Design Theory

Chapter 1. Steiner Triple Systems

1.7. Cyclic Steiner Triple Systems—Proofs of Theorems

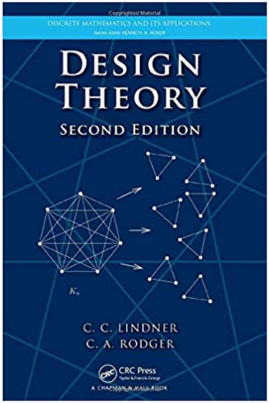

Table of contents

Theorem 1.7.6

Theorem 1.7.6. A cyclic Steiner triple system of order v exists if and only if $v \equiv 1$ or $3 \pmod 6$ and $v \neq 9$.

Proof. For $v \equiv 1$ or $3 \pmod 6$, $v \neq 9$, let $D(v)$ denote the set of difference triples that are a solution to Heffter's Difference Problem. Let $B(v)$ be the collection of base blocks obtained from the difference triples in $D(v)$. Define a cyclic $STS(v)$, (S, T), where $S = \{0, 1, 2, \ldots, v-1\}$ and T is as follows:

(1) If $v = 6n + 1$ then

$$T = \{\{i, x+i, x+y+i\} \mid 0 \leq i \leq v-1, \{0, x, x+y\} \in B(v)\}.$$

(2) If $v = 6n + 3$ then

$$T = \{\{i, x+i, x+y+i\} \mid 0 \leq i \leq v-1, \{0, x, x+y\} \in B(v)\}$$

$$\cup \{\{i, 2n+1+i, 4n+2+i\} \mid 0 \leq i \leq 2n\}.$$

Theorem 1.7.6

Theorem 1.7.6. A cyclic Steiner triple system of order v exists if and only if $v \equiv 1$ or $3 \pmod 6$ and $v \neq 9$.

Proof. For $v \equiv 1$ or $3 \pmod 6$, $v \neq 9$, let $D(v)$ denote the set of difference triples that are a solution to Heffter's Difference Problem. Let $B(v)$ be the collection of base blocks obtained from the difference triples in $D(v)$. Define a cyclic $STS(v)$, (S, T), where $S = \{0, 1, 2, \ldots, v-1\}$ and T is as follows:

(1) If $v = 6n + 1$ then

$$T = \{\{i, x+i, x+y+i\} \mid 0 \leq i \leq v-1, \{0, x, x+y\} \in B(v)\}.$$

(2) If $v = 6n + 3$ then

$$T = \{\{i, x+i, x+y+i\} \mid 0 \leq i \leq v-1, \{0, x, x+y\} \in B(v)\}$$

$$\cup\{\{i, 2n+1+i, 4n+2+i\} \mid 0 \leq i \leq 2n\}.$$

Theorem 1.7.6 (continued 1)

Theorem 1.7.6. A cyclic Steiner triple system of order v exists if and only if $v \equiv 1$ or 3 (mod 6) and $v \neq 9$.

Proof (continued). For (1), there are $3n$ differences and n base blocks, so T contains $vn = v(v-1)/6$ triples. In (2), the set of triples $\{\{i, 2n+1+i, 4n+2+i\} \mid 0 \leq i \leq 2n\}$ (which is of cardinality $v/2 = 2n+1$) is a *short orbit* and $\{0, 2n+1m4n+2\}$ is the base block for the short orbit. For (2), there are $3n+1$ differences, one short orbit base block, and n non-short-orbit base blocks so that T contains $vn + v/3 = v(v-3)/6 + v/3 = (v(v-3)+2v)/6 = (v^2-v)/6 = v(v-1)/6$ triples.

Notice that for any $\{x, y, z\} \in D(v)$, the corresponding triples $\{i, x+i, x+y+i\}$ in T have the three associated differences $(x+i)-(i) = x$, $(x+y+i)-(x+i) = y$, and $(x+y+i)-(i) = x+y \equiv \pm z \pmod{v}$.

Theorem 1.7.6 (continued 1)

Theorem 1.7.6. A cyclic Steiner triple system of order v exists if and only if $v \equiv 1$ or $3 \pmod{6}$ and $v \neq 9$.

Proof (continued). For (1), there are $3n$ differences and n base blocks, so T contains $vn = v(v-1)/6$ triples. In (2), the set of triples $\{\{i, 2n+1+i, 4n+2+i\} \mid 0 \leq i \leq 2n\}$ (which is of cardinality $v/2 = 2n+1$) is a *short orbit* and $\{0, 2n+1m4n+2\}$ is the base block for the short orbit. For (2), there are $3n+1$ differences, one short orbit base block, and n non-short-orbit base blocks so that T contains $vn+v/3 = v(v-3)/6+v/3 = (v(v-3)+2v)/6 = (v^2-v)/6 = v(v-1)/6$ triples.

Notice that for any $\{x, y, z\} \in D(v)$, the corresponding triples $\{i, x+i, x+y+i\}$ in T have the three associated differences $(x+i)-(i) = x$, $(x+y+i)-(x+i) = y$, and $(x+y+i)-(i) = x+y \equiv \pm z \pmod{v}$.

Theorem 1.7.6 (continued 2)

Theorem 1.7.6. A cyclic Steiner triple system of order v exists if and only if $v \equiv 1$ or $3 \pmod 6$ and $v \neq 9$.

Proof (continued). So for any pair of symbols a and b in $\{0, 1, \ldots, v-1\}$, say $a - b = d$ or $b - a = -d$ where we can assume $1 \leq d \leq (v-1)/2$ by Note 1.7.A. Then either (a) $v = 6n + 3$ and $d = 2n + 1$ in which case $\{a, b\}$ is in a triple $\{i, 2n+1+i, 4n+2+i\}$ for some i (that is, the pair a and b appear in a short orbit triple), or (b) otherwise $d \in \{x, y, z\} \in D(v)$ and $\{a, b\} = \{i, x+i, x+y+i\}$ for some i. That is, every pair of symbols occurs in at least one triple of T. Since $|T| = v(v-1)/$, then by Exercise 1.1.4 (S, T) is a Steiner triple system. By construction, (S, T) is cyclic and admits the automorphism $(0, 1, 2, \ldots, v-1)$.

We leave the proof that a cyclic $STS(9)$ does not exist to Exercise 1.7.A. □

Theorem 1.7.6 (continued 2)

Theorem 1.7.6. A cyclic Steiner triple system of order v exists if and only if $v \equiv 1$ or 3 (mod 6) and $v \neq 9$.

Proof (continued). So for any pair of symbols a and b in $\{0, 1, \ldots, v-1\}$, say $a - b = d$ or $b - a = -d$ where we can assume $1 \leq d \leq (v-1)/2$ by Note 1.7.A. Then either (a) $v = 6n + 3$ and $d = 2n + 1$ in which case $\{a, b\}$ is in a triple $\{i, 2n + 1 + i, 4n + 2 + i\}$ for some i (that is, the pair a and b appear in a short orbit triple), or (b) otherwise $d \in \{x, y, z\} \in D(v)$ and $\{a, b\} = \{i, x + i, x + y + i\}$ for some i. That is, every pair of symbols occurs in at least one triple of T. Since $|T| = v(v-1)/$, then by Exercise 1.1.4 (S, T) is a Steiner triple system. By construction, (S, T) is cyclic and admits the automorphism $(0, 1, 2, \ldots, v-1)$.

We leave the proof that a cyclic $STS(9)$ does not exist to Exercise 1.7.A. □