# 1.7. Cyclic Steiner Triple Systems

**Note.** In this section, we present direct constructions of Steiner triple systems. That is, we start with the order of the Steiner triple system and then give the specific triples forming the triple system. Notice that in Sections 1.2 and 1.3 (the Bose and Skolem constructions), the triples were given in terms of quasigroups; we know the quasigroups exist but we did not give the triples directly, but instead only indirectly in terms of *some* quasigroup of a particular order. In Section 1.7 (the Wilson construction) we gave the triples indirectly in terms of a 1-factorization of the deficiency graph of a certain order.

**Note.** We start with the definition of an automorphism of a Steiner triple system. In general, an automorphism of a mathematical object is an isomorphism of the object with itself. An isomorphism, in general, is a bijection (that is, a one to one and onto mapping, or equivalently an injective surjection) of a mathematical object with itself that preserves structure. You see this in Linear Algebra (MATH 2010) when defining an isomorphism between vector spaces (see my online notes on Section 3.3. Coordinatization of Vectors), in Introduction to Graph Theory (MATH 4347/5347) when defining an isomorphism between graphs (see my online on Section 1.2. Subgraphs, Isomorphic Graphs), and in Introduction to Modern Algebra (MATH 4127/5127) when defining an isomorphism between groups (see my notes on Section I.3. Isomorphic Binary Structures where an isomorphic binary structure is defined; by the way, this definition could be applied to quasigroups as well).

**Note.** Since an automorphism involves a bijection, we are interested in the structure of bijections between finite sets; recall that a bijection of a set is also called a permutation of the set. In Introduction to Modern Algebra (MATH 4127/5127), we see that every permutation of a finite set is a product of disjoint cycles (see Theorem 9.8 in Section II.9. Orbits, Cycles, Alternating Groups). This allows us to classify permutations of finite sets in terms of the number of cycles of specific lengths. In particular, if the permutation of a set of size $v$ consists of a single cycle of length $v$ then the permutation is called "cyclic." This idea is the motivation for a cyclic Steiner triple system, as follows.

**Definition.** An *automorphism* of a Steiner triple system $(S, T)$ is a bijection $\alpha : S \to S$ such that $t = \{x, y, z\} \in T$ is and only if $t\alpha = \{x\alpha, y\alpha, z\alpha\} \in T$. (Here, we use the notation "$t\alpha$" to denote "$\alpha(t)$," so we have $\alpha$ applied to both points in $S$ and triples in $T$.) A $STS(v)$ is *cyclic* if it has an automorphism that is a permutation consisting of a single cycle of length $v$.

**Example 1.7.1. (a)** With $S = \{1, 2, 3, 4, 5, 6, 7\}$ and

$$T = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{6, 7, 2\}, \{7, 1, 3\}\},$$

we have that $(S, T)$ is a cyclic $STS(7)$ which admits the automorphism $\alpha = (1, 2, 3, 4, 5, 6, 7)$ (in the standard cyclic notation of Section II.9. Orbits, Cycles, and the Alternating Groups from Introduction to Modern Algebra [MATH 4127/5127]). In fact, this is the example of a $STS(7)$ given in Example 1.1.1 and illustrated in Note 1.1.A.

**(b)** With $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and let $T$ be the set containing the triples

$$\begin{array}{cccc} \{1,2,3\} & \{1,4,7\} & \{1,5,9\} & \{1,6,8\} \\ \{4,5,6\} & \{2,5,8\} & \{2,6,7\} & \{2,4,9\} \\ \{7,8,9\} & \{3,6,9\} & \{3,4,8\} & \{3,5,7\} \end{array}$$

Then $(S, T)$ is a Steiner triple system of order 9 that admits the permutation $\alpha = (1, 2, 3)(4, 5, 6)(7, 8, 9)$ (notice that $\alpha$ fixes the three triples in the first column, and permutes the three triples in each of the other columns). However, $(S, T)$ is not cyclic (though we have not established this).

**Note.** We'll see that a cyclic Steiner triple system exists for all $v \equiv 1$ or 3 (mod 6), except for $v = 9$. This will allow us to give direct constructions of all Steiner triple systems. A solution to this problem of constructing cyclic Steiner triple systems was posed by Lothar Heffter (June 11, 1862–January 1, 1962) in "Ueber Tripelsysteme," *Mathematische Annalen* **49**(1), 101–112 (1897). This paper is available online on the Archive.org webpage. He did not solve the problem, however. It was solved by Rose Peltesohn (May 16, 1913–March 21, 1998) in "Eine Lösung der beiden Heffterschen Differenzenprobleme [A Solution to the Two Heffter Difference Problems]," *Compositio Mathematica*, **6** 251–257 (1939). This paper is available online on the Numdam website, but the result is also given in Appendix A of the text book.

Lothar Heffter

Rose Peltesohn

Lothar Heffter studied in Heidelberg and Berlin. He worked at the University of Kiel and Albert Ludwigs University of Freiburg (founded in 1457); he retired in 1931. His research interests include linear differential equations, the theory of functions, and analytic geometry. He also studied the four-color theorem and criticized an alleged proof due to Percy Heawood. Rose Peltesohn studied at the University of Berlin where she got her Ph.D. in 1936. She was Jewish and emigrated from Germany, through Italy, to Palestine in 1938, where she worked in a bank, as a legal secretary, and a translator in Tel Aviv. Her best known work is the solution to Heffter's difference problem, as we discuss next. This biographical information and the images are from the German Wikipedia website on Lothar Heffter and the Wikipedia webpage on Rose Peltesohn. These websites were all accessed 5/12/2022.

**Definition.** For each integer $v$, define a *difference triple* to be a subset of three distinct elements of $\{1, 2, \ldots, v-1\}$ such that either (i) their sum is 0 (mod $v$), or (ii) one element is the sum of the other two modulo $v$. That is, distinct $x, y, z \in \{1, 2, \ldots, v-1\}$ form a difference triple if $x + y \equiv \pm z \pmod{v}$.

**Note 1.7.A.** Notice that if $x, y, z$ form a difference triple because $x + y \equiv z$ (mod $v$), then $x, y, v - z$ is also a difference triple. We will take advantage of this option of trading $z$ for $-z \equiv v - z \pmod{v}$ when solving Heffter's Difference Problems.

**Note.** We now state **Heffter's First and Second Difference Problems**.

**(1)** Let $v = 6n + 1$. Is it possible to partition the set $\{1, 2, \ldots, 3n\}$ into difference triples?

**(2)** Let $v = 6n + 3$. Is it possible to partition the set $\{1, 2, \ldots, 3n + 1\} \setminus \{2n + 1\}$ into difference triples?

Notice that Heffter's First Difference Problem deals with partitioning the set $\{1, 2, \ldots, (v - 1)/2\}$, and Heffter's Second Difference Problem deals with partitioning the set $\{1, 2, \ldots, (v - 1)/2\} \setminus \{v/3\}$. We'll see below in the proof of Theorem 1.7.6 how the difference $v/3$ plays a special role.

**Example 1.7.2. (b)** A solution to Heffter's First Difference Problem for $v = 13$ requires us to consider the set $\{1, 2, \ldots, 6\}$. The two triples $\{1, 3, 4\}$ and $\{2, 5, 6\}$ offer a solution to the difference problem because $1 + 3 = 4$ and $2 + 5 + 6 \equiv 0$ (mod 13).

**(c)** A solution of Heffter's Second Difference Problem for $v = 9$ requires us to consider the set $\{1, 2, 3, 4\} \setminus \{3\} = \{1, 2, 4\}$. But $\{1, 2, 4\}$ is not a difference triple modulo 9, so there is no solution to Heffter's Second Difference Problem when $v = 9$ and $n = 1$. We'll see that this is the only exception and that there is a solution for all other $n \in \mathbb{N}$.

**(d)** A solution of Heffter's Second Difference Problem for $v = 15$ requires us to consider the set $\{1, 2, 3, 4, 5, 6, 7\} \setminus \{5\} = \{1, 2, 3, 4, 6, 7\}$. The two triples $\{1, 3, 4\}$ and $\{2, 6, 7\}$ offer a solution to the difference problem because $1 + 3 = 4$ and $2 + 6 + 7 \equiv 0 \pmod{15}$.

**Definition.** If $\{x, y, z\}$ is a difference triple (that is, $x + y = \pm z \pmod{v}$), then the corresponding *base block* is the triple $\{0, x, x + y\}$.

**Example 1.7.4.** The base blocks corresponding with the difference triples $\{1, 3, 4\}$ and $\{2, 5, 6\}$ of Example 1.7.2(b) (where $v = 13$) are $\{0, 1, 4\}$ and $\{0, 2, 7\}$. The base blocks corresponding with the difference triples $\{1, 3, 4\}$ and $\{2, 6, 7\}$ of Example 1.7.2(d) (where $v = 15$) are $\{0, 1, 4\}$ and $\{0, 2, 8\}$. Notice that we do not *yet* have a base block corresponding to the omitted difference $v/3 = 5$, but we will (it will be the "short orbit" triple $\{0, 5, 10\}$). With a complete solution of Heffter's Difference Problems, we can then produce cyclic Steiner triple systems of all orders (except for the small order 9). The idea of giving these direct constructions of Steiner triple systems is due to Heffter (1897) and the solution to the difference problem is due to Peltesohn (1939).

**Note.** Peltesohn's solutions to Heffter's First and Second Difference Problems are given in Appendix A. We now go to the construction of the cyclic Steiner triple systems and leave the details of Heffter's difference problems to Appendix A.

**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 $v \neq 9$.

**Example 1.7.7.** In Example 1.7.4 we saw that $\{0,1,4\}$ and $\{0,2,7\}$ are base blocks for a cyclic $STS(13)$. As in the proof of Theorem 1.7.6, we take $S = \{0,1,2,\ldots,12\}$ and the set of triples

$$T = \{\{i, 1_i, 4+i\}, \{i, 2+i, 7+i\} \mid 0 \leq i \leq 12\},$$

where all sums are reduced modulo $v = 13$, form a cyclic $STS(13)$. We also saw in Example 1.7.4 that $\{0,1,4\}$ and $\{0,2,8\}$ are base blocks for a cyclic $STS(15)$, but we also have to include the short orbit block associated with difference 5 or $\{0,5,10\}$. With $S = \{0,1,2,\ldots,14\}$ and the set of triples

$$T = \{\{i, 1+i, 4+i\}, \{i, 2+i, 8+i\} \mid 0 \leq i \leq 14\} \cup \{\{i, 5+i, 10+i\} \mid 0 \leq i \leq 4\},$$

where all sums are reduced modulo $v = 15$, form a cyclic $STS(15)$.

**Note.** You will see in Appendix A that Peltesohn works with values of $v$ modulo 18 and so has to consider six cases (along with seven small cases that do not fit her general patterns). This construction was addressed again in the late

1950s and early 1960s by Skolem (involving $(A, k)$-systems, 1957), O'Keefe (involving $(B, k)$-systems, 1961), and Rosa (involving $(C, k)$-systems and $(D, k)$-systems, 1966). Details are given in my online supplemental notes for Graph Theory 1 (MATH 5410) on Supplement. Graph Decompositions: Triple Systems. In fact, these results, along with several examples, were covered in Chapter II, "Cyclic Steiner Triple Systems," of my master's thesis *Automorphisms of Steiner Triple Systems* (Auburn University, 1987).

*Revised: 9/8/2022*