Chapter V

DIRECT CONSTRUCTION OF STEINER TRIPLE SYSTEMS

5.0 Introduction

In Chapter IV we proved that the condition $n \equiv 1$ or $3 \pmod 6$ is sufficient for the existence of n-STS. In this chapter various methods for direct construction of n-STS for all n with $n \equiv 1$ or $3 \pmod 6$ are provided. Section 5.1 deals with methods of constructing n-STS for any $n \equiv 1$ or $3 \pmod 6$ with $n \geqslant 49$. Material in this section is drawn from [4]. Sections 5.2 and 5.3 give methods for direct construction of n-STS for certain values of n, which include all n such that $7 \leqslant n \leqslant 45$ and $n \equiv 1$ or $3 \pmod 6$. The method given in Section 5.2 is a generalization of that given in [1]. This method gives construction of n-STS for all $n \equiv 1 \pmod 6$ for which a finite field of order n exists. Section 5.3 gives method, due to Doyen [2], for constructing n-STS for all $n \equiv 3 \pmod 6$ and $n \geqslant 9$. The last section, Section 5.4, exhibits the existence of STS with Property I and II mentioned in Chapter III.

5.1 Distribution Method for Constructing n-STS

The methods for constructing n-STS in this section will make use of the distribution of certain 2t integers into t pairs with differences 1,2,.., t. Propositions 5.1.1 - 5.1.8 give such dis-tributions needed in our construction. The truth of these propo-sitions can be verified easily. These proofs will be omitted.

5.1.1 Proposition. Let $t = 4m$ and $m \geqslant 2$. Then the integers $1,2,\ldots,2t$ can be distributed into t pairs (b_r, a_r), $r = 1,\ldots,t$, such that $b_r - a_r = r$ according to Chart I.

Chart I

r	b_r	a_r	
1	$7m + 1$	$7m$	
$2m - 1$	$6m + 1$	$4m + 2$	
$4m - 1$	$6m$	$2m + 1$	
$2k$	$2m + 1 + k$	$2m + 1 - k$	$k = 1,2,\ldots,2m;$
$1 + 2k$	$6m + 1 + k$	$6m - k$	$k = 1,2,\ldots, m - 2;$
$2m - 1 + 2k$	$7m + 1 + k$	$5m + 2 - k$	$k = 1,2,\ldots,m - 1.$

5.1.2 Proposition. Let $t = 4m + 1$ and $m \geqslant 2$. Then the integers $1,2,\ldots, 2t$, can be distributed into t pairs (b_r, a_r), $r = 1,\ldots, t$, such that $b_r - a_r = r$ according to Chart II.

Chart II

r	b_r	a_r	
1	$5m + 3$	$5m + 2$	
$2m - 1$	$8m + 2$	$6m + 3$	
$4m + 1$	$6m + 2$	$2m + 1$	
$2k$	$2m + 1 + k$	$2m + 1 - k$	$k = 1,2,\ldots,2m;$
$1 + 2k$	$6m + 3 + k$	$6m + 2 - k$	$k = 1,2,\ldots, m - 2;$
$2m - 1 + 2k$	$7m + 1 + k$	$5m + 2 - k$	$k = 1,2,\ldots,m.$

5.1.3 <u>Proposition.</u> Let $t = 4m + 2$ and $m \geq 2$. Then the integers $1,2,\ldots,2t - 1, 2t + 1$ can be distributed into t pairs (b_r, a_r), $r = 1,\ldots,t$, such that $b_r - a_r = r$ according to Chart III.

Chart III

r	b_r	a_r	
1	$7m + 5$	$7m + 4$	
$2m + 3$	$8m + 5$	$6m + 2$	
$4m + 1$	$6m + 3$	$2m + 2$	
$2k$	$2m + 2 + k$	$2m + 2 - k$	$k = 1,2,\ldots,2m + 1;$
$1 + 2k$	$6m + 3 + k$	$6m + 2 - k$	$k = 1,2,\ldots,m;$
$2m + 3 + 2k$	$7m + 5 + k$	$5m + 2 - k$	$k = 1,2,\ldots, m - 2.$

5.1.4 <u>Proposition.</u> Let $t = 4m + 3$ and $m \geq 2$. Then the integers $1,2,\ldots,2t - 1, 2t + 1$ can be distributed into t pairs (b_r, a_r), $r = 1,2,\ldots,t$, such that $b_r - a_r = r$ according to Chart IV.

Chart IV ✓ $m \geq 1$

r	b_r	a_r	
1	$5m + 5$	$5m + 4$	
$2m + 1$	$8m + 7$	$6m + 6$	
$4m + 3$	$6m + 5$	$2m + 2$	
$2k$	$2m + 2 + k$	$2m + 2 - k$	$k = 1,2,\ldots, 2m + 1;$
$1 + 2k$	$6m + 6 + k$	$6m + 5 - k$	$k = 1,2,\ldots, m - 1;$
$2m + 1 + 2k$	$7m + 5 + k$	$5m + 4 - k$	$k = 1,2,\ldots, m.$

5.1.5 Proposition. Let $t = 4m$ and $m \geqslant 2$. Then the integers $1, 2, \ldots, t, t + 2, \ldots, 2t, 2t + 1$ can be distributed into t pairs (d_r, c_r), $r = 1, \ldots, t$ such that $d_r - c_r = r$ according to Chart V.

Chart V

r	d_r	c_r	
1	$7m + 2$	$7m + 1$	
$2m + 1$	$6m + 1$	$4m$	
$4m$	$6m$	$2m$	
$2k$	$2m + k$	$2m - k$	$k = 1, 2, \ldots, 2m - 1;$
$1 + 2k$	$6m + 1 + k$	$6m - k$	$k = 1, 2, \ldots, m - 1;$
$2m + 1 + 2k$	$7m + 2 + k$	$5m + 1 - k$	$k = 1, 2, \ldots, m - 1.$

5.1.6 Proposition. Let $t = 4m + 3$ and $m \geqslant 2$. Then the integers $1, \ldots, t, t + 2, \ldots, 2t, 2t + 1$ can be distributed into t pairs (d_r, c_r), $r = 1, \ldots, t$, such that $d_r - c_r = r$ according to Chart VI.

$m \geq 0$

Chart VI

r	d_r	c_r	
1	$7m + 7$	$7m + 6$	
$2m + 3$	$8m + 7$	$6m + 4$	$m \geq 1$
$4m + 3$	$6m + 5$	$2m + 2$	
$2k$	$2m + 2 + k$	$2m + 2 - k$	$k = 1, 2, \ldots, 2m + 1;$
$1 + 2k$	$6m + 5 + k$	$6m + 4 - k$	$k = 1, 2, \ldots, m ;$
$2m + 3 + 2k$	$7m + 7 + k$	$5m + 4 - k$	$k = 1, 2, \ldots, m - 1.$

5.1.7 Proposition. Let $t = 4m + 1$ and $m \geqslant 2$. Then the integers $1,\dots,t,\ t+2,\dots,2t,\ 2t+2$ can be distributed into t pairs (d_r, c_r), $r = 1,\dots,t$, such that $d_r - c_r = r$ according to Chart VII.

Chart VII

r	d_r	c_r	
1	$7m + 4$	$7m + 3$	
$2m + 3$	$8m + 4$	$6m + 1$	
$4m + 1$	$6m + 2$	$2m + 1$	
$2k$	$2m + 1 + k$	$2m + 1 - k$	$k = 1,2,\dots,2m;$
$1 + 2k$	$6m + 2 + k$	$6m + 1 - k$	$k = 1,2,\dots, m;$
$2m + 3 + 2k$	$7m + 4 + k$	$5m + 1 - k$	$k = 1,2,\dots,m - 2.$

5.1.8 Proposition. Let $t = 4m + 2$ and $m \geqslant 2$. Then the integers $1,\dots,t,\ t+2,\dots,2t,\ 2t+2$ can be distributed into t pairs (d_r, c_r), $r = 1,\dots,t$, such that $d_r - c_r = r$ according to Chart VIII

Chart VIII

r	d_r	c_r	
1	$7m + 5$	$7m + 4$	
$2m + 3$	$8m + 6$	$6m + 3$	
$4m + 1$	$6m + 2$	$2m + 1$	
$4m + 2$	$8m + 4$	$4m + 2$	
$2k$	$2m + 1 + k$	$2m + 1 - k$	$k = 1,2,\dots,2m;$
$1 + 2k$	$6m + 3 + k$	$6m + 2 - k$	$k = 1,2,\dots,m;$
$2m + 3 + 2k$	$7m + 5 + k$	$5m + 2 - k$	$k = 1,2,\dots,m - 2.$

5.1.9 Lemma. For any positive integer t, let x and y be distinct numbers from 1 to $6t + 1$. Then

(i) $x - y$ or $y - x$ is congruent modulo $6t + 1$ to one of the integers $1,2,\ldots, 3t$.

(ii) $x - y$ or $y - x$ is congruent modulo $6t + 1$ to one of the integers $1,2,\ldots,3t - 1, 3t + 1$.

Proof : We shall show by cases that $x - y$ or $y - x$ is congruent modulo $6t + 1$ to one of $1,2,\ldots,3t$.

case 1. $1 \leq x,y \leq 3t + 1$.

We may assume that $x > y$. Hence $1 \leq x - y \leq 3t$. Therefore $x - y$ is congruent modulo $6t + 1$ to one of $1,2,\ldots, 3t$.

case 2. $3t + 1 < x , y \leq 6t + 1$.

We may assume that $x > y$. Hence $1 \leq x - y < 3t$. Therefore $x - y$ is congruent modulo $6t + 1$ to one of $1,\ldots, 3t - 1$.

case 3. $1 \leq x \leq 3t + 1$, $3t + 1 < y \leq 6t + 1$.

Then $1 \leq y - x \leq 6t$. If $1 \leq y - x \leq 3t$, then $y - x$ is congruent modulo $6t + 1$ to one of $1,\ldots,3t$. In case $3t < y - x \leq 6t$ we have $-(6t) \leq x - y < -(3t)$. Hence $1 \leq x - y + 6t + 1 < 3t + 1$ so that $x - y$ is congruent modulo $6t + 1$ to one of $1,\ldots,3t$.

case 4. $1 \leq y \leq 3t + 1$, $3t + 1 < x \leq 6t + 1$.

Similarly to case 3 we can show that $x - y$ or $y - x$ is congruent modulo $6t + 1$ to one of $1,\ldots,3t$.

Thus (i) is proved. To prove (ii) we observe from (i) that $x - y$ or $y - x$ is congruent modulo $6t + 1$ to one of $1,\ldots,3t$. Assume that $x - y$ is congruent modulo $6t + 1$ to one of $1,\ldots,3t$. If $x - y$ is congruent modulo $6t + 1$ to one of $1,2,\ldots,3t - 1$, then (ii) is proved. In case that $x - y$ is congruent to $3t$ modulo $6t + 1$ we have $y - x = -3t = -(6t + 1) + (3t + 1)$. Therefore $y - x$ is congruent to $3t + 1$ modulo $6t + 1$. Thus (ii) is proved.

5.1.10 <u>Theorem</u>. Let $n = 6t + 1$ and $t \geqslant 8$. For $r = 1,\ldots,t$, let (b_r, a_r) be defined as in Propositions 5.1.1 - 5.1.4 depending on the residue of t modulo 4. Let $C = \{1,2,\ldots, 6t + 1\}$ and $S(C)$ be the family of the following 3-subsets of C:

$$\{p, p + r, p + t + b_r\} \quad , p \in C, r \in \{1,2,\ldots,t\} ,$$

where each number is taken modulo $6t + 1$.

Then $(C,S(C)$ is n-STS.

<u>Proof</u> : The total number of 3-subsets in $S(C)$ is at most $t(6t + 1) = \frac{1}{6} n(n - 1)$. Thus to show that $(C,S(C))$ is n-STS, it suffices to show that for any 2-subset T of C there exists a 3-subset H in $S(C)$ such that $T \subset H$. Let $T = \{x,y\}$ be any 2-subset of C. In this proof the addition is the addition in the residue class ring modulo $6t + 1$.

case 1. $t \equiv 0$ or $1 \pmod 4$.

By the construction of (b_r, a_r) we have $\{1,2,\ldots, 3t\} = \{1,\ldots,t\ t + b_1,\ldots,t + b_t, t + a_1,\ldots, t + a_t\}$. By Lemma 5.1.9(i) we may assume that $y - x$ is congruent modulo $6t + 1$ to one of $1,2,\ldots,3t$. Thus $y - x = r$ or $y - x = t + b_r$ or $y - x = t + a_r$ for some r, $1 \leq r \leq t$.

case 1(a) $y - x = r$.

Let $H = \{x, x + r, x + t + b_r\}$. Then $H \in S(C)$ and $T \subset H$.

case 1(b) $y - x = t + b_r$.

Let $H = \{x, x + r, x + t + b_r\}$. Then $H \in S(C)$ and $T \subset H$.

case 1(c) $y - x = t + a_r$.

Let $p = y - t - b_r$. Hence $p + r = y - t - b_r + r = y - t - a_r = x$ and $p + t + b_r = y - t - b_r + t + b_r = y$. Let $H = \{p, p + r, p + r + b_r\}$ Then $H \in S(C)$ and $T \subset H$.

case 2. $t \equiv 2$ or $3 \pmod 4$.

By the construction of (b_r, a_r) we have $\{1, \ldots, 3t - 1, 3t + 1\} = \{1, \ldots, t, t + b_1, \ldots, t + b_t, t + a_1, \ldots, t + a_t\}$. By Lemma 5.1.9(ii) we may assume that $y - x$ is congruent modulo $6t + 1$ to one of $1, \ldots, 3t - 1, 3t + 1$. Thus $y - x = r$ or $y - x = t + b_r$ or $y - x = t + a_r$ for some r, $1 \leq r \leq t$. Similarly to case 1 we can prove that there exists H in $S(C)$ such that $T \subset H$.

Hence $(C, S(C))$ is n - STS.

5.1.11 <u>Lemma</u>. For each positive integer t let x and y be distinct numbers from 1 to $6t + 3$ such that neither $x - y$ nor $y - x$ is congruent to $2t + 1$ modulo $6t + 3$. Then

(i) $x - y$ or $y - x$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t + 1$.

(ii) $x - y$ or $y - x$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t + 2$.

<u>Proof</u> : We shall show by cases that $x - y$ or $y - x$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t + 1$.

case 1. $1 \leq x, y \leq 3t + 2$.

We may assume that $x > y$. Hence $1 \leq x - y \leq 3t + 1$. Therefore $x - y$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t+1$.

case 2. $3t + 2 < x, y \leq 6t + 3$.

We may assume that $x > y$. Hence $1 \leq x - y < 3t + 1$ so that $x - y$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t$.

case 3. $1 \leq x \leq 3t + 2$, $3t + 2 < y \leq 6t + 3$.

Then $1 \leq y - x \leq 6t + 2$. If $1 \leq y - x \leq 3t + 1$, then $y - x$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t + 1$. In case $3t + 1 < y - x \leq 6t + 2$ we have $-(6t + 2) \leq x - y < -(3t + 1)$. Hence $1 \leq x - y + 6t + 3 \leq 3t+1$ so that $x - y$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t + 1$.

case 4. $1 < y \leq 3t + 2$, $3t + 2 < x \leq 6t + 3$.

Similarly to case 3 we can show that $x - y$ or $y - x$ must be congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t + 1$.

Thus (i) is proved. To prove (ii) we observe from (i) that $x - y$ or $y - x$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t + 1$. Assume that $x - y$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t, 3t + 1$. If $x - y$ is congruent modulo $6t + 3$ to one of $1, \ldots, 2t, 2t + 2, \ldots, 3t$, then (ii) is proved. Suppose that $x - y$ is congruent to $3t + 1$ modulo $6t + 3$. Hence $y - x = -(3t + 1) = -(6t + 3) + 3t + 2$ so that $y - x$ is congruent modulo $6t + 3$ to $3t + 2$. Thus (ii) is proved.

5.1.12 <u>Theorem</u>. Let $n = 6t + 3$ and $t \geq 8$. For $r = 1, \ldots, t$, let (d_r, c_r) be defined as in Propositions 5.1.5 - 5.1.8 depending on the residue of t modulo 4. Let $C = \{1, 2, \ldots, 6t + 3\}$ and $S(C)$ be the family of the following 3-subsets of C:

(i) $\{p, p + r, p + t + d_r\}$, $r \in \{1,2,\ldots,t\}$ $p \in C$,

(ii) $\{p, p + 2t + 1, p + 4t + 2\}$, $p \in \{1,2,\ldots,2t + 1\}$,

where each number in 3-subsets in S(C) is taken modulo $6t + 3$. Then (C,S(C)) is n-STS.

Proof : It can be seen that the total number of 3-subsets in S(C) is at most $(t)(6t + 3) + 2t + 1 = \frac{1}{6}(6t + 2)(6t + 3) = \frac{1}{6}n(n - 1)$. Thus to show that (C,S(C)) is n-STS, it suffices to show that for any 2-subset T of C there exists a 3-subset H in S(C) such that $T \subset H$. Let $T = \{x,y\}$ be any 2-subset of C. In this proof the addition is the addition in the residue class ring modulo $6t + 3$.

First we assume that neither $x - y$ nor $y - x$ is congruent modulo $6t + 3$ to $2t + 1$.

case 1. $t \equiv 0$ or $3 \pmod 4$.

By the construction of (d_r, c_r) we have $\{1,\ldots,2t,2t + 2,\ldots,3t, 3t + 1\} = \{1,\ldots,t, t + d_1,\ldots,t + d_t, t + c_1,\ldots, t + c_t\}$. By Lemma 5.1.11 (i) we may assume that $y - x$ is congruent modulo $6t + 3$ to one of $1,\ldots,2t, 2t + 2,\ldots,3t, 3t + 1$. Thus $y - x = r$ or $y - x = t + d_r$ or $y - x = t + c_r$ for some r, $1 \leqslant r \leqslant t$.

case 1(a) $y - x = r$.

Let $H = \{x, x + r, x + t + d_r\}$. Then $H \in S(C)$ and $T \subset H$.

case 1(b) $y - x = t + d_r$.

Let $H = \{x, x + r, x + t + d_r\}$. Then $H \in S(C)$ and $T \subset H$.

case 1(c) $y - x = t + c_r$.

Let $p = y - t - d_r$. Hence $p + r = y - t - d_r + r = y - t - c_r = x$ and $p + t + d_r = y - t - d_r + t + d_r = y$. Let $H = \{p, p + r, p + t + d_r\}$. Then $H \in S(C)$ and $T \subset H$.

case 2 $t \equiv 2$ or 3 (mod 6)

By the construction of (d_r, c_r) we have
$\{1,\ldots,2t,2t+2,\ldots,3t,3t+2\} = \{1,\ldots,t,t+c_1,\ldots,t+c_t,t+d_1,\ldots,t+d_t\}$.
By Lemma 5.1.11(ii) we may assume that $y - x$ is congruent modulo $6t+3$ to one of $1,\ldots,2t$, $2t+2,\ldots,3t,3t+2$. Thus $y - x = r$ or $y - x = t + d_r$ or $y - x = t + c_r$ for some r, $1 \leqslant r \leqslant t$. Similarly to case 1 we can show that there exists H in S(C) such that $T \subset H$.

Next we assume that $y - x$ or $x - y$ is congruent to $2t + 1$ modulo $6t + 3$. We shall assume that $x - y$ is congruent to $2t + 1$ modulo $6t + 3$.

case 1. $x > y$.

In this case we have $x - y = 2t + 1$ and $1 \leqslant y \leqslant 4t + 2$. Hence $x = y + 2t + 1$. If $1 \leqslant y \leqslant 2t + 1$, let $H = \{y, y + 2t + 1, y + 4t + 2\}$. Then $H \in S(C)$ and $T \subset H$. In case $2t + 2 \leqslant y \leqslant 4t + 2$, let $z = y - (2t + 1)$. Thus $1 \leqslant z \leqslant 2t + 1$. Let $H = \{z, z + 2t + 1, z+4t+2\}$. Then $H \in S(C)$ and $T \subset H$.

case 2. $x < y$

Since $1 \leqslant x,y \leqslant 6t + 3$, hence $x - y = -(6t+3)+2t+1 = -(4t+2)$. Thus $1 \leqslant x \leqslant 2t + 1$. Let $H = \{x, x + 2t + 1, x + 4t + 2\}$. Then $H \in S(C)$ and $T \subset H$.

Therefore $(C,S(C))$ is n-STS.

5.2 Construction of n-STS, where $n = p^m = 6t+1$, p Is a Prime Number

Given any positive integer n of the form $n = p^m = 6t + 1$, where p is a prime number. We know that a field of p^m elements, $GF(p^m)$, exists and in fact the multiplicative group of such a field is cyclic. We can construct n-STS from $GF(p^m)$ as in the following theorem.

5.1.1 Theorem. Given any positive integer n of the form $n = p^m = 6t + 1$, where p is a prime number. Let g be a generator of the multiplicative group of $F = GF(p^m)$. Let $S(F)$ be the family of the following 3-subsets of F :

$\{k, k + g^r, k + g^{t+r}\}$, where $k \in F$, $r \in \{0, 1, \ldots, t - 1\}$.

Then $(F, S(F))$ is n-STS.

Proof : The total number of 3-subsets in $S(F)$ is at most $nt = \frac{1}{6} n(n - 1)$. Thus to prove that $(F, S(F))$ is n-STS, it suffices to show that for any 2-subset T of F there exists a 3-subset H in $S(F)$ such that $T \subset H$.

First we shall show that for any 2-subset T of F that contains 0 there exists a 3-subset H in $S(F)$ such that $T \subset H$. Let $T = \{0, g^i\}$ be any 2-subset of F that contains 0. We shall show by cases that there exists a 3-subset H in $S(F)$ such that $T \subset H$.

case 1. $0 \leq i \leq t - 1$.

Let $H = \{0, g^i, g^{t+i}\}$. Then $H \in S(F)$ and $T \subset H$.

case 2. $t \leq i \leq 2t - 1$

Hence $i = t + r$, where $0 \leq r \leq t - 1$. Let $H = \{0, g^r, g^{t+r}\}$. Then $H \in S(F)$ and $T \subset H$.

case 3. $2t \leq i \leq 3t - 1$.

Hence $i = 2t + r$, where $0 \leq r \leq t - 1$. Let $H = \{-g^r, -g^r + g^r, -g^r + g^{t+r}\}$. Thus $H \in S(F)$. We shall show that $T \subseteq H$. Since $g^{3t} \neq 1$ while $g^{6t} = 1$, hence $g^{3t} + 1 = 0$. Since $g^{3t} + 1 = (g^t + 1)(g^{2t} - g^t + 1)$, hence $(g^t + 1)(g^{2t} - g^t + 1) = 0$. But $g^t + 1 \neq 0$, therefore $g^{2t} - g^t + 1 = 0$ so that $g^{2t} = g^t - 1$. Hence $-g^r$ and $-g^r + g^{t+r}$ can be written as $-g^r = (-1)g^r = (g^{3t})(g^r) = g^{3t+r}$ and $-g^r + g^{t+r} = (g^t - 1)(g^r) = (g^{2t})(g^r) = g^{2t+r}$. Thus $H = \{g^{3t+r}, 0, g^{2t+r}\}$ and $T \subset H$.

case 4. $3t \leq i \leq 4t - 1$

Hence $i = 3t + r$, where $0 \leq r \leq t - 1$. Let $H = \{-g^r, -g^r + g^r, -g^r + g^{t+r}\}$. By the same argument as in case 3 we have $H \in S(F)$ and $T \subset H$.

case 5. $4t \leq i \leq 5t - 1$

Hence $i = 4t + r$, where $0 \leq r \leq t - 1$. Let $H = \{-g^{t+r}, -g^{t+r} + g^r, -g^{t+r} + g^{t+r}\}$. Thus $H \in S(F)$. Observe that $-g^{t+r} = (-1)(g^{t+r}) = (g^{3t})(g^{t+r}) = g^{4t+r}$ and $g^r - g^{t+r} = (-1)(g^r)(g^t - 1) = (g^{3t})(g^r)(g^{2t}) = g^{5t+r}$. Thus $H = \{g^{4t+r}, g^{5t+r}, 0\}$ and $T \subset H$

case 6. $5t \leq i \leq 6t - 1$

Hence $i = 5t + r$, where $0 \leq r \leq t - 1$. Let $H = \{-g^{t+r}, -g^{t+r} + g^r, -g^{t+r} + g^{t+r}\}$. By the same argument as in case 5 we have $H \in S(F)$ and $T \subset H$.

Next we shall show that for any 2-subset T of F that does not contain 0 there exists a 3-subset H in $S(F)$ such that $T \subset H$. Let $T = \{x, y\}$ be any 2-subset of F such that $x \neq 0$, $y \neq 0$. Let $T_1 = \{x - x, y - x\} = \{0, y - x\}$. Since $x \neq y$, hence $y - x \neq 0$.

Thus T_1 is a 2-subset of F that contains 0. Therefore there exists a 3-subset H_1 in S(F) such that $T_1 \subseteq H_1$. By definition of S(F) we must have $H_1 = \{k_1, k_1 + g^{r_1}, k_1 + g^{t+r_1}\}$, where $k_1 \in F$, $0 \leq r_1 \leq t - 1$. Since $\{0, y - x\} \subset \{k_1, k_1 + g^{r_1}, k_1 + g^{t+r_1}\}$, hence $\{0 + x, y - x + x\} \subseteq \{k_1 + x, k_1 + x + g^{r_1}, k_1 + x + g^{t+r_1}\}$. Let $H = \{k_1 + x, k_1 + x + g^{r_1}, k_1 + x + g^{t + r_1}\}$. Hence $H \in S(F)$ and $T \subseteq H$.

Therefore (F,S(F)) is n-STS.

5.3 Construction of 6t + 3-STS from Cyclic Group of Order 2t + 1

5.3.1 Lemma. Let F be a cyclic group of order 2t + 1. Let g be a generator of F. Then

(i) If $g^{2r} = g^{2s}$, where $0 \leq r, s < 2t + 1$, then $g^r = g^s$.

(ii) for any distinct elements a, b in F, there exists a unique element c in F such that $ab = c^2$.

(iii) If a and b are distinct elements of F, then $a^{-1}b^2$ and $b^{-1}a^2$ are distinct from a and b respectively.

Proof : (i) From $g^{2r} = g^{2s}$ we have $2r + 2s = q(2t + 1)$ for some integer q. Since $2 / 2r + 2s$, hence $2 / q(2t + 1)$. But $2 \nmid 2t + 1$, therefore $2 / q$. Thus $q = 2q'$ for some integer q'. Hence $r + s = q'(2t + 1)$ so that $g^r = g^s$.

(ii) Let a, b be any distinct elements of F. Hence $a = g^m$, $b = g^n$ for some distinct integers m , n , $0 \leq m,n \leq 2t$. If m + n is even, then there exists a unique positive integer r such that $m + n = 2r$. Since $0 \leqslant m, n \leqslant 2t$, hence $0 \leqslant r \leqslant 2t$. Let $c = g^r$. Therefore $c \in F$ and $ab = c^2$. Suppose that there exists $d = g^s$, $0 \leqslant s < 2t + 1$, in F such that $ab = d^2$. Hence $d^2 = c^2$ so that $g^{2s} = g^{2r}$. By (i) we have $g^s = g^r$. Thus $d = c$. In case that $m + n$ is odd we see that $(2t + 1) + (m + n)$ is even. Let r be the integer such that $2r = (2t + 1) + (m + n)$. Choose integers k and s such that $r = k(2t + 1) + s$, where $0 \leqslant s \leqslant 2t$. Let $c = g^s$. Hence $c \in F$. Now $ab = g^{m+n} = g^{2t+1+m+n} = g^{2r} = g^{2k(2t+1)+2s} = g^{2s} = c^2$. The uniqueness of c follows by repeating the same argument as in case that $m + n$ is even.

(iii) Let a, b be distinct elements in F. Hence $a = g^m$, $b = g^n$, for some distinct integers m,n, $0 \leqslant m,n \leqslant 2t$. Suppose that $a^{-1}b^2 = a$. Therefore $b^2 = a^2$ so that $g^{2n} = g^{2m}$. It follows from (i) that $g^m = g^n$. Hence $m = n$ which is a contradiction. Thus $a^{-1}b^2 \neq a$. Similarly we can show that $b^{-1}a^2 \neq b$.

5.3.2 Theorem. Let F be a cyclic group of order $2t + 1$, $t \geqslant 1$. Let $A = F \times \{0,1,2\}$ and let $S(A)$ be the family of the following 3-subsets of A:

(1) $\{a_0, a_1, a_2\}$, where $a \in F$,

(2) $\{a_0, b_0, c_1\}$, $\{a_1, b_1, c_2\}$, $\{a_2, b_2, c_0\}$, where $a \neq b$ and $ab = c^2$.

Then $(A, S(A))$ is $6t + 3$ - STS.

Proof : Let $n = 6t + 3$. The total number of 3-subsets in $S(A)$ of the form (1) is $2t + 1$. For any 2-subset $T = \{x, y\}$ of F, there exists a unique element z in F such that $xy = z^2$. Hence we can form exactly 3 3-subsets in $S(A)$ of the form (2) from T ; namely, $\{x_o, y_o, z_1\}$, $\{x_1, y_1, z_2\}$, $\{x_2, y_2, z_o\}$. Since there are $\binom{2t+1}{2}$ 2-subsets of F, hence the total number of 3-subsets in $S(A)$ of the form (2) is at most $\binom{2t+1}{2}3$. Therefore the total number of 3-subsets in $S(A)$ is at most $2t + 1 + \binom{2t+1}{2}3 = \frac{1}{6}(6t + 3)(6t + 2) = \frac{1}{6}n(n - 1)$. Thus to prove that $(A, S(A))$ is $6t + 3$ - STS, it suffices to show that for any 2-subset T of A there exists a 3-subset H in $S(A)$ such that $T \subset H$. Let $T = \{a_i, b_j\}$ be any 2-subset of A, We shall show by cases that there exists a 3-subset H in $S(A)$ such that $T \subsetneq H$.

case 1. $a = b$, $i \neq j$.

Let $H = \{a_o, a_1, a_2\}$. Then $H \in S(A)$ and $T = \{a_i, a_j\} \in H$.

case 2. $a \neq b$, $i = j$.

By Lemma 5.3.1 (ii) there exists c in F such that $ab = c^2$. Observe that the 3-subsets in $S(A)$ of the form (2) have two elements in the same $G_i = G \times \{i\}$ and the third element in G_{i+1}. Let $H = \{a_i, b_i, c_{i+1}\}$. Then $H \in S(A)$ and $T \subsetneq H$.

case 3. $a \neq b$, $i \neq j$.

Since $i, j \in \{0, 1, 2\}$ and $i \neq j$, hence either $j \equiv i + 1 \pmod 3$ or $i \equiv j + 1 \pmod 3$. If $j \equiv i + 1 \pmod 3$, let $c = a^{-1}b^2$. Therefore by Lemma 5.3.1 (iii) $c \neq a$ and $ac = b^2$. Let $H = \{a_i, c_i, b_j\}$. Then $H \in S(A)$ and $T \subsetneq H$. In case $i \equiv j + 1 \pmod 3$, let $d = b^{-1}a^2$. By Lemma 5.3.1(iii), $d \neq b$ and $bd = a^2$. Let $H = \{b_j, d_j, a_i\}$. Then $H \in S(A)$ and $T \subset H$.

Hence $(A, S(A))$ is $6t + 3$ - STS.

5.3.3 Remark. The construction given in Theorem 5.3.2 make use of properties (ii), (iii) in Lemma 5.3.1 only. Any group F of order $2t + 1$ with properties (ii),(iii), if exists, can be used in the above construction also.

5.4 Existence of STS with Property I and II

The notion of STS with Property I and STS with Property II has been introduced in Chapter III. Yet their existence is not known. In this section we shall show that the STS of order $n \equiv 3 \pmod 6$ constructed as in Theorem 5.3.2 are STS with Property I and II.

5.4.1 Lemma. Let (A,S(A)) and F be defined as in Theorem 5.3.2. Let g be a generator of F. For any positive integer $r \in \{1,2,\ldots, 2t+1\}$, let f_{g^r} be a mapping defined on A by $f_{g^r}(a_i) = (g^r a)_i$ for any $a \in F$, and $i = 0,1,2$. Let f be a mapping defined on A by $f(a_i) = a_{i+1}$ for any $a \in F$ and $i = 0,1,2$. Then

(i) f and f_{g^r} are automorphisms of (A,S(A)).

(ii) Let G be the subgroup of the automorphism group of (A,S(A)) generated by f_g and f. Then G is transitive and abelian.

Proof : (i) It can be verified directly that f_{g^r} and f are both permutations on A. Let H be any triple in S(A). We shall show by cases that f(H) and $f_{g^r}(H)$ belong to S(A).

case 1. H is a triple in S(A) of the form (1). Thus $H = \{x_0,x_1,x_2\}$ for some $x \in F$. Hence $f(x_0) = x_1$, $f(x_1) = x_2$, $f(x_2) = x_0$ so that $f(H) = \{x_0,x_1,x_2\} = H \in S(A)$. Let $y = g^r x$.

Then $y \in F$. Thus $f_{g^r}(x_o) = y_o$, $f_{g^r}(x_1) = y_1$, $f_{g^r}(x_2) = y_2$ so that $f_{g^r}(H) = \{ y_o, y_1, y_2 \} \in S(A)$.

case 2. H is a triple in S(A) of the form (2). Hence there exist distinct a,b,c in F with $ab = c^2$ and there exists an i in $\{0,1,2\}$ such that $H = \{a_i, b_i, c_{i+1}\}$. Hence $f(H) = \{a_{i+1}, b_{i+1}, c_{i+2}\}$ is in S(A). Let $x = g^r a$, $y = g^r b$, $z = g^r c$. Then x,y,z are members of F. Since $ab = c^2$, hence $xy = (g^r a)(g^r b) = g^{2r} ab = g^{2r} c^2 = (g^r c)^2 = z^2$. It follows that $f_{g^r}(H) = \{x_i, y_i, z_{i+1}\} \in S(A)$.

(ii) To show that G is transitive let x_i, y_j be any elements of A. We shall show by cases that there exists an automorphism h in G such that $h(x_i) = y_j$.

case 1. $x = y$.

Thus $i \neq j$. Since $i,j \in \{0,1,2\}$ and $i \neq j$, hence either $j \equiv i + 1 \pmod 3$ or $i \equiv j + 1 \pmod 3$. If $j \equiv i + 1 \pmod 3$, we have $f(x_i) = x_j$. In case $i \equiv j + 1 \pmod 3$ consider the mapping f^{-1} defined on A by $f^{-1}(x_{i+1}) = x_i$ for any $x \in F$ and $i = 0,1,2$. We can verify that f^{-1} is an automorphism of (A,S(A)) such that f^{-1} is the inverse of f. Hence $f^{-1}(x_i) = y_j$.

case 2. $x \neq y$, $i = j$.

In this case there exist distinct integers $m,n, 1 \leq m,n \leq 2t+1$, such that $x = g^m$, $y = g^n$. Let $r = (2t + 1) + (n - m)$. Then $r \in \{1,2,\ldots,2t + 1\}$, and $f_{g^r}(x_i) = (g^{2t+1+n-m} \cdot g^m)_i = (g^n)_i = y_i$.

case 3. $x \neq y$, $i \neq j$.

By case 2 there exists an automorphism h in G such that $h(x_i) = y_i$. Since $i,j \in \{0,1,2\}$ and $i \neq j$, hence we have either

$i \equiv j + 1 \pmod 3$ or $j \equiv i + 1 \pmod 3$. If $i \equiv j + 1 \pmod 3$, then $f^{-1}h(x_i) = f^{-1}(y_i) = y_j$. In case $j \equiv i + 1 \pmod 3$ we see that $f\,h(x_i) = f(y_i) = y_j$.

Hence G is transitive. To show that G is abelian it suffices to show that $ff_g = f_g f$. Let a be any element of A. Thus there exist $x \in F$ and $i \in \{0,1,2\}$ such that $a = x_i$. Hence $ff_g(a) = f((gx)_i) = (gx)_{i+1} = f_g(x_{i+1}) = f_g f(a)$. Therefore $ff_g = f_g f$.

5.4.2 <u>Lemma</u>. Let G be defined as in Lemma 5.4.1. Then $|G| = 6t + 3$.

<u>Proof</u> : Let $S = \{I, f, f^{-1}\}$, where I is the identity mapping, f is defined as in Lemma 5.4.1 and f^{-1} is the inverse of f. Then S is a subgroup of the automorphism group of $(A, S(A))$. Observe that $f_g^r \in S$ only when $f_g^r = I$. Since g has order $2t + 1$, hence $f_g^r \notin S$ as long as $1 \leqslant r < 2t + 1$ but $f_{g}{}^{2t+1} = I \in S$. Observe that G is generated by f_g and S. It follows from Theorem X of [1], p 51, that $|G| = 6t + 3$.

5.4.3 <u>Lemma</u>. Let $(A, S(A))$, g, G be defined as in Lemma 5.4.1. Let $A_o = \{(g^{2t+1})_o, g_o, (g^{t+1})_1\}$ and $\mathcal{F} = \{g(A_o) \;/\; g \in G\}$. Then $|\mathcal{F}| = 6t + 3$.

<u>Proof</u> : We shall show that distinct elements of G maps A_o into distinct triples. Let g_1, g_2 be elements of G such that $g_1(A_o) = g_2(A_o)$. Let S be defined as in the proof of Lemma 5.4.2 and let $D = \{f_g^r \;/\; r = 1,2,\ldots,2t+1\}$. It can be seen that $g_1 = s_1 f_g^{r_1}$, $g_2 = s_2 f_g^{r_2}$ for some s_1, s_2 in S and $f_g^{r_1}$, $f_g^{r_2}$ in D. Hence $s_1 f_g^{r_1}(A_o) = s_2 f_g^{r_2}(A_o)$ so that $s_2^{-1} s_1 (f_g^{r_1}(A_o) = f_g^{r_2}(A_o)$. Note

that $s_2^{-1}s_1\,(f_{g^{r_1}}(A_o)) = s_2^{-1}\,s_1(\,\{(g^{r_1})_o,(g^{r_1+1})_o,(g^{t+r_1+1})_1\})$ is of the form $\{x_o,y_o,z_1\}$ when $s_2^{-1}\,s_1 = I$ and is of the form $\{x_1,y_1,z_2\}$ when $s_2^{-1}\,s_1 = f$, and is of the form $\{x_2,y_2,z_o\}$ when $s_2^{-1}\,s_1 = f^{-1}$. But $f_{g^{r_2}}(A_o) = \{(g^{r_2})_o,(g^{r_2+1})_o,\,(g^{t+r_2+1})_1\}$ is of the form $\{x_o,y_o,z_1\}$. Hence we must have $s_2^{-1}\,s_1 = I$ so that $s_1 = s_2$. Thus $f_{g^{r_1}}(A_o) = f_{g^{r_2}}(A_o)$. But $f_{g^{r_1}}(A_o) = \{(g^{r_1})_o,(g^{r_1+1})_o,(g^{t+r_1+1})_1\}$ and $f_{g^{r_2}}\,(A_o) = \{(g^{r_2})_o,\,(g^{r_2+1})_o,\,(g^{t+r_2+1})_1\}$. Therefore $g^{t+r_1+1} = g^{t+r_2+1}$ so that $g^{r_1} = g^{r_2}$. Hence $f_{g^{r_1}} = f_{g^{r_2}}$ so that $g_1 = s_1f_{g^{r_1}} = s_2f_{g^{r_2}} = g_2$. Thus distinct elements of G maps A_o into distinct triples. Consequently we have $|\mathcal{F}| = |G| = 6t + 3$.

5.4.3 <u>Lemma</u>. Let $(A,S(A))$ and g be defined as in Lemma 5.4.1. Let $\mathcal{F}$ be defined as in Lemma 5.4.2. Then g_o is contained in exactly 3 triples in $\mathcal{F}$.

<u>Proof</u> : Observe that $A_o = \{(g^{2t+1})_o,g_o,(g^{t+1})_1\}$, $f_g(A_o) = \{g_o,\,(g_o^2),\,(g^{t+2})_1\}$, $f^{-1}f_{g^{t+1}}(A_o) = \{(g^{t+1})_2,\,(g^{t+2})_o,\,g_o\}$, are 3 distinct triples in $\mathcal{F}$ that contain g_o. Let H' be a triples in $\mathcal{F}$ that contains g_o. Thus there exists $s \in \{I,f,f^{-1}\}$ and $i \in \{1,2,\ldots,2t+1\}$ such that $H = sf_{g^i}(A_o)$. We shall show that $sf_{g^i} \in \{I,f_g,f^{-1}f_{g^{t+1}}\}$. Suppose that $s = f$. Thus $sf_{g^i}(A_o) = ff_{g^i}(A_o) = \{(g^i)_1,(g^{i+1})_1,(g^{t+i+1})_2\}$ so that $g_o \notin sf_{g^i}(A_o)$. Therefore $s = I$ or f^{-1}.

If $f = I$ we have $sf_{g^i}(A_o) = f_{g^i}(A_o) = \{(g^i)_o, (g^{i+1})_o, (g^{t+i+1})_1\}$. Since $g_o \in sf_{g^i}(A_o)$, hence either $g_o = (g^i)_o$ or $g_o = (g^{i+1})_o$. When $g_o = (g^i)_o$ we have $i = 1$. Thus $sf_{g^i} = f_g$. In case $g_o = (g^{i+1})_o$ we have $i = 0$. Hence $sf_{g^i} = I$.

If $s = f^{-1}$ we have $sf_{g^i}(A_o) = \{(g^i)_2, (g^{i+1})_2, (g^{t+i+1})_o\}$. Since $g_o \in sf_{g^i}(A_o)$, hence $g_o = (g^{t+i+1})_o$ so that $g^i = g^{t+1}$. Thus $f_{g^i} = f_{g^{t+1}}$. Therefore $sf_{g^i} = f^{-1}f_{g^{t+1}}$.

Hence g_o is contained in exactly 3 triples in $\mathcal{F}$.

5.4.5 Theorem. The STS $(A,S(A))$ constructed as in Theorem 5.3.2 is a STS with Property I and II.

Proof : To see that $(A,S(A))$ is a STS with Property I and II, let $A_i = F \times \{i\}$, $i = 0,1,2$, and $\mathcal{F} = \{\{a_o, a_1, a_2\} / \ a \in F\}$. Then A_o, A_1, A_2 and $\mathcal{F}$ satisfy Property I with respect to $(A,S(A))$ so that $(A,S(A))$ is a STS with Property I. Let G, g be defined as in Lemma 5.4.1 and let A_o, $\mathcal{F}$ be defined as in Lemma 5.4.3. Then G, A_o, $\mathcal{F}$ and g_o satisfy Property II with respect to $(A,S(A))$ so that $(A,S(A))$ is a STS with Property II.