1.3. $v \equiv 1 \pmod 6$: The Skolem Construction

Note. In this section, we show that the condition $v \equiv 1 \pmod 6$ is sufficient for the existence of a Steiner triple system of order v. The method of proof is due to Thoralf A. Skolem (May 23, 1887–March 23, 1963). His results appear in "Some remarks on the triple systems of Steiner," *Mathematica Scandinavia*, **6** 273–280 (1958). His original paper can be viewed online through JSTOR and the Mathematica Scandinavica webpage.

Note. Thoralf Skolem was a Norwegian mathematician who published almost 200 papers in the areas of set theory, mathematical logic, Diophantine equations, group theory, and lattice theory. He did not complete his doctorate until he was 40 years old. He was of the opinion that a Ph.D. was unnecessary. He was a research follow at the University of Oslo and was elected to the Norwegian Academy of Science and Letters before getting his Ph.D., so he wasn't wrong. He stayed with the University of Oslo until 1930 and again from 1938 until he retired in 1957. He was president of the Norwegian Mathematical Society and founding editor of *Mathematica Scandinavica*. Notice that his paper on Steiner triple systems appeared after his retirement—it seems that this is a result of secondary interest in his body of work. This biographical information and the image below are from the MacTutor History of Mathematics Archive webpage on Skolem. Additional biographical information is on the Wikipedia webpage on Th. Skolem and in Jens E. Fenstad, "Thoralf Albert Skolem 1887-1963: A Biographical Sketch," *Nordic Journal of Philosophical Logic*, **1**, 99–106 (1996) (each webpage accessed 5/11/2022). None of these sources reference the 1958 paper of triple systems.

Thoralf A. Skolem (May 23, 1887–March 23, 1963)

Definition. A *latin square* (or quasigroup) L of order $2n$ is *half-idempotent* if for $1 \leq i \leq n$ cells (i,i) and $(n+i, n+i)$ of L contain symbol i.

Example 1.3.1. Examples of half-idempotent commutative quasigroups include:

$\circ$	1	2	3	4
1	1	3	2	4
2	3	2	4	1
3	2	4	1	3
4	4	1	3	2

$\circ$	1	2	3	4	5	6
1	1	4	2	5	3	6
2	4	2	5	3	6	1
3	2	5	3	6	1	4
4	5	3	6	1	4	2
5	3	6	1	4	2	5
6	6	1	4	2	5	3

Note. In Exercise 1.3.2(c), a half-idempotent commutative quasigroup of all even orders is to be given. With these structures known to exist, we can now present the Skolem construction.

Note. We start by describing the Skolem construction. Let $v \equiv 1 \pmod 6$, say $v = 6n+1$. Let $(Q, \circ)$ be a half-idempotent commutative quasigroup of order $2n$ where $Q = \{1, 2, \ldots, 2n\}$ (which is known to exist by Exercise 1.3.2(c)). Let S be the Cartesian product $S = \{\infty\} \cup (Q \times \{1, 2, 3\})$. Define the set T that contains the following triples of elements of S:

Type 1: For $1 \le i \le n$ we have the "Type 1" triples $\{(i, 1), (i, 2), (i, 3)\}$ in T.

Type 2: For $1 \le i \le n$ we have the Type 2 triples $\{\infty, (n+i, 1), (i, 2)\}$, $\{\infty, (n+i, 2), (i, 3)\}$, and $\{\infty, (n+i, 3), (i, 1)\}$ in T.

Type 3: For $1 \le i < j \le 2n$ we have the Type 3 triples $\{(i, 1), (j, 1), (i \circ j, 2)\}$, $\{(i, 2), (j, 2), (i \circ j, 3)\}$, $\{(i, 3), (j, 3), (i \circ j, 1)\}$ in T.

It is be shown in Exercise 1.3.7 that (S, T) is a Steiner triple system of order $6n+1$, which we now state as a theorem.

Theorem 1.3.A. A Steiner triple system of all orders $v \equiv 1 \pmod 6$ exists.

Note 1.3.A. Notice that $|S| = 6n+1$ and that T contains triples of S. There are n Type 1 triples, $3n$ Type 2 triples, and $3\binom{2n}{2} = 3\frac{(2n)(2n-1)}{2} = 3n(2n-1)$ Type 3 triples.

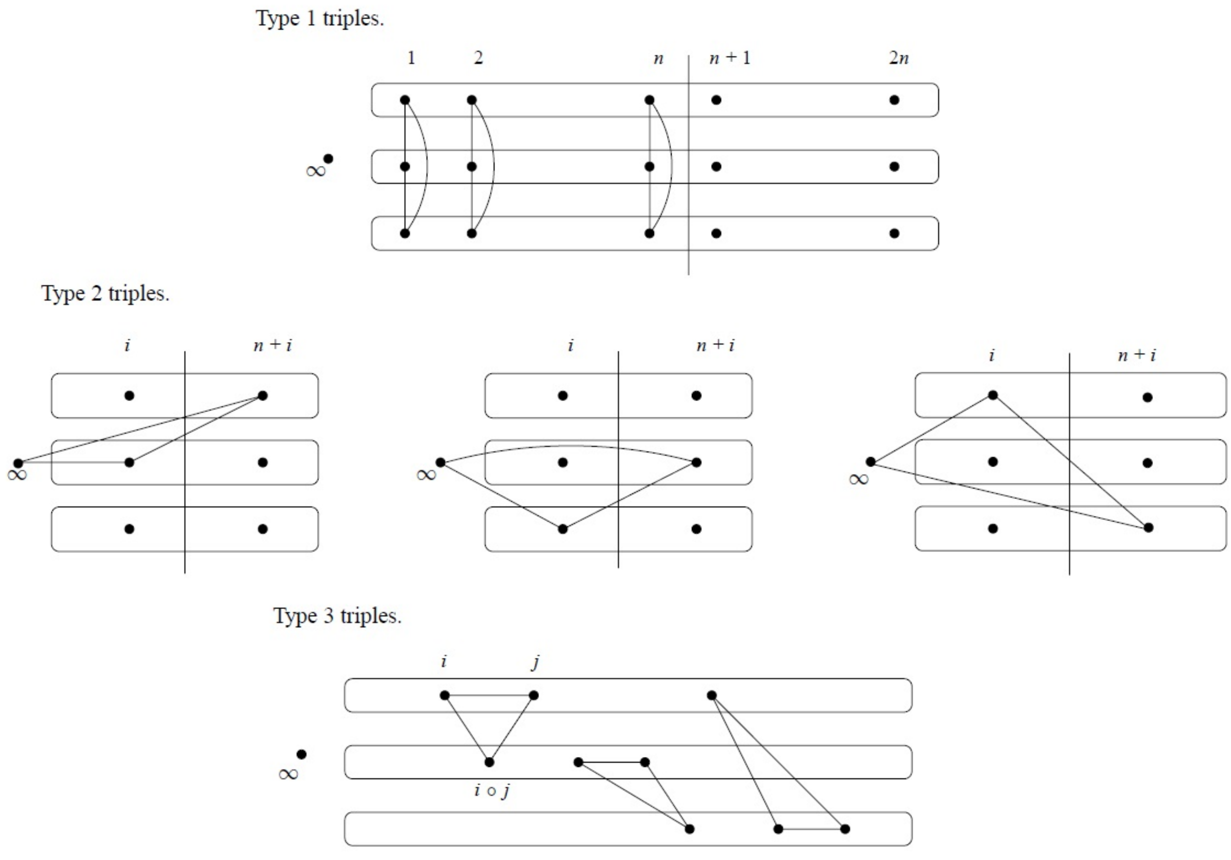

Figure 1.5: The Skolem Construction.

Note. We can now combine the necessary conditions of Lemma 1.1.A with the sufficient conditions of Theorems 1.2.A and 1.3.A to get the following classification of Steiner triple systems.

Theorem 1.3.B. A Steiner triple system of order v exists if and only if $v \equiv 1$ or 3 (mod 6).

Example 1.3.3. We now use the Skolem construction of make a $STS(7)$. We need a half-idempotent commutative quasigroup of order 2, $(Q, \circ)$, we use

$\circ$	1	2
1	1	2
2	2	1

With $S = \{\infty\} \cup (\{1,2\} \times \{1,2,3\})$, set T contains the triples:

Type 1: $\{(1,1),(1,2),(1,3)\}$,

Type 2: $\{\infty,(2,1),(1,2)\}$, $\{\infty,(2,2),(1,3)\}$, $\{\infty,(2,3),(1,1)$$, and

Type 3: $\{(1,1),(2,1),(2,2)\}$, $\{(1,2),(2,2),(2,3)\}$, $\{(1,3),(2,3),(2,1)\}$,

where the third entry in the Type 3 triples result from the fact that $1 \circ 2 = 2$. This is a small Steiner triple system and it is easy to check that each of the $\binom{7}{2} = 21$ pairs of elements of S are in some triple.

Example 1.3.4(b). As in Example 1.2.5, we now consider the Skolem construction based on the following half-idempotent commutative quasigroup given below, and use it to find the triple containing particular given pairs of elements of S. Consider

$\circ$	1	2	3	4	5	6
1	1	3	4	2	5	6
2	3	2	5	4	6	1
3	4	5	3	6	1	2
4	2	4	6	1	3	5
5	5	6	1	3	2	4
6	6	1	2	5	4	3

Based on this half-idempotent commutative quasigroup, we want to find the triple in the $STS(19)$ based on this quasigroup which contains **(i)** $(2,1)$ and $(2,2)$, **(ii)** $(4,1)$ and $(4,2)$, **(iii)** $(4,1)$ and $(1,2)$, and **(iv)** $(4,2)$ and $(6,2)$.

Solution. **(i)** For the pair $(2,1)$ and $(2,2)$, the first "coordinates" are the same so these are contained in a triple of Type 1, namely $\{(2,1),(2,2),(2,3)\}$. This is independent of the quasigroup $(Q,\circ)$.

(ii) For the pair $(4,1)$ and $(4,2)$, the first coordinates are the same but the first coordinates are $4 > 3 = n$, so the pair is contained in a triple of Type 3. This is a Type 3 triple of the sort on the left of Figure 1.5. So we need to find $j \in \{1,2,3\}$ such that $i \circ j = 4 \circ j = 4$, and then the third element in the triple is $(j,1)$. From the quasigroup, we see that we need $j = 2$ and so the triple is $\{(4,1),(4,2),(2,1)\}$.

(iii) For the pair $(4,1)$ and $(1,2)$, the second coordinates are 1 and 2, so the pair is contained in a triple of Type 2. This is a Type 2 triple of the sort on the left of Figure 1.5. So we take ∞ as the third element of the triple of Type 2, and the triple is $\{\infty,(4,1),(1,2)\}$.

(iv) For the pair $(4,2)$ and $(6,2)$, the second coordinates are the same so these are contained in a triple of Type 3. This is a Type 3 triple of the sort in the middle of Figure 1.5. So we take as the third element of the triple as $(4 \circ 6, 3) = (5,3)$, and the triple is $\{(4,2),(6,2),(5,3)\}$.