $K_{v+1}^{*}$.

It is well known that there exists a Tuscan square of order $v$ if and only if $v \neq 1,3,5$ [Til,GoTa]. So we can say that there exists a $M(2, v, v)$ if and only if $v \geq 3$ and $v \neq 4,6$. For the decomposition of $K_{v}^{*}$ into $k$ circuits, our knowledge is less complete. So far, about the non-existence of the $M(2, k, v)$, we have seen that there is no $M(2,4,4), M(2,6,6)$ or $M(2,3,6)$. J.C. Bermond conjectured that (in our terminology): for the existence of $M(2, k, v)$, the necessary condition (*) is also sufficient except in the cases $v=k=4, v=k=6$ and $v=6, k=3$. Now, it is has been proved that this conjecture is true for:
(i) $v \equiv 0$ or $1(\bmod k)(J . C$. Bermond and V. Faber [BerFa] for $k$ even, D. Sotteau [So] for $k$ odd);
(ii) $4 \leq k \leq 16$ and $k$ even (J.C. Bermond [Ber2] for $k=10,12,14$, J.C. Bermond \& V. Faber [BerFa] for $k=4,6,8,16$ );
(iii) $v$ large enough (for a given $k$ ) (R.M. Wilson [Wi2]).

By the condition (i), obviously, if $k$ is a prime power then the conjecture is also true, for example $3 \leq k \leq 13$ and $k$ odd. All that remains for a complete solution of the conjecture is the case $k \geq 15$, where $k$ has at least two distinct prime factors.

Let $C(X)$ be the set of all directed $k$-cycles of a set $X$ containing $v$
elements, then $|C(X)|=\frac{1}{k} v(v-1) \ldots(v-k+1)$. The following problem arises quite naturally: Given a set $X$ of size $v$, for which there exists a $M(2, k, v)$, is it always possible to partition $C(X)$ into $s=(v-2)(v-$ 3) $\ldots(v-k+1)$ subsets $\mathcal{B}_{1}, \mathcal{B}_{2}, \ldots, \mathcal{B}_{s}$ so that each of $\left(X, \mathcal{B}_{1}\right),\left(X, \mathcal{B}_{2}\right)$, $\ldots,\left(X, \mathcal{B}_{s}\right)$ is a $M(2, k, v)$ ? Such a collection of $M(2, k, v)$ is called a large set of pairwise disjoint $M(2, k, v)$; we denote it $L M(2, k, v)$. For $L M(2,3, v)$, i.e., $L M T S(v)$, many results are known (see Chapter II). However, for the existence of $L M(2, k, v)$ with circuit size $k>3$ nothing seems to be known, even though much is known for the $M(2, k, v)$. In this chapter we will start to do this work. In $\S 3.2$ we give construction of $L M(2,2 t+1,2 t+1), L M(2,2 t, 2 t+1)$ and $L M(2,2 t+1,2 t+2)$. For $p$ prime, we give another construction for $L M(2, p, p), L M(2, p-1, p)$ and $L M(2, p, p+1)$ in $\S 3.3$.
3.2 The construction of some $L M(2, k, v)$ 's.

Let $X$ be a set and $\operatorname{Sym}(X)$ the symmetric group on $X$. For a permutation $\xi \in \operatorname{Sym}(X)$ and a directed $k$-cycle $B=\left\langle b_{1}, b_{2}, \ldots, b_{k}\right\rangle$, we denote $B \xi=\left\langle b_{1} \xi, b_{2} \xi, \ldots, b_{k} \xi\right\rangle$ where $b_{i} \xi$ represents the image of the element $b_{i}$ under the permutation $\xi$.

Let $\mathcal{B}$ be a set of directed $k$-cycles on a set $X$, and let $X^{\prime} \subseteq X$. A subgroup $G \leq \operatorname{Sym}(X)$ fixing $X \backslash X^{\prime}$ pointwise is called a complete automorphism group over $X^{\prime}$ of $\mathcal{B}$ if
$1^{\circ}$ for any $\xi \in G$ and any $B \in \mathcal{B}, B \xi \in \mathcal{B} ;$
and
$2^{\circ}$ for any $B$ and $B^{\prime} \in \mathcal{B}$, if there exists $\xi \in \operatorname{Sym}(X)$ fixing $X \backslash X^{\prime}$ pointwise such that $B \xi=B^{\prime}$, then $\xi \in G$. [Of course, this is only possible for $\{B\} \backslash X^{\prime}=\left\{B^{\prime}\right\} \backslash X^{\prime}$, where $\{B\}$ represents the set of the elements in the block $B$.]

In this and the next section, $\mathcal{B}$ will be the set of all directed $k$-cycles of some $M(2, k,|X|)$. We shall identify the subgroup of $\operatorname{Sym}(X)$ fixing $X \backslash X^{\prime}$ pointwise with $\operatorname{Sym}\left(X^{\prime}\right)$.

Lemma 3.2.1.
(1) If $(X, \mathcal{B})$ is a $M(2, k, v)$, then $(X, \mathcal{B} \xi)$ too, where $\xi \in \operatorname{Sym}(X)$ and $\mathcal{B} \xi=\{B \xi \mid B \in \mathcal{B}\}$.
(2) If a set $\mathcal{B}$ has a complete automorphism group $G$ over $X^{\prime} \subseteq X$, then $\left\{\{B \xi\} \mid \xi \in \operatorname{Sym}_{G}\left(X^{\prime}\right)\right\}$ is a collection of pairwise disjoint $\mathcal{B} \xi$, where $\operatorname{Sym}_{G}\left(X^{\prime}\right)$ is a set of right coset representatives for $G$ in $\operatorname{Sym}\left(X^{\prime}\right)$.
(3) If $G=\langle\sigma\rangle$ is the subgroup generated by $\sigma$, av-cyclic permutation on a set $X$ with $v$ elements, then $\operatorname{Sym}(X \backslash\{x\})$ is a set of right coset representatives for $G$ in $\operatorname{Sym}(X)$, for any $x \in X$.

Proof.
(1) The permutation $\xi$ on $X$ induces a permutation on $(X \times X) \backslash \triangle_{x}$, where $\triangle_{x}=\{(x, x) \mid x \in X\}$, so, by the definition of the $M(2, k, v)$, the $\operatorname{system}(X, \mathcal{B} \xi)$ is also a $M(2, k, v)$.
(2) Suppose there exist $B, B^{\prime} \in \mathcal{B}$ and $\xi \neq \eta \in \operatorname{Sym}_{G}\left(X^{\prime}\right)$ such that $B \xi=B^{\prime} \eta$, then $B\left(\xi \eta^{-1}\right)=B^{\prime}$ and $\xi \eta^{-1} \in G$ by the definition of complete automorphism group $G$ over $X^{\prime}$. This implies $G \xi=G \eta$, i.e., $\xi$ and $\eta$ belong to identical right cosets, which is impossible.
(3) For an arbitrary permutation $\zeta \in G(\zeta \neq e, e$ is the unity of $G)$ and any $a \in X, a \zeta \neq a$ is always true, since $\zeta=\sigma^{i}, 1 \leq i \leq v-1$. But for any $\xi \neq \eta \in \operatorname{Sym}_{G}(X \backslash\{x\}), x\left(\xi \eta^{-1}\right)=x$ holds. So $\xi \eta^{-1} \notin G$, i.e., $G \xi \neq G \eta$. $\square$

Below, in this and the next section, we will only use the cases $X=X^{\prime}$ and $X=X^{\prime} \cup\{\infty\}$.

Theorem 3.2.2. There exists an $L M(2,2 t+1,2 t+1)$ for any positive integer $t$.

## Construction.

Let $X=\{0,1,2, \ldots, 2 t-1\}$. Take the directed $(2 t+1)$-cycles

$$
B_{i}=\left\langle\infty, b_{i 0}, b_{i 1}, \ldots, b_{i, 2 t-1}\right\rangle \quad i \in X
$$

where $b_{i, 2 k}=i+k$ and $b_{i, 2 k+1}=i-k-1(\bmod 2 t, 0 \leq k \leq t-1)$. Let $\mathcal{B}_{0}=\left\{B_{0}, B_{1}, \ldots, B_{2 t-1}\right\}$ and $\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}$, where $\xi_{j} \in \operatorname{Sym}(X \backslash\{0\})$. Then $\left\{\left(X \cup\{\infty\}, \mathcal{B}_{j}\right) \mid 0 \leq j \leq(2 t-1)!-1\right\}$ is an $L M(2,2 t+1,2 t+1)$.
Proof. Since $i+k=i-k^{\prime}-1$ implies $k+k^{\prime}+1=0(\bmod 2 t)$, but $1 \leq k+k^{\prime}+1 \leq 2 t-1$, it follows that each $B_{i}$ is indeed a directed ( $2 t+1$ )-cycle.

For $x \in X$, the ordered pair $(\infty, x)$ (or $(x, \infty))$ is covered by the block $B_{x}$ (or $B_{x+t}$ ). For $x \neq y \in X$, the ordered pair $(x, y)$ is covered by the block $B_{x+s}$ (if $y-x=2 s, \bmod 2 t$ ) or $B_{x+s-t}$ (if $y-x=2 s-1$, $\bmod 2 t)$. Thus, $\left(X \cup\{\infty\}, \mathcal{B}_{0}\right)$ is a $M(2,2 t+1,2 t+1)$. And, by Lemma 3.2.1(1), each $\left(X \cup\{\infty\}, \mathcal{B}_{j}\right)$ is also a $M(2,2 t+1,2 t+1)$.

Futhermore, let the $2 t$-cyclic permutation $\sigma=(0,1, \ldots, 2 t-1) \in$ $S y m(X)$. Then the subgroup $G=<\sigma>$ is the complete automorphism group over $X$ of $\left(X \cup\{\infty\}, \mathcal{B}_{0}\right)$. In fact,
$1^{\circ}$ For any $\xi \in G$ (let $\xi=\sigma^{l}, 0 \leq l<2 t$ ) and $B_{i} \in B_{0}$, we have $B_{i} \xi=B_{i} \sigma^{l}=B_{i+l} \in \mathcal{B}_{0}$ (subscripts modulo $2 t$ ).
$2^{\circ}$ For any $B_{i}, B_{j} \in \mathcal{B}_{0}$, if there exists $\xi \in \operatorname{Sym}(X)$ such that $B_{i} \xi=$ $B_{j}$, then it is inevitable that $b_{i l} \xi=b_{j l}(0 \leq l \leq 2 t-1)$, since $\infty \xi=\infty$. So, obviously, $\xi=\sigma^{j-i} \in G$. Thus, by Lemma 3.2.1(3), $\operatorname{Sym}(X \backslash\{0\}) \subseteq$ $S y m_{G}(X)$. But, we have

$$
\left|S y m_{G}(X)\right|=\frac{|\operatorname{Sym}(X)|}{|G|}=\frac{(2 t)!}{2 t}=(2 t-1)!=|\operatorname{Sym}(X \backslash\{0\})|
$$

So, $\operatorname{Sym}(X \backslash\{0\})=\operatorname{Sym}_{G}(X)$. Note that the number $(2 t-1)$ ! is just the desired number of $M(2,2 t+1,2 t+1)$ in an $L M(2,2 t+1,2 t+1)$, therefore, by Lemma 3.2.1(2), our construction is alright.

Theorem 3.2.3. There exists an $L M(2,2 t, 2 t+1)$ for any positive integer $t>1$.

## Construction.

Let $X=\{0,1, \ldots, 2 t-1\}$. Take the directed $2 t$-cycles

$$
\begin{aligned}
B_{i} & =\left\langle\infty, b_{i 0}, b_{i 1}, \ldots, b_{i, 2 t-2}\right\rangle \quad i \in X \\
C & =\langle 0,1, \ldots, 2 t-1\rangle
\end{aligned}
$$

where $b_{i, 2 k}=i+k, 0 \leq k \leq t-1$ and $b_{i, 2 k+1}=i-k-1,0 \leq k \leq$ $t-2(\bmod 2 t)$. Let $\mathcal{B}_{0}=\left\{B_{0}, B_{1}, \ldots, B_{2 t-1}, C\right\}$ and $\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}$, where $\xi_{j} \in \operatorname{Sym}(X \backslash\{0\})$. Then $\left\{\left(X \cup\{\infty\}, \mathcal{B}_{j}\right) \mid 0 \leq j \leq(2 t-1)!-1\right\}$ is an $L M(2,2 t, 2 t+1)$.
Proof. Similar to Theorem 3.2.2, we can see that each $B_{i}$ is indeed a directed $2 t$-cycle. As for the block $C$, it is trivial.

For $x \in X$, the ordered pair $(\infty, x)$ (or $(x, \infty)$ ) appears in the block $B_{x}$ (or $B_{x-t+1}$ ). For $x \neq y \in X$, the ordered pair $(x, y)$ appears in the block $B_{x+s}$ (if $y-x=2 s \bmod 2 t$ ) or $B_{x+s-t}$ (if $y-x=2 s-1 \neq 1$ $\bmod 2 t)$ or $C($ if $y-x=1)$. So, $\left(X \cup\{\infty\}, \mathcal{B}_{0}\right)$ is a $M(2,2 t, 2 t+1)$. And, by Lemma 3.2.1 (1), each $\left(X \cup\{\infty\}, \mathcal{B}_{j}\right)$ is also a $M(2,2 t, 2 t+1)$.

Take the $2 t$-cyclic permutation $\sigma=(0,1, \ldots, 2 t-1) \in \operatorname{Sym}(X)$. Then the subgroup $G=\langle\sigma\rangle$ is a complete automorphism group over $X$ of $\left(X \cup\{\infty\}, \mathcal{B}_{0}\right)$. In fact,
$1^{\circ}$ For any $\xi \in G$ (let $\xi=\sigma^{l}, 0 \leq l<2 t$ ) and $B_{i}$ (or $C$ ) $\in \mathcal{B}_{0}$, we have $B_{i} \xi=B_{i} \sigma^{l}=B_{i+1} \in \mathcal{B}_{0}$ (or $C \sigma=C$ ).
$2^{\circ}$ For any $U, V \in \mathcal{B}_{0}$, if there exists $\xi \in \operatorname{Sym}(X)$ such that $U \xi=V$, then both $U$ and $V$ are $C$ or not, since $\infty \xi=\infty$. If $U=V=C$, let $U$ and $V$ be the $i$-th and the $j$-th shift of $\langle 0,1, \ldots, 2 t-1\rangle$. Then $\xi=\sigma^{j-i} \in G$. If $U=\mathcal{B}_{i}$ and $V=\mathcal{B}_{j}$, just like in the proof of Theorem $3.2 .2,2^{\circ}$, we have also $\xi=\sigma^{j-i} \in G$.

Now continue just as in the proof of Theorem 3.2.2.
Theorem 3.2.4. There exists an $L M(2,2 t+1,2 t+2)$ for any positive integer $t$.

## Construction.

Let $X=\{0,1, \ldots, 2 t\}$. Take the directed $(2 t+1)$-cycles

$$
\begin{aligned}
B_{i} & =\left\langle\infty, b_{i 0}, b_{i 1}, \ldots, b_{i, 2 t-1}\right\rangle \quad i \in X \\
C & =\langle 0, t+1,1, t+2,2, \ldots, 2 t, t\rangle
\end{aligned}
$$

where $b_{i, 2 k}=i+k, 0 \leq k \leq t-1$ and $b_{i, 2 k+1}=i-k-1$ (if $0 \leq$ $\left.k \leq\left[\frac{t}{2}\right]-1\right)$ or $i-k-2\left(\right.$ if $\left.\left[\frac{t}{2}\right] \leq k \leq t-1\right)(\bmod 2 t+1)$. Let $\mathcal{B}_{0}=\left\{B_{0}, B_{1}, \ldots, B_{2 t}, C\right\}$ and $\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}$, where $\xi_{j} \in \operatorname{Sym}(X \backslash\{0\})$. Then $\left\{\left(X \cup\{\infty\}, \mathcal{B}_{j}\right) \mid 0 \leq j \leq(2 t)!-1\right\}$ is an $L M(2,2 t+1,2 t+2)$.

Proof. Firstly, since the following cases are impossible, it follows that each $B_{i}$ is indeed a directed $(2 t+1)$-cycle:
if $i+k=i-k^{\prime}-1$ then $k+k^{\prime}+1 \equiv 0(\bmod 2 t+1)$, but $1 \leq k+k^{\prime}+1 \leq$ $t+\left[\frac{t}{2}\right]-1$;
if $i+k=i-k^{\prime \prime}-2$ then $k+k^{\prime \prime}+2 \equiv 0(\bmod 2 t+1)$, but $\left[\frac{t}{2}\right]+2 \leq$ $k+k^{\prime \prime}+2 \leq 2 t ;$
if $i-k^{\prime}-1=i-k^{\prime \prime}-2$ then $k^{\prime \prime}-k^{\prime} \equiv-1 \equiv 2(\bmod 2 t+1)$, but $1 \leq k^{\prime \prime}-k^{\prime} \leq t-1$.

For $x \in X$, the ordered pair $(\infty, x)$ (or $(x, \infty)$ ) appears in the block $B_{x}$ (or $B_{x+t-1}$ ). For $x \neq y \in X$, the ordered pair $(x, y)$ appears in the block $B_{x+s}$ (if $y-x=2 s-1>t+1$ or $y-x=2 s<t+1, \bmod$ $2 t+1$ ) or $B_{x+s-t}$ (if $y-x=2 s-1<t+1$ or $y-x=2 s>t+1, \bmod$ $2 t+1)$ or $C($ if $y-x=t+1, \bmod 2 t+1)$.

Take the $(2 t+1)$-cyclic permutation $\sigma=(0,1, \ldots, 2 t) \in \operatorname{Sym}(X)$. Then the subgroup $G=\langle\sigma\rangle$ is a complete automorphism group over $X$ of $\left(X \cup\{\infty\}, \mathcal{B}_{0}\right)$. In fact, noting that $C \sigma$ is the 2 nd shift of $C$, it can be obtained similarly to the proof of Theorem 3.2.3. The rest of the proof is also similar.

### 3.3 Another method for the prime case.

In this section we will give another method to construct $L M(2, p, p)$, $L M(2, p-1, p)$ and $L M(2, p, p+1)$ for prime $p$. Their existence has been proved in the last section, but this construction may produce systems that are nonisomorphic to the above ones, since the starting system $\mathcal{B}_{0}$ has a different complete automorphism group.

Below, $F_{p}$ will always be a finite field containing $p$ elements $0,1,2, \ldots$, $p-1$ ( $p$ is an odd prime), and $g$ is a primitive element of $F_{p}^{*}$. Moreover, $\sigma=\left(1, g, g^{2}, \ldots, g^{p-2}\right)$ and $\tau=(0,1,2, \ldots, p-1)$ will represent two fixed permutations in $\operatorname{Sym}\left(F_{p}\right)$.

## Lemma 3.3.1.

(1) The permutations $\sigma$ and $\tau$ generate a subgroup $G=<\sigma, \tau>$ of $\operatorname{Sym}\left(F_{p}\right)$. Its order is $p(p-1)$. Each of its elements can be written in the form $\sigma^{t} \tau^{s}$ or $\tau^{s} \sigma^{t}, 0 \leq t \leq p-2,0 \leq s \leq p-1$. And $\sigma^{t} \tau^{s}=\tau^{s g^{-t}} \sigma^{t}$, $\tau^{s} \sigma^{t}=\sigma^{t} \tau^{s g^{t}}$.
(2) $\operatorname{Sym}\left(F_{p} \backslash\{x, y\}\right)$ is for $x \neq y$ a set of representatives for the right cosets of $G$ in $\operatorname{Sym}\left(F_{p}\right)$.

## Proof.

(1) For an arbitrary element $x$ of $F_{p}$, we have

$$
\begin{aligned}
& \tau \sigma: x \xrightarrow{\tau} x+1 \xrightarrow{\sigma}(x+1) g \\
& \sigma \tau^{g}: x \xrightarrow{\sigma} x g \xrightarrow{\tau^{\theta}} x g+g=(x+1) g,
\end{aligned}
$$

thus $\tau \sigma=\sigma \tau^{g}$. Futhermore, for $0 \leq t \leq p-2$ and $0 \leq s \leq p-1$

$$
\begin{aligned}
& \tau^{s} \sigma=\tau^{s-1}(\tau \sigma)=\tau^{s-1} \sigma \tau^{g}=\tau^{s-2} \sigma \tau^{2 g}=\cdots=\sigma \tau^{s g}, \\
& \tau^{s} \sigma^{t}=\left(\tau^{s} \sigma\right) \sigma^{t-1}=\sigma \tau^{s g} \sigma^{t-1}=\sigma^{2} \tau^{s g^{2}} \sigma^{t-2}=\cdots=\sigma^{t} \tau^{s g^{t}} \\
& \sigma^{t} \tau^{s}=\sigma^{t} \tau^{\left(s g^{-t}\right) g^{t}=\tau^{s g^{-t}} \sigma^{t} .} .
\end{aligned}
$$

Noting that the orders of $\sigma$ and $\tau$ in $S y m\left(F_{p}\right)$ are $p-1$ and $p$ respectively, we can get all conclusions.
(2) Any permutation $\zeta \in G(\zeta \neq e, e$ is unity element of $G)$ fixes one element of $F_{p}$ at most. But for any $\xi \neq \eta \in \operatorname{Sym}\left(F_{p} \backslash\{x, y\}\right)$, the permutation $\xi \eta^{-1} \in \operatorname{Sym}\left(F_{p} \backslash\{x, y\}\right)$ fixes the two elements $x, y$ of $F_{p}$. So $\xi \eta^{-1} \notin G$, i.e., $G \xi \neq G \eta$. But, we have

$$
\left|\operatorname{Sym}\left(F_{p} \backslash\{0,1\}\right)\right|=(p-2)!=\frac{\left|\operatorname{Sym}\left(F_{p}\right)\right|}{|G|},
$$

so we have found representatives for all right cosets of $G . \square$
Below it will be necessary, in some cases, to distinguish the various forms of the same directed cycle. To this end, for a given directed $k$-cycle $B=\left\langle b_{0}, b_{1}, \ldots, b_{k-1}\right\rangle$ we. call the same directed cycle $\left\langle b_{m}, b_{m+1}, \ldots, b_{k-1}, b_{0}, b_{1}, \ldots, b_{m-1}\right\rangle$ the $m$-shift of $B$, and denote it by $B^{(m)}, 0 \leq m \leq k-1$.

The construction of $L M(2, p, p)$.
Take $B_{i}=\left\langle 0, g^{i}, 2 g^{i}, \ldots,(p-1) g^{i}\right\rangle, 0 \leq i \leq p-2$. Let $\mathcal{B}_{0}=$ $\left\{B_{0}, B_{1}, \ldots, B_{p-2}\right\}$ and $\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}$, where $\xi_{j} \in \operatorname{Sym}\left(F_{p} \backslash\{0,1\}\right)$. Then $\left\{\left(F_{p}, \mathcal{B}_{j}\right) \mid 0 \leq j \leq(p-2)!-1\right\}$ is an $L M(2, p, p)$.

Proof. Obviously, each $\mathcal{B}_{i}$ is a directed $p$-cycle. For any $x \neq y \in F_{p}$, let $y-x=g^{i}$ and $x g^{-i}=m$. Then the ordered pair $(x, y)=\left(m g^{i},(m+1) g^{i}\right)$ appears in $B_{i}$ (at the $m$-th position). So, $\left(F_{p}, \mathcal{B}_{0}\right)$ is a $M(2, p, p)$. And, by Lemma 3.2 .1 (1), each ( $F_{p}, \mathcal{B}_{j}$ ) also is.

Furthermore, we point out that the subgroup $G=\langle\sigma, \tau\rangle$ is a complete automorphism group over $F_{p}$ of $\left(F_{p}, \mathcal{B}_{0}\right)$. In fact,
$1^{\circ}$ For any $B_{i}^{(m)} \in \mathcal{B}_{0}$ and $\xi \in G$, we have $B_{i}^{(m)} \xi \in \mathcal{B}_{0}$ since

$$
\begin{aligned}
& B_{0}^{(m)} \tau^{s}=B_{0}^{(m+s)}, B_{0}^{(m)} \sigma^{t}=B_{i}^{(m)} \text { and } \\
& B_{i}^{(m)} \tau^{s}=B_{0}^{(m)} \sigma^{i} \tau^{s}=B_{0}^{(m)} \tau^{s g^{-i}} \sigma^{i}=B_{0}^{\left(m+s g^{-i}\right)} \sigma^{i}=B_{i}^{\left(m+s g^{-i}\right)} \\
& B_{i}^{(m)} \sigma^{t}=B_{0}^{(m)} \sigma^{i+t}=B_{i+t}^{(m)}
\end{aligned}
$$

$2^{\circ}$ For any $B_{i}^{(m)}, B_{j}^{(n)} \in \mathcal{B}_{0}$, if there exists $\xi \in \operatorname{Sym}\left(F_{p}\right)$ such that $B_{i}^{(m)} \xi=B_{j}^{(n)}$, then $\xi=\tau^{(n-m) g^{i}} \sigma^{j-i} \in G\left(\right.$ by $1^{\circ}, B_{i}^{(m)} \tau^{(n-m) g^{i}} \sigma^{j-i}=$ $\left.B_{i}^{\left(m+(n-m) g^{i} g^{-i}\right)} \sigma^{j-i}=B_{i}^{(n)} \sigma^{j-i}=B_{i+(j-i)}^{(n)}=B_{j}^{(n)}\right)$. Thus, by Lemma 3.3.1 (2), $\operatorname{Sym}\left(F_{p} \backslash\{0,1\}\right)$ is a set of representatives for the right cosets of $G$ in $\operatorname{Sym}\left(F_{p}\right)$. Note that the number ( $p-2$ )! is just the desired number of $M(2, p, p)$ 's in an $L M(2, p, p)$, so our construction is alright by Lemma 3.2.1 (2).

The construction of $L M(2, p-1, p)$.
Take $B_{i}=\left\langle 1+i, g+i, g^{2}+i, \ldots, g^{p-2}+i\right\rangle, 0 \leq i \leq p-1$. Let $\mathcal{B}_{0}=\left\{B_{0}, B_{1}, \ldots, B_{p-1}\right\}$ and $\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}$, where $\xi_{j} \in \operatorname{Sym}\left(F_{p} \backslash\{0,1\}\right)$. Then $\left\{\left(F_{p}, \mathcal{B}_{j}\right) ; 0 \leq j \leq(p-2)!-1\right\}$ is an $\operatorname{LM}(2, p-1, p)$.

Proof. For any $x \neq y \in F_{p}$, let $(y-x)(g-1)^{-1}=g^{m}$ and $x-g^{m}=i$. Then the ordered pair $(x, y)=\left(g^{m}+i, g^{m+1}+i\right)$ appears in $B_{i}$ (at the $m$ th position). So, $\left(F_{p}, \mathcal{B}_{0}\right)$ is a $M(2, p-1, p)$. And, by Lemma 3.2.1 (1), each ( $F_{p}, \mathcal{B}_{j}$ ) also is.

For verifying that the subgroup $G=<\sigma, \tau>$ is the complete automorphism group over $F_{p}$ of $\left(F_{p}, \mathcal{B}_{0}\right)$, we have
$1^{\circ}$ For any $B_{i}^{(m)} \in \mathcal{B}_{0}$ and $\xi \in G$, we have $B_{i}^{(m)} \xi \in \mathcal{B}_{0}$ since

$$
\begin{aligned}
& B_{0}^{(m)} \tau^{s}=B_{s}^{(m)}, B_{0}^{(m)} \sigma^{t}=B_{0}^{(m+t)} \text { and } \\
& B_{i}^{(m)} \tau^{s}=B_{0}^{(m)} \tau^{i+s}=B_{i+s}^{(m)} \\
& B_{i}^{(m)} \sigma^{t}=B_{0}^{(m)} \tau^{i} \sigma^{t}=B_{0}^{(m)} \sigma^{t} \tau^{i g^{t}}=B_{0}^{(m+t)} \tau^{i g^{t}}=B_{i g^{t}}^{(m+t)}
\end{aligned}
$$

$2^{\circ}$ For any $B_{i}^{(m)}, B_{j}^{(n)} \in \mathcal{B}_{0}$, if there exists $\xi \in \operatorname{Sym}\left(F_{p}\right)$ such that $B_{i}^{(m)} \xi=B_{j}^{(n)}$, then $\xi=\sigma^{n-m} \tau^{j-i g^{n-m}} \in G\left(\right.$ by $1^{\circ}, B_{i}^{(m)} \sigma^{n-m} \tau^{j-i g^{n-m}}$ $\left.=B_{i g^{n-m}}^{(n)} \tau^{j-i g^{n-m}}=B_{j}^{(n)}\right)$.

Now continue just as in the proof of the above construction.
The construction of $L M(2, p, p+1)$.
Take the directed cycles $B_{i k}=\left\langle 1+i, g+i, \ldots, g^{k}+i, \infty, g^{k+1}+\right.$ $\left.i, \ldots, g^{p-2}+i\right\rangle, 0 \leq i \leq p-1,0 \leq k \leq p-2$, which are obtained from the blocks $B_{i}$ of the above-mentioned $L M(2, p-1, p)$ by inserting a new element $\infty$ between $g^{k}+i$ and $g^{k+1}+i$. Moreover, take $C_{k}=\left\langle 0, g^{k}(g-1), 2 g^{k}(g-1), \ldots,(p-1) g^{k}(g-1)\right\rangle, 0 \leq k \leq p-2$. Let $\mathcal{B}_{0 k}=\left\{B_{o k}, B_{1 k}, \ldots, B_{p-1, k}, C_{k}\right\}$ and $\mathcal{B}_{j k}=\mathcal{B}_{0 k} \xi_{j}$, where $\xi_{j} \in$ $\operatorname{Sym}\left(F_{p} \backslash\{0,1\}\right)$. Then $\left\{\left(F_{p} \cup\{\infty\}, \mathcal{B}_{j k}\right) ; 0 \leq k \leq p-2,0 \leq j \leq\right.$ $(p-2)!-1\}$ is an $L M(2, p, p+1)$.

Proof. Firstly, for a given $k$, we prove that the system $\mathcal{B}_{0 k}$ is a $M(2, p$, $p+1$ ).

For any $x \in F_{p}$, obviously, the ordered pairs ( $x, \infty$ ) and ( $\infty, x$ ) appear in $B_{x-g^{k}, k}$ and $B_{x-g^{k+1}, k}$ respectively. And for any $x \neq y \in F_{p}$, let $(y-x)(g-1)^{-1}=g^{m}$. Then:
if $m \neq k$, let $x-g^{m}=i$, then the ordered pair $(x, y)=\left(g^{m}+\right.$ $\left.i, g^{m+1}+i\right)$ appears in $B_{i k} ;$
if $m=k$, let $x\left(g^{k}(g-1)\right)^{-1}=s$, then the ordered pair $(x, y)=$ $\left(s g^{k}(g-1),(s+1) g^{k}(g-1)\right)$ appears in $C_{k}$.
Furthermore, the number of the blocks in $\mathcal{B}_{0 k}$ is $p+1$, just as desired.
Let us show that the subgroup $G=<\sigma, \tau>$ is the complete automorphism group over $F_{p}$ of the collection $\mathcal{B}=\left\{\mathcal{B}_{0 k} ; 0 \leq k \leq p-2\right\}$.
$1^{\circ}$ For any $U \in \mathcal{B}$,
if $U=C_{k}^{(m)}$, we have $C_{k}^{(m)} \tau^{s}=C_{k}^{\left(m+s\left(g^{k}(g-1)\right)^{-1}\right)}$ and $C_{k}^{(m)} \sigma^{t}$ $=C_{k+t}^{(m)} ;$
if $U=B_{i k}$, we have $B_{i k} \tau^{s}=B_{i+s, k}$ and $B_{i k} \sigma^{t}=B_{g^{t}, k+t}$.
So, $U \xi \in \mathcal{B}$ for any $\xi \in G=\langle\sigma, \tau\rangle$.
$2^{\circ}$ For any $U, V \in \mathcal{B}$, if there exists $\xi \in \operatorname{Sym}\left(F_{p}\right)$ such that $U \xi=V$, then since $\infty \xi=\infty$, there are only two possibilities:

$$
\begin{aligned}
& U=C_{k}^{(m)}, V=C_{l}^{(n)} \text {. Then, by } 1^{\circ}, C_{k}^{(m)} \tau^{(n-m) g^{k}(g-1)} \sigma^{l-k}= \\
& \left.C_{k}^{(n)} \sigma^{l-k}=C_{l}^{(n)}\right) \text {, so } \xi=\tau^{(n-m) g^{k}(g-1)} \sigma^{I-k} ; \\
& \quad U=B_{i k}, V=B_{j j} \text {. Then, by } 1^{\circ}, B_{i k} \sigma^{l-k} \tau^{j-g^{l-k_{i}}}=B_{g^{l-k_{i},} I^{j-g^{l-k}}} \\
& \left.=B_{j l}\right) \text {, so } \xi=\sigma^{l-k} \tau^{j-g^{t-k_{i}}} \text {. } \\
& \text { In both cases } \xi \in G \text {. }
\end{aligned}
$$

Now continue just as in the proof of the first construction (Note: in using Lemma 3.2.1 (2), the collection $\mathcal{B}$ is the union of $p-1 M(2, p, p+$ 1)'s.

### 3.4 Examples.

In this section we give three examples. For comparison, two kinds of construction, by the methods in $\S 3.2$ and $\S 3.3$, are listed simultaneously.

Example 1. $L M(2,7,7)$
(1) (by Theorem 3.2.2) $X=\{0,1,2,3,4,5\}$

$$
\begin{aligned}
\mathcal{B}_{0}: B_{0} & =\langle\infty, 0,5,1,4,2,3\rangle \\
B_{1} & =\langle\infty, 1,0,2,5,3,4\rangle \\
B_{2} & =\langle\infty, 2,1,3,0,4,5\rangle \\
B_{3} & =\langle\infty, 3,2,4,1,5,0\rangle \\
B_{4} & =\langle\infty, 4,3,5,2,0,1\rangle \\
B_{5} & =\langle\infty, 5,4,0,3,1,2\rangle \\
\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}, \xi_{j} \in \operatorname{Sym}(X \backslash\{0\}) & =S_{5} .
\end{aligned}
$$

(2) (by $\S 3.3 L M(2, p, p)$ )
$p=7, g=3, \sigma=(1,3,2,6,4,5), \tau=(0,1,2,3,4,5,6)$.

$$
\begin{aligned}
\mathcal{B}_{0}: B_{0} & =\langle 0,1,2,3,4,5,6\rangle \\
B_{1} & =\langle 0,3,6,2,5,1,4\rangle \\
B_{2} & =\langle 0,2,4,6,1,3,5\rangle \\
B_{3} & =\langle 0,6,5,4,3,2,1\rangle \\
B_{4} & =\langle 0,4,1,5,2,6,3\rangle \\
B_{5} & =\langle 0,5,3,1,6,4,2\rangle
\end{aligned}
$$

$$
\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}, \xi_{j} \in \operatorname{Sym}\left(F_{7} \backslash\{0,1\}\right)=S_{5} .
$$

Example 2. $L M(2,6,7)$
(1) (by Theorem 3.2.3) $X=\{0,1,2,3,4,5\}$

$$
\begin{aligned}
\mathcal{B}_{0}: B_{0} & =\langle\infty, 0,5,1,4,2\rangle \\
B_{1} & =\langle\infty, 1,0,2,5,3\rangle \\
B_{2} & =\langle\infty, 2,1,3,0,4\rangle \\
B_{3} & =\langle\infty, 3,2,4,1,5\rangle \\
B_{4} & =\langle\infty, 4,3,5,2,0\rangle \\
B_{5} & =\langle\infty, 5,4,0,3,1\rangle \\
C & =\langle 0,1,2,3,4,5\rangle
\end{aligned}
$$

$\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}, \xi_{j} \in \operatorname{Sym}(X \backslash\{0\})=S_{5}$.
(2) (by $\S 3.3 L M(2, p-1, p)$ )
$p, g, \sigma, \tau$ are the same as in Example 1 (2).

$$
\begin{aligned}
\mathcal{B}_{0}: B_{0} & =\langle 1,3,2,6,4,5\rangle \\
B_{1} & =\langle 2,4,3,0,5,6\rangle \\
B_{2} & =\langle 3,5,4,1,6,0\rangle \\
B_{3} & =\langle 4,6,5,2,0,1\rangle \\
B_{4} & =\langle 5,0,6,3,1,2\rangle \\
B_{5} & =\langle 6,1,0,4,2,3\rangle \\
B_{6} & =\langle 0,2,1,5,3,4\rangle \\
\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}, \xi_{j} \in \operatorname{Sym}\left(F_{7} \backslash\{0,1\}\right) & =S_{5} .
\end{aligned}
$$

Example 3. $L M(2,5,6)$
(1) (by Theorem 3.2.4) $X=\{0,1,2,3,4\}$

$$
\begin{aligned}
\mathcal{B}_{0}: B_{0} & =\langle\infty, 0,4,1,2\rangle \\
B_{1} & =\langle\infty, 1,0,2,3\rangle \\
B_{2} & =\langle\infty, 2,1,3,4\rangle \\
B_{3} & =\langle\infty, 3,2,4,0\rangle \\
B_{4} & =\langle\infty, 4,3,0,1\rangle \\
C & =\langle 0,3,1,4,2\rangle
\end{aligned}
$$

$\mathcal{B}_{j}=\mathcal{B}_{0} \xi_{j}, \xi_{j} \in \operatorname{Sym}(X \backslash\{0\})=S_{4}$.
(2) (by $\S 3.3 L M(2, p, p+1)$ ) $p=5, g=2, \sigma=(1,2,4,3), \tau=(0,1,2,3,4)$

$$
\begin{aligned}
\mathcal{B}_{00}: B_{00} & =\langle 1, \infty, 2,4,3\rangle & \mathcal{B}_{01}: B_{01} & =\langle 1,2, \infty, 4,3\rangle \\
B_{10} & =\langle 2, \infty, 3,0,4\rangle & B_{11} & =\langle 2,3, \infty, 0,4\rangle \\
B_{20} & =\langle 3, \infty, 4,1,0\rangle & B_{21} & =\langle 3,4, \infty, 1,0\rangle \\
B_{30} & =\langle 4, \infty, 0,2,1\rangle & B_{31} & =\langle 4,0, \infty, 2,1\rangle \\
B_{40} & =\langle 0, \infty, 1,3,2\rangle & B_{41} & =\langle 0,1, \infty, 3,2\rangle \\
C_{0} & =\langle 0,1,2,3,4\rangle & C_{1} & =\langle 0,2,4,1,3\rangle
\end{aligned}
$$

$$
\begin{array}{rlrl}
\mathcal{B}_{02}: B_{02} & =\langle 1,2,4, \infty, 3\rangle & \mathcal{B}_{03}: B_{03} & =\langle 1,2,4,3, \infty\rangle \\
B_{12} & =\langle 2,3,0, \infty, 4\rangle & B_{13} & =\langle 2,3,0,4, \infty\rangle \\
B_{22} & =\langle 3,4,1, \infty, 0\rangle & B_{23} & =\langle 3,4,1,0, \infty\rangle \\
B_{32} & =\langle 4,0,2, \infty, 1\rangle & B_{33}=\langle 4,0,2,1, \infty\rangle \\
B_{42} & =\langle 0,1,3, \infty, 2\rangle & B_{43}=\langle 0,1,3,2, \infty\rangle \\
C_{2} & =\langle 0,4,3,2,1\rangle & C_{3} & =\langle 0,3,1,4,2\rangle
\end{array}
$$

$$
\mathcal{B}_{j k}=\mathcal{B}_{0 k} \xi_{j}, \xi_{j} \in \operatorname{Sym}\left(F_{5} \backslash\{0,1\}\right)=S_{3}
$$

## IV Transitive triple systems

### 4.1 Introduction.

Let $S$ be a set of $v$ elements $(v \geq 3$ ). A transitive triple from $S$ is a collection of three ordered pairs $(x, y),(y, z)$ and $(x, z)$, where $x, y$ and $z$ are distinct elements of $S$. We will denote the transitive triple $\{(x, y),(y, z),(x, z)\}$ by $\langle\langle x, y, z\rangle\rangle$. A transitive triple system on $S$ is a pair $(S, \mathcal{B})$, where $\mathcal{B}$ is a collection of transitive triples from $S$ such that each ordered pair of distinct elements of $S$ belongs to exactly one transitive triple of $\mathcal{B}$. The number $|S|=v$ is called the order of the transitive triple system $(S, B)$, which is denoted by $T T S(v)$. It is a trivial exercise to see that if $(S, \mathcal{B})$ is a $T T S$ of order $v$ then $|\mathcal{B}|=\frac{v(v-1)}{3}$. And it is well known that the spectrum for TTS's is the set of all $v \equiv 0$ or $1(\bmod 3)[\operatorname{LinSt}]$.

Now, let $T(S)$ be the set of all transitive triples of the set $S$ containing $v$ elements, then $|T(S)|=v(v-1)(v-2)$. In view of the fact that a $T T S$ of order $v$ is equipped with $\frac{v(v-1)}{3}$ transitive triples, the following problem is natural: Given a set $S$ of size $v \equiv 0$ or $1(\bmod 3)$, is it always possible to partition $T(S)$ into $3(v-2)$ subsets $\mathcal{B}_{1}, \mathcal{B}_{2}, \ldots, \mathcal{B}_{3(v-2)}$, so that each of $\left(S, \mathcal{B}_{1}\right),\left(S, \mathcal{B}_{2}\right), \ldots,\left(S, \mathcal{B}_{3(v-2)}\right)$ is a $T T S(v)$ ? Such a collection of $T T S(v)$ is called a large set of pairwise disjoint $T T S(v)$. We denote it by $L T T S(v)$.

All known results about $L T T S(v)$ are (see [LinSt], [Lin2]):
(1) Direct construction for $v=3,4,6,7,18,24$ and all $v \equiv 1,3(\bmod 6)$
(2) Recursive construction:

$$
\begin{aligned}
& v \longrightarrow 3 v(v \geq 3, v \neq 6,8) \\
& v+1 \longrightarrow 3 v+1(v \geq 3) \\
& v+2 \longrightarrow n v+2(n \equiv \pm 1(\bmod 6))
\end{aligned}
$$

All that remains for a complete solution of the existence problem for $L T T S$ is a construction for $L T T S\left(2^{n}+2\right)$. C.C.Lindner said, in his paper [Lin2], "The author has struggled valiantly in an attempt to produce a $2+2^{\alpha}$ construction. So far, no luck!" It seems that the construction of an $\operatorname{LTTS}\left(2^{n}+2\right)$ maybe is considerably difficult.

In this chapter we will try to construct $L T T S\left(2^{n}+2\right)$ using the method in §2.4. We give some preliminary results, which include a possible way to construct $\operatorname{LTTS}\left(2^{n}+2\right)$, the partitions of some kinds of transitive triples and some successful examples.

### 4.2 An analysis for order $2^{\boldsymbol{n}}+2$.

let set $S=\left\{\infty_{1}, \infty_{2}\right\} \cup X$, where $X$ is a set containing $v$ elements and $\infty_{1}, \infty_{2} \notin X$. For $T(S)$, the set of all transitive triples of $S$, we list
all kinds of transitive triples (the form, the number of containing triples and the number of covered ordered pairs) as follows:

| form | $\#$ | $\left(\infty_{1}, \infty_{2}\right)$ | $\left(\infty_{2}, \infty_{1}\right)$ | $\left(\infty_{1}, *\right)$ | $\left(*, \infty_{1}\right)$ | $\left(\infty_{2}, *\right)$ | $\left(*, \infty_{2}\right)$ | $(*, *)$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\left\langle\left(\infty_{1}, \infty_{2}, * *\right\rangle\right.$ | $v$ | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| $\left(\left(\infty_{1}, *, \infty_{2}\right\rangle\right\rangle$ | $v$ | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| $\left\langle\left(*, \infty_{1}, \infty_{2}\right\rangle\right\rangle$ | $v$ | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| $\left\langle\left(\infty_{2}, \infty_{1}, *\right)\right\rangle$ | $v$ | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| $\left\langle\left(\infty_{2}, *, \infty_{1}\right\rangle\right\rangle$ | $v$ | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| $\left\langle\left(*, \infty_{2}, \infty_{1}\right\rangle\right\rangle$ | $v$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| $\left\langle\left(\infty_{1}, *, *\right)\right\rangle$ | $v(v-1)$ | 0 | 0 | 2 | 0 | 0 | 0 | 1 |
| $\left\langle\left(*, \infty_{1}, *\right)\right\rangle$ | $v(v-1)$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| $\left\langle\left(*, *, \infty_{1}\right\rangle\right\rangle$ | $v(v-1)$ | 0 | 0 | 0 | 2 | 0 | 0 | 1 |
| $\left\langle\left(\infty_{2}, *, *\right)\right\rangle$ | $v(v-1)$ | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| $\left\langle\left(*, \infty_{2}, *\right)\right\rangle$ | $v(v-1)$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| $\left\langle\left(*, *, \infty_{2}\right\rangle\right\rangle$ | $v(v-1)$ | 0 | 0 | 0 | 0 | 0 | 2 | 1 |
| $(\langle *, *, *\rangle\rangle$ | $v(v-1)(v-2)$ | 0 | 0 | 0 | 0 | 0 | 0 | 3 |

where the \#-column indicates the number of triples, and where the symbol * represents any element of $X$.

By the table and the definition of TTS we can give a possible partition of $T(S) ; \mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}$ and $\mathcal{B}_{x}^{\prime \prime}$, where $x \in X$ and each $\mathcal{B}_{x}$ (and $\mathcal{B}_{x}^{\prime}, \mathcal{B}_{x}^{\prime \prime}$ ) is a $T T S(v+2)$. Of course, such a partition is not the only one. Here, in order to get a simple structure, we set up the partition as symmetrically as possible.

When $v \equiv 1(\bmod 3)$, we can give such an arrangement:

| $\begin{gathered} \mathcal{B}_{x} \\ \left(\left\langle\infty_{1}, \infty_{2}, x\right\rangle\right) \end{gathered}$ | $\begin{gathered} \# \\ 1 \end{gathered}$ | $\begin{gathered} \mathcal{B}_{x}^{\prime} \\ \left\langle\left\langle\infty_{1}, x, \infty_{2}\right\rangle\right\rangle \end{gathered}$ | $\begin{gathered} \# ' \\ 1 \end{gathered}$ | $\begin{gathered} \mathcal{B}_{x}^{\prime \prime} \\ \left\langle\left(x, \infty_{1}, \infty_{2}\right)\right\rangle \end{gathered}$ | $\begin{gathered} \#^{\prime \prime} \\ 1 \end{gathered}$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $\left(\left\langle\infty_{2}, \infty_{1}, x\right\rangle\right)$ | 1 | $\left\langle\left(\infty_{2}, x, \infty_{1}\right)\right\rangle$ | 1 | $\left\langle\left(\infty_{2}, \infty_{1}, x\right)\right\rangle$ | 1 |
| $\langle(\infty, *, *\rangle\rangle$ | $\frac{(v-1)}{3}$ | $\left\langle\left(\infty_{1}, *, *\right)\right\rangle$ | $\frac{(v-1)}{3}$ | \{ $\left.\left\langle\infty_{1}, *, *\right)\right\rangle$ | $\frac{(v-1)}{3}$ |
| (*, $\left.\left.\infty_{1}, *\right\rangle\right\rangle$ | ( $v-1$ ) | ( $\left\langle *, \infty_{1}, * *\right)$ | (v-1) | $\left\langle\left(*, \infty_{1}, *\right\rangle\right\rangle$ | $\frac{(v-1)}{3}$ |
| ( $\left.\left(*, *, \infty_{1}\right\rangle\right\rangle$ | (v) | ( $\langle *, *, \infty, 1)\rangle$ | (v | $\left\langle\left(*, *, \infty_{1}\right)\right\rangle$ | -1) |
| ( $\left.\left.\infty_{3}, *, *\right\rangle\right\rangle$ |  | $\left(\left\langle\infty_{2}, *, *\right)\right\rangle$ | $\frac{(v-1)}{3}$ | $\left\langle\left(\infty_{2}, *, *\right)\right\rangle$ | -1) |
| $\left\langle\left\langle *, \infty_{2, * *\rangle}\right.\right.$ | (v-1) | $\left\langle\left(\left\langle *, \infty_{2}, *\right)\right\rangle\right.$ | $\frac{(v-1)}{3}$ | $\left\langle\left(*, \infty_{2}, * *\right\rangle\right.$ | $\frac{(v-1)}{3}$ |
|  | (v-1) |  | $\frac{(v-1)}{3}$ |  | $\underline{(v-1)}$ |
| $\{(*, *, *)\rangle$ | $(\overline{v-2}) \frac{3-1}{3}$ | $\langle(*, *, *\rangle\rangle$ | $\left(v-{ }^{3}\right) \frac{v-1}{3}$ | $\langle\langle *, *, *\rangle\rangle$ | $\left(v-3_{2}^{2} \frac{v-1}{3}\right.$ |

where the \#-column, \#'-column and \#"-column indicate the numbers of triples in $\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}$ and $\mathcal{B}_{x}^{\prime \prime}$, respectively.

When $v \equiv 2(\bmod 3)$, we have the following possible arrangement:


Below, we only consider the case $v \equiv 1(\bmod 3)$; for $v=2^{n}$ this means $n \equiv 0(\bmod 2)$.

Firstly, imitating §2.4.1, we have these concepts (where $F=G F\left(2^{2 n}\right)$, $F^{*}=F \backslash\{0\}, R=Z_{2^{2 n-1}}=\left\{0,1, \ldots, 2^{2 n}-2\right\}$ and $g$ is a primitive element of $F^{*}$ ):
couple $\alpha C \beta-\alpha, \beta \in R^{*}=R \backslash\{0\}$ and $g^{\alpha}+g^{\beta}=1$.
pair class (PC) $\langle\alpha, \beta\rangle-$ all such ordered pairs $(y, z)$ of $F \backslash\{x\}$ that $z=g^{\alpha} x+g^{\beta} y, \alpha C \beta$ and $x \in F$ is fixed.
triple class (TC) $[\lambda, \mu]-$ all such transitive triples $\langle(u, v, w\rangle\rangle$ of $F$ that $w=g^{\lambda} u+g^{\mu} v$ and $\lambda C \mu$.
And, we will also use some methods and conclusions of $\S 2.4$.
Lemma 4.2.1. For a given element $x \in F$,
(1) Each ordered pair of distinct elements of $F \backslash\{x\}$ belongs to a uniquely determined PC. The total number of the PC is $2^{2 n}-2$. Each PC contains $2^{2 n}-1$ pairwise distinct ordered pairs.
(2) Each transitive triple of distinct elements in $F$ belongs to a uniquely determined TC. The total number of the TC is $2^{2 n}-2$. Each TC contains $2^{2 n}\left(2^{2 n}-1\right)$ pairwise distinct transitive triples.
(3) For the transitive triple $\left\langle\left\langle y, g^{\alpha} x+g^{\beta} y, g^{\gamma} x+g^{\delta} y\right\rangle\right.$, where $y \in$ $F \backslash\{x\}, \alpha, \beta, \gamma, \delta \in R^{*}, \alpha C \beta, \gamma C \delta$ and $\alpha \neq \gamma$, its three ordered pairs belong to the pair classes $\langle\alpha, \beta\rangle,\langle\gamma, \delta\rangle$ and $\langle\operatorname{ind}(\alpha+\delta, \beta+$ $\gamma)-\beta, \delta-\beta>$, respectively. And the transitive triple belongs to the TC [ind $(\alpha+\delta, \beta+\gamma)-\alpha, \gamma-\alpha]$.
(4) For the transitive triple $\left\langle\left\langle y, x, g^{\alpha} x+g^{\beta} y\right\rangle\right\rangle$, where $y \in F \backslash\{x\}$, $\alpha, \beta \in R^{*}$ and $\alpha C \beta$, only one among three ordered pairs, namely ( $y, g^{\alpha} x$ $+g^{\beta} y$ ), belongs to $P C\langle\alpha, \beta\rangle$. And the transitive triple belongs to $T C$ [ $\beta, \alpha$ ].
[Note: for the symbol ind $(\alpha+\delta, \beta+\gamma)$ see $\S 2.4 .1$ (C2).]

## Proof.

(1) and (2) are similar to Lemma 2.4 .1 (1) and Lemma 2.4.2 (2). Note the difference beween cyclic triple and transitive triple.
(3) Let $y=u, g^{\alpha} x+g^{\beta} y=v$ and $g^{\gamma} x+g^{\delta} y=w$, then

$$
\begin{aligned}
& g^{\delta} v+g^{\beta} w=\left(g^{\alpha+\delta}+g^{\beta+\gamma}\right) x \longrightarrow w=\frac{g^{\alpha+\delta}+g^{\beta+\gamma}}{g^{\beta}} x+g^{\delta-\beta} v \\
& g^{\gamma} v+g^{\alpha} w=\left(g^{\beta+\gamma}+g^{\alpha+\delta}\right) u \longrightarrow w=\frac{g^{\alpha+\delta}+g^{\beta+\gamma}}{g^{\alpha}} u+g^{\gamma-\alpha} v .
\end{aligned}
$$

(4) Let $y=u, x=v$ and $g^{\alpha} x+g^{\beta} y=w$. Then $w=g^{\beta} u+g^{\alpha} v$. $\square$

Imitating the method of construction of $\operatorname{LMTS}\left(2^{n}+2\right)$, we can pay attention to the balance of the PC's (for each $\operatorname{TTS}\left(2^{2 n}+2\right)$ ) and the TC's (for all TTS's). But, the following differences between $L M T S$ and LTTS must be considered:
i) For $M T S$, there is only one type of $\infty$-triple (i.e. the triple just containing one of $\infty_{1}$ or $\infty_{2}$ ). But for $T T S$, there are three types: $\left\langle\left\langle\infty, u_{1}, v_{1}\right\rangle\right),\left(\left\langle u_{2}, \infty, v_{2}\right\rangle\right\rangle$ and $\left\langle\left\langle u_{3}, v_{3}, \infty\right\rangle\right\rangle$. So, besides considering the balance of these ordered pairs $\left(u_{i}, v_{i}\right)$ in each TTS, we have to check the balance of those ordered pairs containing $\infty$ and the balance of each type of $\infty$-triple in all $\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}$ and $\mathcal{B}_{x}^{\prime \prime}$.
ii) The triple class TC consists of three $[*, *]$ for $M T S$, and only one $[*, *]$ for TTS. But the total number of all triples in a LTTS is three times that in a $L M T S$ of the same order.

Here, we give a method which can be used to meet the requirements raised in i).

Lemma 4.2.2. For any couple $\lambda C \mu$, there exists an arrangement for $\infty$-triples in $\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}$ and $\mathcal{B}_{x}^{\prime \prime}$ (each part contains $\frac{2^{2 n}-1}{3} \infty$-triples):

$$
\begin{array}{ll}
\text { part } 1 & \left\langle\left\langle\infty, y, g^{\lambda} x+g^{\mu} y\right)\right\rangle \\
\text { part 2 } & \left\langle\left\langle y, \infty, g^{\lambda} x+g^{\mu} y\right\rangle\right\rangle \\
\text { part } 3 & \left\langle\left\langle y, g^{\lambda} x+g^{\mu} y, \infty\right\rangle\right\rangle,
\end{array}
$$

such that following conditions are satisfied:
(1) In each $\mathcal{B}_{x}$ (or $\mathcal{B}_{x}^{\prime}$ or $\mathcal{B}_{x}^{\prime \prime}$ ) all $\infty$-triples cover all ordered pairs in the $P C\langle\lambda, \mu\rangle$.
(2) In each $\mathcal{B}_{x}$ (or $\mathcal{B}_{x}^{\prime}$ or $\mathcal{B}_{x}^{\prime \prime}$ ) all $\infty$-triples cover all ordered pairs $(\infty, u)$ and $(u, \infty)$, where $u \in F, u \neq x$.
(3) Each $\infty$-triple in the form $\langle\langle\infty, u, v\rangle\rangle$ (or $\langle\langle u, \infty, v\rangle\rangle$ or $(\langle u, v, \infty\rangle\rangle)$ , where $u \neq v \in F$, appears in part 1 (or part 2, or part 3) of

$$
\bigcup_{x \in F}\left(\mathcal{B}_{x} \cup \mathcal{B}_{x}^{\prime} \cup \mathcal{B}_{x}^{\prime \prime}\right) .
$$

Proof. Firstly, we consider the mapping $f$ from $F \backslash\{x\}$ into $F \backslash\{x\}$

$$
f: \quad y \longmapsto g^{\lambda} x+g^{\mu} y
$$

We have (*)

$$
\begin{aligned}
& f^{(2)}(y)=f[f(y)]=g^{\lambda}\left(1+g^{\mu}\right) x+g^{2 \mu} y \\
& f^{(3)}(y)=g^{\lambda}\left(1+g^{\mu}+g^{2 \mu}\right)+g^{3 \mu} y
\end{aligned}
$$

$f^{(k)}(y)=g^{\lambda} \sum_{s=0}^{k-1} g^{s \mu} x+g^{k \mu} y=\frac{g^{\lambda}\left(1-g^{k \mu}\right)}{1-g^{\mu}} x+g^{k \mu} y=\left(1-g^{k \mu}\right) x+g^{k \mu} y$.
where $f^{(0)}(y)=y$ and $f^{(k)}(y)=f\left(f^{(k-1)}(y)\right)$. So, $f^{(k)}(y)=y$ if and only if $\left(1-g^{k \mu}\right)(x-y)=0$, i.e., $g^{k \mu}=1$ since $y \in F \backslash\{x\}$. But $g^{k \mu}=1$ means $k \mu \equiv 0\left(\bmod 2^{2 n}-1\right)$. Thus for any $x \in F$ and $y \in F \backslash\{x\}$, under the action of $f$, the smallest period of $y$ is $k=\frac{2^{2 n}-1}{\text { g.c.d }\left(\mu, 2^{2 n}-1\right)}$, which is an odd integer and $k \mid 2^{2 n}-1, k>1$.

Below, we will discuss the three cases:
$1^{\circ} k=3$. In this case, $\mu=\frac{2^{2 n}-1}{3}$ or $\frac{2\left(2^{2 n}-1\right)}{3}$. All numbers in $F \backslash\{x\}$ are separated into $\frac{\mathbf{2}^{3 n}-1}{3}$ circuits with length 3. (Note: Regarding each number $y$ in $F \backslash\{x\}$ as a vertex and making an arc from $y$ to $f(y)$, we will get a directed graph. By the above, this graph consists of some circuits having the same length.) Denote the three numbers in each circuit by $y_{0}^{(t)}, y_{1}^{(t)}, y_{2}^{(t)}$, where $1 \leq t \leq \frac{2^{2 n}-1}{3}$ and $y_{i+1}^{(t)}=f\left(y_{i}^{(t)}\right)$ (the subscript is modulo 3 ). Then we can give the following arrangement:

## $\mathcal{B}_{x}$

$\mathcal{B}_{x}^{\prime}$
$\mathcal{B}_{x}^{\prime \prime}$
part $1\left\langle\left\langle\infty, y_{0}^{(t)}, y_{1}^{(t)}\right\rangle\right\rangle \quad\left\langle\left\langle\infty, y_{1}^{(t)}, y_{2}^{(t)}\right\rangle\right\rangle \quad\left\langle\left\langle\infty, y_{2}^{(t)}, y_{0}^{(t)}\right\rangle\right\rangle$
part $2\left\langle\left(y_{1}^{(t)}, \infty, y_{2}^{(t)}\right\rangle\right\rangle \quad\left\langle\left\langle y_{2}^{(t)}, \infty, y_{0}^{(t)}\right\rangle\right\rangle \quad\left\langle\left\langle y_{0}^{(t)}, \infty, y_{1}^{(t)}\right\rangle\right\rangle$
part $3\left\langle\left\langle y_{2}^{(t)}, y_{0}^{(t)}, \infty\right\rangle\right\rangle \quad\left\langle\left\langle y_{0}^{(t)}, y_{1}^{(t)}, \infty\right\rangle\right\rangle \quad\left\langle\left\langle y_{1}^{(t)}, y_{2}^{(t)}, \infty\right\rangle\right\rangle$
where $1 \leq t \leq \frac{2^{2 n}-1}{3}$. It is trivial to verify the conditions (1)-(3).
$2^{\circ} k=2^{2 n}-1$. In this case, all numbers in $F \backslash\{x\}$ make up a single circuit with length $2^{2 n}-1$. Denote these numbers $y_{0}, y_{1}, \ldots, y_{N-1}$, where $N=2^{2 n}-1$. We give the following arrangement:

$$
\begin{array}{rll}
\mathcal{B}_{x}: & \text { part } 1 & \left\{\left(\infty, y_{2 j+1}, y_{2 j+2}\right\rangle\right\rangle \\
\text { part } 2 & \left\langle\left\langle y_{j+\frac{2 N}{3}}, \infty, y_{j+\frac{2 N}{3}+1}\right\rangle\right\rangle \\
\text { part } 3 & \left\langle\left\langle y_{2 j}, y_{2 j+1}, \infty\right\rangle\right\rangle \\
\mathcal{B}_{x}^{\prime}: & \text { part } 1 & \left\langle\left\langle\infty, y_{2 j+\frac{N}{3}+1}, y_{2 j+\frac{N}{3}+2}\right\rangle\right\rangle \\
\text { part } 2 & \left\{\left\langle y_{j}, \infty, y_{j+1}\right\rangle\right\rangle \\
\text { part } 3 & \left\langle\left\langle y_{2 j+\frac{N}{3}}, y_{2 j+\frac{N}{3}+1}, \infty\right\rangle\right\rangle
\end{array}
$$

$$
\begin{array}{rll}
\mathcal{B}_{x}^{\prime \prime}: & \text { part } 1 & \left\langle\left\langle\infty, y_{2 j+\frac{2 N}{3}+1}, y_{2 j+\frac{2 N}{3}+2}^{3}\right\rangle\right\rangle \\
\text { part } 2 & \left\langle\left\langle y_{j+\frac{N}{3}}, \infty, y_{j+\frac{N}{3}+1}\right\rangle\right\rangle \\
\text { part 3 } & \left\langle\left\langle y_{2 j+\frac{2 N}{3}}^{3}, y_{2 j+\frac{2 N}{3}+1, \infty}\right\rangle\right\rangle y_{y_{0}}
\end{array}
$$

where $0 \leq j \leq \frac{N}{3}-1$ and the subscript is modulo $N$. In order to verify the conditions (1)-(3), we can look at the digraph, which is the arrangement for $\mathcal{B}_{x}$, where the arcs mm, ...... and - represent the ordered pairs in part 1,2 and 3 , respectively. And for $\mathcal{B}_{x}^{\prime}$ (or $\mathcal{B}_{x}^{\prime \prime}$ ), the subscript of each vertex in the digraph will be increased by $\frac{N}{3}\left(\right.$ or $\left.\frac{2 N}{3}\right), \bmod N$.

$3^{\circ} 3<k<2^{2 n}-1$. In this case, all numbers in $F \backslash\{x\}$ are separated into $\frac{N}{k}$ circuits with length $k$.

If $3 \mid k$, our construction will be similar to the case $1^{\circ}$ (all circuits are the same ...) and $2^{\circ}$ (each circuit is separated into three parts...).

Or else $3 \left\lvert\, \frac{N}{k}\right.$, we separate all circuits into three types and denote all numbers in each circuit as (let $k=2 m+1$, since $k$ is odd):
type $1 y_{0}^{(t)}, y_{1}^{(t)}, \ldots, y_{2 m}^{(t)}\left(y_{j+1}=f\left(y_{j}\right)\right)$,
type $2 z_{0}^{(t)}, z_{1}^{(t)}, \ldots, z_{2 m}^{(t)}\left(z_{j+1}=f\left(z_{j}\right)\right), 1 \leq t \leq \frac{N}{3 k}$.
type $3 \quad r_{0}^{(t)}, r_{1}^{(t)}, \ldots, r_{2 m}^{(t)}\left(r_{j+1}=f\left(r_{j}\right)\right)$,
Now, we can give the following arrangement:

| $\mathcal{B}_{x}$ | $\mathcal{B}_{x}^{\prime}$ | $\mathcal{B}_{x}^{\prime \prime}$ |
| :---: | :---: | :---: |
| part $1\left\langle\left\langle\infty, y_{2 j-1}^{(t)}, y_{2 j}^{(t)}\right\rangle\right\rangle$ | ( $\left.\left.\infty, y_{2 j}^{(t)}, y_{2 j+1}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle\infty, y_{0}^{(t)}, y_{1}^{(t)}\right\rangle\right\rangle$ |
| $\left\langle\left\langle\infty, z_{2 j}^{(t)}, z_{2 j+1}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle\infty, z_{0}^{(t)}, z_{1}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle\infty, z_{2 j-1}^{(t)}, z_{2 j}^{(t)}\right\rangle\right\rangle$ |
| $\left\langle\left\langle\infty, r_{0}^{(t)}, r_{1}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left(\left\|\infty, r_{2 j-1}^{(t)}, r_{2 j}^{(t)}\right\rangle\right\rangle\right.$ | $\left\langle\left\langle\infty, r_{2 j}^{(t)}, r_{2 j+1}^{(t)}\right\rangle\right\rangle$ |
| part $2\left\langle\left\langle y_{2 m}^{(t)}, \infty, y_{0}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle y_{0}^{(t)}, \infty, y_{1}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle y_{i}^{(t)}, \infty, y_{i+1}^{(t)}\right\rangle\right\rangle$ |
| $\left\langle\left\langle z_{0}^{(t)}, \infty, z_{1}^{(t)}\right)\right\rangle$ | $\left\langle\left\langle z_{i}^{(t)}, \infty, z_{i+1}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle z_{2 m}^{(t)}, \infty, z_{0}^{(t)}\right\rangle\right\rangle$ |
| $\left\langle\left\langle r_{i}^{(t)}, \infty, r_{i+1}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle r_{2 m}^{(t)}, \infty, r_{0}^{(t)}\right\rangle\right\rangle$ | $\left\langle\left\langle r_{0}^{(t)}, \infty, r_{1}^{(t)}\right\rangle\right\rangle$ |
| rt $3\left\langle\left(y_{2 j-2}^{(t)}, y_{2 j-1}^{(t)}, \infty\right)\right\rangle$ | $\left\langle\left\langle y_{2 j-1}^{(t)}, y_{2 j}^{(t)} ; \infty\right\rangle\right\rangle$ | $\left\langle\left\langle y_{2 m}^{(t)}, y_{0}^{(t)}, \infty\right\rangle\right\rangle$ |
| $\left\langle\left\langle z_{2 j-1}^{(t)}, z_{2 j}^{(t)}, \infty\right)\right\rangle$ | $\left\langle\left\langle z_{2 m}^{(t)}, z_{0}^{(t)}, \infty\right\rangle\right\rangle$ | $\left\langle\left\langle z_{2 j-2}^{(t)}, z_{2 j-1}^{(t)}, \infty\right)\right\rangle$ |
| $\left\langle\left\langle r_{2 m}^{(t)}, r_{0}^{(t)}, \infty\right\rangle\right\rangle$ | ( $\left.\left\langle r_{2 j-2}^{(t)}, r_{2 j-1}^{(t)}, \infty\right\rangle\right\rangle$ | $\left\langle\left\langle r_{2 j-1}^{(t)}, r_{2 j}^{(t)}, \infty\right)\right\rangle$ |

where $1 \leq j \leq m, 1 \leq i \leq 2 m-1$ and all subscripts are modulo $2 m+1$.
In order to verify the conditions (1)-(3), we can look at the digraphs, which are the arrangement for $\mathcal{B}_{x}$, where the arcs mmi, ...... and --represent the ordered pairs in part 1,2 and 3 , respectively. For $\mathcal{B}_{x}^{\prime}$,

substitute the symbols $r, y, z$ for $y, z, r$ in the digraphs. And for $\mathcal{B}_{x}^{\prime \prime}$, the symbols in the digraphs will be substituted by $z, r, y$.

Finally, we point out that for any given couple $\lambda C \mu$, we have

$$
\bigcup_{x \in F}\left\{\left(y, g^{\lambda} x+g^{\mu} y\right) ; y \in F \backslash\{x\}\right\}=(F \times F) \backslash\{(t, t) ; t \in F\} .
$$

This completes the proof.
4.3 A way to construct $\operatorname{LTTS}\left(2^{2 n}+2\right)$.

Now, by the last section, we will try to construct $\operatorname{LTTS}\left(2^{2 n}+2\right)$ for $n>1$. Denote $\operatorname{LTTS}\left(2^{2 n}+2\right)=\left\{\left(X, \mathcal{B}_{x}\right) \mid x \in F\right\} \cup\left\{\left(X, \mathcal{B}_{x}^{\prime}\right) \mid x \in\right.$ $F\} \cup\left\{\left(X, \mathcal{B}_{x}^{\prime \prime}\right) \mid x \in F\right\}$, where $X=\left\{\infty_{1}, \infty_{2}\right\} \cup F$ and $F=G F\left(2^{2 n}\right)$. Each collection $\mathcal{B}_{x}$ (and $\mathcal{B}_{x}^{\prime}, \mathcal{B}_{x}^{\prime \prime}$ ) contains the following transitive triples.
(where $<*, *>$ and $[*, *]$ represent the PC and TC respectively)

## $\mathcal{B}_{x}:$

part 1 ( It contains 2 triples.)

$$
\left\langle\left\langle\infty_{1}, \infty_{2}, x\right\rangle\right\rangle, \quad\left\langle\left\langle x, \infty_{2}, \infty_{1}\right\rangle\right\rangle
$$

part 2 (It contains $3 \cdot \frac{2^{2 n}-1}{3}$ triples, where $j=1,2$.)

$$
\left\langle\left\langle\infty_{j}, y, g^{\lambda_{j}} x+g^{\mu_{j}} y\right\rangle\right\rangle
$$

$$
\left\langle\left\langle y, \infty_{j}, g^{\left.\left.\left.\lambda_{j} x+g^{\mu_{j}} y\right)\right\rangle\right\rangle \quad\left\langle\lambda_{j}, \mu_{j}\right\rangle}\right.\right.
$$

$$
\left\langle\left\langle y, g^{\lambda_{j}} x+g^{\mu_{j}} y, \infty_{j} j\right\rangle\right.
$$

part 3 (It contains $2^{2 n}-1$ triples.)

$$
\begin{array}{lll}
\left(\left\langle y, x, g^{\lambda} x+g^{\mu} y\right\rangle\right\rangle & \langle\lambda, \mu\rangle & {[\mu, \lambda]}
\end{array}
$$

part 4 (It contains $\frac{2^{2 n}-7}{3}\left(2^{2 n}-1\right)$ triples, where $1 \leq i \leq \frac{2^{2 n}-7}{3}$.)
$\left\langle\left\langle y, g^{\alpha_{i}} x+g^{\beta_{i}} y, g^{\gamma_{i}} x+g^{\delta_{i}} y\right\rangle\right\rangle\left\langle\alpha_{i}, \beta_{i}\right\rangle\left\langle\gamma_{i}, \delta_{i}\right\rangle\left\langle *, \delta_{i}-\beta_{i}\right\rangle$
$\left[*, \gamma_{i}-\alpha_{i}\right]$
part 5 (It contains $2 \cdot \frac{2^{2 n}-1}{3}$ triples, where $\theta=\frac{2^{2 n}-1}{3}$.)
$\left\langle\left\langle y, g^{\theta} x+g^{2 \theta} y, g^{2 \theta} x+g^{\boldsymbol{\theta}} y\right\rangle\right\rangle\langle\theta, 2 \theta\rangle\langle 2 \theta, \theta\rangle\langle\theta, 2 \theta\rangle[2 \theta, \theta]$
$\left\langle\left\langle y, g^{2 \theta} x+g^{\theta} y, g^{\theta} x+g^{2 \theta} y\right\rangle\right\rangle(2 \theta, \theta\rangle\langle\theta, 2 \theta)\langle 2 \theta, \theta\rangle[\theta, 2 \theta]$
$\mathcal{B}_{x}^{\prime}$ :
part 1 (It contains 2 triples.)

$$
\left\langle\left\langle\infty_{1}, x, \infty_{2}\right\rangle\right\rangle, \quad\left\langle\left\langle\infty_{2}, x, \infty_{1}\right\rangle\right\rangle
$$

part 2 and part 5 are the same as the corresponding parts of $\mathcal{B}_{x}$.
part 3 (It contains $2^{2 n}-1$ triples.)

$$
\left\langle\left\langle y, x, g^{\lambda^{\prime}} x+g^{\mu^{\prime}} y\right\rangle\right\rangle \quad \quad\left\langle\lambda^{\prime}, \mu^{\prime}\right\rangle \quad\left[\mu^{\prime}, \lambda^{\prime}\right]
$$

part 4 (It contains $\frac{2^{2 n}-7}{3}\left(2^{2 n}-1\right)$ triples, where $1 \leq i \leq \frac{2^{2 n}-7}{3}$.)
$\left\langle\left\langle y, g^{\alpha_{i}^{\prime}} x+g^{\beta_{i}^{\prime}} y, g^{\gamma_{i}^{\prime}} x+g^{\delta_{i}^{\prime}} y\right\rangle\right\rangle\left\langle\alpha_{i}^{\prime}, \beta_{i}^{\prime}\right\rangle\left\langle\gamma_{i}^{\prime}, \delta_{i}^{\prime}\right\rangle\left\langle *, \delta_{i}^{\prime}-\beta_{i}^{\prime}\right\rangle$ $\left[*, \gamma_{i}^{\prime}-\alpha_{i}^{\prime}\right]$
$\mathcal{B}_{x}^{\prime \prime}$ :
part 1 (It contains 2 triples.)

$$
\left\langle\left\langle x, \infty_{1}, \infty_{2}\right\rangle\right\rangle, \quad\left\langle\left\langle\infty_{2}, \infty_{1}, x\right\rangle\right\rangle
$$

part 2 and part 5 are the same as the corresponding parts of $\mathcal{B}_{\boldsymbol{x}}$.
part 3 (It contains $2^{2 n}-1$ triples.)

$$
\left\langle\left\langle y, x, g^{\lambda^{\prime \prime}} x+g^{\mu^{\prime \prime}} y\right\rangle\right\rangle \quad\left\langle\lambda^{\prime \prime}, \mu^{\prime \prime}\right\rangle \quad\left[\mu^{\prime \prime}, \lambda^{\prime \prime}\right]
$$

part 4 (It contains $\frac{2^{2 n}-7}{3}\left(2^{2 n}-1\right)$ triples, where $1 \leq i \leq \frac{2^{2 n}-7}{3}$.)
$\left\langle\left\langle y, g^{\alpha_{i}^{\prime \prime}} x+g^{\beta_{i}^{\prime \prime}} y, g^{\gamma_{i}^{\prime \prime}} x+g^{\delta_{i}^{\prime \prime}} y\right\rangle\right\rangle\left\langle\alpha_{i}^{\prime \prime}, \beta_{i}^{\prime \prime}\right\rangle\left\langle\gamma_{i}^{\prime \prime}, \delta_{i}^{\prime \prime}\right\rangle\left\langle *, \delta_{i}^{\prime \prime}-\beta_{i}^{\prime \prime}\right\rangle$

$$
\left[*, \gamma_{i}^{\prime \prime}-\alpha_{i}^{\prime \prime}\right]
$$

Part 5 of $\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}$ and $\mathcal{B}_{x}^{\prime \prime}$ is arranged by a general method provided by following lemma.

Lemma 4.3.1. For a couple $\lambda C \mu$, let $k$ and $t$ be the smallest positive integers such that $k \mu \equiv 0$ and $2^{t} \mu \equiv \mu\left(\bmod 2^{2 n}-1\right)$. If $3 \mid k$, then there exists a partition of all transitive triples belonging to all $T C[\mu, \lambda],[2 \mu, 2 \lambda], \ldots$ and $\left[2^{t-1} \mu, 2^{t-1} \lambda\right]$ such that all ordered pairs in these triples occupy exactly all $P C<\lambda, \mu>,<2 \lambda, 2 \mu>, \ldots$ and $<$ $2^{t-1} \lambda, 2^{t-1} \mu>$.

Proof. Firstly, we give the following transitive triples, which occupy the required PC and TC (by Lemma 4.2.1 (3)), where $x \in F$ and $y \in F \backslash\{x\}$ :

$$
\begin{aligned}
& \left\langle\left\langle y, g^{\lambda} x+g^{\mu} y, g^{2 \lambda} x+g^{2 \mu} y\right\rangle\right) \\
& \langle\lambda, \mu\rangle(2 \lambda, 2 \mu\rangle\langle\lambda, \mu\rangle[\mu, \lambda] \\
& \left(\left\langle y, g^{2 \lambda} x+g^{2 \mu} y, g^{2^{2} \lambda} x+g^{2^{2} \mu} y\right\rangle\right\rangle \\
& (2 \lambda, 2 \mu)\left\langle 2^{2} \lambda, 2^{2} \mu\right\rangle(2 \lambda, 2 \mu)[2 \mu, 2 \lambda] \\
& \left\langle\left\langle y, g^{2^{2} \lambda} x+g^{2^{2} \mu} y, g^{2^{3} \lambda} x+g^{2^{3} \mu} y\right\rangle\right\rangle \\
& \left\langle 2^{2} \lambda, 2^{2} \mu\right\rangle\left(2^{3} \lambda, 2^{3} \mu\right\rangle\left\langle 2^{2} \lambda, 2^{2} \mu\right\rangle\left[2^{2} \mu, 2^{2} \lambda\right] \\
& \left\langle\left(y, g^{2^{t-2} \lambda} x+g^{2^{t-2}} \boldsymbol{\mu} y, g^{2^{t-1} \lambda} x+g^{2^{t-1} \mu} y\right\rangle\right\rangle \\
& \left(2^{t-2} \lambda, 2^{t-2} \mu\right)\left(2^{t-1} \lambda, 2^{t-1} \mu\right\rangle\left(2^{t-2} \lambda, 2^{t-2} \mu\right)\left[2^{t-2} \mu, 2^{t-2} \lambda\right] \\
& \left\langle\left(y, g^{2^{t-1} \lambda} x+g^{2^{t-1}} \mu y, g^{\lambda} x+g^{\mu} y\right\rangle\right) \\
& \left\langle 2^{t-1} \lambda, 2^{t-1} \mu\right\rangle(\lambda, \mu)\left(2^{t-1} \lambda, 2^{t-1} \mu\right\rangle\left[2^{t-1} \mu, 2^{t-1} \lambda\right]
\end{aligned}
$$

Let $f_{i}$ be the mapping from $F \backslash\{x\}$ into $F \backslash\{x\}(0 \leq i \leq t-1)$

$$
f_{i}: \quad y \longmapsto g^{2^{i} \lambda} x+g^{2^{i} \mu} y .
$$

Then, for any $y \in F \backslash\{x\}$, the smallest period of $y$ under the action of $f_{0}$ (further each $f_{i}$ ) is $k$. Let $s=\frac{2^{2 n}-1}{k}$ and $k=3 m$ (since $3 \mid k$ ), then all numbers in $F \backslash\{x\}$, under the action of $f_{0}$, are separated into $s$ circuits of length $3 m$. Denote all numbers in each circuit by $y_{0}^{(t)}, y_{1}^{(t)}, \ldots, y_{3 m-1}^{(t)}$, $1 \leq t \leq s$, where $y_{p+1}^{(t)}=f_{0}\left(y_{p}^{(t)}\right), 0 \leq p \leq 3 m-1$ (here and in what follows, all subscripts are modulo $3 m$ ).

By Lemma 4.2.2 (*), we have

$$
f_{0}^{\left(2^{i}\right)}(y)=\left(1-g^{2^{i} \mu}\right) x+g^{2^{\mu}} y=g^{2^{i} \lambda} x+g^{2^{i} \mu} y=f_{i}(y) .
$$

Futhermore,

$$
f_{i}\left(y_{p}^{(t)}\right)=f_{0}^{\left(2^{i}\right)}\left(y_{p}^{(t)}\right)=y_{p+2^{i}}^{(t)} \text { and } f_{i}^{(j)}\left(y_{p}^{(t)}\right)=f_{0}^{\left(2^{i} j\right)}\left(y_{p}^{(t)}\right)=y_{p+2^{i} j}^{(t)}
$$

And we specify $f_{i}^{(0)}(y)=y$ and $f_{i}^{(1)}(y)=f_{i}(y)$.
Below, we can denote all above-mentioned transitive triples by $\left\langle\left\langle f_{i}^{(0)}(y), f_{i}^{(1)}(y), f_{i}^{(2)}(y)\right\rangle\right\rangle$,
which belongs to $\mathrm{TC}\left[2^{i} \mu, 2^{i} \lambda\right]$, where $0 \leq i \leq t-1$ and $y \in F \backslash\{x\}$. These triples contain all ordered pairs $\left(y, f_{i}(y)\right)$.

Now, we give the following partition of all above-mentioned triples:

$$
\begin{aligned}
& \left.(*): \quad\left\langle\left\langle y_{2^{i}(3 j+2)-2}^{(t)}, y_{2^{i}(3 j+3)-2}^{(t)}, y_{2^{i}(3 j+4)-2}^{(t)}\right\rangle\right\rangle \text { (in } \mathcal{B}_{x}\right) \\
& \left.(*)^{\prime}: \quad\left\langle\left\langle y_{2^{\prime}(3 j+2)-1}^{(t)}, y_{2^{i}(3 j+3)-1}^{(t)}, y_{2^{i}(3 j+4)-1}^{(t)}\right\rangle\right\rangle \text { (in } \mathcal{B}_{x}^{\prime}\right) \\
& (*)^{\prime \prime}: \quad\left\langle\left\langle y_{2^{i}(3 j+2)}^{(t)}, y_{2^{i}(3 j+3)}^{(t)}, y_{2^{i}(3 j+4)}^{(t)}\right\rangle \text { (in } \mathcal{B}_{x}^{\prime \prime}\right)
\end{aligned}
$$

where $0 \leq i \leq t-1,0 \leq j \leq m-1,1 \leq t \leq s$.
For given $x \in F$, let us show that any ordered pair $P=\left(y, f_{i}(y)\right)$ is covered by a certain transitive triple in (*) ((*)' and (*)" are similar), where $y \in F \backslash\{x\}$ and $0 \leq i \leq t-1$. Let $y=y_{p}^{(t)}(0 \leq p \leq 3 m-1$, $1 \leq t \leq s$. Below, for brevity, the superscript $t$ will be omitted).

Since g.c.d $\left(2^{i}, 3 m\right)=1$, there exists a positive integer $q(1 \leq q \leq$ $3 m-1)$ such that $2^{i} q \equiv 1(\bmod 3 m)$. Let $j \equiv\left(p-\left(2^{i+1}-2\right)\right) q$ $(\bmod 3 m)$, then $p \equiv 2^{i}(j+2)-2(\bmod 3 m)$ and $P=\left(y_{p}, f_{i}\left(y_{p}\right)\right)=$ $\left(y_{2^{i}(j+2)-2}, y_{2^{i}(j+3)-2}\right)$. If $j \equiv 0$ or $1(\bmod 3)$, then $P$ is covered by a certain triple in $(*)$, obviously. If $j=3 j^{\prime}+2\left(0 \leq j^{\prime} \leq m-1\right)$, then

$$
\begin{aligned}
& 2^{i}(j+2)-2=2^{i-1}\left[3\left(2 j^{\prime}+2\right)+2\right]-2, \\
& 2^{i}(j+3)-2=2^{i-1}\left[3\left(2 j^{\prime}+2\right)+4\right]-2 .
\end{aligned}
$$

$P$ will be also covered by another triple in (*).
Finally, we will prove, for any $x \in F$, that any transitive triple $T=$ $\left\langle\left\langle f_{i}^{(0)}(y), f_{i}^{(1)}(y), f_{i}^{(2)}(y)\right\rangle\right\rangle$ is in $(*)$ or $(*)^{\prime}$ or $(*)^{\prime \prime}$, where $y \in F \backslash\{x\}$ and $0 \leq i \leq t-1$. Let $y=y_{p}^{(t)}(0 \leq p \leq 3 m-1,1 \leq t \leq s$. Below, the superscript $t$ will omitted, too).

Let $2^{i} q \equiv 1(\bmod 3 m)$ and $j \equiv p q(\bmod 3 m), 0 \leq q \leq 3 m-1$, $0 \leq j \leq 3 m-1$, then $p=2^{i} j$ and

$$
T=\left\langle\left\langle f_{i}^{(0)}\left(y_{p}\right), f_{i}^{(1)}\left(y_{p}\right), f_{i}^{(2)}\left(y_{p}\right)\right\rangle\right\rangle=\left\langle\left\langle y_{2^{i} j}, y_{2^{i}(j+1)}, y_{2^{i}(j+2)}\right\rangle\right\rangle
$$

If $j \equiv 2(\bmod 34)$ then, obviously, T is in $(*)^{\prime \prime}$. Furthermore, we note the following facts:
(1) $q \not \equiv 0(\bmod 3)$, since $2^{i} q \equiv 1(\bmod 3 m)$;
(2) If $2^{i} q \equiv 1(\bmod 3 m)$ and $q \equiv 1$ or $2(\bmod 3)$ then $2^{i-1} q^{\prime} \equiv 1$ $(\bmod 3 m)$ and $q^{\prime} \equiv 2$ or $1(\bmod 3)$.
Thus we have:
If $j=3 j^{\prime}$, when $q \equiv 1(\bmod 3)$, let $q^{\prime}=3 q^{\prime \prime}+2$, then $2^{i} j=2^{i}\left[3\left(q^{\prime \prime}+\right.\right.$ $\left.\left.j^{\prime}\right)+2\right]-2$ and $T \in(*)$; when $q \equiv 2(\bmod 3)$, let $q=3 q^{\prime \prime}+2$, then $2^{i} j=2^{i}\left[3\left(q^{\prime \prime}+j^{\prime}\right)+2\right]-1$ and $T \in(*)^{\prime}$.

If $j=3 j^{\prime}+1$, when $q \equiv 1(\bmod 3)$, let $q=3 q^{\prime \prime}+1$, then $2^{i} j=$ $2^{i}\left[3\left(q^{\prime \prime}+j^{\prime}\right)+2\right]-1$ and $T \in(*)^{\prime} ;$ when $q \equiv 2(\bmod 3)$, let $q^{\prime}=3 q^{\prime \prime}+1$, then $2^{i} j=2^{i}\left[3\left(q^{\prime \prime}+j^{\prime}\right)+2\right]-2$ and $T \in(*)$.

This completes the proof.
We give an example: $F=G F\left(2^{6}\right), \mu=7$. In this case, $t=6$ and $k=9$. All numbers in $F \backslash\{x\}$ are separated into 7 circuits with length 9. We only list one circuit and only write down the subscript $j$ of the vertex $y_{k}$.

|  | $\mathcal{B}_{x}$ |  |  | $\mathcal{B}_{x}^{\prime}$ | $\mathcal{B}_{x}^{\prime \prime}$ |  |  |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 012 | 345 | 678 | 123 | 456 | 780 | 234 | 567 | 801 |
| 246 | 813 | 570 | 357 | 024 | 681 | 468 | 135 | 702 |
| 615 | 048 | 372 | 726 | 150 | 483 | 837 | 261 | 504 |
| 543 | 210 | 876 | 654 | 321 | 087 | 765 | 432 | 108 |
| 318 | 642 | 075 | 420 | 753 | 186 | 531 | 864 | 207 |
| 840 | 516 | 273 | 051 | 627 | 384 | 162 | 738 | 405 |

### 4.4 Two sufficient conditions and examples.

Theorem 4.4.1. Let $R=Z_{2^{2 n-1}}=\left\{0,1, \ldots, 2^{2 n}-2\right\}$ and $\theta=\frac{2^{2 n}-1}{3}$. If there exist two numbers $\mu_{1} \neq \mu_{2} \in R^{*} \backslash\{\theta, 2 \theta\}$ and six subsets of $\tilde{R}=R^{*} \backslash\left\{\theta, 2 \theta, \mu_{1}, \mu_{2}\right\}$ such that the following conditions are satisfied, then there exists an $\operatorname{LTTS}\left(2^{2 n}+2\right)$ :
(1) Each of these subsets $\left\{\beta_{i}\right\}_{i},\left\{\delta_{i}\right\}_{i},\left\{\beta^{\prime}\right\}_{i},\left\{\delta_{i}\right\}_{i},\left\{\beta^{\prime \prime}\right\}_{i}$ and $\left\{\delta^{\prime \prime}{ }_{i}\right\}_{i}$ contains $\frac{2^{2 n}-7}{3}$ elements and $\delta_{i}-\beta_{i}, \delta_{i}-\beta_{i}^{\prime}, \delta^{\prime \prime}{ }_{i}-\beta^{\prime \prime}{ }_{i} \in \tilde{R}$, for any $i$ (these differences are one-to-one).
(2) $\left\{\beta_{i}\right\}_{i},\left\{\delta_{i}\right\}_{i}$ and $\left\{\delta_{i}-\beta_{i}\right\}_{i}$ are pairwise disjoint (between $\left\{\beta^{\prime}\right\}_{i}$, $\left\{\delta^{\prime}\right\}_{i}$ and $\left\{\delta^{\prime}{ }_{i}-\beta^{\prime}\right\}_{i}$, between $\left\{\beta^{\prime \prime}{ }_{i}\right\}_{i},\left\{\delta^{\prime \prime}\right\}_{i}$ and $\left\{\delta^{\prime \prime}{ }_{i}-\beta^{\prime \prime}{ }_{i}\right\}_{i}$ also .
(3) $\left\{\lambda, \lambda^{\prime}, \lambda^{\prime \prime}\right\} \cup\left\{\gamma_{i}-\alpha_{i}\right\}_{i} \cup\left\{\gamma_{i}^{\prime}-\alpha_{i}^{\prime}\right\}_{i} \cup\left\{\gamma_{i}^{\prime \prime}-\alpha^{\prime \prime}{ }_{i}\right\}_{i}=R^{*} \backslash\{\theta, 2 \theta\}$, where $\lambda C \mu, \alpha_{i} C \beta_{i}, \gamma_{i} C \delta_{i}$ and $\{\mu\} \cup\left\{\beta_{i}\right\}_{i} \cup\left\{\gamma_{i}\right\}_{i} \cup\left\{\gamma_{i}-\beta_{i}\right\}_{i}=\tilde{R}$ (and similar for these parameters with ' and ").
Proof. By Lemma 4.2.1, these parameters satisfying conditions (1)-(3) will enable all PC and TC to be balanced for the construction in the beginning of this section. And, by Lemma 4.2.2 and 4.3.1, these triples in part 2 and part 5 can be separated successfully into $\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}$ and $\mathcal{B}_{x}^{\prime \prime}$. As for those triples in parts $3,4,5$, which don't need to be separated (of course, some of them may be done by Lemma 4.3.1 also), have been well done by Lemma 4.2.1.
Example. For $R=Z_{15}$ (i.e. $n=2$ ), by the conditions (1)-(3) in the lemma, we have already found a lot of solutions by computer search as follows:

| $\mu_{1} \mu_{2}$ | 2 | 3 | 4 | 6 | 7 | 8 | 9 | 11 | 12 | 13 | 14 |
| :--- | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 2 | 2 | 2 | 4 | 2 | 2 | 4 | 8 | 44 | 2 | 16 |
| 2 |  | 4 | 2 | 2 | 8 | 2 | 44 | 2 | 4 | 16 | 2 |
| 3 |  |  | 44 | 28 | 4 | 4 | 28 | 2 | 0 | 4 | 44 |
| 4 |  |  |  | 4 | 2 | 2 | 4 | 16 | 2 | 2 | 8 |
| 6 |  |  |  |  | 2 | 44 | 0 | 4 | 28 | 44 | 4 |
| 7 |  |  |  |  |  | 16 | 44 | 2 | 4 | 2 | 2 |
| 8 |  |  |  |  |  |  | 2 | 2 | 4 | 8 | 2 |
| 9 |  |  |  |  |  |  |  | 4 | 28 | 2 | 4 |
| 11 |  |  |  |  |  |  |  |  | 44 | 2 | 2 |
| 12 |  |  |  |  |  |  |  |  |  | 4 | 2 |
| 13 |  |  |  |  |  |  |  |  |  |  | 2 |

The total number of solutions is 682 and for any $\mu_{1} \neq \mu_{2} \in R^{*} \backslash\{5,10\}$, except $\left(\mu_{1}, \mu_{2}\right)=(3,12)$ and $(6,9)$, there exist all the solutions. Here, we only select one of them, $\left(\mu_{1}, \mu_{2}\right)=(1,2)$, and give the corresponding LTTS(18).
$\left\{\beta_{i}\right\}_{i=1}^{3}=\{4,8,12\},\left\{\beta_{i}^{\prime}\right\}_{i=1}^{3}=\{12,9,14\},\left\{\beta_{i}^{\prime \prime}\right\}_{i=1}^{3}=\{3,8,9\}$,
$\left\{\delta_{i}\right\}_{i=1}^{3}=\{7,6,11\},\left\{\delta_{i}^{i}\right\}_{i=1}^{3}=\{3,13,7\},\left\{\delta^{\prime \prime}{ }_{i}\right\}_{i=1}^{3}=\{14,12,7\}$,
$\operatorname{LTTS}(18)=\left\{\left(X, \mathcal{B}_{x}\right) ; x \in F_{16}\right\} \cup\left\{\left(X, \mathcal{B}_{x}^{\prime}\right) ; x \in F_{16}\right\} \cup\left\{\left(X, B_{x}^{\prime \prime}\right) ; x \in\right.$ $\left.F_{16}\right\}$, where $X=\left\{\infty_{1}, \infty_{2}\right\} \cup F_{16},<*, *>$ and $[*, *]$ represent the PC
and TC respectively.

| $\mathcal{B}_{x}$ : |  | (PC) | (TC) | (\#) |
| :---: | :---: | :---: | :---: | :---: |
| (1) | $\left\langle\left\langle\infty_{1}, \infty_{2}, x\right\rangle\right\rangle$ |  |  | 1 |
|  | $\left\langle\left\langle x, \infty_{2}, \infty_{1}\right\rangle\right\rangle$ |  |  | 1 |
| (2) | $\left\langle\left\langle\infty_{1}, y, g^{4} x+g y\right\rangle\right\rangle$ |  |  | 5 |
|  | $\left\langle\left\langle y, \infty_{1}, g^{4} x+g y\right\rangle\right\rangle$ | $\langle 4,1\rangle$ |  | 5 |
|  | $\left\langle\left\langle y, g^{4} x+g y, \infty_{1}\right\rangle\right\rangle$ |  |  | 5 |
|  | $\left\langle\left\langle\infty_{2}, y, g^{8} x+g^{2} y\right\rangle\right\rangle$ |  |  | 5 |
|  | $\left\langle\left\langle y, \infty_{2}, g^{8} x+g^{2} y\right\rangle\right)$ | $\langle 8,2\rangle$ |  | 5 |
|  | $\left\langle\left\langle y, g^{8} x+g^{2} y, \infty_{2}\right\rangle\right\rangle$ |  |  | 5 |
| (3) | $\left\langle\left\langle y, x, g^{7} x+g^{9} y\right\rangle\right\rangle$ | $\langle 7,9\rangle$ | [9,7] | 15 |
| (4) | $\left\langle\left\langle y, g x+g^{4} y, g^{9} x+g^{7} y\right\rangle\right\rangle$ | $\langle 1,4\rangle\langle 9,7\rangle\langle 14,3\rangle$ | [2,8] | 15 |
|  | $\left\langle\left\langle y, g^{2} x+g^{8} y, g^{13} x+g^{6} y\right\rangle\right\rangle$ | $\langle 2,8\rangle\langle 13,6\rangle\langle 6,13\rangle$ | [12,11] | 15 |
|  | $\left\langle\left\langle y, g^{11} x+g^{12} y, g^{12} x+g^{11} y\right\rangle\right\rangle$ | $\langle 11,12\rangle\langle 12,11\rangle\langle 3,14\rangle$ | $[4,1]$ | 15 |
| (5) | $\left\langle\left\langle y, g^{5} x+g^{10} y, g^{10} x+g^{5} y\right\rangle\right\rangle$ | $\langle 5,10\rangle\langle 10,5\rangle\langle 5,10\rangle$ | [10,5] | 5 |
|  | $\left\langle\left\langle y, g^{10} x+g^{5} y, g^{5} x+g^{10} y\right\rangle\right\rangle$ | $\langle 10,5\rangle\langle 5,10\rangle\langle 10,5\rangle$ | [5,10] | 5 |
| $\mathcal{B}_{\boldsymbol{x}}^{\prime}$ : |  |  |  |  |
| (3) | $\left\langle\left\langle y, x, g^{12} x+g^{11} y\right\rangle\right\rangle$ | $\langle 12,11\rangle$ | [11,12] | 15 |
| (4) | $\left\langle\left\langle y, g^{11} x+g^{12} y, g^{14} x+g^{3} y\right\rangle\right\rangle$ | $\langle 11,12\rangle\langle 14,3\rangle\langle 13,6\rangle$ | [14,3] | 15 |
|  | $\left\langle\left\langle y, g^{7} x+g^{9} y, g^{6} x+g^{13} y\right\rangle\right)$ | $\langle 7,9\rangle\langle 6,13\rangle\langle 1,4\rangle$ | [3,14] | 15 |
|  | $\left\langle\left\langle y, g^{3} x+g^{14} y, g^{9} x+g^{7} y\right\rangle\right)$ | $\langle 3,14\rangle\langle 9,7\rangle\langle 2,8\rangle$ | [13,6] | 15 |
| $\mathcal{B}_{\boldsymbol{x}}^{\prime \prime}$ : |  |  |  |  |
| (3) | $\left\langle\left\langle y, x, g^{13} x+g^{6} y\right\rangle\right\rangle$ | $\langle 13,6\rangle$ | [6,13] | 15 |
| (4) | $\left\langle\left\langle y, g^{14} x+g^{3} y, g^{3} x+g^{14} y\right\rangle\right\rangle$ | $\langle 14,3\rangle\langle 3,14\rangle\langle 12,11\rangle$ | [1,4] | 15 |
|  | $\left\langle\left\langle y, g^{2} x+g^{8} y, g^{11} x+g^{12} y\right\rangle\right\rangle$ | $\langle 2,8\rangle\langle 11,12\rangle\langle 1,4\rangle$ | [7,9] | 15 |
|  | $\left\langle\left\langle y, g^{7} x+g^{9} y, g^{9} x+g^{7} y\right\rangle\right\rangle$ | $\langle 7,9\rangle\langle 9,7\rangle\langle 6,13\rangle$ | [8,2] | 15 |

where $y \in F \backslash\{x\}$ and the forms of parts 1,2 and 5 in $\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}$ and $\mathcal{B}_{x}^{\prime \prime}$ are the same (of course, these triples are distinct: part 1-trivial, part 2-by Lemma 4.2.2 and part 5-by Lemma 4.3.1). This construction of a $L T T S(18)$ has been verified in detail by use of the computer.

It is regrettable that even though the way, pointed by Theorem 4.4.1, seems feasible, up to now we have not been able to find a suitable general method to choose these parameters in the theorem. The value of our work lies in that:
i) We give a possible way to construct $\operatorname{LTTS}\left(2^{2 n}+2\right)$ that most likely will work in general, and indeed give some successful examples.
ii) In cases where an $\operatorname{LTTS}\left(2^{2 n}+2\right)$ was known already, our system may be nonisomorphic to the known system. For example, the only
previously known $L T T S(18)$ is the one constructed in [LinSt]. It is not difficult to show that $\operatorname{LTTS}(18)$ is nonisomorphic to our $\operatorname{LTTS}(18)$ (see also $\S 2.6$ ).
iii) The methods employed in Lemma 4.2.2 and 4.3.1 are useful for other design problems.

Finally, we give another sufficiency theorem. It is only for $\operatorname{LTTS}\left(2^{4}+\right.$ 2), but this idea can perhaps be generalized.

Theorem 4.4.2. If $\mu_{1}+\mu_{2}=2^{4}-1$ and $3 \nmid \mu_{1}$, then $3 \mid \lambda_{1}$ or $3 \mid \lambda_{2}$ (suppose $3 \mid \lambda_{2}$ ). The following arrangement of the parameters will satisfy all conditions in Theorem 4.4.1.

$$
\begin{aligned}
& \left\{\beta_{i}\right\}_{i=1}^{3}=\left\{2 \mu_{1}, 2 \lambda_{2},-\lambda_{1}\right\},\left\{\delta_{i}\right\}_{i=1}^{3}=\left\{-2 \lambda_{2}, \lambda_{2}, \lambda_{1}\right\}, \\
& \left\{\beta_{i}^{\prime}\right\}_{i=1}^{3}=\left\{2 \lambda_{1}, \lambda_{2},-2 \lambda_{1}\right\},\left\{\delta_{i}^{\prime}\right\}_{i=1}^{3}=\left\{2 \lambda_{2},-\lambda_{2},-\lambda_{1}\right\}, \\
& \left\{\beta_{i}^{\prime \prime}\right\}_{i=1}^{3}=\left\{2 \mu_{1}, 2 \lambda_{2},-2 \lambda_{1}\right\}\left(\text { or }\left\{\lambda_{1},-\lambda_{2}, \lambda_{2}\right\}\right), \\
& \left.\left\{\delta^{\prime \prime}{ }_{i}^{3}\right\}_{i=1}^{3}=\left\{-2 \mu_{1},-2 \lambda_{2}, \lambda_{1}\right\} \text { (or }\left\{2 \mu_{1}, 2 \lambda_{2},-\lambda_{1}\right\}\right) . \\
& \text { where the two sets for } \beta_{i}^{\prime \prime} \text { and } \delta_{i}^{\prime \prime} \text { are one-to-one. }
\end{aligned}
$$

Proof. Firstly, we point out that for any $n$ the condition $\mu_{1}+\mu_{2}=$ $2^{2 n}-1$ implies $\lambda_{1}-\mu_{1}=\lambda_{2}$ and $\lambda_{2}-\mu_{2}=\lambda_{1}$. For $2 n=4$, there are four such $\left\langle\lambda_{1}, \mu_{1}\right\rangle-\left\langle\lambda_{2}, \mu_{2}\right\rangle$ :

$$
\langle 4,1\rangle-\langle 3,14\rangle,\langle 2,8\rangle-\langle 9,7\rangle,\langle 8,2\rangle-\langle 6,13\rangle,\langle 1,4\rangle-\langle 12,11\rangle
$$

where the primitive element $g$ of $F_{16}^{*}$ satisfies $g^{4}+g+1=0$. By the conditions we have $5 \lambda_{2} \equiv 0, \lambda_{1} \equiv 4 \mu_{1}$ and $4 \lambda_{1} \equiv \mu_{1}\left(\bmod 2^{4}-1\right)$. It is easy to see that the elements

$$
\pm \lambda_{1}, \pm 2 \lambda_{1}, \pm \lambda_{2}, \pm 2 \lambda_{2}, \mu_{1}, \mu_{2}, 2 \mu_{1} \text { and } 2 \mu_{2}
$$

exactly are all elements of the set $Z_{15}^{*} \backslash\{\theta, 2 \theta\}$, where $\theta=\frac{2^{4}-1}{3}=$ 5. According to the given arrangement of the parameters, we can give the following construction (Only for Parts 3, 4 and their PC and TC. As for Part 2, its PC is same: $\left\langle\lambda_{1}, \mu_{1}\right\rangle$ and $\left.<\lambda_{2}, \mu_{2}\right\rangle$ ):

| $\mathcal{B}_{x}$ : part 3 | $\left\langle 2 \lambda_{2}, 2 \mu_{2}\right\rangle$ | [ $2 \mu_{2}, 2 \lambda_{2}$ ] |
| :---: | :---: | :---: |
|  | $p^{\left(2 \lambda_{1}, 2 \mu_{1}\right\rangle}\left\langle-2 \lambda_{1},-2 \lambda_{2}\right\rangle\left\langle-2 \lambda_{2},-2 \lambda_{1}\right\rangle$ | $\left[2 \lambda_{2}, 2 \mu_{2}\right]$ |
| part 4 | $\begin{cases}\left(2 \mu_{2}, 2 \lambda_{2}\right\rangle & \left\langle\mu_{2}, \lambda_{2}\right) \quad\left\langle-\lambda_{1},-\lambda_{2}\right\rangle\end{cases}$ | $\left[\lambda_{1}, \mu_{1}\right]$ |
|  | $\left(-\lambda_{2},-\lambda_{1}\right)\left\langle\mu_{1}, \lambda_{1}\right\rangle \quad, \quad\left(2 \mu_{1}, 2 \lambda_{1}\right\rangle$ | $\left[\mu_{1}, \lambda_{1}\right]$ |
| $\mathcal{B}_{x}^{\prime}: \mathbf{p a r t} 3$ | (2 $\lambda_{1}, 2 \mu_{1}$ ) | [ $2 \mu_{1}, 2 \lambda_{1}$ ] |
|  | $\int^{\left(2 \mu_{1}, 2 \lambda_{1}\right\rangle} \quad\left\langle 2 \mu_{2}, 2 \lambda_{2}\right\rangle \quad\left\langle 2 \lambda_{2}, 2 \mu_{2}\right)$ | $\left[-\lambda_{2},-\lambda_{1}\right]$ |
| part 4 | $\left\{\begin{array}{l}\left(\mu_{2}, \lambda_{2}\right\rangle\end{array} \quad\left(-\lambda_{1},-\lambda_{2}\right\rangle\left\langle-2 \lambda_{1},-2 \lambda_{2}\right)\right.$ | $\left[-\lambda_{1},-\lambda_{2}\right]$ |
|  | ( $\left(-2 \lambda_{2},-2 \lambda_{1}\right\rangle\left\langle-\lambda_{2},-\lambda_{1}\right\rangle\left\langle\mu_{1}, \lambda_{1}\right)$ | $\left[\mu_{2}, \lambda_{2}\right]$ |
| $\mathcal{B}_{x}^{\prime \prime}$ : part 3 | (2 $\left.\mu_{1}, 2 \lambda_{1}\right)$ | [ $2 \lambda_{1}, 2 \mu_{1}$ ] |
|  | $\left(\begin{array}{ll}\left(2 \lambda_{1}, 2 \mu_{1}\right\rangle & \left(2 \lambda_{2}, 2 \mu_{2}\right)\end{array} \quad\left(-\lambda_{2},-\lambda_{1}\right)\right.$ | [ $2 \lambda_{2}, 2 \mu_{2}$ ] |
| part 4 | $\left\{\left(2 \mu_{2}, 2 \lambda_{2}\right\rangle \quad\left(-2 \lambda_{1},-2 \lambda_{3}\right\rangle\left\langle m u_{2}, \lambda_{2}\right\rangle\right.$ | $\left[-2 \lambda_{1},-2 \lambda_{2}\right]$ |
|  | $\left(\left\langle-2 \lambda_{2},-2 \lambda_{1}\right\rangle\left\langle\mu_{1}, \lambda_{1}\right\rangle \quad\left\langle-\lambda_{1},-\lambda_{2}\right\rangle[\right.$ | $\left[-2 \lambda_{2},-2 \lambda_{1}\right]$ |

here, we give two solutions: $\left(\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}, \mathcal{B}_{x}^{\prime \prime}\right)$ and $\left(\mathcal{B}_{x}, \mathcal{B}_{x}^{\prime}, \hat{\mathcal{B}}_{x}^{\prime \prime}\right)$. One can easily verify that both are indeed $\operatorname{LTTS}(18)$.

Examples. By the theorem, we have the following eight $\operatorname{LTTS}(18)$, where only the second coordinate of the PC and TC are written down.


## V. Steiner triple systems

5.1 Introduction. A Steiner triple system of order $v$ (briefly $S T S(v)$ ) on the set $S$ is a pair $(S, \mathcal{B})$, where $|S|=v$ and $\mathcal{B}$ is a set of 3 -subsets of $S$ (called triples) such that any two elements of $S$ are contained in exactly one triple of $\mathcal{B}$. This kind of design was introduced by W.S.B. Woolhouse (1844) and J. Steiner (1853). T.P. Kirkman (1847) and M. Reiss (1859) independently proved the following existence theorem:

There exists a $S T S(v)$ if and only if $v \equiv 1$ or $3(\bmod 6)$.
Two $S T S(v)$ on the same set $S$ are said to be disjoint if they have no triples in common. If there exist $v-2$ pairwise disjoint $S T S(v)$, then we call them a large set of disjoint $S T S(v)$ and denote the collection by $L S T S(v)$, The research work on the existence of $L S T S(v)$ 's has a long history. Many mathematicians, such as T.P. Kirkman, J.J. Sylvester, A. Cayley, J. Doyen, A. Kotzig, R.H.F. Denniston, S. Schreiber, R.M. Wilson, T. Teirlinck, A. Rosa made constributions to this problem, see [Ki2], [Sy], [Ca], [Do], [KLR], [De], [Sch], [Wi1], [Tei1], [Ro]. In 1983, a Chinese teacher of physics at a middle school, Lu Jiaxi, announced the following result $[\mathrm{Lu}]$, which is the best up to now:

For $v \equiv 1$ or $3(\bmod 6), v>7$ and $v \notin\{141,283,501,789,1501,2365\}$, there exists an $L S T S(v)$.
For the remaining unknown six orders, he has once given an imaginative method to solve them. But, it is unfortunate that he died shortly before realizing his idea.

In this chapter, our purpose is to make some efforts towards solving the remaining existence problem of $L S T S(v)$ 's. Our work includes two aspects. First, in $\S 5.2$ and $\S 5.3$, we will discuss the possibility to construct $\operatorname{LSTS}(p+2$ ) for an odd prime $p \neq 3$ (note: 139, 281, 499, 787 and 1499 are all prime). And, in $\S 5.4$ and $\S 5.5$, we will give some results about $L D$ designs, introduced by Lu Jiaxi and playing an important rôle in his imaginative method.

Although, at present, we have not found a construction of $\operatorname{LSTS}(v)$ for the remaining six orders $v$, it is most likely possible, and our method is useful for getting some nonisomorphic $L S T S(v)$ from known ones and for further research.
5.2 A way to construct $L S T S\left(p^{n}+2\right)$.

Let $F$ be a finite field containing $p^{n}$ elements, where $p$ is an odd prime number, $p \neq 3$ and $n$ is a positive integer. Its zero and unity
elements are denoted by 0 and 1 , respectively. Let $g$ be a primitive element of $F^{*}=F \backslash\{0\}$ and define elements $\infty_{1}, \infty_{2} \notin F$. Let $R=$ $Z_{p^{n}-1}=\left\{0,1, \ldots, p^{n}-2\right\}$ be the residue class ring modulo ( $p^{n}-1$ ). Below denote $m=\frac{p^{n}-1}{2}$ and $g^{\theta}=2(\theta \in R)$. Note $g^{m}=-1$.

Similar to §2.4.1, a couple (denoted by $\alpha C \beta$-unordered, or $\langle\alpha, \beta\rangle-$ ordered) means $g^{\alpha}+g^{\beta}=1$ and $\alpha, \beta \in R^{*}=R \backslash\{0\}$. We have:
(CP1) If $\alpha C \beta$ then $\alpha \neq \beta$ except if $\alpha=\beta=-\theta$ (call $(-\theta) C(-\theta)$ single couple).
(CP2) If $\alpha C \beta$ then $\beta C \alpha,(m+\alpha-\beta) C(-\beta),(-\alpha) C(m+\beta-\alpha)$ and ( $\left.p^{t} \alpha\right) C\left(p^{t} \beta\right)$ for an arbitrary positive integer $t$.
(CP3) If $\alpha C \beta$ and $\gamma C \delta$ then $(\alpha-\lambda) C(\gamma-\mu),(\mu-\gamma) C(\alpha-\gamma)$ and $(\gamma-\alpha) C(\lambda-\alpha)$, where $\lambda=\operatorname{ind}(\alpha+\delta, m+\beta+\gamma), \mu=\operatorname{ind}(m+\alpha+\delta, \beta+\gamma)$. (For the symbol ind $(*, *)$ see §2.4.1.)

Fix an element $x \in F$. For an (unordered) pair $\{y, z\}$ of distinct elements in $F \backslash\{x\}$, similar to $\S 2.4 .1$, we can write $z=g^{\alpha} x+g^{\beta} y$, where $\alpha C \beta$. Moreover, $y=g^{m+\alpha-\beta} x+g^{-\beta} z$. Then we say that the pair $\{y, z\}$ over $F \backslash\{x\}$ belongs to the pair class (PC)

$$
\left\{\begin{array}{r}
<\alpha, \beta> \\
<m+\alpha-\beta,-\beta>
\end{array}\right\}
$$

(briefly $\left\{\begin{array}{c}\beta \\ -\beta\end{array}\right\}$, the two couples are unordered). When $\beta=-\beta$, i.e. $\beta=\frac{p^{n}-1}{2}=m$ (the corresponding $\alpha=\theta$ ), call $\left\{\begin{array}{l}m \\ m\end{array}\right\}$ half pair class (HPC).
Lemma 5.2.1. For a given element $x \in F$,
(1) Each (unordered) pair of distinct elements of $F \backslash\{x\}$ belongs to a uniquely determined PC. The total number of the PC's is $\frac{p^{n}-3}{2}+1$ (one of them is the HPC). The HPC contains $\frac{p^{n}-1}{2}$ pairwise distinct pairs, and each other PC contains $p^{n}-1$ pairwise distinct pairs.
(2) For a so-called $y$-triple $\left(y, g^{\alpha} x+g^{\beta} y, g^{\gamma} x+g^{\delta} y\right)$, where $y \in F \backslash\{x\}$, $\alpha C \beta, \gamma C \delta$ and $\alpha \neq \gamma$, its three pairs belong to $P C:\left\{\begin{array}{r}\beta \\ -\beta\end{array}\right\},\left\{\begin{array}{r}\delta \\ -\delta\end{array}\right\}$ and $\left\{\begin{array}{l}\beta-\delta \\ \delta-\beta\end{array}\right\}$, respectively.

For a so-called $\infty$-triple $\left(\infty_{j}, y, g^{\alpha} x+g^{\beta} y\right)$ or $x$-triple $\left(x, y, g^{\alpha} x+g^{\beta} y\right)$, where $j=1,2$, only one among its three pairs, i.e. $\left(y, g^{\alpha} x+g^{\beta} y\right)$, belongs to the $P C\left\{\begin{array}{r}\beta \\ -\beta\end{array}\right\}$.

Proof. We only need to show that, for the sets of ordered pairs,

$$
\left\{\left(y, g^{\alpha} x+g^{\beta} y\right) ; y \in F \backslash\{x\}\right\} \cap\left\{\left(g^{\alpha} x+g^{\beta} y, y\right) ; y \in F \backslash\{x\}\right\} \neq \phi
$$

$$
\text { if and only if }\left\{\begin{array}{r}
\beta \\
-\beta
\end{array}\right\} \text { is the HPC. }
$$

In fact, if there are $y, y^{\prime} \in F \backslash\{x\}$ such that $y=g^{\alpha} x+g^{\beta} y^{\prime}$ and $g^{\alpha} x+$ $g^{\beta} y=y^{\prime}$, then $y=g^{\alpha} x+g^{\beta}\left(g^{\alpha} x+g^{\beta} y\right)$, this implies $g^{\alpha}\left(1+g^{\beta}\right)(x-y)=0$. But $y \neq x, g^{\alpha} \neq 0$, so $g^{\beta}=-1, \beta=m$, i.e., $\left\{\begin{array}{c}\beta \\ -\beta\end{array}\right\}=\left\{\begin{array}{l}m \\ m\end{array}\right\}$ is a HPC. The converse is trivial. All other conclusions can be seen from Lemma 2.4.1.

For a triple ( $u, v, w$ ) of distinct elements in $F$, similar to $\S 2.4 .1$ we can write $v=g^{\alpha} u+g^{\beta} v$, where $\alpha C \beta$. Moreover, we have also $w=$ $g^{-\beta} v+g^{m+\alpha-\beta} u$ and $u=g^{m+\beta-\alpha} w+g^{-\alpha} v$. Then we say the triple ( $u, v, w$ ) belongs to the triple class (TC)

$$
\left[\begin{array}{l}
\langle\alpha, \beta\rangle\langle-\beta, m+\alpha-\beta\rangle\langle m+\beta-\alpha,-\alpha\rangle \\
\langle\beta, \alpha\rangle\langle m+\alpha-\beta,-\beta\rangle\langle-\alpha, m+\beta-\alpha\rangle
\end{array}\right] \text {. }
$$

Note that its first row has property ( T ) of $\S 2.4 .1$ (but the six couples are unordered).

## Lemma 5.2.2.

(1) There are three types of TC:

$$
\begin{gathered}
A T C:\left[\begin{array}{l}
\left\langle\frac{m}{3},-\frac{m}{3}\right\rangle\left\langle\frac{m}{3},-\frac{m}{3}\right\rangle\left\langle\frac{m}{3},-\frac{m}{3}\right\rangle \\
\left\langle-\frac{m}{3}, \frac{m}{3}\right\rangle\left\langle-\frac{m}{3}, \frac{m}{3}\right\rangle\left\langle-\frac{m}{3}, \frac{m}{3}\right\rangle
\end{array}\right] ; \\
B T C:\left[\begin{array}{l}
\langle\theta, m\rangle<m, \theta\rangle<-\theta,-\theta\rangle \\
\langle m, \theta\rangle\langle\theta, m\rangle\langle-\theta,-\theta\rangle
\end{array}\right] ; \\
C T C:\left[\begin{array}{l}
\langle\alpha, \beta\rangle\langle-\beta, m+\alpha-\beta\rangle\langle m+\beta-\alpha,-\alpha\rangle \\
\langle\beta, \alpha\rangle\langle m+\alpha-\beta,-\beta\rangle\langle-\alpha, m+\beta-\alpha\rangle
\end{array}\right] .
\end{gathered}
$$

When $p^{n} \equiv 1(\bmod 6)$, the total number of ATC, BTC and CTC is 1 , 1 and $\frac{p^{n}-7}{6}$, respectively. When $p^{n} \equiv 5(\bmod 6)$, the total number of $A T C, B T C$ and $C T C$ is 0,1 and $\frac{p^{n}-5}{6}$.
(2) Each triple of distinct elements in $F$ belongs to uniquely determined TC. Each ATC contains $\frac{n^{n}\left(\rho^{n}-1\right)}{3}$ pairwise distinct triples; each

BTC contains $\frac{p^{n}\left(p^{n}-1\right)}{2}$ pairwise distinct triples; and each CTC contains $p^{n}\left(p^{n}-1\right)$ pairwise distinct triples.
(3) The $y$-triple $\left(y, g^{\alpha} x+g^{\beta} y, g^{\gamma} x+g^{\delta} y\right.$ ) belongs to $T C$

$$
\left[\begin{array}{l}
<\alpha-\lambda, \gamma-\mu><\mu-\gamma, \alpha-\gamma><\gamma-\alpha, \lambda-\alpha> \\
<\gamma-\mu, \alpha-\lambda><\alpha-\gamma, \mu-\gamma><\lambda-\alpha, \gamma-\alpha>
\end{array}\right]
$$

where $\lambda=$ ind $(\alpha+\delta, m+\beta+\gamma)$ and $\mu=\operatorname{ind}(m+\alpha+\delta, \beta+\gamma)$. And the $x$-triple ( $x, y, g^{\alpha} x+g^{\beta} y$ ) belongs to $T C$

$$
\left[\begin{array}{l}
<m+\alpha-\beta,-\beta><\beta, \alpha><-\alpha, m+\beta-\alpha> \\
<-\beta, m+\alpha-\beta><\alpha, \beta><m+\beta-\alpha,-\alpha>
\end{array}\right] .
$$

Proof. First, we point out that for an odd prime $p \neq 3$ and a positive integer $n$ always $p^{n} \equiv \pm 1(\bmod 6)($ since $p \equiv \pm 1(\bmod 6))$.
(1) For a TC

$$
\left[\begin{array}{l}
<\alpha, \beta><-\beta, m+\alpha-\beta><m+\beta-\alpha,-\alpha> \\
<\beta, \alpha><m+\alpha-\beta,-\beta><-\alpha, m+\beta-\alpha>
\end{array}\right] .
$$

we consider two special cases:
i) If there are two equal couples in the $T C$ 's first row, then

$$
\left\{\begin{array}{l}
\alpha=-\beta, \beta=m+\alpha-\beta \longrightarrow \alpha=-\frac{m}{3}, \beta=\frac{m}{3} ; \text { or } \\
\alpha=m+\beta-\alpha, \beta=-\alpha \longrightarrow \alpha=\frac{m}{3}, \beta=-\frac{m}{3} ; \text { or } \\
-\beta=m+\beta-\alpha, m+\alpha-\beta=-\alpha \longrightarrow \beta=m+2 \alpha \longrightarrow \\
g^{\alpha}-g^{2 \alpha}=1 \longrightarrow g^{3 \alpha}=-1 \longrightarrow \alpha= \pm \frac{m}{3}\left(\beta=\mp \frac{m}{3}\right) .
\end{array}\right.
$$

These all give ATC and only for $p^{n} \equiv 1(\bmod 6)$, since $3 \mid m$ and $m=$ $\frac{p^{n}-1}{2}$.
ii) If there are two such couples that $\langle\lambda, \mu\rangle$ and $\langle\mu, \lambda\rangle$ in the $T C$ 's first row, then

$$
\left\{\begin{array}{l}
\beta=-\beta, \alpha=m+\alpha-\beta \longrightarrow 2 \beta=0 \longrightarrow \beta=m(\alpha=\theta) ; \\
\beta=m+\beta-\alpha, \alpha=-\alpha \longrightarrow 2 \alpha=0 \longrightarrow \alpha=m(\beta=\theta) \\
-\beta=-\alpha, m+\alpha-\beta=m+\beta-\alpha \longrightarrow \alpha=\beta \longrightarrow \alpha=\beta=-\theta .
\end{array}\right.
$$

These all give BTC and only one.
Except i) and ii) all other TC are called CTC (its six couples are pairwise different).

Since each ATC (or BTC, or CTC) consists of two (or three, or six) distinct couples, and the total number of the ordered couples is $p^{n}-2$, we have the conclusion about $T C$ 's number.
(2) For $(u, w) \neq\left(u^{\prime}, w^{\prime}\right)$ if $\left(u, g^{\alpha} u+g^{\beta} w, w\right)=\left(u^{\prime}, g^{\alpha} u+g^{\prime} \beta w^{\prime}, w^{\prime}\right)$ then we have the following five possibilities:
i) $u=u^{\prime}, g^{\alpha} u+g^{\beta} w=w^{\prime}, w=g^{\alpha} u+g^{\prime} \beta w^{\prime} \longrightarrow\left(g^{\beta}+1\right)\left(w-w^{\prime}\right)=$ $0 \longrightarrow g^{\boldsymbol{\theta}}=-1 \longrightarrow \beta=m$;
ii) $w=w^{\prime}, g^{\alpha} u+g^{\beta} w=u^{\prime}, u=g^{\alpha} u^{\prime}+g^{\beta} w^{\prime} \longrightarrow\left(g^{\alpha}+1\right)\left(u-u^{\prime}\right)=$ $0 \longrightarrow g^{\alpha}=-1 \longrightarrow \alpha=m$;
iii) $u=w^{\prime}, w=u^{\prime}, g^{\alpha} u+g^{\beta} w=g^{\alpha} u^{\prime}+g^{\beta} w^{\prime} \longrightarrow\left(g^{\alpha}-g^{\beta}\right)(u-w)=$ $0 \longrightarrow g^{\alpha}=g^{\beta} \longrightarrow \alpha=\beta=-\theta$;
iv) $u=g^{\alpha} u^{\prime}+g^{\beta} w^{\prime}, g^{\alpha} u+g^{\beta} w=w^{\prime}, w=u^{i} \longrightarrow\left(g^{\alpha+\beta}-1\right) u+\left(g^{\alpha}+\right.$ $\left.g^{2 \beta}\right) w=0 \longrightarrow\left(g^{2 \beta}-g^{\beta}+1\right)(w-u)=0 \longrightarrow g^{2 \beta}-g^{\beta}+1=0 \longrightarrow \beta=$ $\pm \frac{m}{3}$;
v) $u=w^{\prime}, g^{\alpha} u+g^{\beta} w=u^{\prime}, w=g^{\alpha} u^{\prime}+g^{\beta} w^{\prime} \longrightarrow\left(g^{\alpha+\beta}-1\right) w+\left(g^{2 \alpha}+\right.$ $\left.g^{\beta}\right) u=0 \longrightarrow\left(g^{2 \alpha}-g^{\alpha}+1\right)(u-w)=0 \longrightarrow g^{2 \alpha}-g^{\alpha}+1=0 \longrightarrow \alpha= \pm \frac{m}{3}$. The cases i), ii) and iii) give BTC, and the cases iv) and v) give ATC.

As there are $p^{n}\left(p^{n}-1\right)$ ordered pairs ( $u, w$ ) of distinct elements in $F$, each CTC (which does not touch upon anyone of $i$ )-v)) contains $p^{n}\left(p^{n}-1\right)$ distinct triples. For ATC, by iv) and v), the ordered pairs $(u, w),\left(w, g^{\alpha} u+g^{\beta} w\right)$ and $\left(g^{\alpha} u+g^{\beta} w, u\right)$ give the same triples, where $\langle\alpha, \beta\rangle=\left\langle\frac{m}{3},-\frac{m}{3}\right\rangle$ or $\left\langle-\frac{m}{3}, \frac{m}{3}\right\rangle$. So, each ATC contains $\frac{p^{n}\left(p^{n}-1\right)}{3}$ distinct triples. For BTC, by i) (or ii), or iii)) the ordered pairs ( $u, w$ ) and ( $u, g^{\alpha} u+g^{\beta} w$ ) (or ( $g^{\alpha} u+g^{\beta} w, w$ ), or ( $w, u$ )) give the same triples, where $\langle\alpha, \beta\rangle=\langle\theta, m\rangle$ (or $\langle m, \theta\rangle$, or $\langle-\theta,-\theta\rangle$ ). So, each BTC contains $\frac{p^{n}\left(p^{n}-1\right)}{2}$ distinct triples.
(3) Similar to the proof of Lemma 2.4 .2 (3).

For brevity, we can denote the ATC, BTC and CTC (using the simple symbol of the PC) by

$$
\left[\left\{\begin{array}{c}
\frac{m}{3} \\
-\frac{m}{3}
\end{array}\right\}\right],\left[\left\{\begin{array}{c}
m \\
m
\end{array}\right\},\left\{\begin{array}{c}
\theta \\
-\theta
\end{array}\right\}\right] \text { and }\left[\left\{\begin{array}{c}
\alpha \\
-\alpha
\end{array}\right\},\left\{\begin{array}{c}
\beta \\
-\beta
\end{array}\right\},\left\{\begin{array}{c}
m+\alpha-\beta \\
m+\beta-\alpha
\end{array}\right\}\right],
$$

respectively. By definition, each ATC (or BTC, or CTC) consists of one (or two, or three) different PC, and consists of two (or three, or six) different numbers. Furthermore, we can say that each PC belongs to a unique TC. The table below gives all couples and TC for $p^{\boldsymbol{n}} \leq 25$
$(p \neq 2,3)$.

| $p^{n}$ $(g)$ | Couples | ATC | BTC | CTC |
| :---: | :---: | :---: | :---: | :---: |
| $p=5$ $(g=2)$ | ${ }_{1} C_{2} \quad{ }_{3} C_{3}$ |  | [ $\left.\left\{_{2}^{2}\right\},\left\{\begin{array}{l}1 \\ 3\end{array}\right\}\right]$ |  |
| $p=7$ $(g=3)$ | ${ }_{1} C_{5} \quad{ }_{2} C_{3}{ }_{4} C_{4}$ | [ $\left.\left.\begin{array}{l}1 \\ 5\end{array}\right\}\right]$ | $\left[\left\{\begin{array}{l}3 \\ 3\end{array}\right\},\left\{\begin{array}{l}2 \\ 4\end{array}\right\}\right]$ |  |
| $p=11$ $(g=2)$ | $\begin{array}{lll} \hline & { }_{1} C_{5} & { }_{2} C_{3} \\ { }_{4} C_{7} & { }_{6} C_{8} & \\ \hline \end{array} C_{9} .$ |  | [ $\left.\left\{\begin{array}{l}5 \\ 5\end{array}\right\},\left\{\begin{array}{l}1 \\ 9\end{array}\right\}\right]$ | $\left[\left\{\begin{array}{l}2 \\ 8\end{array}\right\},\left\{\begin{array}{l}3 \\ 7\end{array}\right\},\left\{\begin{array}{l}4 \\ 6\end{array}\right\}\right]$ |
| $p=13$ $(g=2)$ | $\begin{array}{lll} \hline{ }^{1} C_{6} & { }_{2} C_{10} & { }_{3} C_{5} \\ { }_{4} C_{7} & { }_{8} C_{9} & { }_{11} C_{11} \\ \hline \end{array}$ | $\left[\left\{\begin{array}{l}2 \\ 10\end{array}\right\}\right]$ | $\left.\left[\begin{array}{l}6 \\ 6\end{array}\right\},\left\{\begin{array}{l}1 \\ 11\end{array}\right\}\right]$ | $\left.\left[\begin{array}{l}3 \\ 9\end{array}\right\},\left\{\begin{array}{l}4 \\ 8\end{array}\right\},\left\{\begin{array}{l}5 \\ 7\end{array}\right\}\right]$ |
| $p=17$ $(g=3)$ | $\begin{array}{rrrr}  & & { }_{1} C_{6} & { }_{2} C_{2} \\ { }_{3} C_{10} & { }_{4} C_{5} & { }_{7} C_{111} \\ { }_{8} C_{14} & { }_{9} C_{12} & { }_{13} C_{15} \\ \hline \end{array}$ |  | $\left[\left\{\begin{array}{l}8 \\ 8\end{array}\right\},\left\{\begin{array}{l}2 \\ 14\end{array}\right\}\right]$ | $\left.\begin{array}{c} {\left[\begin{array}{c} 1 \\ 18 \end{array}\right\},\left\{\begin{array}{l} 3 \\ 13 \end{array}\right\},\left\{\begin{array}{l} 6 \\ \hline 6 \end{array}\right\}} \\ {\left[\left\{\begin{array}{l} 1 \\ 12 \end{array}\right\},\left\{\begin{array}{l} 5 \\ 11 \end{array}\right\},\left\{\begin{array}{l} 7 \\ 7 \end{array}\right\}\right.} \end{array}\right]$ |
| $p=19$ $(g=2)$ | $\begin{array}{ccc}{ }_{1} C_{9} & { }_{2} C_{4} & { }_{3} C_{15} \\ { }_{5} C_{6} & { }_{7} C_{14} & { }_{8} C_{12}\end{array}$ ${ }_{10} C_{13} \quad{ }_{11} C_{16} \quad{ }_{17} C_{17}$ | $\left[\left\{\begin{array}{l}3 \\ 15\end{array}\right\}\right]$ | [ $\left.\left.{ }_{9}^{9}\right\},\left\{\begin{array}{l}1 \\ 17\end{array}\right\}\right]$ | $\left.\begin{array}{l} {\left[\left\{\begin{array}{l} 2 \\ 16 \end{array}\right\},\left\{\begin{array}{l} 4 \\ 14 \end{array}\right\},\left\{\begin{array}{l} 7 \\ 11 \end{array}\right]\right.} \\ {\left[\left\{\begin{array}{l} 5 \\ 13 \end{array}\right\},\left\{\begin{array}{l} 6 \\ 12 \end{array}\right\},\left\{\begin{array}{l} 8 \\ 10 \end{array}\right\}\right.} \end{array}\right]$ |
| ( $\begin{gathered}p=23 \\ (g=5)\end{gathered}$ |  |  | $\left[\left\{\begin{array}{l}11 \\ 11\end{array}\right\},\left\{\begin{array}{l}2 \\ 20\end{array}\right\}\right]$ |  |
| $\left(\begin{array}{c}p=25 \\ \left(g^{2}=9+3\right)\end{array}\right.$ | ${ }_{1} C_{5}$ ${ }_{2} C_{3}$ ${ }_{4} C_{20}$ <br> ${ }_{6} C_{12}$ ${ }_{7} C_{9}$ ${ }_{8} C_{19}$ <br> ${ }_{10} C_{15}$ ${ }_{11} C_{21}$ ${ }_{13} C_{22}$ <br> ${ }_{14} C_{17}$ ${ }_{16} C_{23}$ ${ }_{18} C_{18}$ |  | $\left[\left\{\begin{array}{l}11 \\ 11\end{array}\right\},\left\{\begin{array}{l}2 \\ 20\end{array}\right\}\right]$ |  |

Now, we can give an arrangement to construct $\operatorname{LSTS}\left(p^{n}+2\right)=\{(F \cup$ $\left.\left.\left\{\infty_{1}, \infty_{2}\right\}, \mathcal{B}_{x}\right) \mid x \in F\right\}$, where $\mathcal{B}_{x}$ contains the following triples (where $y \in F \backslash\{x\}$ and (\#) denote the number of triples)

| (TRIPLE) | (PC) | (TC) | (\#) |
| :---: | :---: | :---: | :---: |
| $\left(\infty_{1}, \infty_{2}, x\right)$ |  |  | 1 |
| $\left(\infty_{1}, y, g^{\lambda} x+g^{\mu} y\right)$ | $\left\{\begin{array}{c}\mu \\ -\mu\end{array}\right\}$ |  | $\frac{p^{n}-1}{2}$ |
| $\left(\infty_{2}, y, g^{\lambda} x+g^{\mu} y\right)$ | $\left\{\begin{array}{l}\mu \\ \mu \\ -\mu\end{array}\right\}$ |  | $\frac{p^{n}-1}{2}$ |
| $\left(x, y, g^{\theta} x+g^{m} y\right)$ | $\left\{\begin{array}{l}m \\ m\end{array}\right\}$ | ${ }^{B T C}$ | $\frac{n^{2}-1}{2}$ |
| $\left(y, g^{\alpha_{i}} x+g^{\beta_{i}} y, g^{\gamma_{i}} x+g^{\delta_{i}} y\right.$ ) | $\left\{\begin{array}{c}\beta_{i} \\ -\beta_{i}\end{array}\right\},\left\{\begin{array}{c}\delta_{i} \\ \delta_{i} \\ \delta_{i}\end{array}\right\}$, | (CTC) | $t\left(p^{n}-1\right)$ |
| $\left(y, g^{\alpha} x+g^{\frac{3 m}{3}} y, g^{\alpha+\frac{m}{3}} x+g^{\frac{4 m}{3}} y\right)$ | \{ $\frac{\frac{2 m}{\frac{2 m}{m}} \frac{1}{3}}{}$ | atc | $\frac{p^{n}-1}{3}$ |

where $\lambda C \mu, \alpha_{i} C \beta_{i}, \gamma_{i} C \delta_{i}, \alpha C \frac{2 m}{3}, 1 \leq i \leq t, t=\frac{p^{n}-7}{6}$ or $\frac{p^{n}-5}{6}$ (if $p^{n} \equiv 1$ or $-1(\bmod 6))$, and there is part 5 only if $p^{n} \equiv 1(\bmod 6)$. The total number of triples in each $B_{x}$ is $1+\frac{2}{3}\left(p^{n}-1\right)+\frac{p^{n}-5}{6}\left(p^{n}-1\right)=\frac{\left(p^{n}+1\right)\left(p^{n}+2\right)}{6}$, which is exactly as expected.

## About Part 2.

Considering the pairs containing an element $\infty\left(\infty_{1}\right.$ or $\left.\infty_{2}\right)$, the construction of part 2 must meet such condition that all pairs $\left\{y, g^{\lambda} x+g^{\mu} y\right\}$ should be a partition of the set $F \backslash\{x\}$, for the selected $\frac{p^{n}-1}{2} y$. So, by the expression (*) in the proof of Lemma 4.2.2 (which still holds for $G F\left(p^{n}\right)$ ), we need that

$$
k=\frac{p^{n}-1}{\text { g.c.d. }\left(\mu, p^{n}-1\right)} \equiv 0 \quad(\bmod 2) .
$$

If the condition is satisfied, let $y_{0}^{(j)}, y_{1}^{(j)}, \ldots, y_{k-1}^{(j)}\left(1 \leq j \leq \frac{p^{n}-1}{k}\right)$ be all numbers in $F \backslash\{x\}$, where $y_{i+1}^{(j)}=g^{\lambda} x+g^{\mu} y_{i}^{(j)}(0 \leq i \leq k-2)$. Then the following construction of part 2 will be alright:

$$
\begin{array}{r}
\left(\infty_{1}, y_{2 i}^{(j)}, y_{2 i+1}^{(j)}\right) \text { and }\left(\infty_{2}, y_{2 i+1}^{(j)}, y_{2 i+2}^{(j)}\right) \\
0 \leq i \leq \frac{k-2}{2}, 1 \leq j \leq \frac{p^{n}-1}{k}
\end{array}
$$

These triples will exactly contain all pairs $\left\{\infty_{1}, y\right\},\left\{\infty_{2}, y\right\}$ (where $y \in$ $F \backslash\{x\}$ ) and all pairs belonging the pair class $\left\{\begin{array}{c}\mu \\ -\mu\end{array}\right\}$.

## About Part 3.

By the same reason (for the pairs containing $x$ ), for the selected $\frac{p^{n}-1}{2}$ $y$, all pairs $\left\{y, g^{\theta} x+g^{m} y\right\}$ should also be a partition of the set $F \backslash\{x\}$. And since $m=\frac{p^{n}-1}{2}$ and $\frac{p^{n}-1}{g . c . d .\left(m, p^{n}-1\right)}=2$, this condition holds. Let $y_{0}^{(j)}, y_{1}^{(j)}\left(1 \leq j \leq \frac{p^{n}-1}{2}\right)$ be all numbers in $F \backslash\{x\}$, where $y_{1}^{(j)}=g^{\theta} x+$ $g^{m} y_{0}^{(j)}$ (and also $y_{0}^{(j)}=g^{\theta} x+g^{m} y_{1}^{(j)}$ ). Then the triples $\left(x, y_{0}^{(j)}, y_{1}^{(j)}\right)$ and $\left(x, y_{1}^{(j)}, y_{0}^{(j)}\right)$ are identical. So, if we select these triples (to form the part 3):

$$
\left(x, y_{0}^{(j)}, y_{1}^{(j)}\right) \quad 1 \leq j \leq \frac{p^{n}-1}{2}
$$

then they will contain all pairs $\{x, y\}$ (where $y \in F \backslash\{x\}$ ) and all pairs belonging to the half pair class $\left\{\begin{array}{c}m \\ m\end{array}\right\}$. And the triples of part 2 in $\underset{x \in F}{ } \mathcal{B}_{x}$ will be exactly all triples in the unique $B T C$ :

$$
\left[\begin{array}{l}
\langle\theta, m\rangle\langle m, \theta\rangle\langle-\theta,-\theta\rangle \\
\langle m, \theta\rangle\langle\theta, m\rangle\langle-\theta,-\theta\rangle
\end{array}\right] .
$$

## About Part 5.

Firstly, we show that if $\alpha C \frac{2 m}{3}$ then $\left(\alpha+\frac{m}{3}\right) C \frac{4 m}{3}$. In fact, since $g^{\alpha}+g^{\frac{2 m}{3}}=1$, we have $g^{\alpha+\frac{m}{3}}+g^{m}=g^{\frac{m}{3}}$, but $g^{m}=-1$ thus $g^{\alpha+\frac{m}{3}}-g^{\frac{m}{3}}=$ 1 , i.e., $g^{\alpha+\frac{m}{3}}+g^{\frac{4 m}{3}}=1$. Obviously, the triple contains three same PC $\left\{\begin{array}{c}\frac{2 m}{3} \\ \frac{4 m}{3}\end{array}\right\}$ and belongs the unique $A T C$ :

$$
\left[\begin{array}{l}
\left.\left\langle\frac{m}{3},-\frac{m}{3}\right\rangle<\frac{m}{3},-\frac{m}{3}><\frac{m}{3},-\frac{m}{3}\right\rangle \\
\left.\left\langle-\frac{m}{3}, \frac{m}{3}\right\rangle<-\frac{m}{3}, \frac{m}{3}><-\frac{m}{3}, \frac{m}{3}\right\rangle
\end{array}\right] .
$$

Note that $\frac{2 m}{3}=\frac{p^{n}-1}{3}$, so $\frac{p^{n}-1}{\text { g.c.d. }\left(\frac{2 m}{3}, p^{n}-1\right)}=3$. By the above, all numbers in $F \backslash\{x\}$ can be denoted $y_{0}^{(j)}, y_{1}^{(j)}, y_{2}^{(j)}\left(1 \leq j \leq \frac{p^{n}-1}{3}\right)$, where $y_{i+1}^{(j)}=$ $g^{\alpha} x+g^{\frac{2 m}{3}} y_{i}^{(j)}\left(i=0,1,2\right.$ and $\left.y_{3}^{(j)}=y_{0}^{(j)}\right)$. Moreover, we have yet $y_{2}^{(j)}=g^{\alpha+\frac{m}{3}} x+g^{\frac{4 m}{3}} y_{0}^{(j)}$ (see the expression (*) in the proof of Lemma 4.2.2). Therefore, if we select these triples (to construct the part 5):

$$
\left(y_{0}^{(j)}, y_{1}^{(j)}, y_{2}^{(j)}\right) \quad 1 \leq j \leq \frac{p^{n}-1}{3},
$$

then they will contain all pairs belonging the pair class $\left\{\begin{array}{c}\frac{2 m}{3} \\ \frac{4 m}{3}\end{array}\right\}$. And the triples of part 5 in $\bigcup_{x \in F} \mathcal{B}_{x}$ will be exactly all triples in that ATC.

### 5.3 A sufficient condition and examples.

Now, through the analysis in the last section, our main task will be the choice of those parameters in part 4.
Denote $\tilde{R}=\{1,2, \ldots, m-1\} \subset R=Z_{p^{n-1}}=\left\{0,1,2, \ldots, p^{n}-2\right\}$, where $m=\frac{\mathbf{p}^{n}-1}{2}$. For $\lambda \in R^{*}=R \backslash\{0\}$, denote $\tilde{\lambda}=\min \{\lambda,-\lambda\}$. Obviously, $\tilde{\lambda} \in \tilde{R}$.
Theorem 5.3.1. When $p^{n} \equiv 1$ (or -1) mod 6, if there exist two $t$ subsets $\left\{\beta_{i}\right\}_{i},\left\{\delta_{i}\right\}_{i}$ of $R^{*} \backslash\left\{m, \frac{2 m}{3}, \frac{4 m}{3}\right\}$ (or $R^{*} \backslash\{m\}$ ), $t=\frac{p^{n}-7}{6}$ (or $\frac{\mathbf{p}^{n}-5}{6}$ ), such that the following conditions are satisfied, then there exists $a n \operatorname{LSTS}\left(p^{n}+2\right)$.
(1) $\left\{\tilde{\beta}_{i}\right\}_{i},\left\{\tilde{\delta}_{i}\right\}_{i}$ and $\left\{\beta_{i} \sim \delta_{i}\right\}_{i}$ are pairwise disjoint $t$-subsets of the set $\tilde{R} \backslash\left\{\frac{2 m}{3}\right\}$ (or $\tilde{R}$ ).
(2) Let $\{\tilde{\mu}\} \cup\left\{\tilde{\beta}_{i}\right\}_{i=1}^{t} \cup\left\{\tilde{\delta}_{i}\right\}_{i=1}^{t} \cup\left\{\beta_{i} \sim \delta_{i}\right\}_{i=1}^{t}=\tilde{R} \backslash\left\{\frac{2 m}{3}\right\}$ (or $\tilde{R}$ ), then $\frac{p^{n}-1}{\text { g.c.d. }\left(\bar{\mu}, \bar{P}^{n}-1\right)}$ is even.
(3) All numbers of the set $\left\{\alpha_{i}-\gamma_{i}\right\}_{i}$ belong to different CTC, where $\alpha_{i} C \beta_{i}$ and $\gamma_{i} C \delta_{i}(1 \leq i \leq t)$.

Proof. When we, according to the arrangement given in the last section, make use of these chosen parameters $\beta_{i}, \delta_{i}$ (and $\alpha_{i}, \gamma_{i}$ ) to construct $\operatorname{LSTS}\left(2^{n}+2\right)$, the condition (1) will ensure the balance of all PC (see Lemma 5.2.1), the condition (2) will ensure the success of the part 2 (see "About Part 2") and the condition (3) will ensure the balance of all TC (see Lemma 5.2.2).

## Example 1.

$p=13, g=2, \mathrm{PC}$ and TC see Table ( $\S 5.2$ ).
$\operatorname{LSTS}(15)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F_{13}, \mathcal{B}_{x}\right) \mid x \in F_{13}\right\}, \mathcal{B}_{x}$ consists of following triples (where $y \in F_{13} \backslash\{x\}$ and the symbol (\#) denotes the number of triples, for the selection method of parts 2,3 and 5 see $\S 5.2$ ):

|  |  | (PC) | (TC) | (\#) |
| :---: | :---: | :---: | :---: | :---: |
| (1) | $\left(\infty_{1}, \infty_{2}, x\right)$ |  |  | 1 |
| (2) | $\left(\infty_{1}, y, g^{3} x+g^{5} y\right)$ | $\left\{\begin{array}{l}5 \\ 7\end{array}\right\}$ |  | 6 |
|  | $\left(\infty_{2}, y, g^{3} x+g^{5} y\right)$ | $\left\{{ }_{7}^{5}\right\}$ |  | 6 |
|  | $\left(x, y, g x+g^{6} y\right)$ | $\left\{\begin{array}{l}6 \\ 6\end{array}\right\}$ | $\left.\left[\begin{array}{l}6 \\ 6\end{array}\right\},\left\{\begin{array}{l}1 \\ 1\end{array}\right\}\right]$ | 6 |
|  | $\left.y, g^{2} x+g^{10} y, g^{6} x+g y\right)$ | $\left\{\begin{array}{c}10 \\ 2\end{array}\right\}\left\{\begin{array}{l}11 \\ 11\end{array}\right\}$ | $\left[\left\{\begin{array}{l}3 \\ 9\end{array}\right\},\left\{\begin{array}{l}4 \\ 8\end{array}\right\},\left\{\begin{array}{l}5 \\ 7\end{array}\right]\right.$ | 12 |
|  | , $, g^{7} x+g^{4} y, g^{9} x+g^{8} y$ ) | $\left\{\begin{array}{l}4 \\ 8\end{array}\right\}$ | $\left[\left\{\begin{array}{l}2 \\ 10\end{array}\right\}\right]$ | 4 |

There is still another construction for $L S T S(15)$.

|  |  | (PC) | (TC) | (\#) |
| :---: | :---: | :---: | :---: | :---: |
| (1) | $\left(\infty_{1}, \infty_{2}, x\right)$ |  |  | 1 |
| (2) | $\left(\infty_{1}, y, g^{6} x+g y\right)$ | $\left\{\begin{array}{l}1 \\ 11\end{array}\right\}$ |  | 6 |
|  | $\left(\infty_{2}, y, g^{6} x+g y\right)$ | $\left\{\begin{array}{l}1 \\ 11\end{array}\right\}$ |  | 6 |
| (3) | $\left(x, y, g x+g^{6} y\right.$ ) | $\left\{{ }_{6}^{6}\right\}$ | $\left[\left\{\begin{array}{l}6 \\ 6\end{array}\right\},\left\{\begin{array}{l}1 \\ 11\end{array}\right]\right.$ | 6 |
|  | , $g^{4} x+g^{7} y, g^{8} x+g^{9} y$ ) | $\left\{\begin{array}{l}7 \\ 5\end{array}\right\}\left\{\begin{array}{l}\text { 9 }\end{array}\right\}\left\{\begin{array}{l}10 \\ 2\end{array}\right\}$ | $\left[\left\{\begin{array}{l}3 \\ 9\end{array}\right\},\left\{\begin{array}{l}4 \\ 8\end{array}\right\},\left\{\begin{array}{l}5 \\ 7\end{array}\right\}\right.$ | 12 |
|  | , $g^{7} x+g^{4} y, g^{9} x+g^{8} y$ ) | $\left\{\begin{array}{l}4 \\ 8\end{array}\right\}$ | [ $\left.\left\{\begin{array}{l}2 \\ 10\end{array}\right\}\right]$ | 4 |

In the construction by us each $S T S(15)$ is not resolvable, so it is nonisomorphic to the known $\operatorname{LSTS}(15)$ (by [De] using computer), which is a large set of disjoint $K T S(15)$. Moreover, our construction is also nonisomorphic to another known $\operatorname{LSTS}(15)$ (see [Tei2]), since our one has that character mentioned in $\S 2.6$, but his construction satisfies $\mathcal{B}_{i}=$ $\mathcal{B}_{0}+i$ for all $i \in F_{13}$ (let the $\operatorname{LSTS}(15)=\left\{B_{i} ; i \in F_{13}\right\}$ ).

## Example 2.

$p=31, g=3$
$1 \mathrm{C} 9,2 \mathrm{C} 27,3 \mathrm{C} 20,4 \mathrm{C} 11,5 \mathrm{C} 25,6 \mathrm{C} 6,7 \mathrm{C} 21,8 \mathrm{C} 19,10 \mathrm{C} 28,12 \mathrm{C} 13$, $14 \mathrm{C} 17,15 \mathrm{C} 24,16 \mathrm{C} 18,22 \mathrm{C} 26,23 \mathrm{C} 29$
$\operatorname{LSTS}(33)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F_{31}, \mathcal{B}_{x}\right) \mid x \in F_{31}\right\}, \mathcal{B}_{x}$ consists of the following triples (where $y \in F_{31} \backslash\{x\}$ and $j=1,2$ ):

|  | (PC) | (TC) | (\#) |
| :---: | :---: | :---: | :---: |
| (1) $\left(\infty_{1}, \infty_{2}, x\right)$ |  |  | 1 |
| (2) $\left(\infty_{j}, y, g^{4} x+g^{11} y\right)$ | $\left\{\begin{array}{l}11 \\ 19\end{array}\right\}$ |  | 30 |
| (3) $\left(x, y, g^{24} x+g^{15} y\right)$ | $\left\{\begin{array}{l}15 \\ 15 \\ 15\end{array}\right\}$ | $\left[\left\{\begin{array}{l}6 \\ 24\end{array}\right\},\left\{\begin{array}{l}15 \\ 15\end{array}\right\}\right]$ | 15 |
| (4) $\left(y, g^{7} x+g^{21} y, g^{14} x+g^{17} y\right)$ | $\left\{\begin{array}{c}21 \\ 9\end{array}\right\}\left\{\begin{array}{c}17 \\ 13\end{array}\right\}\left\{\begin{array}{c}4 \\ 26\end{array}\right\}$ | $\left[\left\{\begin{array}{c}1 \\ 29\end{array}\right\},\left\{\begin{array}{c}7 \\ 23\end{array}\right\},\left\{\begin{array}{l}9 \\ 21\end{array}\right\}\right]$ | 30 |
| $\left(y, g^{6} x+g^{6} y, g^{26} x+g^{22} y\right)$ | $\left\{\begin{array}{c}6 \\ 64 \\ 27\end{array}\right\}\left\{\begin{array}{l}22 \\ 8\end{array}\right\}\left\{\begin{array}{l}14 \\ 16\end{array}\right\}$ | $\left[\left\{\begin{array}{c}2 \\ 28\end{array}\right\},\left\{\begin{array}{c}3 \\ 37 \\ 27\end{array}\right\},\left\{\begin{array}{c}10 \\ 20 \\ 20\end{array}\right\}\right]$ | 30 |
| $\left(y, g^{2} x+g^{27} y, g^{10} x+g^{28} y\right)$ | $\left.\left\{\begin{array}{c}24 \\ 3\end{array}\right\}\left[\begin{array}{c}28 \\ 2\end{array}\right\} \begin{array}{c}16 \\ 1 \\ 1\end{array}\right\}$ | $\left[\left\{\begin{array}{l}4 \\ 26\end{array}\right\},\left\{\begin{array}{c}8 \\ 22\end{array}\right\},\left\{\begin{array}{l}11 \\ 19\end{array}\right\}\right]$ | 30 |
| $\left(y, g^{21} x+g^{7} y, g^{5} x+g^{25} y\right)$ | $\left\{\begin{array}{c}7 \\ 23\end{array}\right\}\left\{\begin{array}{c}25 \\ 5\end{array}\right\}\left\{\begin{array}{l}12 \\ 18\end{array}\right\}$ | $\left[\left\{\begin{array}{l}12 \\ 18\end{array}\right\},\left\{\begin{array}{l}13 \\ 17\end{array}\right\},\left\{\begin{array}{l}14 \\ 16\end{array}\right\}\right]$ | 30 |
| (5) $\left(y, g^{28} x+g^{10} y, g^{3} x+g^{20} y\right)$ | $\left\{\begin{array}{l}10 \\ 20\end{array}\right\}$ | $\left[\left\{\begin{array}{l}5 \\ 25\end{array}\right\}\right]$ | 10 |

For $\operatorname{LSTS}(33)$, we have still three other solutions. For brevity, below we will only write down part 2,4 (part $1,3,5$ are the same as above), and for triples $\left(\infty_{j}, y, g^{\lambda} x+g^{\mu} y\right)$ and $\left(y, g^{\alpha} x+g^{\beta} y, g^{\gamma} x+g^{\delta} y\right)$ denote by $\langle\lambda, \mu\rangle$ and $\langle\alpha, \beta\rangle\langle\gamma, \delta\rangle$, for $\mathrm{PC}\left\{\begin{array}{c}\beta \\ -\beta\end{array}\right\}$ denote by $\{\bar{\beta}\}$, where $\bar{\beta}=\min \{\beta,-\beta\}$, for TC (which consists of some PC) use similar symbol.

The second $L S T S(33)$ :
(2) $\quad\langle 21,7\rangle$
(4) $\langle 13,12\rangle\langle 20,3\rangle$
\{7\}
$\langle 6,6\rangle(26,22)$
$\langle 4,11\rangle\langle 12,13\rangle$
$\langle 11,4)\langle 25,5\rangle$

| $\{12\}\{3\}\{9\}$ | $[1,7,9]$ |
| :---: | :---: |
| $\{6\}\{8\}\{14\}$ | $[2,3,10]$ |
| $\{11\}\{13\}\{2\}$ | $[4,8,11]$ |
| $\{4\}\{5\}\{1\}$ | $[12,13,14]$ |

The third $\operatorname{LSTS}(33)$ :

| $(2)$ | $\langle 1,9\rangle$ | $\{9\}$ |  |
| :---: | :---: | :---: | :---: |
| (4) | $\langle 15,24\rangle(22,26\rangle$ | $\{6\}\{4\}\{2\}$ | $[1,7,9]$ |
|  | $\langle 9,1\rangle\langle 29,23\rangle$ | $\{1\}\{7\}\{8\}$ | $[2,3,10]$ |
|  | $\langle 5,25\rangle\langle 13,12\rangle$ | $\{5\}\{12\}\{13\}$ | $[4,8,11]$ |
|  | $\langle 18,16\rangle\langle 2,27\rangle$ | $\{14\}\{3\}\{11\}$ | $[12,13,14]$ |

The fourth $L S T S(33)$ :

| (2) | $\langle 1,9\rangle$ | $\{9\}$ |  |
| :---: | :---: | :---: | :---: |
| (4) | $\langle 20,3)\langle 27,2\rangle$ | $\{3\}\{2\}\{1\}$ | $[1,7,9]$ |
|  | $\langle 6,6\rangle(26,22\rangle$ | $\{6\}\{8\}\{14\}$ | $[2,3,10]$ |
|  | $\langle 5,25\rangle\langle 13,12\rangle$ | $\{5\}\{12\}\{13\}$ | $[4,8,11]$ |
|  | $(8,19\rangle\langle 22,26\rangle$ | $\{11\}\{4\}\{7\}$ | $[12,13,14]$ |

## Example 3.

$p=37, g=2$
$1 \mathrm{C} 18,2 \mathrm{C} 8,3 \mathrm{C} 14,4 \mathrm{C} 31,5 \mathrm{C} 27,6 \mathrm{C} 30,7 \mathrm{C} 22,9 \mathrm{C} 32,10 \mathrm{C} 11,12 \mathrm{C} 28$, $13 \mathrm{C} 15,16 \mathrm{C} 21,17 \mathrm{C} 25,19 \mathrm{C} 26,20 \mathrm{C} 23,24 \mathrm{C} 34,29 \mathrm{C} 33,35 \mathrm{C} 35$
$\operatorname{LSTS}(39)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F_{37}, \mathcal{B}_{x}\right) \mid x \in F_{37}\right\}, \mathcal{B}_{x}$ consists of the following triples:

The first solution:

| $(1)$ | $\left(\infty_{1}, \infty_{2}, x\right)$ |  |  | 1 |
| :---: | :---: | :---: | :---: | :---: |
| (2) | $\langle 25,17\rangle$ | $\{17\}$ |  | 36 |
| (3) | $(1,18\rangle$ | $\{18\}$ | $[1,18]$ | 18 |
| $(4)$ | $\langle 8,2)\langle 20,23\rangle$ | $\{2\}\{13\}\{15\}$ | $[2,8,12]$ | 36 |
|  | $\langle 3,14\rangle(10,11\rangle$ | $\{14\}\{11\}\{3\}$ | $[3,7,14]$ | 36 |
|  | $\langle 4,31\rangle(31,4\rangle$ | $\{5\}\{4\}\{9\}$ | $[4,5,9]$ | 36 |
|  | $(6,30\rangle(23,20\rangle$ | $\{6\}\{16\}\{10\}$ | $[10,11,17]$ | 36 |
|  | $(2,8\rangle\langle 18,1\rangle$ | $\{8\}\{1\}\{7\}$ | $[13,15,16]$ | 36 |
| (5) | $\langle 28,12\rangle\langle 34,24\rangle$ | $\{12\}$ | $[6]$ | 12 |

The second solution:

| $(2)$ | $\langle 15,13\rangle$ | $\{13\}$ |  |
| :---: | :---: | :---: | :---: |
| (4) | $\langle 13,15\rangle\langle 25,17\rangle$ | $\{15\}\{17\}\{2\}$ | $[2,8,12]$ |
|  | $\langle 3,14\rangle\langle 10,11\rangle$ | $\{14\}\{11\}\{3\}$ | $[3,7,14]$ |
|  | $(4,31\rangle\langle 31,4\rangle$ | $\{5\}\{4\}\{9\}$ | $[4,5,9]$ |
|  | $\langle 6,30\rangle\langle 23,20\rangle$ | $\{6\}\{16\}\{10\}$ | $[10,11,17]$ |
|  | $(2,8\rangle\langle 18,1\rangle$ | $\{8\}\{1\}\{7\}$ | $[13,15,16]$ |

The third solution:

| (2) | $\langle 15,13\rangle$ | $\{13\}$ |  |
| :---: | :---: | :---: | :---: |
| (4) | $\langle 18,1\rangle(30,6\rangle$ | $\{1\}\{6\}\{5\}$ | $[2,8,12]$ |
|  | $(3,14\rangle\langle 10,11\rangle$ | $\{14\}\{11\}\{3\}$ | $[3,7,14]$ |
|  | $\langle 11,10\rangle\langle 2,8)$ | $\{10\}\{8\}\{2\}$ | $[4,5,9]$ |
|  | $\langle 5,27\rangle(22,7\rangle$ | $\{9\}\{7\}\{16\}$ | $[10,11,17]$ |
|  | $\langle 9,32\rangle(25,17\rangle$ | $\{4\}\{17\}\{15\}$ | $[13,15,16]$ |

## Example 4.

$p=79, g=3$
1C43, 2C51, 3C77, 4C39, 5C23, 6C60, 7C38, 8C40, 9C29, 10C76, $11 \mathrm{C} 22,12 \mathrm{C} 14,13 \mathrm{C} 65,16 \mathrm{C} 24,17 \mathrm{C} 20,18 \mathrm{C} 63,19 \mathrm{C} 49,21 \mathrm{C} 55,25 \mathrm{C} 30$, 26C33, 27C68, 28C56, 31C54, 32C45, 34C48, 35C75, 36C58, 37C64,

41C66, 42C61, 44C53, 46C52, 47C62, 50C67, 57C73, 59C69, 70C71, 74C74
$\operatorname{LSTS}(81)=\left\{\left(\left\{\infty_{1}, \infty_{2}\right\} \cup F_{79}, \mathcal{B}_{x}\right) ; x \in F_{79}\right\}, \mathcal{B}_{x}$ consists of the following triples:

| $(1)$ | $\left(\infty_{1}, \infty_{2}, x\right)$ |  |  | 1 |
| :---: | :---: | :---: | :---: | :---: |
| (2) | $\langle 35,75\rangle$ | $\{3\}$ |  | 78 |
| (3) | $\langle 4,39\rangle$ | $\{39\}$ | $[4,39]$ | 39 |
| (4) | $\langle 11,22\rangle\langle 8,40\rangle$ | $\{22\}\{38\}\{18\}$ | $[1,3,35]$ | 78 |
|  | $\langle 1,43\rangle\langle 69,59\rangle$ | $\{35\}\{19\}\{16\}$ | $[2,10,27]$ | 78 |
|  | $\langle 2,51\rangle\langle 23,5\rangle$ | $\{27\}\{5\}\{32\}$ | $[5,21,23]$ | 78 |
|  | $\langle 3,77\rangle\langle 66,41\rangle$ | $\{1\}\{37\}\{36\}$ | $[6,15,18]$ | 78 |
|  | $\langle 9,29\rangle\langle 17,20\rangle$ | $\{29\}\{20\}\{9\}$ | $[7,8,38]$ | 78 |
|  | $\langle 15,72\rangle\langle 34,48\rangle$ | $\{6\}\{30\}\{24\}$ | $[9,19,29]$ | 78 |
|  | $\langle 26,33\rangle\langle 54,31\rangle$ | $\{33\}\{31\}\{2\}$ | $[11,22,28]$ | 78 |
|  | $\langle 37,64\rangle\langle 74,74\rangle$ | $\{14\}\{4\}\{10\}$ | $[12,14,37]$ | 78 |
|  | $\langle 13,65\rangle\langle 44,53\rangle$ | $\{13\}\{25\}\{12\}$ | $[16,24,31]$ | 78 |
|  | $\langle 20,17\rangle\langle 56,28\rangle$ | $\{17\}\{28\}\{11\}$ | $[17,20,36]$ | 78 |
|  | $\langle 21,55\rangle\langle 55,21\rangle$ | $\{23\}\{21\}\{34\}$ | $[25,30,34]$ | 78 |
|  | $\langle 40,8\rangle\langle 72,15\rangle$ | $\{8\}\{15\}\{7\}$ | $[26,32,33]$ | 78 |
| (5) | $\langle 33,26\rangle\langle 46,52\rangle$ | $\{26\}$ | $[13]$ | 26 |

### 5.4 About LD designs.

In the third paper of [Lu], for constructing LSTS, Lu Jiaxi introduced a kind of auxiliary design-LD design, which played an important role in his work. And, by his imagination, the designs will be able to solve the LSTS problem for the remaining six orders. Besides, in our opinion, it is also worth investigating the LD designs as a new kind of combinatorial design.

Let $\boldsymbol{X}$ be a set of $n$ elements. We call a collection consisting of $n+2$ sets $\mathcal{L}^{1}, \mathcal{L}^{2}$ and $\mathcal{L}_{x}(x$ runs over $X$ ) a LD design of order $n$ and denote it by $L D(n)=L D[X]=\left\{\mathcal{L}^{1}, \mathcal{L}^{2}, \mathcal{L}_{x} \mid x \in X\right\}$, if the following conditions (C1)-(C5) are satisfied:
(C1) Each $\mathcal{L}_{x}$ consists of ordered triples of the set $X \backslash\{x\}$. Each $\mathcal{L}^{j}$ ( $j=1,2$ ) consists of ordered quadruples of the set $X$.
(C2) For any $x \in X,\left(F_{4}^{*} \times(X \backslash\{x\}), \mathcal{G}_{x}, \mathcal{A}_{x}\right)$ forms a transversal design $T(3, n-1)$, where $\mathcal{G}_{x}=\left\{\{z\} \times(X \backslash\{x\}) \mid z \in F_{4}^{*}\right\}, \mathcal{A}_{x}=\left\{\left\{\left(g^{0}, x_{0}\right),\left(g^{1}, x_{1}\right.\right.\right.$ $\left.\left.),\left(g^{2}, x_{2}\right)\right\} \mid\left(x_{0}, x_{1}, x_{2}\right) \in \mathcal{L}_{x}\right\}$ and $g$ is a fixed primitive element of $F_{4}^{*}$ (so $F_{4}=\left\{0, g^{0}, g^{1}, g^{2}\right\}$ ).
(C3) For any $j \in\{1,2\},\left(F_{4} \times X, \mathcal{G}, \mathcal{A}^{j}\right)$ forms a transversal design $T(4, n)$, where $\mathcal{G}=\left\{\{z\} \times X \mid z \in F_{4}\right\}$ and $\mathcal{A}^{j}=\left\{\left\{\left(g^{0}, x_{0}\right),\left(g^{1}, x_{1}\right),\left(g^{2}\right.\right.\right.$, $\left.\left.\left.x_{2}\right),\left(0, x_{3}\right)\right\} \mid\left(x_{0}, x_{1}, x_{2}, x_{3}\right) \in \mathcal{L}^{j}\right\}$.
(C4) There exists an element $c_{0} \in X$ such that ( $x, x, x, c_{0}$ ) belongs to $\mathcal{L}^{j}$, for arbitrary $x \in X$ and $j \in\{1,2\}$
(C5) For any ordered triple ( $x_{0}, x_{1}, x_{2}$ ) of the set $X$, either there exists $x$ such that $\left(x_{0}, x_{1}, x_{2}\right) \in \mathcal{L}_{x}$, or there exist $x_{3}$ and $j$ such that $\left(x_{0}, x_{1}, x_{2}, x_{3}\right) \in \mathcal{L}^{j}$.
By definition, it is a kind of design that consists of several transversal designs having a certain balanced connection. By the equivalency between the transversal design and the orthogonal Latin squares, the definition can be stated as:
$L D(n)=L D[X]=\left\{A^{1}, A^{2}, A_{x} ; x \in X\right\}$, where $X=\{0,1,2, \ldots, n-$ 1) and
i) Each $A_{x}$ is an $n \times n$ array $\left(a_{s t}^{x}\right)_{0}^{n-1}$ with $a_{s x}^{x}=a_{x t}^{x}=\infty(o \leq s, t \leq$ $n-1)$ and $\tilde{A_{x}}=\left(a_{a t}^{x}\right)_{s \neq x, t \neq x}$ is a Latin square over $X \backslash\{x\}$.
ii) Each $A^{j}=\left(\alpha_{s t}^{j}\right)_{0}^{n-1}(j=1,2)$ is an idempotent Latin square over $X$ having $n$ disjoint transversals.
iii) For any $s, t \in X,\left\{a_{s t}^{x}\right\}_{x \in X} \cup\left\{\alpha_{s t}^{j}\right\}_{j_{\in\{1,2\}}}=X \cup\{\infty\}$, where the element $\infty$ appears twice (if $s \neq t$ ) or element $x$ appears twice (if $s=t=x$ ).
It is easy to verify the equivalence of both definitions. Here we only point out that

$$
\begin{gathered}
A_{x}=\left(a_{s t}^{x}\right) \text { if and only if } \mathcal{L}_{x}=\left\{\left(s, t, a_{s t}^{x}\right)\right\}, \\
A^{j}=\left(\alpha_{s t}^{j}\right) \text { if and only if } \mathcal{L}^{j}=\left\{\left(s, t, \alpha_{s t}^{j}, *\right)\right\},
\end{gathered}
$$

where $\alpha_{a t}^{j}$ belongs to the $k$ th transversal.
As an example, we give $L D(4)=L D[X](X=\{0,1,2,3\})$ :

$$
\begin{aligned}
& A_{0}=\left[\begin{array}{cccc}
\infty & \infty & \infty & \infty \\
\infty & 3 & 2 & 1 \\
\infty & 2 & 1 & 3 \\
\infty & 1 & 3 & 2
\end{array}\right], A_{1}=\left[\begin{array}{cccc}
2 & \infty & 0 & 3 \\
\infty & \infty & \infty & \infty \\
0 & \infty & 3 & 2 \\
3 & \infty & 2 & 0
\end{array}\right], \\
& A_{2}=\left[\begin{array}{cccc}
3 & 1 & \infty & 0 \\
1 & 0 & \infty & 3 \\
\infty & \infty & \infty & \infty \\
0 & 3 & \infty & 1
\end{array}\right], A_{3}=\left[\begin{array}{cccc}
1 & 0 & 2 & \infty \\
0 & 2 & 1 & \infty \\
2 & 1 & 0 & \infty \\
\infty & \infty & \infty & \infty
\end{array}\right], \\
& A^{1}=\left[\begin{array}{llll}
0 & 3 & 1 & 2 \\
2 & 1 & 3 & 0 \\
3 & 0 & 2 & 1 \\
1 & 2 & 0 & 3
\end{array}\right], A^{2}=\left[\begin{array}{llll}
0 & 2 & 3 & 1 \\
3 & 1 & 0 & 2 \\
1 & 3 & 2 & 0 \\
2 & 0 & 1 & 3
\end{array}\right] .
\end{aligned}
$$

A class of special $L D$ designs, $L D^{*}$ designs, was also introduced by Lu. The $L D^{*}$ design satisfies besides (C1)-(C5) the condition:
(C6) $\left(F_{4} \times X, \mathcal{G}, \mathcal{A}^{0}\right)$ forms a transversal design $T(4, n)$, where $\mathcal{G}$ is as in (C3) and $\mathcal{A}^{0}=\left\{\left\{\left(g^{0}, x_{0}\right),\left(g^{1}, x_{1}\right),\left(g^{2}, x_{2}\right),\left(0, x_{3}\right)\right\} ;\left(x_{0}, x_{2}, x_{3}, *\right) \in\right.$ $\left.\mathcal{L}^{1},\left(x_{1}, x_{2}, x_{3}, *^{\prime}\right) \in \mathcal{L}^{2}\right\}$.

The main use of the $L D$ design for $L S T S$ designs is the following theorem (see [Lu] III, Theorem 1):

If there exist both an $L D(n)$ and an $L S T S(n+2)$, then there exists an $L S T S(3 n)$ also. (**)

Of course, for giving full play to the theorem's rôle, one must investigate the existence of $L D$ designs. All known results about $L D$ and $L D^{*}$ designs in [Lu] are listed as follows:
(1) For any positive integer $\alpha>1$, there exists an $L D^{*}\left(2^{\alpha}\right)$.
(2) For $n \equiv 5(\bmod 8)$, there exists an $L D(n)$. For $n=5$ even an $L D^{*}(n)$ exists.
(3) For $n \equiv 7(\bmod 12)$, there exists an $L D(n)$. For $n=7,19$ even an $L D^{*}(n)$ exists.
(4) For $n \equiv 11(\bmod 12)$ except $n=23,47,59,83,107,167,179,227$, $263,299,347,383,719,767,923$ and 1439, there exists an $L D(n)$. For $n=11$ even an $L D^{*}(n)$ exists.
(5) If there exist both an $L D^{*}\left(n_{1}\right)$ and an $L D\left(n_{2}\right)$, then there exists an $L D\left(n_{1} n_{2}\right)$.
(6) For odd prime $p$ and positive integer $\alpha$, if there exists an $L D\left(p^{\alpha}\right)$ then there exists an $L D\left(3 p^{\alpha}\right)$.
(7) For prime power $q>4$ and positive integer $n$, if there exists an $L D(1+n)$ then there exists an $L D(1+q n)$.
(8) For odd prime power $q \geq 7$ and $0 \leq t \leq 2^{r-1}-3(r>2)$, if there exist both an $L D(1+q)$ and an $L D(1+(q-1) t)$ then there exists an $L D\left(1+(q-1) t+2^{r} q\right)$.
(9) For odd prime power $q, q^{\prime} \geq 7$ and $0 \leq t \leq\left(2^{r-1}-3\right)\left(q^{\prime}-3\right)$ ( $r>2$ ), if there exist both an $L D\left(1+q q^{\prime}\right)$ and an $L D(1+(q-1) t)$ then there exists an $L D\left(1+(q-1) t+2^{r} q q^{\prime}\right)$.
(10) For $n=2,3,6$ there does not exist an $L D(n)$.

By these conclusions, there are 33 unknown orders in $n \leq 110$ for $L D(n)$. And there are only 9 known orders for these same $n$ for $L D^{*}(n)$. We have done some study for the designs and give the following results:
(A) For $n>1$, if there exists an $L D(n)$, then there exists an $L D(3 n)$.
(B) For prime power $q>4$ and $n \neq 6$, if there exists an $L D^{*}(1+n)$ then there exists an $L D^{*}(1+q n)$.
(C) If there exist both an $L D^{*}(m)$ and a symmetric $L D^{*}(n)$ then there exists an $L D^{*}(m n)$, where the symmetric condition means ( $i_{0}, i_{1}, i_{2}, i_{3}$ )
$\in \mathcal{L}^{1}$ if and only if $\left(i_{1}, i_{0}, i_{2}, i_{3}\right) \in \mathcal{L}^{2}\left(\right.$ let $L D^{*}(n)=\left\{\mathcal{L}^{1}, \mathcal{L}^{2}, \mathcal{L}_{x} ; x \in\right.$ $\left.I_{n}\right\}$ ).
By (A), which construction and proof will be shown in next section, we will get a lot of new orders for $L D$, for example $12,24,48,66,72,89$, $102,108, \ldots$. Therefore, the remaining unknown orders less than 110 will be only $9,10,14,17,18,23,26,27,30,38,41,42,46,47,54,59,62,68$, $73,74,83,86,90,98$ and 107. And, by (B) and (C), the known orders for $L D^{*}$ will be extended, for instance the number of known orders for $n \leq 110$ has grown to 50 from 9 .

Finally, to show the imaginative way by Lu Jiaxi to construct the $L S T S(v)$ for the remaining six orders $v$, we give the following concepts.
Let $L D(n)=\left\{\mathcal{L}^{1}, \mathcal{L}^{2}, \mathcal{L}_{x} ; x \in X\right\}$ and $L D(m)=\left\{\hat{\mathcal{L}^{1}}, \hat{\mathcal{L}^{2}}, \hat{\mathcal{L}_{x}} ; x \in \hat{X}\right\}$, where $|X|=n,|\hat{X}|=m$ and $\hat{X} \subseteq X$. If $\hat{\mathcal{L}}^{j} \subseteq \mathcal{L}^{j}$ for any $j \in\{1,2\}$ and $\hat{\mathcal{L}_{x}} \subseteq \mathcal{L}_{x}$ for any $x \in \hat{X}$, then call the $L D(n)$ contains sub- $L D(m)$. Denote $D_{m}=\{n ; \exists \operatorname{LD}(n)$ containing sub- $L D(m)\}$. Obviously, for any positive integer $m, D_{m} \subset D$ and $D_{1}=D$, where $D=\{n \mid \exists L D(n)\}$. in addition, if $n \in D_{m}$ then $D_{n} \supset D_{m}$. The imaginative way by Lu consist of three steps [20].
Step 1. Prove the theorem: If $m+q^{\prime} \in D_{m}$ then $m+q q^{\prime} \in D_{m+q^{\prime}}$, where $m$ is a positive integer, $q, q^{\prime}$ are prime powers and $q \geq 5$.

Step 2. Prove $47 \in D$ and $39 \in D_{7}$.
Step 3. Complete the construction $\operatorname{LSTS}(v)$ for $v=141,283,501$, 789, 1501 and 2365:

$$
\begin{array}{r}
47 \in D \quad \longrightarrow \operatorname{LSTS}(141) \longrightarrow \operatorname{LSTS}(283) \\
\underset{\left(m=7, q^{\prime}=32\right)}{39 \in D_{7}} \xrightarrow[\longrightarrow(\#)]{\longrightarrow} 167 \in D_{39} \subset D \longrightarrow \operatorname{LSTS}(501) m \operatorname{LSTS}(1501) \\
\longrightarrow 263 \in D_{39} \subset D \longrightarrow \operatorname{LSTS}(789) \longrightarrow \operatorname{LSTS}(2365)
\end{array}
$$

where (\#) means by Step 1, $\longrightarrow$ means by above-mentioned (**), $\Longrightarrow$ means by $\operatorname{LSTS}(v) \Longrightarrow \operatorname{LSTS}(2 v+1)$ ( $[\mathrm{Ro}])$ and $\rightarrow$ means by $\operatorname{LSTS}(1$ $+4 v)$ mas $\operatorname{LSTS}(1+12 v)$ ([Lu] IV). Now, Step 1 has been completed (by Lu Jiaxi and Liou Kai). So, the complete solution for the existence of LSTS only remains the Step 2, if running the way.
5.5 A recursive construction for $L D(3 n)$.

Let $I_{n}=\{0,1, \ldots, n-1\}$ be a set of $n$ elements ( $n>1$ ) and $Z_{3}=$ $\{0,1,2\}$ be the residue class ring modulo 3. Suppose there exists an $L D(n)=L D\left[I_{n}\right]=\left\{\hat{\mathcal{L}}^{1}, \hat{\mathcal{L}}^{2}, \hat{\mathcal{L}}_{t} \mid t \in I_{n}\right\}$, where $c_{0}=0$ in the condition (C4) satisfied by the design. For convenience, we denote $\hat{\mathcal{L}}^{1}=M$ and
$\bar{M}=\left\{\left(i_{0}, i_{1}, i_{2}\right) \mid \exists i_{3} \in I_{n}\right.$ such that $\left.\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in M\right\}$. We define the following mappings from $I_{n}$ into $I_{n}$ :

If $(0, j, x, \alpha)$ and $(i, j, y, \beta) \in M$, let
$g_{i}: x \longmapsto y$ ( $g_{i}$ is denoted by $f_{1}$ or $f_{2}$ when $\beta=0$ or 1 )
$\phi_{j}: y \longmapsto i$
$\psi_{i}: y \longmapsto j$
$\sigma: i \longmapsto y$ (only for $\beta=1$ ).
It is easy to see that these mappings are all one-to-one. And we have

$$
\left\{\begin{array}{l}
f_{1}(x)=i \text { if and only if } g_{i}(x)=i, \\
f_{2}(x)=\sigma(i) \text { if and only if } g_{i}(x)=\sigma(i) .
\end{array}\right.
$$

Now, we will construct $L D(3 n)=L D\left[Z_{3} \times I_{n}\right]=\left\{\mathcal{L}^{1}, \mathcal{L}^{2}, \mathcal{L}_{x, t} \mid x \in\right.$ $\left.Z_{3}, t \in I_{n}\right\}$ as follows (where $k$ runs over $Z_{3}$ ).

The system $\mathcal{L}^{j}(j=1,2)$ consists of three parts (each part gives $3 n^{2}$ ordered quadruples):
part 1. $\left(\left(k, i_{0}\right),\left(k, i_{1}\right),\left(k, i_{2}\right),\left(0, i_{3}\right)\right)$ provided $\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in \hat{\mathcal{L}}^{j}$;
part 2. $\left(\left(k, i_{0}\right),\left(k+1, i_{1}\right),\left(k-1, f_{j}\left(i_{2}\right)\right),\left(1, i_{3}\right)\right)$ provided $\left(i_{0}, i_{1}, i_{2}, i_{3}\right)$ $\in \bar{M}$;
part 3. $\left(\left(k, i_{1}\right),\left(k-1, i_{0}\right),\left(k+1, f_{j}\left(i_{2}\right)\right),\left(2, i_{3}\right)\right)$ provided $\left(i_{0}, i_{1}, i_{2}, i_{3}\right)$ $\in \bar{M}$.
The system $\mathcal{L}_{0, t}\left(t \in I_{n}\right)$ consists of eight parts:
part 1. $\left(\left(0, i_{0}\right),\left(0, i_{1}\right),\left(0, i_{2}\right)\right)$ provided $\left(i_{0}, i_{1}, i_{2}\right) \in \hat{\mathcal{L}}_{t}$ and $i_{0} \neq t \neq i_{1}$; this gives $(n-1)^{2}$ ordered triples.
part 2. $\left(\left(0, i_{0}\right),\left( \pm 1, i_{1}\right),\left( \pm 1, \psi_{t}\left(i_{2}\right)\right)\right)$ provided $\left(i_{0}, i_{1}, i_{2}\right) \in \bar{M}$ and $i_{0} \neq t$; this gives $2 n(n-1)$ ordered triples.
part 3. $\left(\left( \pm 1, i_{1}\right),\left(0, i_{0}\right),\left( \pm 1, \psi_{t}\left(i_{2}\right)\right)\right)$ provided $\left(i_{0}, i_{1}, i_{2}\right) \in \bar{M}$ and $i_{0} \neq t$; this gives $2 n(n-1)$ ordered triples.
part 4. $\left(\left(1, i_{0}\right),\left(2, i_{1}\right),\left(0, g_{t}\left(i_{2}\right)\right)\right),\left(\left(2, i_{1}\right),\left(1, i_{0}\right),\left(0, g_{t}\left(i_{2}\right)\right)\right)$ provided $\left(i_{0}, i_{1}, i_{2}\right) \in \bar{M}$ and $g_{t}\left(i_{2}\right) \neq t, \sigma(t)$; this gives $2 n(n-2)$ ordered triples.
part 5. $\left(\left(1, i_{0}\right),\left(2, i_{1}\right),\left(1, i_{0}\right)\right),\left(\left(2, i_{1}\right),\left(1, i_{0}\right),\left(1, i_{0}\right)\right)$ provided $\left(i_{0}, i_{1}\right.$, $\left.i_{2}\right) \in \bar{M}$ and $g_{t}\left(i_{2}\right)=t$; this gives $2 n$ ordered triples.
part 6. $\left(\left(1, i_{0}\right),\left(2, i_{1}\right),\left(2, i_{1}\right)\right),\left(\left(2, i_{1}\right),\left(1, i_{0}\right),\left(2, i_{1}\right)\right)$ provided $\left(i_{0}, i_{1}\right.$, $\left.i_{2}\right) \in \bar{M}$ and $g_{t}\left(i_{2}\right)=\sigma(t)$; this gives $2 n$ ordered triples.
part 7. $\left(\left(1, i_{0}\right),\left(1, i_{1}\right),\left(2, \psi_{i_{2}}\left(g_{i}^{-1}(\sigma(t))\right)\right)\right),\left(\left(2, i_{0}\right),\left(2, i_{1}\right),(1\right.$, $\left.\phi_{i_{2}}\left(g_{t}^{-1}(t)\right)\right)$ ) provided $\left(i_{0}, i_{1}, i_{2}\right) \in \bar{M}$ and $i_{0} \neq i_{1}$; this gives $2 n(n-1)$ ordered triples.
part 8 . $(( \pm 1, i),( \pm 1, i),(0, \sigma(t)))$ provided $i \in I_{n}$; this gives $2 n$ ordered triples.

The system $\mathcal{L}_{x, t}\left(x \in Z_{3} \backslash\{0\}, t \in I_{n}\right)$ consists of the ordered triples $\left(\left(k_{0}+x, i_{0}\right),\left(k_{1}+x, i_{1}\right),\left(k_{2}+x, i_{2}\right)\right)$ provided $\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right),\left(k_{2}, i_{2}\right)\right) \in$ $\mathcal{L}_{0, t}$.

Theorem 5.5.1. For $n>1$, if there exists an $L D(n)$ then there exists an $L D(3 n)$, which is given by the above-mentioned construction. [Ka3]

## Proof.

We only need to verify the conditions (C3), (C2) and (C5), respectively.
(C3) By the construction of $\mathcal{L}^{j}(j=1,2)$, the total number of the ordered quadruples in each $\mathcal{L}^{j}$ is $3 \cdot 3 n^{2}=(3 n)^{2}$. Therefore, we only need to show that for any ordered pair $P=\left(\left(k_{s}, i_{s}\right),\left(k_{t}, i_{t}\right)\right)$ of the set $Z_{3} \times I_{n}$ there exists an ordered quadruple of $\mathcal{L}^{j}$ such that its two components in the $s$ th and the $t$ th positions just are $\left(k_{s}, i_{s}\right)$ and $\left(k_{t}, i_{t}\right)$ respectively, where $0 \leq s<t \leq 3$.

1. $P=\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right)\right)$
(1) If $k_{0}=k_{1}$, let $i_{2}, i_{3} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in \hat{\mathcal{L}}^{j}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{0}, i_{1}\right),\left(k_{0}, i_{2}\right),\left(0, i_{3}\right)\right) \in$ part 1 .
(2) If $k_{0} \equiv k_{1}-1(\bmod 3)$, let $i_{2}, i_{3} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in$ $\bar{M}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right),\left(k_{0}-1, f_{j}\left(i_{2}\right)\right),\left(1, i_{3}\right)\right) \in$ part 2.
(3) If $k_{0} \equiv k_{1}+1(\bmod 3)$, let $i_{2}, i_{3} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}, i_{3}\right) \in$ $\bar{M}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right),\left(k_{0}+1, f_{j}\left(i_{2}\right)\right),\left(2, i_{3}\right)\right) \in$ part 3.
2. $P=\left(\left(k_{0}, i_{0}\right),\left(k_{2}, i_{2}\right)\right)$ (similarly, $\left.P=\left(\left(k_{1}, i_{1}\right),\left(k_{2}, i_{2}\right)\right)\right)$
(1) If $k_{0}=k_{2}$, let $i_{1}, i_{3} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in \hat{\mathcal{L}}^{j}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{0}, i_{1}\right),\left(k_{0}, i_{2}\right),\left(0, i_{3}\right)\right) \in$ part 1.
(2) If $k_{0} \equiv k_{2}+1(\bmod 3)$, let $i_{2}^{\prime}=f_{j}^{-1}\left(i_{2}\right)$ and $i_{1}, i_{3} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime}, i_{3}\right) \in \bar{M}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{0}+1, i_{1}\right),\left(k_{2}, i_{2}\right),\left(1, i_{3}\right)\right) \in$ part 2.
(3) If $k_{0} \equiv k_{2}-1(\bmod 3)$, let $i_{2}^{\prime}=f_{j}^{-1}\left(i_{2}\right)$ and $i_{1}, i_{3} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}^{\prime}, i_{3}\right) \in \bar{M}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{0}-1, i_{1}\right),\left(k_{2}, i_{2}\right),\left(2, i_{3}\right)\right) \in$ part 3.
3. $P=\left(\left(k_{0}, i_{0}\right),\left(k_{3}, i_{3}\right)\right)$ (similarly, $\left.P=\left(\left(k_{1}, i_{1}\right),\left(k_{3}, i_{3}\right)\right)\right)$
(1) If $k_{3}=0$, let $i_{1}, i_{2} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in \hat{\mathcal{L}}^{j}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{0}, i_{1}\right),\left(k_{0}, i_{2}\right),\left(0, i_{3}\right)\right) \in$ part 1.
(2) If $k_{3}=1$, let $i_{1}, i_{2} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in \bar{M}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{0}+1, i_{1}\right),\left(k_{0}-1, f_{j}\left(i_{2}\right)\right),\left(1, i_{3}\right)\right) \in \operatorname{part} 2$.
(3) If $k_{3}=2$, let $i_{1}, i_{2} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}, i_{3}\right) \in \bar{M}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{0}-1, i_{1}\right),\left(k_{0}+1, f_{j}\left(i_{2}\right)\right),\left(2, i_{3}\right)\right) \in \operatorname{part} 3$.
4. $P=\left(\left(k_{2}, i_{2}\right),\left(k_{3}, i_{3}\right)\right)$
(1) If $k_{3}=0$, let $i_{0}, i_{1} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}, i_{3}\right) \in \hat{\mathcal{L}}^{j}$, then $P \subset\left(\left(k_{2}, i_{0}\right),\left(k_{2}, i_{1}\right),\left(k_{2}, i_{2}\right),\left(0, i_{3}\right)\right) \in$ part 1 .
(2) If $k_{3}=1$, let $i_{2}^{\prime}=f_{j}^{-1}\left(i_{2}\right)$ and $i_{0}, i_{1} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime}, i_{3}\right)$ $\in \bar{M}$, then $P \subset\left(\left(k_{2}+1, i_{0}\right),\left(k_{2}-1, i_{1}\right),\left(k_{2}, i_{2}\right),\left(1, i_{3}\right)\right) \in$ part 2.
(3) If $k_{3}=2$, let $i_{2}^{\prime}=f_{j}^{-1}\left(i_{2}\right)$ and $i_{0}, i_{1} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}^{\prime}, i_{3}\right)$ $\in \bar{M}$, then $P \subset\left(\left(k_{2}-1, i_{0}\right),\left(k_{2}+1, i_{1}\right),\left(k_{2}, i_{2}\right),\left(2, i_{3}\right)\right) \in$ part 3.
(C2) By the construction of $\mathcal{L}_{x, t}\left(x \in Z_{3}, t \in I_{n}\right)$, the total number of the ordered triples in each $\mathcal{L}_{x, t}$ is $(n-1)^{2}+4 n(n-1)+2 n(n-2)+$ $4 n+2 n(n-1)+2 n=(3 n-1)^{2}$. Therefore, we only need to show that for any ordered pair $P=\left(\left(k_{s}, i_{s}\right),\left(k_{t}, i_{t}\right)\right)$ of the set $\left(Z_{3} \times I_{n}\right) \backslash\{(0, t)\}$ there exists an ordered triple of $\mathcal{C}_{0, t}$ such that its two components in the $s$ th and the $t$ th positions just are $\left(k_{s}, i_{s}\right)$ and ( $k_{t}, i_{t}$ ) respectively, where $0 \leq s<t \leq 2$.
5. $P=\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right)\right)$
(1) If $k_{0}=k_{1}=0$ (then $i_{0} \neq t \neq i_{1}$ ), let $i_{2} \in I_{n} \backslash\{t\}$ such that $\left(i_{0}, i_{1}, i_{2}\right) \in \hat{\mathcal{L}}_{t}$, then $P \subset\left(\left(0, i_{0}\right),\left(0, i_{1}\right),\left(0, i_{2}\right)\right) \in \operatorname{part} 1$.
(2) If $k_{0}=0 \neq k_{1}$ (then $\left.i_{0} \neq t\right)$, let $i_{2} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}\right) \in \bar{M}$, then $P \subset\left(\left(0, i_{0}\right),\left(k_{1}, i_{1}\right),\left(k_{1}, \psi_{t}\left(i_{2}\right)\right)\right) \in$ part 2 .
(3) If $k_{0} \neq 0=k_{1}$ (then $\left.i_{1} \neq t\right)$, let $i_{2} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}\right) \in \bar{M}$, then $P \subset\left(\left(k_{0}, i_{0}\right),\left(0, i_{1}\right),\left(k_{0}, \psi_{t}\left(i_{2}\right)\right)\right) \in$ part 3 .
(4) If $k_{0}=k_{1} \neq 0$, then when $i_{0}=i_{1}, P \subset\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right),(0, \sigma(t))\right.$ $\in$ part 8. And when $i_{0} \neq i_{1}$, let $i_{2} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}\right) \in \bar{M}$, then $P \subset\left(\left(1, i_{0}\right),\left(1, i_{1}\right),\left(2, \psi_{i_{2}}\left(g_{t}^{-1}(\sigma(t))\right)\right)\right) \in$ part 7 (if $\left.k_{0}=1\right)$ or $P \subset\left(\left(2, i_{0}\right),\left(2, i_{1}\right),\left(1, \phi_{i_{2}}\left(g_{t}^{-1}(t)\right)\right)\right) \in$ part 7 (if $\left.k_{0}=2\right)$.
(5) If $k_{0}=1, k_{1}=2$, let $i_{2} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}\right) \in \bar{M}$, then

$$
P \subset\left\{\begin{aligned}
\left(\left(1, i_{0}\right),\left(2, i_{1}\right),\left(1, i_{0}\right)\right) & \in \operatorname{part} 5\left(\text { when } g_{t}\left(i_{2}\right)=t\right) \\
\left(\left(1, i_{0}\right),\left(2, i_{1}\right),\left(2, i_{1}\right)\right) & \in \text { part } 6\left(\text { when } g_{t}\left(i_{2}\right)=\sigma(t)\right) \\
\left(\left(1, i_{0}\right),\left(2, i_{1}\right),\left(0, g_{t}\left(i_{2}\right)\right)\right) & \in \text { part } 4 \text { (otherwise })
\end{aligned}\right.
$$

(6) If $k_{0}=2, k_{1}=1$, let $i_{2} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}\right) \in \bar{M}$, then

$$
P \subset\left\{\begin{aligned}
\left(\left(2, i_{0}\right),\left(1, i_{1}\right),\left(1, i_{1}\right)\right) & \in \operatorname{part} 5\left(\text { when } g_{t}\left(i_{2}\right)=t\right) \\
\left(\left(2, i_{0}\right),\left(1, i_{1}\right),\left(2, i_{0}\right)\right) & \in \operatorname{part} 6\left(\text { when } g_{t}\left(i_{2}\right)=\sigma(t)\right) \\
\left(\left(2, i_{0}\right),\left(1, i_{1}\right),\left(0, g_{t}\left(i_{2}\right)\right)\right) & \in \operatorname{part} 4 \text { (otherwise) }
\end{aligned}\right.
$$

2. $P=\left(\left(k_{0}, i_{0}\right),\left(k_{2}, i_{2}\right)\right)$
(1) If $k_{0}=k_{2}=0$, similar to the case $1(1)$.
(2) If $k_{0}=0 \neq k_{2}$ (then $i_{0} \neq t$ ), let $i_{2}^{\prime}=\psi_{t}^{-1}\left(i_{2}\right)$ and $i_{1} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{t}\right) \in \bar{M}$, then $P \subset\left(\left(0, i_{0}\right),\left(k_{2}, i_{1}\right),\left(k_{2}, i_{2}\right)\right) \in$ part 2 .
(3) If $k_{0} \neq 0=k_{2}$ (then $i_{2} \neq t$ ), then when $i_{2}=\sigma(t) P \subset$ $\left(\left(k_{0}, i_{0}\right),\left(k_{0}, i_{0}\right),\left(0, i_{2}\right)\right) \in$ part 8. And else let $i_{2}^{\prime}=g_{t}^{-1}\left(i_{2}\right)$ and $i_{1} \in I_{n}$ such that

$$
\left\{\begin{array}{l}
\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}\left(\text { if } k_{0}=1\right), \text { then } P \subset\left(\left(1, i_{0}\right),\left(2, i_{1}\right),\left(0, i_{2}\right)\right) \in \text { part } 4 \\
\left(i_{1}, i_{0}, i_{2}^{\prime}\right) \in \bar{M}\left(\text { if } k_{0}=2\right), \text { then } P \subset\left(\left(2, i_{0}\right),\left(1, i_{1}\right),\left(0, i_{2}\right)\right) \in \text { part } 4
\end{array}\right.
$$

(4) If $k_{0}=k_{2} \neq 0$, let $i_{2}^{\prime}=\psi_{t}^{-1}\left(i_{2}\right)$ and $i_{1} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}^{\prime}\right) \in \bar{M}$, then when $i_{1} \neq t, P \subset\left(\left(k_{0}, i_{0}\right),\left(0, i_{1}\right),\left(k_{2}, i_{2}\right)\right) \in$ part 3. And when $i_{1}=t$ we have $\left(t, i_{2}, i_{2}^{\prime}\right),\left(t, i_{0}, i_{2}^{\prime}\right) \in \bar{M}$ so $i_{0}=i_{2}$.
i) If $k_{0}=1$, let $\bar{i}_{2}=g_{t}^{-1}(t)$ and $\bar{i}_{1} \in I_{n}$ such that $\left(i_{0}, \bar{i}_{1}, \bar{i}_{2}\right) \in \bar{M}$, then $P \subset\left(\left(1, i_{0}\right),\left(2, \bar{i}_{1}\right),\left(1, i_{0}\right)\right) \in$ part 5.
ii) If $k_{0}=2$, let $\bar{i}_{2}=g_{t}^{-1}(\sigma(t))$ and $\bar{i}_{1} \in I_{n}$ such that $\left(\bar{i}_{1}, i_{0}, \bar{i}_{2}\right) \in$ $\bar{M}$, then $P \subset\left(\left(2, i_{0}\right),\left(1, \overline{i_{1}}\right),\left(2, i_{0}\right)\right) \in$ part 6.
(5) If $1=k_{0} \neq k_{2} \neq 0$, let $i_{2}^{\prime}, i_{1} \in I_{n}$ such that $\psi_{i_{2}^{\prime}}\left(g_{t}^{-1}(\sigma(t))\right)=i_{2}$ and $\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}$.
i) If $i_{0} \neq i_{1}$ then $P \subset\left(\left(1, i_{0}\right),\left(1, i_{1}\right),\left(2, i_{2}\right)\right) \in$ part 7 .
ii) If $i_{0}=i_{1}$ (then $i_{2}^{\prime}=i_{0}$ by (C4)), let $\bar{i}_{2}=g_{t}^{-1}(\sigma(t))$ then $\left(i_{0}, i_{2}, \bar{i}_{2}\right) \in \bar{M}$ and $g_{t}\left(\bar{i}_{2}\right)=\sigma(t)$, so $P \subset\left(\left(1, i_{0}\right),\left(2, i_{2}\right),\left(2, i_{2}\right)\right) \in$ part 6.
(6) If $2=k_{0} \neq k_{2} \neq 0$, let $i_{2}^{\prime}, i_{1} \in I_{n}$ such that $\psi_{i_{2}^{\prime}}\left(g_{i}^{-1}(t)\right)=i_{2}$ and $\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}$.
i) If $i_{0} \neq i_{1}$ then $P \subset\left(\left(2, i_{0}\right),\left(2, i_{1}\right),\left(1, i_{2}\right)\right) \in$ part 7 .
ii) If $i_{0}=i_{1}$ (then $i_{2}^{\prime}=i_{0}$ by (C4)), let $\bar{i}_{2}=g_{t}^{-1}(t)$ then $\left(i_{2}, i_{0}, \bar{i}_{2}\right) \in \bar{M}$ and $g_{t}\left(\bar{i}_{2}\right)=t$, so $P \subset\left(\left(2, i_{0}\right),\left(1, i_{2}\right),\left(1, i_{2}\right)\right) \in$ part 5.
3. $P=\left(\left(k_{1}, i_{1}\right),\left(k_{2}, i_{2}\right)\right)$
(1) If $k_{1}=k_{2}=0$ (or $k_{1}=0 \neq k_{2}$ or $k_{1} \neq 0=k_{2}$ ) then similar to the case $2(1)$ (or $2(2)$ or $2(3)$ ).
(2) If $k_{1}=k_{2} \neq 0$, let $i_{2}^{\prime}=\psi_{t}^{-1}\left(i_{2}\right)$ and $i_{0} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}$, then when $i_{0} \neq t, P \subset\left(\left(0, i_{0}\right),\left(k_{1}, i_{1}\right),\left(k_{2}, i_{2}\right)\right) \in$ part 2 ; when $i_{0}=t$ similar to the case $i_{1}=t$ in 2(4).
(3) If $k_{1} \neq k_{2} \neq 0 \neq k_{1}$ then similar to the case 2(5)(6).
(C5) We will show that for any ordered triple $T=\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right),\left(k_{2}\right.\right.$ , $i_{2}$ ) ) of the set $Z_{3} \times I_{n}$ there exists an $\mathcal{L}_{x, t}\left(x \in Z_{3}, t \in I_{n}\right)$ or an $\mathcal{L}^{j}(j=$ $1,2)$ such that $T \in \mathcal{L}_{x, t}$ or $\left(T \mid\left(k_{3}, i_{3}\right)\right)=\left(\left(k_{0}, i_{0}\right),\left(k_{1}, i_{1}\right),\left(k_{2}, i_{2}\right),\left(k_{3}, i_{3}\right.\right.$ )) $\in \mathcal{L}^{j}$. Below, for brevity, we also denote the last case by $T \in \mathcal{L}^{j}$.

1. $k_{0}=k_{1}=k_{2}(=k)$
(1) If $\left(i_{0}, i_{1}, i_{2}\right) \in \hat{\mathcal{L}}_{t}$ then $T \in$ part 1 of $\mathcal{L}_{k, t}$.
(2) If $\left(i_{0}, i_{1}, i_{2}\right) \in \hat{\mathcal{L}}^{j}$ then $T \in$ part 1 of $\mathcal{L}^{j}$.
2. $k_{0}=k_{1} \neq k_{2}$
(1) If $i_{0}=i_{1}$, let $t=\sigma^{-1}\left(i_{2}\right)$ then $T \in \operatorname{part} 8$ of $\mathcal{L}_{k_{2}, t}$.
(2) If $i_{0} \neq i_{1}$, let $i_{2}^{\prime} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}$
i) When $k_{2} \equiv k_{0}+1(\bmod 3)$, let $t=\sigma^{-1} f_{2}\left(\psi_{i_{2}^{\prime}}^{-1}\left(i_{2}\right)\right)$, i.e., $\sigma(t)$ $=f_{2}\left(\psi_{i_{2}^{\prime}}^{-1}\left(i_{2}\right)\right)=g_{t}\left(\psi_{i_{2}^{\prime}}^{-1}\left(i_{2}\right)\right)$, then $T \in$ part 7 of $\mathcal{L}_{k_{0}-1, t}$.
ii) When $k_{2} \equiv k_{0}-1(\bmod 3)$, let $t=f_{1}\left(\phi_{i_{2}^{1}}^{-1}\left(i_{2}\right)\right)$, i.e., $t=$ $g_{t}\left(\phi_{i_{2}^{\prime}}^{-1}\left(i_{2}\right)\right)$, then $T \in$ part 7 of $\mathcal{L}_{k_{0}+1, t}$.
3. $k_{0} \equiv k_{1}-1(\bmod 3)$
(1) If $k_{2}=k_{1}$, let $i_{2}^{\prime} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}$
i) When $i_{2}=i_{1}$, let $t=\sigma^{-1} f_{2}\left(i_{2}^{\prime}\right)$ i.e. $\sigma(t)=g_{t}\left(i_{2}^{t}\right)$, then $T \in$ part 6 of $\mathcal{L}_{k_{0}-1, t}$.
ii) When $i_{2} \neq i_{1}$, let $t \in I_{n}$ such that $\psi_{t}\left(i_{2}^{\prime}\right)=i_{2}$, then $t \neq i_{0}$ (or else, from $\left(t, i_{2}, i_{2}^{\prime}\right) \in \bar{M}, i_{2}=i_{1}$, a contradition) so $T \in$ part 2 of $\mathcal{L}_{k_{0}, t}$.
(2) If $k_{2} \equiv k_{1}-1(\bmod 3)$, let $i_{2}^{\prime} \in I_{n}$ such that $\left(I_{1}, i_{0}, i_{2}^{\prime}\right) \in \bar{M}$
i) when $i_{2}=i_{0}$, let $i_{2}^{\prime} \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}$, let $t=f_{1}\left(i_{2}^{\prime}\right)$ i.e. $t=g_{t}\left(i_{2}^{\prime}\right)$ then $T \in$ part 5 of $\mathcal{L}_{k_{0}-1, t}$.
ii) when $i_{2} \neq i_{0}$, let $i_{2}^{\prime}, t \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}^{\prime}\right) \in \bar{M}$ and $\psi_{t}\left(i_{2}^{\prime}\right)=i_{2}$ then $t \neq i_{1}$ (or else, from $\left(t, i_{2}, i_{2}^{\prime}\right) \in \bar{M}, i_{2}=i_{0}$, a contradition) so $T \in$ part 3 of $\mathcal{L}_{k_{1}, t}$.
(3) If $k_{2} \equiv k_{1}+1(\bmod 3)$, let $i_{2}^{\prime}, i_{3}, t \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime} i_{3}\right) \in$ $M$ and $g_{t}\left(i_{2}^{\prime}\right)=i_{2}$
i) When $i_{2}=t$ (then $t=g_{t}\left(i_{2}^{\prime}\right)$ i.e. $\left.f_{1}\left(i_{2}^{\prime}\right)=t=i_{2}\right)$ then $T \in$ part 2 of $\mathcal{C}^{1}$.
ii) When $i_{2}=\sigma(t)$ (then $\sigma(t)=g_{t}\left(i_{2}^{\prime}\right)$ i.e. $\left.f_{2}\left(i_{2}^{\prime}\right)=\sigma(t)=i_{2}\right)$ then $T \in$ part 2 of $\mathcal{L}^{2}$.
iii) Or else $T \in$ part 4 of $\mathcal{L}_{k_{2}, t}$.
4. $k_{0} \equiv k_{1}+1(\bmod 3)$
(1) If $k_{2}=k_{1}$
i) when $i_{2}=i_{1}$, let $i_{2}^{\prime}, t \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}^{\prime}\right) \in \bar{M}$ and $t=f_{1}\left(i_{2}^{\prime}\right)$ i.e. $t=g_{t}\left(i_{2}^{\prime}\right)$ then $T \in$ part 5 of $\mathcal{L}_{k_{0}+1, t}$.
ii) when $i_{2} \neq i_{1}$, let $i_{2}^{\prime}, t \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime}\right) \in \bar{M}$ and $\psi_{t}\left(i_{2}^{\prime}\right)=i_{2}$ then $t \neq i_{0}$ (see $\left.3(1)\right)$ so $T \in$ part 2 of $\mathcal{L}_{k_{0}, t}$.
(2) If $k_{2} \equiv k_{1}+1(\bmod 3)$, let $i_{2}^{\prime} \in I_{n}$ such that $\left(i_{1}, i_{0}, i_{2}^{\prime}\right) \in \bar{M}$
i) When $i_{2}=i_{0}$, let $t=\sigma^{-1} f_{2}\left(i_{2}^{t}\right)$ i.e. $\sigma(t)=g_{t}\left(i_{2}^{t}\right)$, then $T \in$ part 6 of $\mathcal{L}_{k_{0}+1, t}$.
ii) When $i_{2} \neq i_{1}$, let $t \in I_{n}$ such that $\psi_{t}\left(i_{2}^{\prime}\right)=i_{2}$, then $t \neq i_{1}$ (see $3(2)$ ), so $T \in \operatorname{part} 3$ of $\mathcal{L}_{k_{1}, t}$.
(3) If $k_{2} \equiv k_{1}-1(\bmod 3)$, let $i_{2}^{\prime}, i_{3}, t \in I_{n}$ such that $\left(i_{0}, i_{1}, i_{2}^{\prime} i_{3}\right) \in$ $M$ and $g_{t}\left(i_{2}^{\prime}\right)=i_{2}$
i) When $i_{2}=t$ (then $t=g_{t}\left(i_{2}^{\prime}\right)$ i.e. $\left.f_{1}\left(i_{2}^{\prime}\right)=t=i_{2}\right)$ then $T \in$ part 3 of $\mathcal{L}^{\mathbf{1}}$.
ii) When $i_{2}=\sigma(t)$ (then $\sigma(t)=g_{t}\left(i_{2}^{\prime}\right)$ i.e. $\left.f_{2}\left(i_{2}^{\prime}\right)=\sigma(t)=i_{2}\right)$ then $T \in$ part 3 of $\mathcal{L}^{2}$.
iii) Or else $T \in$ part 4 of $\mathcal{L}_{k_{2}, t}$.

The proof is completed.
Below, for more direct perception, we will explain the construction method using Latin square language through the example $L D(4) \rightarrow$
$L D(12)$. In the statement, all mappings $\xi\left(g_{i}, f_{1}, f_{2}, \phi_{j}, \psi_{i}\right.$ and $\left.\sigma\right)$ will appear in the form of a permutation, and denote $\xi(A)=\left[\xi\left(a_{i j}\right)\right]$ and $[x, A]=\left[\left(x, a_{i j}\right)\right]$ for the array $A=\left[a_{i j}\right]$ and $x \in Z_{3}$. The array $A^{T}$ denotes the transpose of the array $A$. The symbol $\langle i, j\rangle$ denotes the position on the intersection of the $i$ th row and the $j$ th column of an array.

Take the example mentioned in $\S 5.4$ as the known $L D(4)=L D\left[I_{4}\right]=$ $\left\{\hat{L}^{1}, \hat{L}^{2}, \hat{L}^{t} ; t \in I_{4}\right\}$ :

$$
\begin{gathered}
\hat{L}^{1}=\left[\begin{array}{cccc}
(0) & 3 & \underline{1} & 2 \\
2 & (1) & 3 & \underline{0} \\
\underline{3} & 0 & (2) & 1 \\
1 & \underline{2} & 0 & (3)
\end{array}\right]=M, \quad \hat{L}^{2}=\left[\begin{array}{llll}
0 & 2 & 3 & 1 \\
3 & 1 & 0 & 2 \\
1 & 3 & 2 & 0 \\
2 & 0 & 1 & 3
\end{array}\right] \\
\hat{L}_{0}=\left[\begin{array}{cccc}
\infty & \infty & \infty & \infty \\
\infty & 3 & 2 & 1 \\
\infty & 2 & 1 & 3 \\
\infty & 1 & 3 & 2
\end{array}\right], \quad \hat{L}_{1}=\left[\begin{array}{cccc}
2 & \infty & 0 & 3 \\
\infty & \infty & \infty & \infty \\
0 & \infty & 3 & 2 \\
3 & \infty & 2 & 0
\end{array}\right] \\
\hat{L}_{2}=\left[\begin{array}{cccc}
3 & 1 & \infty & 0 \\
1 & 0 & \infty & 3 \\
\infty & \infty & \infty & \infty \\
0 & 3 & \infty & 1
\end{array}\right], \quad \hat{L}_{3}=\left[\begin{array}{cccc}
1 & 0 & 2 & \infty \\
0 & 2 & 1 & \infty \\
2 & 1 & 0 & \infty \\
\infty & \infty & \infty & \infty
\end{array}\right]
\end{gathered}
$$

where the symbols (*) and $\pm$ denote the elements $*$ belonging to the transversals $\beta=0$ and $\beta=1$ in Latin square $M$, respectively.

By the array $M$ and the definitions of all mappings, we have:

$$
\begin{aligned}
g_{0} & =\left(\begin{array}{llll}
0 & 3 & 1 & 2 \\
0 & 3 & 1 & 2
\end{array}\right), g_{1}=\left(\begin{array}{llll}
0 & 3 & 1 & 2 \\
2 & 1 & 3 & 0
\end{array}\right), g_{i}=\binom{\text { Oth row of } M}{i \text { th row of } M} \\
g_{2} & =\left(\begin{array}{llll}
0 & 3 & 1 & 2 \\
3 & 0 & 2 & 1
\end{array}\right), g_{3}=\left(\begin{array}{llll}
0 & 3 & 1 & 2 \\
1 & 2 & 0 & 3
\end{array}\right), \\
\phi_{0} & =\left(\begin{array}{llll}
0 & 2 & 3 & 1 \\
0 & 1 & 2 & 3
\end{array}\right), \phi_{1}=\left(\begin{array}{llll}
3 & 1 & 0 & 2 \\
0 & 1 & 2 & 3
\end{array}\right), \phi_{j}=\binom{\text { column } j \text { of } M}{\text { the row index }} \\
\phi_{2} & =\left(\begin{array}{llll}
1 & 3 & 2 & 0 \\
0 & 1 & 2 & 3
\end{array}\right), \phi_{3}=\left(\begin{array}{llll}
2 & 0 & 1 & 3 \\
0 & 1 & 2 & 3
\end{array}\right), \\
\psi_{0} & =\left(\begin{array}{llll}
0 & 3 & 1 & 2 \\
0 & 1 & 2 & 3
\end{array}\right), \psi_{1}=\left(\begin{array}{llll}
2 & 1 & 3 & 0 \\
0 & 1 & 2 & 3
\end{array}\right), \\
\psi_{2} & =\left(\begin{array}{llll}
3 & 0 & 2 & 1 \\
0 & 1 & 2 & 3
\end{array}\right), \psi_{3}=\left(\begin{array}{llll}
1 & 2 & 0 & 3 \\
0 & 1 & 2 & 3
\end{array}\right),
\end{aligned}
$$

$$
\begin{gathered}
f_{1}=\left(\begin{array}{llll}
0 & 3 & 1 & 2 \\
0 & 1 & 2 & 3
\end{array}\right)\left\{\begin{array}{c}
\text { the 0th row of } M \\
\beta=0
\end{array}\right\}\left(\begin{array}{llll}
0 & 3 & 1 & 2 \\
3 & 2 & 1 & 0
\end{array}\right)=f_{2} . \\
\sigma=\left(\begin{array}{llll}
0 & 1 & 2 & 3 \\
1 & 0 & 3 & 2
\end{array}\right)\left\{\begin{array}{c}
\text { the row index } \\
\beta=1
\end{array}\right\} \\
\text { Let } A=f_{1}(M)=\left[\begin{array}{llll}
0 & 1 & 2 & 3 \\
3 & 2 & 1 & 0 \\
1 & 0 & 3 & 2 \\
2 & 3 & 0 & 1
\end{array}\right], B=f_{2}(M)=\left[\begin{array}{llll}
3 & 2 & 1 & 0 \\
0 & 1 & 2 & 3 \\
2 & 3 & 0 & 1 \\
1 & 0 & 3 & 2
\end{array}\right] .
\end{gathered}
$$

Then we get

$$
\begin{gathered}
L^{1}=\left[\begin{array}{ccc}
\left(0, \hat{\mathcal{L}}^{1}\right) & (2, A) & \left(1, A^{T}\right) \\
\left(2, A^{T}\right) & \left(1, \hat{\mathcal{L}}^{1}\right) & (0, A) \\
(1, A) & \left(0, A^{T}\right) & \left(2, \hat{\mathcal{L}}^{1}\right)
\end{array}\right] \text { and } \\
L^{2}=\left[\begin{array}{ccc}
\left(0, \hat{\mathcal{L}}^{2}\right) & (2, B) & \left(1, B^{T}\right) \\
\left(2, B^{T}\right) & \left(1, \hat{\mathcal{L}^{2}}\right) & (0, B) \\
(1, B) & \left(0, B^{T}\right) & \left(2, \hat{\mathcal{L}^{2}}\right)
\end{array}\right] .
\end{gathered}
$$

Let $C_{t}$ be the array $\left[0, g_{t}(M)\right]$ after substitution of elements $(0, t)$ and $(0, \sigma(t))$ in the position $\langle i, j\rangle$ for $(1, i)$ and $(2, j)$. Below, for brevity, we will denote the element $(i, j)$ by $i j$ in an array.

$$
\left.\begin{array}{l}
{\left[0, g_{0}(M)\right]=\left[\begin{array}{llll}
00 & 03 & 01 & 02 \\
02 & 01 & 03 & 00 \\
03 & 00 & 02 & 01 \\
01 & 02 & 00 & 03
\end{array}\right] \xrightarrow[\sigma(0)=1]{t=0}\left[\begin{array}{lll}
10 & 03 & 22 \\
02 & 21 & 03 \\
11 \\
03 & 12 & 02 \\
23 \\
20 & 02 & 13
\end{array}\right)=C_{0}}
\end{array}\right]=\left[\begin{array}{llll}
02 & 01 & 03 & 00 \\
00 & 03 & 01 & 02 \\
01 & 02 & 00 & 03 \\
03 & 00 & 02 & 01
\end{array}\right] \xrightarrow[\sigma(1)=0]{t=1}\left[\begin{array}{llll}
02 & 10 & 03 & 23 \\
20 & 03 & 11 & 02 \\
12 & 02 & 22 & 03 \\
03 & 21 & 02 & 13
\end{array}\right]=C_{1} .
$$

The following diagram shows the procedure from array $C_{t}$ to array $E_{t}$ and $F_{t}$ (take $t=0$ as example), where the symbols (*) and $\pm$ represent
the second component $*$ of the element $(1, *)$ and $(2, *)$ in array $C_{t}$. By the construction of $C_{t}$, the element $*$ in the $\langle i, i\rangle$ position of array $U_{t}$ is $\psi_{i}\left(g_{t}^{-1}(\sigma(t))\right)$, and the element (*) in the $<j, j>$ position of array $V_{t}$ is $\phi_{j}\left(g_{t}^{-1}(t)\right)$. The arrays $P_{t}=\xi_{t}(M), Q_{t}=\eta_{t}(M)$, where

$$
\begin{aligned}
\xi_{t} & =\left(\begin{array}{cccc}
0 & 1 & 2 & 3 \\
\psi_{0}(x) & \psi_{1}(x) & \psi_{2}(x) & \psi_{3}(x)
\end{array}\right), \\
\eta_{t} & =\left(\begin{array}{cccc}
0 & 1 & 2 & 3 \\
\phi_{0}(x) & \phi_{1}(x) & \phi_{2}(x) & \phi_{3}(x)
\end{array}\right)
\end{aligned}
$$

and $x=g_{t}^{-1}(\sigma(t)), y=g_{t}^{-1}(t)$. The array $E_{t}\left(\right.$ or $\left.F_{t}\right)$ is the array $\left[2, P_{t}\right]$ (or $\left[1, Q_{t}\right]$ ) after substitution of all its elements on the main diagonal by $(0, \sigma(t))$.

$\left(\begin{array}{llll}01 & 13 & 11 & 12 \\ 11 & 01 & 10 & 13 \\ 12 & 11 & 01 & 10 \\ 13 & 10 & 12 & 01\end{array}\right) \mathrm{F}_{\mathrm{t}}$

Similarly, we can get $E_{1}, F_{1}, E_{2}, F_{2}, E_{3}, F_{3}$.

Let $D_{\boldsymbol{\imath}}$ be the array $\psi_{t}(M)$ after substitution of all elements in its $t$ th row for element $\infty$. For example,

$$
\psi_{0}(M)=\left[\begin{array}{llll}
0 & 1 & 2 & 3 \\
3 & 2 & 1 & 0 \\
1 & 0 & 3 & 2 \\
2 & 3 & 0 & 1
\end{array}\right] \rightarrow D_{0}=\left[\begin{array}{cccc}
\infty & \infty & \infty & \infty \\
3 & 2 & 1 & 0 \\
1 & 0 & 3 & 2 \\
2 & 3 & 0 & 1
\end{array}\right]
$$

Finally we get $\left(t \in I_{n}\right)$

$$
\begin{aligned}
L_{0, t} & =\left[\begin{array}{ccc}
\left(0, \hat{L}_{t}\right) & \left(1, D_{t}\right) & \left(2, D_{t}\right) \\
\left(1, D_{t}^{T}\right) & E_{t} & C_{t} \\
\left(2, D_{t}^{T}\right) & C_{t}^{T} & F_{t}
\end{array}\right], \\
L_{1, t} & =\left[\begin{array}{ccc}
F_{t}^{\prime} & \left(0, D_{t}^{T}\right) & C_{t}^{\prime T} \\
\left(0, D_{t}\right) & \left(1, \hat{L}_{t}\right) & \left(2, D_{t}\right) \\
C_{t}^{\prime} & \left(2, D_{t}^{T}\right) & E_{t}^{\prime}
\end{array}\right], \\
L_{2, t} & =\left[\begin{array}{ccc}
E_{t}^{\prime \prime} & C_{t}^{\prime \prime} & \left(0, D_{t}^{T}\right) \\
C_{t}^{\prime \prime} & F_{t}^{\prime \prime} & \left(1, D_{t}^{T}\right) \\
\left(0, D_{t}\right) & \left(1, D_{t}\right) & \left(2, \hat{L}_{t}\right)
\end{array}\right]
\end{aligned}
$$

where the arrays $E_{t}^{\prime}$ (or $F_{t}^{\prime}$ ) and $E_{t}^{\prime \prime}$ (or $F_{t}^{\prime \prime}$ ) are obtained by substitution of all elements $(x+1, y)$ and $(x-1, y)$, respectively. The first component of the element $(x, \infty)$ in the array $\left(x, \hat{\mathcal{L}}_{t}\right)$ is omitted.

## References

[BerFa] J.C. Bermond and V. Faber, Decomposition of the complete directed graph into $k$-circuits, J.Combin. Theory (B) 21 (1976), p. 146155.
[Ber1] J.C. Bermond, An application of the solution of Kirkman's schoolgirl problem: the decomposition of the symmetric oriented complete graph into 3 -circuits, Discrete Math. 8 (1974), p. 301-304.
[Ber2] J.C. Bermond, Cycles dans les graphes et G-configurations, Thesis, Univ. of Paris XI (Orsay), April 1975.
[Ca] A. Cayley, On the triadic arrangements of seven and fifteen things, London Edinburgh and Dublin Philos. Mag. and J. Sci. (3) 37 (1850), 50-53 (Collected Mathematical papers I, 481-484).
[CoCo] C.J. Colbourn and M.J. Colbourn, Disjoint cyclic Mendelsohn triple systems, Ars Combin. 11 (1981), p. 3-8.
[De] R.H.F. Denniston, Some packings with Steiner triple systems, Discrete Math. 9 (1974), 213-227.
[Do] J. Doyen, Construction of disjoint Steiner triple systems, Proc. Amer. Math. Soc. 32 (1972), 409-416.
[GoTa] S.W. Golomb and H. Taylor, Tuscan squares - a new family of combinatorial designs, Ars Combin. 20-B (1985), 115-132.
[Ka1] Kang Qingde and Chang Yanxun, Symmetric Mendelsohn triple systems and large sets of disjoint Mendelsohn triple systems, Science Bulletin (P.R.China), 14 (1988), p. 1115.
[Ka2] Kang Qingde, The construction of large sets of disjoint Mendel. sohn triple systems of order $2^{n}+2$, to appear in Science Bulletin.
[Ka3] Kang Qingde, A recurrence construction of LD-design, Acta mathematicae applicatae sinica (P.R.China), vol.10, No.4 (1987), p. 481490.
[Ka4] Kang Qingde, The large sets problem of triple systems in combinatorial designs, to appear in China.
[Ki1] T.P. Kirkman, On a problem in combinations, Cambridge and Dublin Math. J. 2 (1847), 191-204.
[Ki2] T.P. Kirkman, On the puzzle of the fifteen young ladies, London, Edinburgh and Dublin Philos. Mag. and J. Sci.(4) 23 (1862), 198-204.
[KLR] A. Kotzig, C.C. Lindner \& A. Rosa, Latin squares with no subsquares of order two and disjoint Steiner triple systems, Utilitas Math. 7 (1975) 287-294.
[Lin1] C.C. Lindner, On the number of disjoint Mendelsohn triple systems, J.Combin. Theory (A) 30 (1981), p. 326-330.
[Lin2] C.C. Lindner, Construction of large sets of pairwise disjoint transitive triple systems II, Discrete Math. 65 (1987), p. 65-74.
[LinSt] C.C. Lindner and A.P. Street, Construction of large sets of pairwise disjoint transitive triple systems, Eur. J. Combin. 4 (1983), p. 335-346.
[Lu] Lu Jiaxi, On large sets of disjoint Steiner triple systems I-VI, J. Combin. Theory (A) 34 (1983), p. 140-182 and 37 (1984), p. 136-192.
[Men] N.S. Mendelsohn, A natural generalization of Steiner triple systems, Computers in Number Theory, p. 323-338, Academic Press, New York, 1971.
[Re] M. Reiss, Über eine Steinersche combinatorische Aufgabe, welche in 45 sten Bande dieses Journals, Seite 181, gestellt worden ist, J. reine angew. Math. 56 (1859), 326-344.
[Ro] A. Rosa, A theorem on the maximum number of disjoint Steiner triple systems, J. Combin. Theory (A) 18 (1975), p. 305-312.
[Sch] S. Schreiber, Covering all triples on $n$ marks by disjoint Steiner systems, J. Combin. Theory (A) 15 (1973), 347-350.
[So] D. Sotteau, Decomposition of $K_{n}^{*}$ into circuits of odd length, Discrete Math. 15 (1976), p. 185-191.
[St] J. Steiner, Combinatorische Aufgabe, J. reine angew. Math. 45 (1853), 181-182.
[Sy] J.J. Sylvester, On the fifteen young ladies problem, Proc. London Math. Soc. 7 (1875-76) 235-236.
[Tei1] L. Teirlinck, On the maximum number of disjoint Steiner triple systems, Discrete Math. 6 (1973), 299-300.
[Tei2] L. Teirlinck, On large sets of disjoint quadruple systems, Ars Combin. 17 (1984), p. 173-176.
[Tei3] L. Teirlinck, On large sets of disjoint ordered designs, Ars Combin. 25 (1988), p. 31-37.
[Tei4] L. Teirlinck, Locally trivial $t$-designs and $t$-designs without repeated blocks, to appear (in Discrete Math.).
[TeiLin] L. Teirlinck and C.C. Lindner, The construction of large sets of idempotent quasigroups, Eur. J. Combin. 9 (1988), p. 83-89.
[Til] T.W. Tillson, A Hamilton decomposition of $K_{2 m}^{*}, 2 m \geq 8, \mathrm{~J}$. Combin. Theory (B) 29 (1980), p. 68-74.
[Wil] R. M. Wilson, Some partitions of all triples into Steiner triple systems, in: Hypergraph Seminar (Ohio State University 1972), Lecture Notes in Math. 411, Springer, Berlin 1974, pp. 267-277.
[Wi2] R.M. Wilson, Decomposition of complete graphs into subgraphs isomorphic to a given graph, in Proc. 5th British Combinatorial Conference, Aberdeen, July 1975, Congressus Numerantium 15, Utilitas Math. p. 647-659.
[Wo] W.S.B. Woolhouse, Prize question 1793, Lady's and Gentleman's Diary (1844).
[Wu] Wu Lisheng, On large sets of disjoint Mendelsohn triple systems, J.Suzhou Univ. vol.3, No. 2 (1987), p. 1-4.

## Curriculum vitae

The author of this thesis was born in Shanghai, P.R.China on October 22nd, 1942. From 1960 to 1964 he studied in the Math. Dept. of Hebei-Beijing Normal College. From 1964 to 1978 he was a teacher of mathematics at some middle school in Tangshan and Qinhuangdao. From 1978 to 1981 he studied in the Math. Dept. of Nankai Univ. and received the Master's degree. From 1982 on he has taught mathematics in Hebei Normal College as a lecturer and professor. From September 1988 to August 1989 he worked at Eindhoven University of Technology in the Netherlands as a visiting scholar. He is a member of the council of the Chinese Institute of Combinatorial Mathematics and director of the council of Hebei Institute of Combinatorial mathematics.

Address of the author:

Dept. of Math., Hebei Normal College, Shijiazhuang, China.

# Nederlandse samenvatting van de inhoud van het proefschrift 

# 'Large sets of block designs' 

van Kang Qingde

Dit proefschrift gaat over het probleem: Bestaan er zgn. grote collecties blokkenpatronen (proefopzetten, 'block designs') - d.w.z. collecties blokkenpatronen zodanig dat elk mogelijk blok in precies één van teze pationen voorkomt?
Voor Steiner tripelsystemen is dit een klassiek probleem, al door Cayley gesteld, en recentelijk door Lu Jiaxi vrijwel geheel opgelost. In hoofdstuk 5 geven we enkele altematieve constructies voor collecties $\operatorname{LSTS}\left(p^{n}+2\right)$ met $p$ een priemgetal groter dan 3, en behalen nieuwe resultaten voor LD-patronen (dit zijn hulpstructuren ingevoerd door Lu Jiaxi ten einde de zes opengebleven gevallen te behandelen).
De blokken van een Steiner tripelsysteem kunnen in grafentheoretische terminologie beschreven worden als ongerichte 3-cykels. Er zijn twee wezenlijk verschillende manieren om de kanten van een 3cykel te oriënteren, zodat het gerichte analogon bij blokgrootte 3 in twee gevallen uiteenvalt, namelijk dat waarbij de blokken transitieve toernooien op 3 punten zijn, en dat waarbij de blokken gerichte 3cykels zijn. Het eerste geval wordt onderzocht in hoofstuk 4; het tweede (dat van de Mendelsohn tripelsystemen) in hoofdstuk 2. De belangrijkste resultaten van hoofdstuk 2 zijn een recursieve constructie (LMTS $(v+2) \rightarrow L M T S(u v+2)$ voor $u \neq \pm 1(\bmod 6))$ en twee directe constructies (van LMTS $(v)$ voor $v \equiv 1$ of $3(\bmod 6)$ en van $L M T S\left(2^{n}+2\right)$ voor $\left.n \geq 3\right)$. Ten slotte worden in hoofdstuk 3 in plaats van 3-cykels nu $k$-cykels bekeken voor willekeurige $k$.

# PROPOSITIONS 

accompanying the dissertation

## LARGE SETS OF BLOCK DESIGNS

by Kang Qingde

Eindhoven, August 18, 1989

1. (see [1])

Let

$$
A=I_{n}+\left(\begin{array}{cc}
0 & P_{k} \\
Q_{n-k} & 0
\end{array}\right)
$$

be a matrix of order $n$, where $I_{n}$ is a unit matrix of order $n$,

$$
P_{k}=\left(\begin{array}{cccc}
a_{1} & & & 0 \\
& a_{2} & & \\
& & \ddots & \\
0 & & & a_{k}
\end{array}\right), \quad Q_{n-k}=\left(\begin{array}{cccc}
a_{k+1} & & & 0 \\
& a_{k+2} & & \\
& & \ddots & \\
0 & & & a_{n}
\end{array}\right)
$$

$1 \leq k \leq n-1$ and all $a_{i}= \pm 1(1 \leq i \leq n)$. Denote $d=g . c . d .(k, n)$. Then the matrix equation $A X=0$ has a binary solution (i.e., $X=\left(x_{1}\right.$, $\left.x_{2}, \ldots, x_{n}\right)^{T}$, all $x_{i}= \pm 1$ ) if and only if

$$
\#\left\{a_{j}=1 \mid j \equiv i \quad(\bmod d)\right\} \equiv 0 \quad(\bmod 2), \quad \forall 1 \leq i \leq d
$$

And when the condition is satisfied, the equation has $2^{d}$ binary solutions.
2. (see [1])

Let $C C R_{n}$ be a shift register sequence of order $n$ generated by the Boolean function $x_{n}=1+x_{0}$. Then in the $C C R$ 's factor-incident graph:
i) There are $\mathrm{B}(n)=\frac{1}{2} \varphi(2 n)$ loops.
ii) There are $\mathrm{C}(n)$ quadruple-lines, where

$$
C(n)=\left\{\begin{aligned}
& \sum_{\substack{d \mid n \\
d \neq n}} 2^{d-3}\left(\frac{n}{d}-2\right) \varphi\left(\frac{n}{d}\right)-\frac{1}{4} \varphi(n), \quad n \equiv 1(\bmod 2), \\
& \sum_{\substack{2|d| n \\
2 \nmid n}} 2^{d-3}\left(\frac{n}{d}-2\right) \varphi\left(\frac{n}{d}\right)+\left\{\begin{array}{l}
\frac{n-2}{2} \varphi\left(\frac{n}{2}\right), n \\
\frac{n-2}{4} \varphi\left(\frac{n}{2}\right), n
\end{array}>0(\bmod 4)\right.
\end{aligned}\right.
$$

where $\varphi$ is Euler $\varphi$-function.

## 3. (see [1])

Let $P C R_{n}$ be a shift register sequences of order $n$ generated by the Boolean function $x_{n}=x_{0}$. Then in the $P C R$ 's factor-incident graph:
i) There are no loops or quadruple-lines.
ii) There are $\mathrm{D}(\mathrm{n})$ double-lines, where

$$
D(n)=\sum_{\substack{d \mid n \\ d \neq n}} 2^{d-2}\left(\frac{n}{d}-2\right) \varphi\left(\frac{n}{d}\right)
$$

4. (see [2])

A fault-free tiling of a rectangle with $a \times b$ tiles exists if and only if the size of the rectangle is:

$$
\begin{aligned}
& \text { (if } a>1)\left\{\begin{array} { r } 
{ p a \times q b \quad ( p \geq 2 b = 1 , q \geq 2 a + 1 ) } \\
{ p a b \times q }
\end{array} \quad \left(p \geq 3 \text { and }\left\{\begin{array}{r}
q \geq 2 a b+1 \\
q=a b+s a+t b<2 a b
\end{array}\right)\right.\right. \\
& \text { (if } a=1) \quad p b \times q \quad(p \geq 3, q \geq 2 b+1 \text { and }(p b, q) \neq(6,6))
\end{aligned}
$$

5. (see [2])

A t-fault-free tiling of a rectangle with $1 \times b$ tiles exists only if the size of the rectangle is $p b \times q$, where $p \geq 3$

$$
q \geq \frac{b(p-2)+p(b-1)[q]}{(b-1) p-b}
$$

$($ where $1 \leq t \leq b,[q] \equiv q(\bmod b)), t \leq[q] \leq b+t-1)$.
6. (see [2])

A 2 -fault-free tiling of a rectangle with $1 \times 2$ tiles exists if and only if the size of the rectangle is $2 p \times q$, where $p \geq 3, q \geq 7$ and $(p, q) \neq(3,7)$, $(3,9)$ and $(4,7)$.
7. (see [3])

If $8 k+5$ is a prime power then there exists a $C B H R(16 k+12)$, i.e., a Complete Balanced Howell Rotation for $16 k+12$ partnerships.
8. The product graph $P_{m} \times C_{4 n}$ is $k$-graceful, where $m, n, k$ are any positive integers, $P_{m}$ is a path with $m$ vertices and $C_{4 n}$ is a circuit with $4 n$ vertices.

## 9. (Chang Yanxun \& Kang Qingde)

Let $q=p^{n}$ be a prime power. S.W. Golomb conjectured the following (see [4], conjecture C). Any nonzero element in $G F(q)$ can be written as a sum of two primitive elements of $G F(q)$. This conjecture is true if one of the following cases holds:
(1) $q>7 \times 10^{11}$;
(2) $n \geq 2$ and $p^{n} \neq 4$.

On the other hand, for $q=3,4,5,7,11,13,19,31,43$ and 61 not every nonzero element in $G F(q)$ is the sum of two primitive elements.
10. For a nonsingular Boolean function $x_{n}=x_{0}+f\left(x_{1}, x_{2}, \ldots, x_{n-1}\right)$ and $x_{k}^{(0)} \in F_{2}(1 \leq k \leq n-1)$, if $f\left(x_{1}^{(0)}, x_{2}^{(0)}, \ldots, x_{n-1}^{(0)}\right)=1$ then the number

$$
s^{(0)}=\sum_{k=1}^{n-1} x_{k}^{(0)} 2^{n-1-k}
$$

is called a small term of the function $f$. And the collection of all small terms of $f$ is denoted $S_{f}$.

If the Boolean function $f$ will generate a de Bruijn sequence of order $n$, then
(1) In each of the following sets there exists a number, at least, which does not belong to $S_{f}$ :

```
    \(\left\{\frac{1}{3}\left(2^{n-1}-1\right), \frac{2}{3}\left(2^{n-1}-1\right)\right\}\), if \(n \equiv 1(\bmod 2)\);
    \(\left\{\frac{1}{5}\left(2^{n}-4\right), \frac{1}{5}\left(2^{n+1}-3\right), \frac{1}{3}\left(2^{n-1}-2\right), \frac{1}{5}\left(3 \cdot 2^{n-1}-1\right)\right\}\), if \(n \equiv 2\)
\((\bmod 4) ;\)
    \(\left\{\frac{1}{17}\left(2^{n}-16\right), \frac{1}{17}\left(2^{n+1}-15\right), \frac{1}{17}\left(2^{n+2}-13\right), \frac{1}{17}\left(2^{n+3}-9\right), \frac{1}{17}(15\right.\).
\(\left.\left.2^{n-1}-1\right), \frac{1}{17}\left(13 \cdot 2^{n-1}-2\right), \frac{1}{17}\left(9 \cdot 2^{n-1}-4\right), \frac{1}{17}\left(2^{n-1}-8\right)\right\}\), if \(n \equiv 4\)
\((\bmod 8) ;\)
```

$\left\{\frac{1}{17}\left(3 \cdot 2^{n}-14\right), \frac{1}{17}\left(5 \cdot 2^{n}-12\right), \frac{1}{17}\left(3 \cdot 2^{n+1}-11\right), \frac{1}{17}\left(7 \cdot 2^{n}-10\right)\right.$,
$\left.\frac{1}{17}\left(3 \cdot 2^{n-1}-7\right), \frac{1}{17}\left(5 \cdot 2^{n-1}-6\right), \frac{1}{17}\left(7 \cdot 2^{n-1}-5\right), 11\left(11 \cdot 2^{n-1}-3\right)\right\}$, $n \equiv 4(\bmod 8)$.
(2) In each of the following sets there exists a number, at least, which is contained in $S_{f}$ :

$$
\begin{aligned}
& \left\{\frac{1}{3}\left(2^{n}-1\right), \frac{2}{3}\left(2^{n-2}-1\right)\right\}, \text { if } n \equiv 0(\bmod 2) ; \\
& \left\{\frac{1}{7}\left(2^{n}-1\right), \frac{2}{7}\left(2^{n}-1\right), \frac{4}{7}\left(2^{n-3}-1\right)\right\}, \text { if } n \equiv 0(\bmod 3) ; \\
& \left.\left\{\frac{3}{7} 2^{n}-1\right), \frac{1}{7}\left(3 \cdot 2^{n-1}-5\right), \frac{1}{7}\left(5 \cdot 2^{n-1}-6\right)\right\}, \text { if } n \equiv 0(\bmod 3) ; \\
& \left\{\frac{1}{31}\left(2^{n}-1\right), \frac{2}{31}\left(2^{n}-1\right), \frac{4}{31}\left(2^{n}-1\right), \frac{8}{31}\left(2^{n}-1\right), \frac{16}{31}\left(2^{n-3}-1\right)\right\}, \text { if }
\end{aligned}
$$

$n \equiv 0(\bmod 5) ;$
$\left\{\frac{3}{31}\left(2^{n}-1\right), \frac{6}{31}\left(2^{n}-1\right), \frac{12}{31}\left(2^{n}-1\right), \frac{1}{31}\left(17 \cdot 2^{n-1}-24\right), \frac{1}{31}\left(3 \cdot 2^{n-1}-\right.\right.$ 17) $\}$, if $n \equiv 0(\bmod 5)$;

$$
\left\{\frac{5}{31}\left(2^{n}-1\right), \frac{9}{31}\left(2^{n}-1\right), \frac{10}{31}\left(2^{n}-1\right), \frac{1}{31}\left(9 \cdot 2^{n-1}-20\right), \frac{1}{31}\left(5 \cdot 2^{n-1}-\right.\right.
$$ $18)\}$, if $n \equiv 0(\bmod 5)$;

$$
\left\{\frac{7}{31}\left(2^{n}-1\right), \frac{14}{31}\left(2^{n}-1\right), \frac{1}{31}\left(7 \cdot 2^{n-1}-19\right), \frac{1}{31}\left(19 \cdot 2^{n-1}-25\right), \frac{1}{31}(25 .\right.
$$

$\left.\left.2^{n-1}-28\right)\right\}$, if $n \equiv 0(\bmod 5)$;
$\left\{\frac{11}{31}\left(2^{n}-1\right), \frac{13}{31}\left(2^{n}-1\right), \frac{1}{31}\left(11 \cdot 2^{n-1}-21\right), \frac{1}{31}\left(13 \cdot 2^{n-1}-22\right)\right.$,
$\left.\frac{1}{31}\left(21 \cdot 2^{n-1}-26\right)\right\}$, if $n \equiv 0(\bmod 5)$;
$\left\{\frac{15}{31}\left(2^{n}-1\right), \frac{1}{31}\left(15 \cdot 2^{n-1}-23\right), \frac{1}{31}\left(23 \cdot 2^{n-1}-27\right), \frac{1}{31}\left(27 \cdot 2^{n-1}-29\right)\right.$, $\left.\frac{1}{31}\left(29 \cdot 2^{n-1}-30\right)\right\}$, if $n \equiv 0(\bmod 5)$.

## (References)

[1] Kang Qingde, On the multiple-lines in CCR's and PCR's factorincident graphs, Acta Mathematicae Applicatae Sinica, 3 (1986), 352369.
[2] Kang Qingde, On fault-free tilings, Science Bulletin, vol. 31, No. 17 (1986), 1222.
[3] F.K. Hwang, Q.D. Kang and J.E. Yu, Complete Balanced Howell Rotations for $16 k+12$ partnerships, J. Combin. Theory (A) 1 (1984), 66-72.
[4] S.W. Golomb, Algebraic constructions for Costas arrays, J. Combin. Theory (A) 37 (1984), 13-21.

