1.3 Steiner Triple Systems

Definition 1.3.1 A Steiner triple system of order \( v \), denoted \( STS(v) \) is a \( (v, 3, 1) \)-BIBD.

Example 1.3.2 The following blocks constitute an \( STS(9) \).

\[
\begin{align*}
\{1, 2, 3\} & \quad \{1, 5, 9\} \quad \{1, 6, 8\} \quad \{1, 4, 7\} \\
\{4, 5, 6\} & \quad \{2, 6, 7\} \quad \{2, 4, 9\} \quad \{2, 5, 8\} \\
\{7, 8, 9\} & \quad \{3, 4, 8\} \quad \{3, 5, 7\} \quad \{3, 6, 9\}.
\end{align*}
\]

Example 1.3.3 The block \( \{1, 2, 3\} \) constitutes an “STS(3)”. We use the term “STS(3)” loosely, as this is not technically a BIBD (it is not incomplete). However, this design is useful in constructing STSs of higher order.

A natural question to ask is “For what values of \( v \) does an \( STS(v) \) exist?”. We consider the following theorem which gives a necessary condition for the existence of an \( STS(v) \).

Theorem 1.3.4 If an \( STS(v) \) exists, then \( v \equiv 1, 3 \pmod{6} \).

Proof. Since \( \lambda(n) = b(n) \), \( v(v - 1) = bk(k - 1) = 6b \). This is only satisfied when \( v \equiv 0, 1, 3, 4 \pmod{6} \). Moreover \( r = \frac{\lambda(v - 1)}{k - 1} = \frac{v - 1}{2} \), which gives \( v \equiv 1, 3, 5 \pmod{6} \). Therefore, \( v \equiv 1, 3 \pmod{6} \). \( \square \)

In fact, the condition that \( v \equiv 1, 3 \pmod{6} \) is also a sufficient condition for the existence of an \( STS(v) \). Before we prove this result we require the following two lemmas.

Lemma 1.3.5 If an \( STS(n) \) exists, so too does an \( STS(2n + 1) \).

Proof. Consider an \( STS(n) \) on the symbols \( x_0, x_1, \ldots, x_{n-1} \). Theorem 1.3.4 requires that \( n \) be odd so \( n - 1 \) is even (we rely on \( n \) being odd in several parts of our proof). We claim that an \( STS(2n + 1) \) is given by the blocks of the \( STS(n) \) plus the following blocks.

\[
\begin{align*}
\{i, n, x_i\}, 0 \leq i & \leq n - 1 \\
\{i + j \pmod{n}, i - j \pmod{n}, x_i\}, 0 \leq i & \leq n - 1, 1 \leq j \leq \frac{n - 1}{2}
\end{align*}
\]

In verifying that all of the blocks are of size three, our only concern is that two elements of the form \( i + j \) and \( i - j \) might be the same (in modulo \( n \)). Now \( i + j \equiv i - j \pmod{n} \) gives \( 2j \equiv 0 \pmod{n} \), however, \( n \) being odd gives \( j = 0 \), which is not permitted. As such, we can conclude that all the blocks are of size three.

It remains to show that each pair of elements is found exactly once in the design. In doing so, observe that an \( STS(2n + 1) \) should have \( b = \frac{(2n + 1)(2n)}{6} = \frac{2n^2 + n}{3} \) triples and that the proposed design has

\[
\frac{n(n - 1)}{6} + n + \frac{n - 1}{2} = \frac{4n^2 + 2n}{6} = \frac{2n^2 + n}{3}
\]

triples as well. Thereby, to show that each pair occurs exactly once in the design, we need only show that each pair occurs at least once in the design. We consider a series of cases.

- Consider a pair of the form \( (x_k, x_i) \). They occur together in a triple of the original \( STS(n) \).
- Consider a pair of the form \( (x_k, k), (x_k, n) \), or \( (k, n) \), \( k \neq n \). They occur together in the triple \( \{k, n, x_k\} \).
Consider a pair of the form \((x_k, l)\), where \(k \neq l \neq n\). Now either \(l - k \equiv \frac{n-1}{2}\) or \(k - l \equiv \frac{n-1}{2}\). Assuming that \(l - k \equiv \frac{n-1}{2}\), the pair occurs together in the triple \(\{k + (l - k) \ (mod\ n), k - (l - k) \ (mod\ n), x_k\}\). If \(k - l \equiv \frac{n-1}{2}\), the pair can be found in the triple \(\{k + (k - l) \ (mod\ n), k - (k - l) \ (mod\ n), x_k\}\), which is in fact the same triple (note that the triple does not occur twice as only one of \(l - k \ (mod\ n)\) an \(k - l \ (mod\ n)\) is no more than \(\frac{n-1}{2}\).

Consider a pair of the form \((k,l)\), where \(k \neq n, l \neq n\). Now either \(\alpha = \frac{l-k \ (mod\ n)}{2} \in \mathbb{N}\) or \(\frac{k-l \ (mod\ n)}{2} \in \mathbb{N}\) (since \(n\) is odd, one of \(l - k \ (mod\ n)\) and \(k - l \ (mod\ n)\) is even); Assume without loss of generality that \(\alpha = \frac{l-k \ (mod\ n)}{2} \in \mathbb{N}\). Since \(k \neq n, l \neq n\), we also know that \(l - k \ (mod\ n) \leq n - 1\). The pair \((k,l)\) occur together in the triple \(\{(k+\alpha) + (\alpha) \ (mod\ n), (k+\alpha) - (\alpha) \ (mod\ n), x_{k+\alpha}\} = \{l \ (mod\ n), k \ (mod\ n), x_{k+\alpha}\}\).

Having shown that all possible pairs occur together in at least one triple, we conclude that the presented design is an STS(\(2n+1\)), which gives the desired result.

\[\square\]

**Example 1.3.6** An STS(7) can be constructed from the STS(3) given by \(\{x_0, x_1, x_2\}\). The blocks of the STS(7) are

\[
\begin{align*}
\{x_0, x_1, x_2\} & \\
\{0, 3, x_0\} & \{1, 3, x_1\} \{2, 3, x_2\} \\
\{1, 2, x_0\} & \{2, 0, x_1\} \{0, 1, x_2\}
\end{align*}
\]

Similar to Lemma 1.3.5 we have the following lemma which will also be needed to prove that \(v \equiv 1, 3 \ (mod\ 6)\) is sufficient for the existence of an STS(v).

**Lemma 1.3.7** If an STS(n) exists, so too does an STS(2n + 7).

**Theorem 1.3.8** If \(v \equiv 1, 3 \ (mod\ 6)\), there exists an STS(v).

**Proof.** (By Induction) The base cases are \(v = 3\) and \(v = 9\), which have been illustrated in Examples 1.3.2 and 1.3.2.

Let \(v = k\), \((k \equiv 1, 3 \ (mod\ 6))\). Assume that there exist and STS(l) for all \(l < k \ (l \equiv 1, 3 \ (mod\ 6))\). We consider four cases, depending on the congruence of \(k\) modulo 12 (\(k = 12m + 1, k = 12m + 3, k = 12m + 7, k = 12m + 9\)).

- Let \(k = 12m + 1\). By the induction hypothesis there exists an STS(\(6m - 3\)), where \(k = 2(6m - 3) + 7\), so Lemma 1.3.7 there is an STS(\(k\)).
- Let \(k = 12m + 3\). By the induction hypothesis there exists an STS(\(6m + 1\)), where \(k = 2(6m + 1) + 1\), so Lemma 1.3.5 there is an STS(\(k\)).
- Let \(k = 12m + 7\). By the induction hypothesis there exists an STS(\(6m + 3\)), where \(k = 2(6m + 3) + 1\), so Lemma 1.3.5 there is an STS(\(k\)).
- Let \(k = 12m + 9\). By the induction hypothesis there exists an STS(\(6m + 1\)), where \(k = 2(6m + 1) + 7\), so Lemma 1.3.7 there is an STS(\(k\)).

That is, there exists an STS(\(k\)). By induction, there exists an STS(\(v\)) if \(v \equiv 1, 3 \ (mod\ 6)\). \[\square\]

Observe that the base case did not require \(v = 7\) as this can be created from an “STS(3)”.

2
1.4 Cyclic Steiner Triple Systems

1.4.1 Definition and Example

**Definition 1.4.1** An STS($v$) is cyclic if whenever \{a, b, c\} is triple, so is \{a + 1, b + 1, c + 1\} (mod $v$). We will denote a cyclic STS($v$) by CSTS($v$).

**Example 1.4.2** The triples \{0 + i, 1 + i, 3 + i\}, 0 ≤ i ≤ 6, constitute a CSTS(7).

**Example 1.4.3** The following triples constitute a CSTS(15)
\{0 + i, 2 + i, 8 + 1\}, 0 ≤ i ≤ 14
\{0 + i, 1 + i, 4 + 1\}, 0 ≤ i ≤ 14
\{0 + i, 5 + i, 10 + 1\}, 0 ≤ i ≤ 4.

In fact the necessary (and sufficient) condition for the existence of an STS($v$) is also sufficient for the existence of a CSTS($v$). That is, a CSTS($v$) exists for all $v ≡ 1, 3 \pmod{6}$. Before we prove this result we need to introduce the concept of a cyclic difference system.

1.4.2 Cyclic Difference Systems

Before defining a cyclic difference system we require the definition of a cyclic difference set.

**Definition 1.4.4** A $(v,k,λ)$ cyclic difference set is a $k$-set $D = \{d_1, \ldots, d_k\}$ for which each non-zero element $d$ of $\mathbb{Z}_v$ can be expressed as a difference of members of $D$ (i.e. $d = d_i - d_j$) in exactly $λ$ ways.

Henceforth, we will assume all our cyclic difference sets to be incomplete.

**Example 1.4.5** The set \{0, 1, 3\} is a $(7,3,1)$ cyclic difference set. The differences obtained are
\begin{align*}
0 - 1 &= -1 ≡ 6 \pmod{7}, \quad 1 - 0 = 1, \\
0 - 3 &= -3 ≡ 4, \quad 3 - 0 = 3, \\
1 - 3 &= -2 ≡ 5, \quad 3 - 1 = 2.
\end{align*}

**Example 1.4.6** The set \{0, 1, 3, 9\} is a $(13,4,1)$ cyclic difference set.

**Definition 1.4.7** A translate of a $(v,k,λ)$ cyclic difference set $D = \{d_1, \ldots, d_k\}$ is a set $\{d_1 + \alpha, \ldots, d_k + \alpha\}$, where $\alpha \in \mathbb{Z}_v$. It is denoted by $D + \alpha$.

**Example 1.4.8** Recall the $(13,4,1)$ cyclic difference set $D = \{0,1,3,9\}$. Its translates are as follows.
\begin{align*}
D + 0 &= \{0,1,3,9\} & D + 5 &= \{5,6,8,1\} & D + 9 &= \{9,10,12,5\} \\
D + 1 &= \{1,2,4,10\} & D + 6 &= \{6,7,9,2\} & D + 10 &= \{10,11,0,6\} \\
D + 2 &= \{2,3,5,11\} & D + 7 &= \{7,8,10,3\} & D + 11 &= \{11,12,1,7\} \\
D + 3 &= \{3,4,6,12\} & D + 8 &= \{8,9,11,4\} & D + 12 &= \{12,0,2,8\} \\
D + 4 &= \{4,5,7,0\}
\end{align*}

Observe that the translates of the $(13,4,1)$ cyclic difference set presented in Example 1.4.8 yield a symmetric $(13,4,1)$-BIBD. In fact this is true in general.
Theorem 1.4.9 The translates of a \((v,k,\lambda)\) cyclic difference set give a symmetric \((v,k,\lambda)\)-BIBD.

Proof. Let \(D\) be a \((v,k,\lambda)\) cyclic difference set. Trivially, the translates are all of size \(k\) where \(k < v\). Moreover, there are \(v\) translates, so the design is symmetric. It remains to show that each pair of elements occurs exactly \(\lambda\) times.

Consider a pair of elements \(a\) and \(b\). Since \(a = d_i + (a - d_i), a \in D + (a - d_i)\) for all \(i\). Similarly, \(b \in D + (b - d_j)\) for all \(j\). Thereby, \(a\) and \(b\) are in the same translate whenever \(a - d_i = b - d_j\), which gives \(a - b = d_i - d_j\). But by the definition of a cyclic difference set there are exactly \(\lambda\) combinations of \(i\) and \(j\) which give the non-zero difference of \(a - b\). That is, the elements \(a\) and \(b\) are paired \(\lambda\) times, giving the desired result. 

Now that we have been introduced to cyclic difference sets we are prepared to define cyclic difference systems.

Definition 1.4.10 A \((v,k,\lambda)\) cyclic difference system is a family of \(k\)-sets \(\{D_1, \ldots, D_t\}\) such that each non-zero element \(d\) of \(\mathbb{Z}_v\) can be expressed as a difference of members of some \(D_i\) in exactly \(\lambda\) ways. The \(k\)-sets are often referred to as base blocks.

Example 1.4.11 The sets \(\{0,1,4\}\) and \(\{0,2,7\}\) constitute a \((13,3,1)\) cyclic difference system. The differences obtained are

\[
\begin{align*}
0 - 1 &= -1 \equiv 12 \pmod{13}, & 1 - 0 &= 1, \\
0 - 4 &= -4 \equiv 9, & 4 - 0 &= 4, \\
1 - 4 &= -3 \equiv 10, & 4 - 1 &= 3, \\
0 - 2 &= -2 \equiv 11, & 2 - 0 &= 2, \\
0 - 7 &= -7 \equiv 6, & 7 - 0 &= 7, \\
2 - 7 &= -5 \equiv 8, & 7 - 2 &= 5.
\end{align*}
\]

Example 1.4.12 The sets \(\{0,1,2\}\), \(\{0,2,8\}\), \(\{0,3,7\}\), \(\{0,4,7\}\), and \(\{0,5,10\}\) are a \((16,3,2)\) cyclic difference system.

Similar to the translates of a cyclic difference set we define the translates of the base blocks of cyclic difference system. However, the translates of base blocks in cyclic difference systems are not always unique. For instance, in Example 1.4.12 the base block has \(\{0,5,10\}\) has only five unique translates. Base blocks such as these are often referred to as short blocks.

The natural question to ask is “how do cyclic difference systems relate to CSTSs?” To answer this question we must really consider the cases \(v \equiv 1 \pmod{6}\) and \(v \equiv 3 \pmod{6}\) separately.

- \(v = 6m + 1\)

Such a CSTS has \(b = \frac{1}{6}(6m + 1)(6m) = m(6m + 1)\) blocks. If we can find an \(m\) block \((6m + 1,3,1)\) cyclic difference system, the translates will give an CSTS\((6m + 1)\).

Theorem 1.4.13 Suppose that \(\{1, \ldots, 3m\}\) can be partitioned into \(m\) triples \(\{a,b,c\}\), where \(a + b \equiv c \pmod{6m + 1}\) or \(a + b \equiv -c \pmod{6m + 1}\). Then the \(m\) triples \(\{0,a,a+b\}\) form a \((6m + 1,3,1)\) cyclic difference system (which can be used to make a CSTS\((6m + 1)\)).

Proof. The differences that result from the triple \(\{0,a,a+b\}\) are \(\pm a, \pm b, \text{ and } \pm (a + b) = \pm c\). But the blocks \(\{a,b,c\}\) partition the set \(\{1, \ldots, 3m\}\) so the differences obtained are \(\pm 1, \ldots, \pm 3m\), which are all the non-zero differences in \(\mathbb{Z}_{6m+1}\). □
But how do we find such partitions? One such partition is known as a Skolem triple system.

**Definition 1.4.14** A Skolem triple system of order $m$ is a partition of $\{1, \ldots, 3m\}$ into $m$ triples of the form $\{i, a_i, i + a_i\}$, $1 \leq i \leq m$.

**Theorem 1.4.15** A Skolem triple system of order $m$ can only exist if $m \equiv 0, 1 \pmod{4}$.

**Proof.** Consider a Skolem triple system consisting of the triples $\{i, a_i, i + a_i\}, 1 \leq i \leq m$.

Now

$$\sum_{i=1}^{m} (i + a_i) = \sum_{i=1}^{m} \frac{2(i + a_i)}{2} = \frac{\sum_{i=1}^{m} i + \sum_{i=1}^{m} a_i + \sum_{i=1}^{m} (i + a_i)}{2} = \frac{\sum_{k=1}^{3m} k}{2} = \frac{3m(3m + 1)}{4},$$

But $\frac{3m(3m + 1)}{4}$ is only an integer if $m \equiv 0, 1 \pmod{4}$. □

In fact, this necessary conditions on the existence of a Skolem triple system is also sufficient. Thereby, a cyclic STS($6m + 1$) exists for all $m \equiv 0, 1 \pmod{4}$. To deal with the remaining cases ($m \equiv 2, 3 \pmod{4}$) we rely on a structure called an O’Keefe triple system which is very similar to a Skolem triple system.

**Definition 1.4.16** An O’Keefe triple system of order $m$ is a partition of $\{1, \ldots, 3m - 1, 3m + 1\}$ into triples of the form $\{i, a_i, i + a_i\}$, $1 \leq i \leq m$.

**Theorem 1.4.17** An O’Keefe triple system of order $m$ exists if and only if $m \equiv 2, 3 \pmod{4}$.

Observe that if the unique triple containing $3m + 1$ is replaced by the triple $\{i, a_i, 3m\}$, this partition of $\{1, \ldots, 3m\}$ will satisfy the requirements of Theorem 1.4.13 ($i + a_i = 3m + 1 \equiv -3m \pmod{6m + 1}$). Thereby, a CSTS($6m + 1$) exists if $m \equiv 2, 3 \pmod{4}$, which in turn gives that an CSTS($v$) exists if $v \equiv 1 \pmod{6}$.

- $v = 6m + 3$

Such a CSTS contains

$$b = \frac{1}{6}(6m + 3)(6m + 2) = \frac{36m^2 + 30m + 6}{6} = 6m^2 + 5m + 1 = (2m + 1) + m(6m + 3)$$

blocks. Since this is not a multiple of $6m + 3$ we cannot simply use the $6m + 3$ translates of a cyclic difference system with $m$ triples. We can, however, use the translates of $m$ triples along with $2m + 1$ translates of a short block.

**Definition 1.4.18** A modified cyclic difference system of triples over $\mathbb{Z}_{6m+3}$ is a set of $m$ triples which contain all the non-zero differences of $\mathbb{Z}_{6m+3}$ except $2m + 1$ and $4m + 2$.

**Theorem 1.4.19** If a modified cyclic difference system of triples over $\mathbb{Z}_{6m+3}$ exists, so does a CSTS($6m + 3$).

**Proof.** Take all the translates of the triples in the modified cyclic difference system; this will contain all the pairs except those differing by $2m + 1$ and $4m + 2$. To complete the CSTS, include the first $2m + 1$ triples of the short block $\{0, 2m + 1, 4m + 2\}$. □

We obtain modified cyclic difference systems using Rosa triple systems.
**Definition 1.4.20** A Rosa triple system of order \( m \) is a partition of \([1, \ldots, 2m, 2m + 2, \ldots, 3m + 1] \) or \([1, \ldots, 2m, 2m + 2, \ldots, 3m, 3m + 2] \) into triples of the form \( \{i, a_i, i + a_i\} \), \( 1 \leq i \leq m \).

**Theorem 1.4.21** A Rosa triple system of order \( m \) exists for all \( m \geq 2 \).

From Theorem 1.4.21 we get that a CSTS(\( v \)) exists if \( v \equiv 3 \pmod{6} \), providing \( v \neq 9 \). This in turn gives the following theorem.

**Theorem 1.4.22** There exists a CSTS(\( v \)) for all \( v \equiv 1, 3 \pmod{6} \), \( v \neq 9 \).

### 1.5 \( t \)-designs

In a BIBD we have each pair of elements occurring in the same block exactly \( \lambda \) times. This notion of balancing pairs can also be extended to subsets of larger size. To this effect we consider the definition of a \( t \)-design.

**Definition 1.5.1** A \( t-(v,k,\lambda) \) design is a pair \( (V,B) \), where \( V \) is a \( v \)-set and \( B \) is a collection of \( k \)-subset of \( V \) (blocks), such that every \( t \)-subset of \( V \) occurs in exactly \( \lambda \) blocks. A \( t-(v,k,\lambda) \) design is sometimes referred to as a \( (v,k,\lambda) \) \( t \)-design.

**Example 1.5.2** A \( (v,k,\lambda) \)-BIBD is a \( 2-(v,k,\lambda) \) design.

**Example 1.5.3** The following are the blocks of a \( 3-(8,4,1) \) design.

\[ \{0 + i, 1 + i, 3 + i, 7\}, \quad 0 \leq i \leq 6 \]
\[ \{0 + i, 2 + i, 3 + i, 4 + i\}, \quad 0 \leq i \leq 6 \]

**Theorem 1.5.4** If \( 1 < s < t \) then a \( t-(v,k,\lambda) \) design is also an \( s-(v,k,\lambda_s) \) design, where

\[ \lambda_s = \frac{\lambda^{(v-s)}(k-s)}{(t-s)} \]

**Proof.** Consider a \( t-(v,k,\lambda) \) design \( (V,B) \). It suffices to show that each \( s \)-subset of \( V \) occurs in \( \lambda_s \) blocks of \( (V,B) \).

Let \( A \) be an \( s \)-subset of \( V \), let \( \lambda_A \) be the number of times \( A \) occurs in \( (V,B) \), and let \( N \) be the number of pairs of the form \( (D,B) \), where \( D \) is a \( t \)-subset of \( V \) containing \( A \) and \( B \) is a block of \( B \) containing \( D \). Now, if \( A \) appears in a block \( B \), there are \( t-s \) choices for the remaining members of \( D \) which are to be taken from the \( k-s \) remaining members of \( B \). But \( A \) appears in \( \lambda_A \) such blocks, so \( N = \lambda_A \binom{k-s}{t-s} \). On the other hand, if \( A \) is contained in a \( t \)-subset \( D \) of \( V \), then there are \( t-s \) choices for the remaining elements of \( D \) which are to be chosen from the \( v-s \) remaining elements of \( V \). However, each such \( t \)-element subset \( D \) occurs in exactly \( \lambda \) blocks, so \( N = \lambda \binom{v-s}{t-s} \).

Having \( \lambda_A = \frac{\lambda^{(v-s)}(k-s)}{(t-s)} \), we observe that this value is independant of the choice of \( A \), so all \( s \)-subsets of \( V \) occur in \( \frac{\lambda^{(v-s)}(k-s)}{(t-s)} \) blocks, giving the desired result. \( \square \)