

1. Does there exist a binary $(15, 17, 5)$ -code?

Solution : **YES**. Note that if a code has minimum distance 5 then it is two-error correcting. It follows from the Gilbert-Varshamov Bound that there exists a binary code C of length 15 such that $d(C) = 5$ and

$$|C| \geq \frac{2^{15}}{\binom{15}{0} + \binom{15}{1} + \binom{15}{2} + \binom{15}{3} + \binom{15}{4}} = \frac{32768}{1941} \approx 16.88$$

Hence $|C| \geq 17$.

Let $\mathbf{x}, \mathbf{y} \in C$ with $d_H(\mathbf{x}, \mathbf{y}) = 5$ and $C' \subseteq C$ such that $\mathbf{x}, \mathbf{y} \in C'$ and $|C'| = 17$. Then C' is a binary $(15, 17, 5)$ -code. \square

2. Does there exist a binary one-error correcting code of length 8 containing 29 codewords?

Solution : **NO**. Let C be a binary one-error correcting code of length 8. Then it follows from the Sphere Packing Bound that

$$|C| \leq \frac{2^8}{\binom{8}{0} + \binom{8}{1}} = \frac{256}{9} \approx 28.44$$

So $|C| \leq 28$. \square

3. Prove that there does not exist a binary one-error correcting code of length 6 with 9 codewords.

Proof : Suppose that C is a binary one-error correcting code of length 6 with 9 codewords. Then there are at least five codewords with the same digit in the first position. At least three of these five codewords, say $\mathbf{x}, \mathbf{y}, \mathbf{z}$, have the same digit in the second position.

Since C is one-error correcting, we know that $d(C) \geq 3$. So \mathbf{x} and \mathbf{y} are different in at least three positions, say positions 3, 4 and 5. Thus $x_i \neq y_i$ for $i = 3, 4, 5$. Let $i \in \{3, 4, 5\}$. Since $x_i, y_i, z_i \in \{0, 1\}$ and $x_i \neq y_i$, we conclude that either $z_i = x_i$ or $z_i = y_i$. So $\{3 \leq i \leq 5 : z_i = x_i\} \cup \{3 \leq i \leq 5 : z_i = y_i\} = \{3, 4, 5\}$. Hence one of these sets contains at least two elements. But then either $d_H(\mathbf{z}, \mathbf{x}) \leq 2$ or $d_H(\mathbf{z}, \mathbf{y}) \leq 2$, a contradiction.

Hence there does not exist a binary one-error correcting code of length 6 with 9 codewords. \square

4. Let $t \in \mathbb{N}$. Put $n = 2t + 1$. Prove that the code

$$C = \{\underbrace{00 \dots 00}_{n \text{ times}}, \underbrace{11 \dots 11}_{n \text{ times}}\}$$

is a perfect binary t -error correcting code of length n .

Proof : We easily get that $|C| = 2$ and $d(C) = 2t + 1$. So C is binary t -error correcting code of length $2t + 1$. To prove that C is perfect, we need to show that

$$|C| = \frac{m^n}{\sum_{i=0}^t \binom{n}{i} (m-1)^i}$$

So we need to prove that

$$2 = \frac{2^{2t+1}}{\sum_{i=0}^t \binom{2t+1}{i}}$$

which is equivalent to showing that

$$\sum_{i=0}^t \binom{2t+1}{i} = 2^{2t}$$

Put

$$A = \sum_{i=0}^t \binom{2t+1}{i} = \binom{2t+1}{0} + \binom{2t+1}{1} + \cdots + \binom{2t+1}{t-1} + \binom{2t+1}{t}$$

and

$$B = \sum_{i=t+1}^{2t+1} \binom{2t+1}{i} = \binom{2t+1}{t+1} + \binom{2t+1}{t+2} + \cdots + \binom{2t+1}{2t} + \binom{2t+1}{2t+1}$$

Then using Newton's Binomial Theorem, we find

$$A + B = \left(\sum_{i=0}^t \binom{2t+1}{i} \right) + \left(\sum_{i=t+1}^{2t+1} \binom{2t+1}{i} \right) = \sum_{i=0}^{2t+1} \binom{2t+1}{i} = \sum_{i=0}^{2t+1} \binom{2t+1}{i} 1^i 1^{2t+1-i} = (1+1)^{2t+1} = 2^{2t+1}$$

Recall that $\binom{n}{k} = \binom{n}{n-k}$ for all $n, k \in \mathbb{N}$ with $0 \leq k \leq n$. Hence we get that

$$\begin{aligned} A &= \binom{2t+1}{0} + \binom{2t+1}{1} + \cdots + \binom{2t+1}{t-1} + \binom{2t+1}{t} \\ &= \binom{2t+1}{(2t+1)-0} + \binom{2t+1}{(2t+1)-1} + \cdots + \binom{2t+1}{(2t+1)-(t-1)} + \binom{2t+1}{(2t+1)-t} \\ &= \binom{2t+1}{2t+1} + \binom{2t+1}{2t} + \cdots + \binom{2t+1}{t+2} + \binom{2t+1}{t+1} \\ &= B \end{aligned}$$

Thus $2^{2t+1} = A + B = 2A$. Hence $A = 2^{2t}$. □

5. Let n be an integer with $n \geq 2$. Let C be the binary code of length n consisting of all words containing an even number of ones. So if $n = 3$ then $C = \{000, 110, 101, 011\}$.

Find $|C|$ and $d(C)$.

Solution : Note that

$$\underbrace{000 \dots 000}_{n \text{ times}} \quad \text{and} \quad 11 \underbrace{00 \dots 00}_{n-2 \text{ times}}$$

are two distinct codewords. Since the distance between these two codewords is 2, we get that $d(C) \leq 2$.

Suppose that $d(C) = 1$. Then there exist distinct codewords $\mathbf{x}, \mathbf{y} \in C$ with $d_H(\mathbf{x}, \mathbf{y}) = 1$. So \mathbf{x} and \mathbf{y} are distinct in exactly one position, say the first position. Then $x_1 \neq y_1$ and $x_i = y_i$ for all $2 \leq i \leq n$. Since the code is binary, we have that either $(x_1, y_1) = (1, 0)$ or $(x_1, y_1) = (0, 1)$, say $(x_1, y_1) = (1, 0)$. Since \mathbf{x} is a codeword and $x_1 = 1$, we have that (x_2, \dots, x_n) contains an odd number of ones. Similarly, since \mathbf{y} is a codeword and $y_1 = 0$, we have that (y_2, \dots, y_n) contains an even number of ones. But that is a contradiction since $(x_2, \dots, x_n) = (y_2, \dots, y_n)$.

So $d(C) > 1$. Hence $d(C) = 2$.

Next, we count how many codewords there are. A codeword is of the form

$$x_1 x_2 \dots x_{n-1} x_n$$

where $x_i \in \{0, 1\}$ for all $1 \leq i \leq n$ and (x_1, \dots, x_n) contains an even number of ones. So we can choose x_1, x_2, \dots, x_{n-1} . But then x_n is determined : if (x_1, \dots, x_{n-1}) contains an odd number of ones then $x_n = 1$; if (x_1, \dots, x_{n-1}) contains an even number of ones then $x_n = 0$.

Hence

$$|C| = \underbrace{2 \cdot 2 \cdot \dots \cdot 2 \cdot 2}_{n-1 \text{ times}} = 2^{n-1} \quad \square$$

Remark : This counting argument is basically proving that the map

$$C \rightarrow \{0,1\}^{n-1} : (x_1, x_2, \dots, x_{n-1}, x_n) \rightarrow (x_1, x_2, \dots, x_{n-1})$$

is a bijection.

6. Consider the ternary code $\{000, 111, 222\}$. Suppose we have a channel and a constant p such that for all distinct $a, b \in \{0, 1, 2\}$, we have that the probability $P(a|b)$ that the symbol a is received if the symbol b is transmitted, is equal to p (e.g., if $p = 5\%$ and we transmit the symbol 0, then there is a 5% chance we receive the symbol 1, a 5% chance we receive the symbol 2 and a 90% chance we receive the symbol 0).

We use the following decoding algorithm when receiving a word $y_1y_2y_3$:

- (a) If $y_1y_2y_3$ contains three different symbols, we declare a decoding error.
- (b) If $y_1y_2y_3$ contains at most two different symbols, we decode as aaa where a is the symbol that shows up at least twice in $y_1y_2y_3$.

So we declare a decoding error if we receive 120 but decode as 111 if we receive 121.

We transmit the codeword 000 and use the decoding algorithm to decode the received word.

- (a) Calculate the probability that we declare a decoding error. Evaluate this if $p = 5\%$.
- (b) Calculate the probability that we decode correctly as 000. Evaluate this if $p = 5\%$.

Solution : If $y_1y_2y_3$ is a ternary word then we denote by $P(y_1y_2y_3|000)$ the probability that we receive the word $y_1y_2y_3$ if we transmit the codeword 000. Note that the probability that we receive the symbol we transmit is $1 - 2p$.

(a) We will declare a decoding error if we receive any of the following words :

$$\{012, 021, 102, 201, 120, 210\}$$

If $y_1y_2y_3 \in \{012, 021, 102, 201, 120, 210\}$ then $P(y_1y_2y_3|000) = (1-2p)p^2$. So the probability that we declare a decoding error is

$$\boxed{6(1-2p)p^2}$$

For $p = 5\%$ this becomes

$$\boxed{1.35\%}$$

(b) We will decode correctly if we receive any of the following words :

$$\{000, 001, 002, 010, 020, 100, 200\}$$

We easily get that $P(000|000) = (1-2p)^3$ and $P(y_1y_2y_3|000) = (1-2p)^2p$ if $y_1y_2y_3 \in \{001, 002, 010, 020, 100, 200\}$. So the probability that we decode correctly is

$$\boxed{6(1-2p)^2p + (1-2p)^3}$$

For $p = 5\%$, this becomes

$$\boxed{97.2\%}$$
