1.2. $v \equiv 3$ (mod 6): The Bose Construction

Note. In this section, we show that the condition $v \equiv 3 \pmod 6$ is sufficient for the existence of a Steiner triple system of order v. The method of proof is due to Raj Chandra Bose (June 19, 1901–October 31, 1987). Bose was born in India where he was educated and worked for the Indian Statistical Institute. He published several papers on statistics and block designs (including the paper of interest in this section) while working for the Indian Statistical Institute. He was chair of the Department of Statistics at the University of Calcutta from 1945 to 1947. He kept a busy work schedule and, in spite of the fact that he had published many well-received research papers, he did not get his doctorate until 1947 (after Ronald A. Fisher examined Bose's research and supported his candidacy). Starting in 1947, Bose spent time at several U.S. universities, including Virginia Polytechnic Institute at Blacksburg and the University of California in Berkeley. In 1949 he took a professorship at the university of North Carolina at Chapel Hill where he stayed until his first retirement in 1971. He next took a position at Colorado State University and was there until his second retirement in 1980. Bose made contributions to statistics, coding theory, and combinatorics. In his later years, his interests related to the interconnections between the structure of designs and graphs. This biographical information and the image below are from the MacTutor History of Mathematics Archive webpage on Bose (accessed 5/9/2022).

Raj Chandra Bose (June 19, 1901–October 31, 1987)

Note. The results of this section appear in Bose's "On the Construction of Balanced Incomplete Block Designs," *Annals of Eugenics*, **9**, 353–399 (1939). A copy of the paper is available online in the *Annals of Human Genetics* webpage (accessed 5/9/2022). Of course that journal title "Annals of Eugenics" jumps out at one! The term "eugenics" was coined by Francis Galton in 1883 (well before the development of the science of genetics). The idea was that "desirable" human traits were hereditary, and it discounted the impact of environmental factors (such as access to resources). The journal *Annals of Eugenics* was established in 1925 by Karl Pearson who is credited with establishing the discipline of mathematical statistics (but it seems that he held beliefs in line with some of the darker elements of eugenics). Pearson's involvement gave the journal an interest in biostatistics and mathematical statistics. Ronald Fisher became editor in 1934 and the focus of the journal moved more to traditional genetics and mathematical statistics. Many

of the concepts of eugenics (and "social Darwinism," an idea unrelated to Charles Darwin's ideas of biological speciation) were attractive to early 20th century racists (sadly, some of the ideas persist up to today). Eugenics has been described as "scientific racism." Of course, it met its nightmarish climax in Nazi Germany in the 1930s and 1940s. Following the second world war, the term "eugenics" was dropped from use almost universally. The *Annals of Eugenics* changed its name to *Annals of Human Genetics* in 1954. This historical information is largely based on the Wikipedia pages on eugenics, Karl Pearson, and Annals of Human Genetics (all accessed 5/9/2022). If you follow the link to Bose's 1939 paper given above, you will find that a statement is attached that includes the following:

> The work of eugenicists was often pervaded by prejudice against racial, ethnic and disabled groups. Publication of this material online is for scholarly research purposes is not an endorsement or promotion of the views expressed in any of these articles or eugenics in general.

Some of the early mathematical models in population genetics were published in the journal. For example, J.B.S. Haldane and Ronald Fisher also published papers in the issue that contains Bose's paper. It is not surprising that a paper related to experimental design would appear in such a journal (especially given the involvement of R. A. Fisher). Anyhow, we move on from this discussion and now turn our attention to some necessary definitions in the explanation of Bose's construction.

Definition. A *latin square* of *order* n is an $n \times n$ array, each cell of which contains exactly one of the symbols in $\{1, 2, \ldots, n\}$, such that each row and each column of the array contains each of the symbols in $\{1, 2, \ldots, n\}$ exactly once. We refer to

the entry in row i and column j as being in *cell* (i, j). A *quasigroup* of order n is a pair $(Q, \circ)$ where Q is a set of size n and "$\circ$" is a binary operation on Q such that for every pair of elements $a, b \in Q$, the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions.

Note. In the study of groups, such as in Modern Algebra 1 (MATH 5410), we always consider associative binary operations; see my online notes for this class on I.1. Semigroups, Monoids, and Groups (notice Definition I.1.1). This is not required in a quasigroup, so this gives us a genuinely new structure. Our goals are different here from those in group theory, since our interests lie in *combinatorial* properties of quasigroups and not in their *algebraic* properties. The "uniqueness" condition of a quasigroup and the "exactly one" condition of a latin square implies that there is little difference between a quasigroup and a latin square. In fact, Lindner and Rodger state (see page 4): "As far as we are concerned a quasigroup is just a latin square with a headline and a sideline."

Example 1.2.1(c). Here we have a latin square of order 3 (left) and a quasigroup of order 3 (right):

1	2	3
3	1	2
2	3	1

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

Definition. A latin square is *idempotent* is cell (i, i) contains symbol i for $1 \leq i \leq n$. A latin square is *commutative* if sells (i, j) and (j, i) contain the same symbol for all $1 \leq i, j \leq n$.

Example 1.2.2. Here we have a latin squares of orders 3 and 5 which are both idempotent and commutative:

1	3	2
3	2	1
2	1	3

1	4	2	5	3
4	2	5	3	1
2	5	3	1	4
5	3	1	4	2
3	1	4	2	5

Notice that the commutivity is easily recognized by considering the symmetry of the array with respect to the main diagonal.

Note. We need idempotent commutative quasigroups of order $2n+1$ for each $n \in \mathbb{N}$ (here, $\mathbb{N}$ represents the natural numbers $\{1, 2, 3, \ldots\}$). In Exercise 1.2.3(a,iii) it is to be shown that such quasigroups exist by rearranging the Cayley table (i.e., the addition table) for the additive group $\mathbb{Z}_{2n+1}$ of integers modulo $2n + 1$. With these structures known to exist, we can now present the Bose construction. We argue symbolically, but give illustrations from the text book to enhance the the ideas; the authors comment in the Preface (see page ix): "The figures describing the constructions in this text go a long way to helping students understand and enjoy this branch of mathematics, and should be used at ALL opportunities."

Note. We start by describing the Bose construction. Let $v = 6n + 3$ where $n \in \mathbb{N}$. Let $(Q, \circ)$ be an idempotent commutative quasigroup of order $2n + 1$, where $Q = \{1, 2, \ldots, 2n+1\}$ (which is known to exist by Exercise 1.2.3(a,iii)). Let set S be the Cartesian product $S = Q \times \{1, 2, 3\}$. We now consider "types" of triples. Define set T that contains the following triples of elements of S:

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

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

We'll prove below that (S, T) is a Steiner triple system of order $6n + 3$.

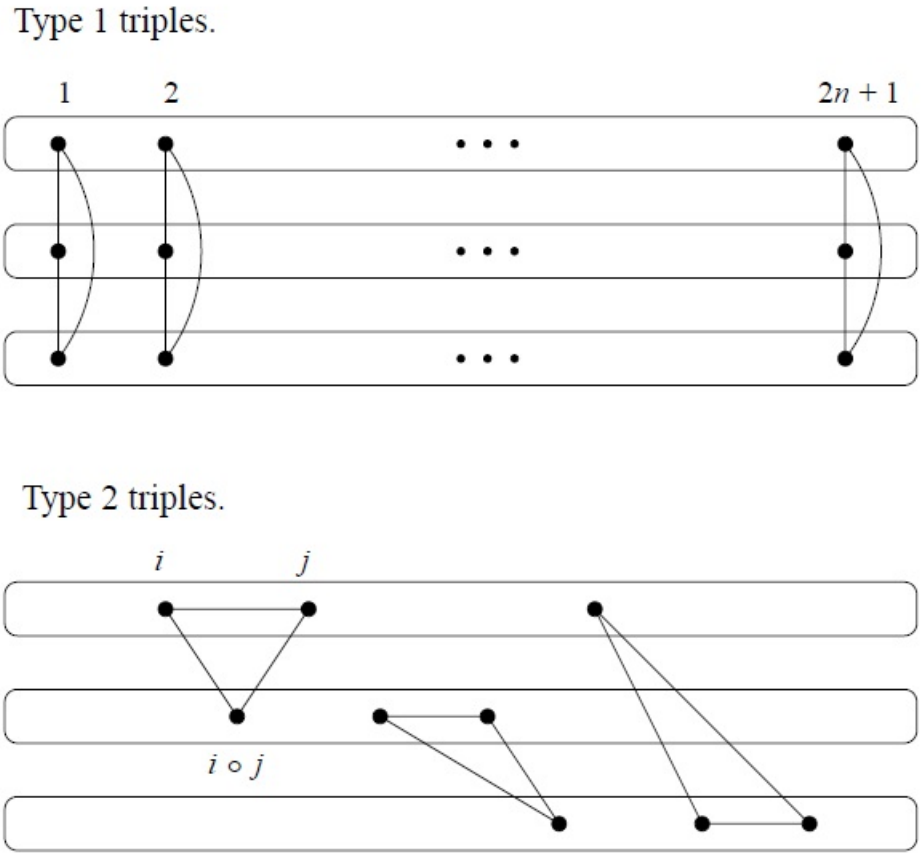

Figure 1.4: The Bose Construction.

Notice that $|S| = 6n+3$ and that T contains triples of S. There are $2n+1$ Type 1 triples and $3\binom{2n+1}{2} = 3n(2n+1)$ Type 2 triples. In the proof, we need to establish that each pair of elements of S occur in exactly one triple.

Theorem 1.2.A. A Steiner triple system of all orders $v \equiv 3 \pmod 6$ exist.

Example 1.2.4. We now illustrate the Bose construction to construct a Steiner triple system of order 9. We need a idempotent commutative quasigroup of order 3. We use:

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

Let $S = \{1,2,3\} \times \{1,2,3\}$. Then $|S| = 9$ as needed. The triples in set T are:

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

Type 2:

$i=1,\ j=2$

$\{(1,1),(2,1),(1\circ 2 = 3,2)\}$

$\{(1,2),(2,2),(1\circ 2 = 3,3)\}$

$\{(1,3),(2,3),(1\circ 2 = 3,1)\}$

$i=1,\ j=3$

$\{(1,1),(3,1),(1\circ 3 = 2,2)\}$

$\{(1,2),(3,2),(1\circ 3 = 2,3)\}$

$\{(1,3),(3,3),(1\circ 3 = 2,1)\}$

$i=2,\ j=3$

$\{(2,1),(3,1),(2\circ 3 = 1,2)\}$

$\{(2,2),(3,2),(2\circ 3 = 1,3)\}$

$\{(2,3),(3,3),(2\circ 3 = 1,1)\}$

Example 1.2.5 (modified). We now consider some properties of the Bose construction when used to make a Steiner triple system of order 15. We need a idempotent commutative quasigroup of order 5. We create one based on $\mathbb{Z}_5$, as in Exercise 1.2.3(a,iii). We have the Cayley table for $\mathbb{Z}_5$ (below left), marginal entries changed to match the diagonal entries(below center; there is no *algebraic* structure to preserve here), and then the renaming of the symbols as $0 \mapsto 1$, $1 \mapsto 4$, $2 \mapsto 2$, $3 \mapsto 5$, and $4 \mapsto 3$ to get a quasigroup $(Q, \circ)$ with diagonal entries 1, 2, 3, 4, 5 (in order), though it differs from the one in the book's Example 1.2.5.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\circ$	0	2	4	1	3
0	0	1	2	3	4
2	1	2	3	4	0
4	2	3	4	0	1
1	3	4	0	1	2
3	4	0	1	2	3

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

Based on idempotent commutative quasigroup $(Q, \circ)$, we want to find the triple in the $STS(15)$ base on this quasigroup which contains **(i)** $(3, 1)$ and $(3, 3)$, **(ii)** $(3, 2)$ and $(5, 2)$, and **(iii)** $(3, 2)$ and $(5, 3)$.

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

(ii) For elements $(3, 2)$ and $(5, 2)$ of S, the first coordinates are different so these are contained in a triple of Type 2. They are in triple $\{(3, 2), (5, 2), (3 \circ 5, 3)\}$. In quasigroup $(Q, \circ)$ we have $3 \circ 5 = 4$ so the triple of T containing the two given elements is $\{(3, 2), (5, 2), (4, 3)\}$. Notice that we can list the elements in the order

$(5, 2)$ and $(3, 1)$ and we still get the same triple because, by commutivity, $5 \circ 3 = 4$ also.

(iii) For elements $(3, 2)$ and $(5, 3)$ of S, the first coordinates are different so these are contained in a triple of Type 2. We see from Figure 1.4 that the only Type 2 triples to contain elements of S with second coordinates 2 and 3 are of the form $\{(i, 2), (j, 2), (i \circ j, 3)\}$. So we must have $i = 3$ and $i \circ j = 3 \circ j = 5$. We see from quasigroup $(Q, \circ)$ that we must have $j = 2$ so that the triple is $\{(3, 2), (2, 2), (5, 3)\}$. Notice that we can take $j = 3$ (instead of $i = 3$) since, by commutivity, $i \circ j = i \circ 3 = 5$ implies that $i = 2$, and we get the same triple. $\square$

Revised: 8/29/2022