32032 Feedback Quiz, 2022/23, Week 02: Parameters. Bounds

Open books. 10–15 minutes. Not for credit. To be marked in class.

Recall that all $(n,M,d)_q$-codes satisfy the following bound on M: $M \leq q^n / \left(\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \right)$, called the **Hamming bound**. Here $t = [(d-1)/2]$. Codes which attain this bound are *perfect*.

Furthermore, all $[n,k,d]_q$-codes satisfy $k \leq n-d+1$, the **Singleton bound**. Codes which attain this bound are called *MDS codes*. You will have to use these two bounds in the questions below.

Question 1 ♣ This question is about the binary repetition code of length 7, defined as $\mathrm{Rep}(7,\mathbb{F}_2) = \{0000000, 1111111\}$. Fill in the blanks:

$\mathrm{Rep}(7,\mathbb{F}_2)$ *is a* $(\square,\square,\square)_{\square}$ *code and a* $[\square,\square,\square]_{\square}$ *code which can detect up to* $\square$ *bit errors and can correct up to* $\square$ *bit errors per codeword. Its rate is* $\square$.

You now need to use the formulas for the Hamming bound and the Singleton bound and do a calculation to decide if the following are true:

- ◯ The binary repetition code of length 7 is perfect
- ◯ The binary repetition code of length 7 is an MDS code

Question 2 What is the upper bound on the information dimension k of a binary linear code of length 31 and minimum distance 3 dictated by the **Singleton bound**?

◯ 22 ◯ 23 ◯ 24 ◯ 25 ◯ 26 ◯ 27 ◯ 28 ◯ 29 ◯ 30 ◯ 31

Question 3 What is the upper bound on the **information dimension** k of a binary code of length 31 and minimum distance 3 dictated by the **Hamming bound**? (*Careful*: dimension is k, not M)

◯ 22 ◯ 23 ◯ 24 ◯ 25 ◯ 26 ◯ 27 ◯ 28 ◯ 29 ◯ 30 ◯ 31

Question 4 Assuming that you answered Questions 2 and 3 correctly, what conclusion can you make from the answers?

- ◯ A binary code of length 31 and minimum distance 3 cannot be perfect.
- ◯ A binary code of length 31 and minimum distance 3 cannot be MDS.

CORRECTED

32032 Feedback Quiz, 2022/23, Week 02: Parameters. Bounds

Open books. 10–15 minutes. Not for credit. To be marked in class.

Recall that all $(n,M,d)_q$-codes satisfy the following bound on M: $M \leq q^n / \Big(\sum_{i=0}^{t} \binom{n}{i} (q-1)^i\Big)$, called the **Hamming bound**. Here $t = [(d-1)/2]$. Codes which attain this bound are *perfect*.

Furthermore, all $[n,k,d]_q$-codes satisfy $k \leq n-d+1$, the **Singleton bound**. Codes which attain this bound are called *MDS codes*. You will have to use these two bounds in the questions below.

Question 1 ♣ This question is about the binary repetition code of length 7, defined as $\mathrm{Rep}(7,\mathbb{F}_2) = \{0000000, 1111111\}$. Fill in the blanks:

$\mathrm{Rep}(7,\mathbb{F}_2)$ *is a* $\Big(\boxed{7}, \boxed{2}, \boxed{7}\Big)_{\boxed{2}}$ *code and a* $\Big[\boxed{7}, \boxed{1}, \boxed{7}\Big]_{\boxed{2}}$ *code which can detect up to* $\boxed{6}$ *bit errors and can correct up to* $\boxed{3}$ *bit errors per codeword. Its rate is* $\boxed{1/7}$.

You now need to use the formulas for the Hamming bound and the Singleton bound and do a calculation to decide if the following are true:

- ⊗ The binary repetition code of length 7 is perfect
- ⊗ The binary repetition code of length 7 is an MDS code

Explanation: From the definition, $n = 7$, $M = 2$ and $q = 2$ (binary), so $k = \log_2 M = 1$. The minimum distance is $d = 7$, by inspection. This code can detect up to $d-1 = 6$ errors and can correct up to $t = \left[\frac{d-1}{2}\right] = 3$ errors. The rate is $R = k/n = 1/7$.
Calculation: $t = [(7-1)/2] = 3$ so the denominator of the Hamming bound is

$$\binom{7}{0}(1)^0 + \binom{7}{1}(1)^1 + \binom{7}{2}(1)^2 + \binom{7}{3}(1)^3 = 1+7+\frac{7\times 6}{1\times 2}+\frac{7\times 6\times 5}{1\times 2\times 3} = 1+7+21+35 = 64.$$

The Hamming bound says $M \leq 2^7/64 = 2^7/2^6 = 2$. Since $M = 2$ for this code, the bound is attained and the code **is perfect.**
$k = 1 = 7-7+1$ so the Singleton bound is attained and the code **is MDS.**

Question 2 What is the upper bound on the information dimension k of a binary linear code of length 31 and minimum distance 3 dictated by the **Singleton bound**?

○ 22 ○ 23 ○ 24 ○ 25 ○ 26 ○ 27 ○ 28 ⊗ 29 ○ 30 ○ 31

Explanation: Recall the Singleton bound: $k \leq n - d + 1$. Here $n = 31$, $d = 3$ so $k \leq 31 - 3 + 1$. Answer: 29.

Question 3 What is the upper bound on the **information dimension** k of a binary code of length 31 and minimum distance 3 dictated by the **Hamming bound**? (*Careful*: dimension is k, not M)

○ 22 ○ 23 ○ 24 ○ 25 ⊗ 26 ○ 27 ○ 28 ○ 29 ○ 30 ○ 31

Explanation: It is convenient to use the Hamming bound in the **logarithmic form** (taking log_q of both sides) $k \leq n - \log_q \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$. Note that $t = [(d(C)-1)/2]$. Hence we have $t = 1$ and the log-Hamming bound becomes $k \leq n - \log_2(1+n) = n - \log_2(1+n)$. Substituting $n = 31$, we get $k \leq 31 - \log_2(32) = 31 - 5 = 26$. Answer: 26.

Question 4 Assuming that you answered Questions 2 and 3 correctly, what conclusion can you make from the answers?

○ A binary code of length 31 and minimum distance 3 cannot be perfect.

⊗ A binary code of length 31 and minimum distance 3 cannot be MDS.

Explanation: The Hamming bound says that every such code will have information dimension at most 26. Hence, attaining the Singleton bound is impossible because that would need $k = 29$ which is prohibited by the Hamming bound. *As a matter of fact, there are perfect* $[31, 26, 3]_2$ *codes which will be seen later in the course.*