32032 Feedback Quiz, 2022/23, Week 04: Weight enumerator and P_{undetect}

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

Some questions below refer to the *weight enumerator*. Recall that the weight enumerator of a linear code C is the polynomial $W_C(x,y)$ in two variables, defined as $W_C(x,y) = \sum_{\underline{c} \in C} x^{n-w(\underline{c})} y^{w(\underline{c})}$, or equivalently as $A_0 x^n + A_1 x^{n-1} y + \cdots + A_n y^n$ where n is the length of C and A_i is the number of codevectors of C of weight i.

Consider E_4, the even weight code of length 4 which is a subspace of $\mathbb{F}_2^4$.

Question 1 The weight of E_4 is:

○ 0 ○ 1 ○ 2 ○ 3 ○ 4

Question 2 E_4 is a perfect code:

○ No ○ Yes

Question 3 Alice needs to trasmit information (a stream of bits) to Bob over a noisy channel. She wants to use the code E_4 for error detection. In order to do that, Alice needs to split her stream of bits into messages and encode each message into a codevector of E_4. How many bits should be in each message?

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 8

Question 4 Write down the weight enumerator of E_4:

$$W_{E_4}(x,y) = \boxed{}$$

A codevector of E_4 is sent via BSC(p). What is the probability $P_{\text{undetect}}(E_4)$ of an undetected error?

○ $(1-p)^4$ ○ 0 ○ p^4 ○ $6(1-p)^2p^2 + p^4$ ○ $(1-p)^3$

Write down the **leading term** of $P_{\text{undetect}}(E_4)$. (The leading term is Ap^d where $A \neq 0$ and $P_{\text{undetect}}(E_4)$ is a polynomial of the form Ap^d+(higher powers of p).

$$P_{\text{undetect}}(E_4) \approx \boxed{}\, p^{\boxed{}}$$

Question 5 The space $\mathbb{F}_2^4$ is partitioned into cosets of E_4. How many cosets?

○ 1 ○ 2 ○ 4 ○ 8 ○ 16

CORRECTED

32032 Feedback Quiz, 2022/23, Week 04: Weight enumerator and P_{undetect}

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

Some questions below refer to the *weight enumerator*. Recall that the weight enumerator of a linear code C is the polynomial $W_C(x,y)$ in two variables, defined as $W_C(x,y) = \sum_{\underline{c} \in C} x^{n-w(\underline{c})} y^{w(\underline{c})}$, or equivalently as $A_0 x^n + A_1 x^{n-1} y + \cdots + A_n y^n$ where n is the length of C and A_i is the number of codevectors of C of weight i.

Consider E_4, the even weight code of length 4 which is a subspace of $\mathbb{F}_2^4$.

Question 1 The weight of E_4 is:

○ 0 ○ 1 ⊗ 2 ○ 3 ○ 4

Explanation: The weight of the code is positive by definition, so 0 is wrong, and this is the even weight code, hence cannot have codevectors of odd weight 1. So weight 2 is the next possible candidate, and indeed $E_4 \ni 1100$, a vector of weight 2 which is minimum positive weight in E_4. Thus, $w(E_4) = 2$.

Question 2 E_4 is a perfect code:

⊗ No ○ Yes

Explanation: The minimum distance is 2 which is even. The minimum distance of a perfect code is odd. So E_4 is not perfect.

Question 3 Alice needs to trasmit information (a stream of bits) to Bob over a noisy channel. She wants to use the code E_4 for error detection. In order to do that, Alice needs to split her stream of bits into messages and encode each message into a codevector of E_4. How many bits should be in each message?

○ 1 ○ 2 ⊗ 3 ○ 4 ○ 5 ○ 8

Explanation: In general, codevectors of a linear code of dimension k encode messages of length k. Here $k = \dim E_4 = 3$. The most natural encoder takes a 3-bit binary word (x_1, x_2, x_3) and outputs the codevector (x_1, x_2, x_3, x_4) of E_4, where $x_4 = x_1 + x_2 + x_3$ is the parity check bit, appended to the message.

Question 4 Write down the weight enumerator of E_4:

$$W_{E_4}(x,y) = \boxed{x^4 + 6x^2y^2 + y^4}$$

A codevector of E_4 is sent via BSC(p). What is the probability $P_{\text{undetect}}(E_4)$ of an undetected error?

○ $(1-p)^4$ ○ 0 ○ p^4 ⊗ $6(1-p)^2p^2 + p^4$ ○ $(1-p)^3$

Write down the **leading term** of $P_{\text{undetect}}(E_4)$. (The leading term is Ap^d where $A \neq 0$ and $P_{\text{undetect}}(E_4)$ is a polynomial of the form Ap^d+(higher powers of p).

$$P_{\text{undetect}}(E_4) \approx \boxed{\mathbf{6}}\, p^{\boxed{\mathbf{2}}}$$

Explanation: We need to work out the weight enumerator of E_4. The code has one codevector of weight 0, namely 0000. The code has six codevectors of weight 2: you can start with 0011 and write down all codevectors of weight 2, or, better, realise that we are talking about the number of ways to choose two positions for 1s out of four positions, which gives $\binom{4}{2} = 6$ choices. Finally, the code has one codevector of weight 4, namely 1111. Hence the weight enumerator is

$$W_{E_4}(x,y) = x^4 + 6x^2y^2 + y^4.$$

Recall the formula $P_{\text{undetect}}(C) = W_C(1-p, p) - (1-p)^n$. In the case $C = E_4$ we have $(1-p)^4 + 6(1-p)^2p^2 + p^4 - (1-p)^4$ which is the answer as indicated.
All terms with p^0 and p^1 cancel, and the term containing p^2 comes from $6(1-p)^2p^2$ — that term is $6p^2$.

Question 5 The space $\mathbb{F}_2^4$ is partitioned into cosets of E_4. How many cosets?

○ 1 ⊗ 2 ○ 4 ○ 8 ○ 16

Explanation: Each coset of a linear code C is a set of the form $\underline{v} + C$ and so has the same cardinality as C. The space $\mathbb{F}_q^n$ is partitioned into cosets, each of cardinality $\#C$, hence the number of cosets is $\dfrac{\#\mathbb{F}_q^n}{\#C}$. In our example this is $\dfrac{\#\mathbb{F}_2^4}{\#E_4} = \dfrac{2^4}{8} = 2$.