Steiner Systems

DMM Power Round 2025 Solutions

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 $S(2, 3, 7)$.

Solution. $\{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 5, 6\}, \{2, 4, 7\}, \{3, 5, 7\}, \{3, 4, 6\}\}$. There are many other correct Steiner systems, but for every single system, we are able to label the elements as a, b, c, d, e, f, g such that the blocks are $\{a, b, c\}, \{a, d, e\}, \{a, f, g\}, \{b, e, f\}, \{b, d, g\}, \{c, e, g\}, \{c, d, f\}$.

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

Solution. There are $\binom{8}{2} = 28$ 2-subsets of 8 elements, but every triplet contains 3 2-subsets. Since 3 does not divide 28, we have a contradiction.

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 $\frac{(n-3)(n-7)}{6}$.

Solution. There are $\frac{n(n-1)}{6}$ triples. Aside from a block $b = \{a, d, c\}$, each of a, d, c is in exactly $\frac{(n-3)}{2}$ triples by counting pairs $(a, -)$. Thus, we can compute $\frac{n(n-1)}{6} - 1 - \frac{3(n-3)}{2} = \frac{(n-3)(n-7)}{6}$.

Problem 4. [3] Find the number of permutations of $S(2,3,7)$ that preserve the blocks of the system.
Implicit is the assumption that the answer is the same for every Steiner system, so we just pick one.
Answer: 168.
Solution For ease of writeup, we label the 7 elements

$$S = \{1, (1,0), (1,1), (2,0), (2,1), (3,0), (3,1)\},$$

and the blocks are

$$\{1, (1,0), (1,1)\}, \{1, (2,0), (2,1)\}, \{1, (3,0), (3,1)\},$$

$$\{(1,0), (2,1), (3,0)\}, \{(1,0), (2,0), (3,1)\}, \{(1,1), (2,1), (3,1)\}, \{(1,1), (2,0), (3,0)\}$$

One can check that the permutations of S that fix 1 and all blocks are

$$\Gamma_1 := \{\sigma \circ \rho = \rho \circ \sigma : \sigma \in \{id, ((1,0),(1,1))((2,0)(2,1)), ((1,0)(1,1))((3,0)(3,1)), ((2,0)(2,1))((3,0),(3,1))\}\}$$

Here ρ satisfies $\rho(1) = 1$, and there exists a permutation π on $\{1,2,3\}$ such that $\rho((j,k)) = (\pi(j),k)$ for all $j = 1,2,3$ and $k = 0,1$
Note Γ_1 has 24 elements. Now note that for every $j \in S$, there exists τ such that $\tau(1) = j$. Then the permutations of S that fix the blocks of the system and sends 1 to j is precisely $\tau\Gamma_1 = \{\tau \circ \gamma : \gamma \in \Gamma_1\}$. Since $|S| = 7$, for every j there are 24 permutations that sends 1 to j and fixes all blocks. Thus, there are a total of $24 \cdot 7 = 168$ permutations in total.

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.

Solution.

i) Each block will contain $\binom{4}{3} = 4$ triplets, and in total there are $\binom{8}{3} = 56$ triplets, so there must be $56/4 = 14$ blocks.

ii) Generalizing from above, we see that $\binom{k}{t}$ is the number of t-sets in each block, and there are a total of $\binom{n}{t}$ t-sets, so the number of blocks is $\frac{\binom{n}{t}}{\binom{k}{t}}$, which must be an integer.

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).

Solution.

i) Any triple $\{a,b,c\}$ contains three 2-element subsets and our system contains $\binom{n}{2}$ 2-element subset. As every pair appears in a unique triple, we have that the number of triples is $\frac{n(n-1)}{6}$. For any given element x, the triples containing x partition the remaining elements into pairs, so $n-1$ is even, which means n is odd. Therefore, $n \equiv 1, 3,$ or 5 (mod 6). However, if $n = 6m+5$, we can compute the number of blocks to be $\frac{(6m+5)(6m+4)}{6}$, which is not an integer, so that case is eliminated.

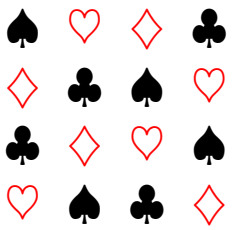
ii) Since every pair of distinct elements of an $S(2,4,n)$ is contained in a unique block, and each block contains $\binom{4}{2} = 6$ such pairs, the total number of pairs $\binom{n}{2}$ must be divisible by 6, and thus 12 must divide $n(n-1)$.

Also, any element occurs in a block with three further elements, so the total number of other elements, $n-1$, must be divisible by 3. These two conditions imply that $n \equiv 1$ or 4 (mod 12) is necessary for an $S(2,4,n)$ to exist.

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.

Solution.

i) Fix a symbol $s \in \{1, \ldots, n\}$. In a Latin square, each symbol appears exactly once in every row, hence exactly n times in the whole square. In row s, the unique occurrence of s is at (s, s) (by idempotence). Thus s does not appear at (s, j) with $j \neq s$. Similarly, in column s, the unique occurrence of s is again (s, s), so s does not appear at (i, s) with $i \neq s$. Therefore, every other occurrence of s must lie at positions (i, j) with $i \neq s$ and $j \neq s$. But since the square is symmetric, such occurrences come in symmetric pairs (i, j) and (j, i). Hence the total number of occurrences of s is $1 + 2k$ for some integer k, i.e., an odd number. On the other hand, we know each symbol appears exactly n times. Thus n must be odd, which is a contradiction.

ii) One can verify that the operation

$$a \otimes b \equiv (k+1)(a+b) \pmod{2k+1}$$

will always produce a commutative idempotent latin square if $n = 2k + 1$.

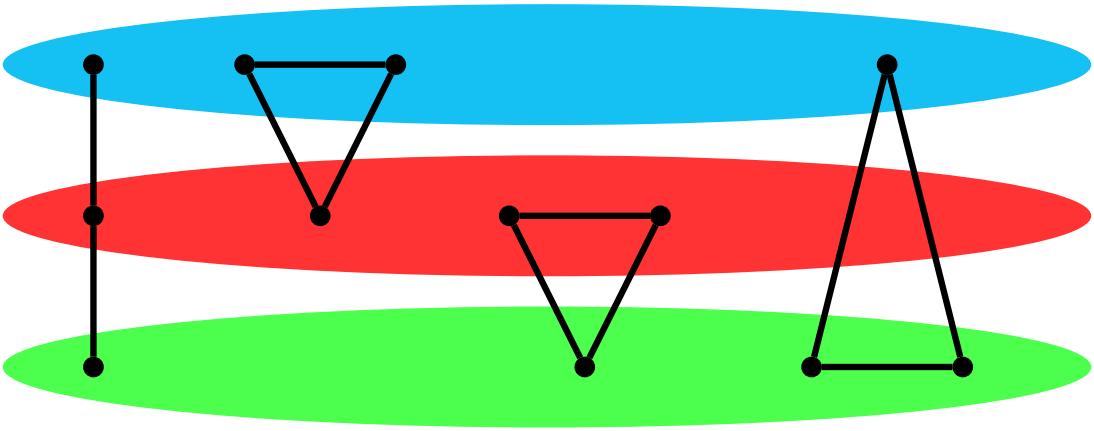
So where are we going with all of this?

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.

Solution.

i) There are $2n + 1$ triples of type 1 and $\frac{3(2n+1)(2n)}{2} = 6n^2 + 3n$ triples of type 2. Thus, the number of blocks is $6n^2 + 5n + 1$.

ii) Let (a, b) and (c, d) be distinct elements of ς. If $a = c$ then this pair is in a triple of type 1. If $b = d$, the pair is in a triple of type 2.

We now also assume that $b \neq d$. Now, either $d \equiv b + 1 \pmod 3$ or $d \equiv b - 1 \pmod 3$. In the first case, let x be the unique solution of $a \otimes x = c$ in Q. The triple containing the pair is thus $\{(a, b), (x, b), (c, d)\}$. In the second case, let y be the unique solution of $y \otimes c = a$ in Q. The triple is then $\{(y, d), (c, d), (a, b)\}$.

iii) We first note that the number of blocks in $S(2, 3, 6n + 3) = \frac{\binom{6n+3}{2}}{3} = 6n^2 + 5n + 1$, which agrees with the number of triples we found in part (i). Since we have the exact same number of triples/blocks and in part (ii) proved that every pair is contained within a triple (block), we have shown the required property for a 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.

Solution. Let $a(2) = 1, a(3) = n + 1, a(4) = 2, \cdots, a(2n) = n, a(2n + 1) = 2n$ and $a(x) = a(x + 2n)$ for every x. Then set $i \otimes j = a(i + j)$. Since $a(x), \cdots, a(x + 2n - 1)$ is a permuation of $1, \cdots, 2n$, we can verify that this will produce a commutative half-idempotent latin square.

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

Solution.

i) There are n triples of type 1, $3n$ triples of type 2 and $\frac{3(2n)(2n-1)}{2}$ triples of type 3. This gives us a total of $6n^2 + n$ triples.

ii) Any pair including the symbol ∞ is contained in a type 2 triple. Suppose (a, b) and (c, d) are a pair of elements in S. If $a = c$ and $a \leq n$, then the pair is contained in a triple of type 1.

Now suppose that $a = c$ and $a > n$. Since $b \neq d$, either $d = b + 1 \pmod 3$ or $d = b - 1 \pmod 3$. In the first case, let x be the unique solution of $a \otimes x = a$ in Q. Since $a > n$, $x \neq a$. The triple containing the pair is thus $\{(a, b), (x, b), (a, d)\}$. In the second case, let y be the unique solution of $y \otimes a = a$ in Q. Again, $y \neq a$ and the triple is then $\{(y, d), (a, d), (a, b)\}$.

We can now assume that $a \neq c$. If $b = d$, then a triple of type 3 contains the pair, so we can also assume that $b \neq d$. Again, either $d = b + 1 \pmod 3$ or $d = b - 1 \pmod 3$. In the first case, let x be the unique solution of $a \otimes x = c$ in Q. If $x \neq a$, then the type 3 triple $\{(a, b), (x, b), (c, d)\}$ contains the pair. If on the other hand $x = a$, then $a > n$, since $a \neq c$. In this case, $a = n + c$ and the pair is in the type 2 triple $\{\infty, (c, d), (n + c, b)\}$. The other possibility for d is treated similarly.

iii) We first note that the number of blocks in $S(2, 3, 6n + 1) = \frac{\binom{6n+1}{2}}{3} = 6n^2 + n$, which agrees with the number of triples we found in part (i). Since we have the exact same number of triples/blocks and in part (ii) proved that every pair is contained within a triple (block), we have shown the required property for a Steiner System.

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 $d(y, c) \leq t$.

Solution. If a codeword $c \in C$ is sent and at most t symbol errors occur, the received word y satisfies $d(y, c) \leq t$, so some codeword is within radius t of y. Suppose there are distinct $c_1, c_2 \in C$ with $d(y, c_1) \leq t$ and $d(y, c_2) \leq t$. By the triangle inequality,

$$d(c_1, c_2) \leq d(c_1, y) + d(y, c_2) \leq 2t \leq d - 1,$$

contradicting that the minimum distance of C is d. Therefore the Hamming balls of radius t around codewords are pairwise disjoint. Any word with at most t errors lies in exactly one such ball, so C corrects $t = \lfloor (d-1)/2 \rfloor$ errors.

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 $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ 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.

Solution. For the sake of contradiction, assume that $x = r_1 + r_2 + \cdots + r_k = s_1 + s_2 + \cdots + s_m$, where x is a codeword and r_i and s_j are basis codewords. Furthermore, we may assume $r_1, \cdots, r_k$ and $s_1, \cdots, s_m$ are distinct. We can then write

$$0 = r_1 + r_2 + \cdots + r_k - (s_1 + s_2 + \cdots + s_{m-1} + s_m) = r_1 + r_2 + \cdots + r_k + (s_1 + s_2 + \cdots + s_{m-1} + s_m)$$

Each basis codeword appears either zero, one, or two times among $r_1, \cdots, r_k, s_1, \cdots, s_m$. If $\{b_s : s \in S\}$ is the set of codewords that appear once, then $0 = \sum_{s \in S} b_s$. By condition 2 in the previous definition, we can see that S must be the empty set. Thus, every word that appear among $\{r_1, \cdots, r_k\}$ must appear in $\{s_1, \cdots, s_m\}$, and vice versa.

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.

Solution.

1. Let $d_{\min} = \min_{x \neq y \in C} d(x, y)$. Choose $x \neq y$ attaining it and set $c = x - y \in C$, $c \neq 0$. Then

   $$\mathrm{wt}(c) = d(x, y) = d_{\min},$$

   so the minimum nonzero weight $w_{\min}$ satisfies $w_{\min} \leq d_{\min}$.

2. Let $c \in C \setminus \{0\}$ attain $w_{\min} = \mathrm{wt}(c)$. Then

   $$d(c, 0) = \mathrm{wt}(c) = w_{\min},$$

   hence $d_{\min} \leq w_{\min}$.

Therefore $d_{\min} = w_{\min}$.

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.

Solution.

i) Let $b_1, \cdots, b_{12}$ be the codewords associated to the rows. For the displayed matrix A,

- every row has weight 8 (even), and
- any two distinct rows intersect in an even number of positions (in fact, exactly 4).

Thus, $w(b_i b_j)$ is even for all $i \neq j$ and $w(b_i)$ is also even. Let $x = \alpha_1 b_1 + \cdots \alpha_{12} b_{12}$ and $y = \beta_1 b_1 + \cdots + \beta_{12} b_{12}$ for unique $\alpha_1, \cdots, \alpha_{12}, \beta_1, \cdots, \beta_{12} \in \{0, 1\}$

We now have that

$$xy = \alpha_1\beta_1 b_1 b_1 + \cdots \alpha_1\beta_{12} b_1 b_{12} + \cdots + \alpha_{12}\beta_1 b_{12} b_1 + \cdots \alpha_{12}\beta_{12} b_{12} b_{12}.$$

Each $b_i b_j$ has even weight, so their sum has even weight as well.

ii) Recall the identity for binary vectors u, v:

$$w(u + v) = w(u) + w(v) - 2\, w(uv) \tag{1}$$

where uv is the product. From part (i) we know that for the displayed matrix A:

- each basis codeword b_i has weight $w(b_i) = 8 \equiv 0 \pmod 4$
- the product of two codewords is even

We induct on the number of generators in the sum. Let $y = b_1 + \cdots + b_{l-1} + b_l$. The base case, $l = 1$, is clear. We now assume that $w(b_1 + \cdots + b_{l-1}) \equiv 0 \pmod 4$, and we will show that $w(b_1 + \cdots + b_l) \equiv 0 \pmod 4$.

Because $w(b_i b_\ell) \equiv 0 \pmod 2$ and $w(x + y) \equiv w(x) + w(y) \pmod 2$, we have

$$w(y b_\ell) \equiv \sum_i w(b_i b_\ell) \equiv 0 \pmod 2.$$

By equation (1),

$$w(y + b_\ell) = w(y) + w(b_\ell) - 2\, w(y b_\ell) \equiv 0 + 0 - 2 \cdot 0 \equiv 0 \pmod 4.$$

Completing the inductive step.

iii) We first note certain properties of the basis. Let A be the 12×12 matrix that is the right half of our basis.

- Each row of A has weight 7.
- Any two distinct rows of A coincide in ≤ 4 locations $\implies$ the sum of any two rows in A has weight ≥ 6.
- The sum of any three rows of A has odd weight ≥ 7 as pairwise cancellations remove an even number of 1s.

By ii), we only have to show there is no codeword of weight 4 that is a linear combination of our basis vectors. Note that we must use at most 4 rows (basis vectors), as the left side of the matrix will always contribute m ones, where m is the number of rows we select.

- Four rows from A: We need to find a combination of rows who sum has a weight of 0. So, in each column there must be an even number of 1s. Since there are 12 columns, we can write $x_0 + x_2 + x_4 = 12$, where x_i is the number of columns with i ones in it. We also know that the total number of ones is $4 \cdot 7 = 28$, and so we can write $2x_2 + 4x_4 = 28$. There are also $\binom{4}{2} = 6$ pairs of rows. For each x_2, there is exactly one pair that contributes and for each x_4, 6 columns contribute. So, $x_2 + 6x_4 = 18$. Trying to solve this system of equations for x_2 and x_4, we get that $x_0 = -1$, which is clearly impossible.
- Three rows from A: The total weight will be $3 + w(\text{sum of three rows in A}) \geq 1 + 7 \neq 4$.

- Two rows from A: The total weight will be $2 + w(\text{sum of two rows in A}) \geq 2 + 6 = 8 > 4$.
- One row from A: The total weight is 8.

So, it is impossible to get a weight 4 codeword. Combining this with the previous result, we conclude that the minimum weight (which implies the minimum distance) is at least 8, which is the last property of the Golay code that is not immediately given by the basis.

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.

Solution.

i) Let A_w be the number of codewords of weight w in $\mathcal{G}_{24}$. Since the code contains $\mathbf{1}$ (the all-ones vector), all weights are divisible by 4, and the minimum nonzero weight is 8, the only possible weights are $0, 8, 12, 16, 24$ with $A_0 = A_{24} = 1$ and $A_8 = A_{16} = x$, $A_{12} = y$. Because $\mathcal{G}_{24}$ is 12-dimensional,

$$1 + x + y + x + 1 = 2^{12} \quad \Rightarrow \quad 2x + y = 4094.$$

It's clear that for any two columns, there must exist codewords that have 1 in one column and 0 in the other, so for any pair of coordinates (i, j) exactly 2^{10} codewords have 1's in both positions. Double counting unordered pairs of 1's gives

$$x\binom{8}{2} + y\binom{12}{2} + x\binom{16}{2} + \binom{24}{2} = \binom{24}{2} \cdot 2^{10},$$

i.e.

$$148x + 66y = 276 \cdot 1023.$$

Solving the two linear equations yields $x = 759$ and $y = 2576$. Hence there are 759 weight-8 codewords in $\mathcal{G}_{24}$.

ii) From the formula we derived in 5 (ii), we get $b = \frac{\binom{24}{5}}{\binom{8}{5}} = 759$.

iii) Let O be the set of supports of weight-8 codewords ("octads") of the extended binary Golay code $\mathcal{G}_{24}$. Suppose a 5–subset $S \subseteq \{1, \ldots, 24\}$ is contained in two distinct octads $B_1, B_2 \in O$. Then for their indicator vectors $\mathbf{1}_{B_1}, \mathbf{1}_{B_2} \in \mathcal{G}_{24}$,

$$\text{wt}(\mathbf{1}_{B_1} + \mathbf{1}_{B_2}) = |B_1 \triangle B_2| = |B_1| + |B_2| - 2|B_1 \cap B_2| \leq 8 + 8 - 2 \cdot 5 = 6,$$

contradicting the minimum distance 8 of $\mathcal{G}_{24}$. Hence each 5–subset is contained in at most one octad.

Double–count pairs (S, B) with $S \subset B$, $|S| = 5$, $B \in O$. Fix B: there are $\binom{8}{5} = 56$ such S. Thus the number of pairs is $|O| \cdot 56$. From part (i), $|O| = 759$, so

$$|O| \cdot 56 = 759 \cdot 56 = 42504 = \binom{24}{5},$$

the total number of 5–subsets of $\{1, \ldots, 24\}$. Since by uniqueness each 5–subset is in at most one octad, equality forces that every 5–subset lies in exactly one octad.