Steiner Systems

DMM Power Round 2025

For questions asking you to **find**, **evaluate**, **give**, or **compute**, you do not need to give any additional justification for your answer, and there are no partial credits available for wrong answers. For questions asking you to **show** or to **prove**, in order to receive full credits you should show a concrete, precise proof, but partial credits are available for these questions.

There are **50 points** in total, and the point value of each question is written beside the problem number.

1 Defining a System

Definition 1. A **Steiner System** with parameters t, k, n, written as $S(t, k, n)$ is a set S of n elements together with k-element subsets (called blocks), with the property that each t-element subset of S is contained in exactly one of the k-element subsets. In other words, it is contained in exactly one block.

For example, consider the following *candidate* for $S(2, 3, 7) = \{\{1, 2, 3\}, \{4, 5, 6\}, \{1, 3, 5\}, \{3, 5, 7\}, \{2, 4, 7\}\}$. We first note that there are 7 elements within the set S (1-7), and are split into blocks of size 3, satisfying our requirement for $n = 7$ and $k = 3$. However, issues arise when checking the condition that every 2 element subset of S is contained in exactly one block. Firstly, the 2 element subset $\{1, 3\}$ appears in two blocks (blocks 1 and 3), which contradicts our definition. In addition, the 2 element subset $\{3, 4\}$ does not appear in our blocks at all.

Problem 1. **[1]** Find a correct Steiner System for $S(2, 3, 7)$.

Problem 2. **[1]** Show that there exists no Steiner System for $S(2, 3, 8)$.

Definition 2. We define a **permutation** of a Steiner System to be a reordering of the elements within the system.

For example, in the Steiner System $S(2, 2, 3) = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, we can reorder (map) the elements as follows: $1 \to 2$, $2 \to 3$, $3 \to 1$. This results in the system $S(2, 2, 3) = \{\{2, 3\}, \{2, 1\}, \{3, 1\}\}$. Note that this reordering preserves the blocks (all blocks in the original system appear in the reordered system). This is not always the case.

Problem 3. **[1]** Let b be a given a block in a $S(2, 3, n)$ Steiner System. Show that the number of blocks in $S(2, 3, n)$ that are disjoint (share no elements) from b is equal to $\frac{(n-3)(n-7)}{6}$.

Problem 4. **[3]** Find the number of permutations of $S(2, 3, 7)$ that preserve the blocks of the system.

We will now explore conditions placed the on parameters of Steiner Systems in relation to each other. These are called divisibility conditions.

Problem 5. We will start by investigating a condition on the number of blocks of a system.

i) **[1]** Find the number of blocks in $S(3, 4, 8)$.

ii) **[1]** Show that $\binom{k}{t}$ must be a factor of $\binom{n}{t}$ in order for the Steiner System $S(t, k, n)$ to exist.

Problem 6. We now move on to conditions on n based on varying values of k and t

i) **[2]** Show that if a Steiner System $S(2, 3, n)$ exists, then n must be either 1 or 3 $(mod\ 6)$.

ii) **[2]** Show that if a Steiner System $S(2, 4, n)$ exists, then n must be either 1 or 4 $(mod\ 12)$.

2 Latin Squares and Quasigroups

Definition 3. A **Latin Square** is a $n \times n$ square matrix whose entries consist of n symbols such that each symbol appears exactly once in each row and column.

For example, the follow matrix represents a 4×4 square matrix whose entries are the four suits in a deck of cards:

♠	♡	♢	♣
♢	♣	♠	♡
♣	♢	♡	♠
♡	♠	♣	♢

Definition 4. A **quasigroup** $(S, \otimes)$ is a set S together with a binary operation $(\otimes)$ such that:

1. The operation is closed (i.e. $a \otimes b$ is an element of S for all a, b in S).
2. Given a, b in S, the equations:
   i) $a \otimes x = b$
   ii) $y \otimes a = b$

   have unique solutions for x and y. Note that x, y can vary for different a, b.

For example, a simple quasigroup is given by the set $\{0, 1, 2\}$ with the operation $\otimes$ defined by $a \otimes b = 2a + b + 1 \pmod 3$ where the operations on the right are the usual multiplication and addition modulo 3. The multiplication table for this quasigroup is given below:

$(\otimes)$	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

Definition 5. A quasigroup (latin square) is **idempotent** if $a \otimes a = a$ for all a in S (cell (i, i) contains symbol i for $1 \leq i \leq n$.)

Definition 6. A quasigroup (latin square) is **commutative** if $a \otimes b = b \otimes a$ for all a, b (cells (i, j) and (j, i) contain the same symbol for $1 \leq i, j \leq n$.)

Examples of commutative idempotent latin squares:

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

Problem 7. We now investigate the properties of commutative idempotent latin squares of even and odd size

i) **[2]** Prove that there exists no commutative idempotent latin square of size n if n is even.

ii) **[1]** Prove that for any $n = 2k + 1$, there exists a commutative idempotent latin square of size n.

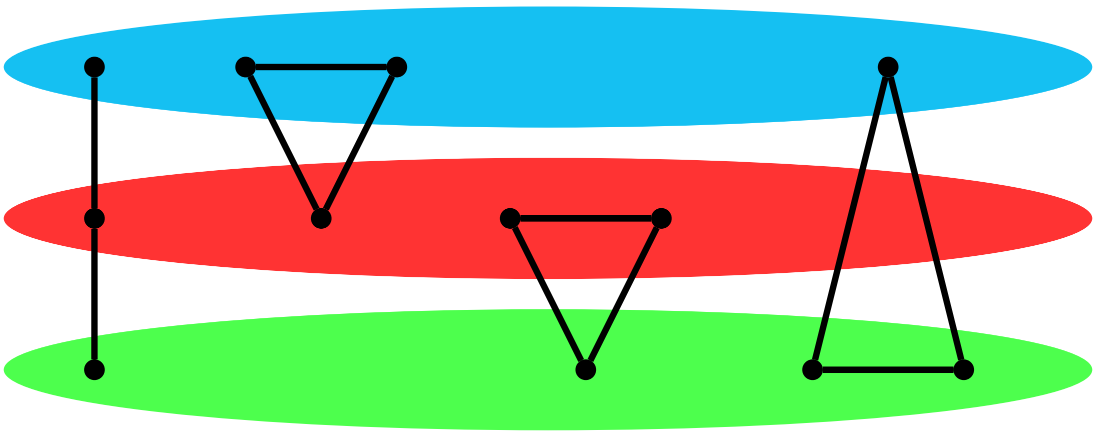
So where are we going with all of this?

3 Bose and Skolem Constructions

Definition 7. The **Bose construction** is formulated as follows. We create a set ς with $6n+3$ elements utilizing a commutative idempotent quasigroup $(Q, \otimes)$ of order $2n+1$. The set of elements ς consists of the $6n+3$ ordered pairs of $Q \times \{0,1,2\}$. We also label triples of two types:

1. $\{(i,0),(i,1),(i,2)\}$ for each i in Q.
2. $\{(i,k),(j,k),(i \otimes j, k+1 \pmod 3)\}$ for $i \neq j$ in Q.

We can visualize the triples by considering 3 copies of Q:



Problem 8. We now show with the Bose construction above that there always exists a valid Steiner System of type $S(2,3,6n+3)$ for any integer n.

i) **[1]** How many triples (blocks) exist in this construction?

ii) **[3]** Prove that each pair of distinct elements in ς are contained in a triple (block).

iii) **[1]** Use the results above to show that the set ς can be split into triples (blocks) that form a $S(2,3,6n+3)$ Steiner System.

Definition 8. A latin square (quasigroup) L of size $2n$ is **half-idempotent** if the cells (i,i) and $(n+i,n+i)$ contain the symbol i, for every $1 \leq i \leq n$.

Some examples follow:

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

1	4	2	5	3	6
4	2	5	3	6	1
2	5	3	6	1	4
5	3	6	1	4	2
3	6	1	4	2	5
6	1	4	2	5	3

Problem 9. **[2]** Prove that commutative half-idempotent latin squares exist for all even size n.

Definition 9. The **Skolem construction** is formulated as follows. We create a set ς with $6n+1$ elements consisting of the $6n$ ordered pairs of $Q \times \{0,1,2\}$, where $(Q, \otimes)$ is a commutative half-idempotent quasigroup of size $2n$, together with a special symbol called ∞. To describe the triples we assume that quasigroup Q has symbols $\{1,2,\cdots,2n\}$. The triples can then be described as:

1. $\{(i,0),(i,1),(i,2)\}$ for $1 \leq i \leq n$.

2. $\{\infty, (i,k), (n+i, k-1 \pmod 3)\}$ for $1 \le i \le n$, integer k.
3. $\{(i,k), (j,k), (i \otimes j, k+1 \pmod 3)\}$ for $1 \le i < j \le 2n$, integer k.

Problem 10. We now show that with the Skolem construction, we can create a Steiner System $S(2, 3, 6n+1)$ for any integer n.

i) **[1]** How many triples (blocks) exist in this construction?

ii) **[4]** Show that each pair of elements in ς is contained in a triple (block).

iii) **[1]** Conclude that the set ς can be split into triples (blocks) that for a $S(2, 3, 6n+1)$ Steiner System.

(Hint for (ii): Suppose (a, b) and (c, d) are a pair of elements in ς. Consider casework on the relationship between a, c, and n)

And now we have proved that in a Steiner System $S(2, 3, n)$, the condition that n is 1 or 3 (mod 6) (necessary for the Steiner System to exist as we saw in Problem 6.i), is also *sufficient*. In other words, a valid Steiner System of the form $S(2, 3, n)$ exists if and only if n is of the form $6m + 1$ or $6m + 3$. Ta-da!

4 A Connection to Golay Codes

Definition 10. A **binary code** of length n is a set of binary strings (strings with only 0s and 1s) with n digits. Call elements of this set codewords. The (Hamming) distance between codewords is the number of indices in which the corresponding value in each digit differs. For example $d(1, 0) = 1$ and $d(1011, 1000) = 2$.

Definition 11. The **minimum distance** of a code is the minimum distance between any two codewords x, y in the code, where $x \neq y$.

Definition 12. An **error** in a codeword is a single digit that was flipped $(0 \to 1, 1 \to 0)$. For example, if we intended to send the codeword 1011 and instead received 0111, we note two errors.

Problem 11. **[2]** Show that a code of minimum distance d can correct $t = \lfloor (d-1)/2 \rfloor$ errors; i.e., argue that for each received word y with at most t errors (assuming that the intended sent word is a valid word in the code), there exists exactly one codeword c with $d(y, c) \le t$.

Definition 13. The **weight** of a binary codeword is the number of ones in the string.

Definition 14. We define the **addition** of two codewords to be their digit-wise XOR. That is, we take each digit from the codeword, and if they match, we write a 0, and if they are different, we write a 1. For example, $1011+1010+0001$.

We define the **product** of two codewords to be their digit-wise AND. That is, we take each digit from the codeword, and if they both are 1, we write a 1, and if they are different, we write a 0. For example, $(1011)(1010) = 1010$.

Definition 15. We call a binary code **linear** if it has the property that given two codewords x, y, their sum $x + y$ is also always a codeword.

Definition 16. A **basis** $\{b_1, b_2, \cdots, b_n\}$ for a linear binary code C is a set of codewords that hold the following properties:

1. Any codeword can be expressed as a sum of (possibly 0) b_i.
2. There does not exist $k > 0$ and $1 \le i_1 < i_2 < \cdots < i_k \le n$ such that $b_{i_1} + \cdots + b_{i_k} = 0$.

We also denote the **size** of the basis set as the dimension of the linear code.

Problem 12. **[2]** Given a linear code and a basis, show that any codeword can be expressed as a unique sum of basis codewords.

Problem 13. [2] Show that in a linear code, the minimum nonzero distance between two codewords is equal to the minimum nonzero weight of a codeword.

Definition 17. A **Golay code** is a linear code of length 24, dimension 12, and minimum distance 8.

Problem 14. A basis of a binary code can be naturally expressed as a matrix, where the rows are the basis codewords. We will devote the rest of this problem to showing that the following matrix represents a valid basis for a Golay code.

$$G = \left[\begin{array}{cccccccccccc|cccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&1&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&1&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&1&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&1&1&1&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&1&0&0&1&1&1&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&1&0&0&1&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&1&1&1&0&0&1&0&0&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&1&0&1&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&1
\end{array}\right]$$

i) **[2]** Show that the weight of the product xy of any two distinct codewords in the Golay code is even.

ii) **[3]** Show that the weight of any codeword is a multiple of 4.

iii) **[4]** Conclude that the basis satisfies the defining properties of the Golay code.

Problem 15. We now show that the Golay code actually contains a Steiner System $S(5, 8, 24)$!

i) **[3]** Find the number of codewords of weight 8 in the Golay Code.

ii) **[1]** Find the number of blocks in the Steiner System $S(5, 8, 24)$.

iii) **[3]** Show that every subset of 5 letters is contained in exactly one block as defined by a codeword from the Golay Code.