

Name: \_\_\_\_\_ Student ID: \_\_\_\_\_ Score: \_\_\_\_\_

1. (50%) Prove that among all continuous random variables of mean  $\mu$  and variance  $\sigma^2$ , Gaussian random variable has the largest differential entropy.

Hint: Let  $X$  be the Gaussian random variable of mean  $\mu$  and variance  $\sigma^2$ . Let  $Y$  be an arbitrary random variable of the same mean and variance as  $X$ . Then,

$$\begin{aligned}
 h(X) &= \int_{\mathbb{R}} f_X(x) \log_2 \frac{1}{f_X(x)} dx \\
 &= \int_{\mathbb{R}} f_X(x) \left[ \frac{1}{2} \log_2(2\pi\sigma^2) + \log_2(e) \cdot \frac{(x-\mu)^2}{2\sigma^2} \right] dx \\
 &= \int_{\mathbb{R}} f_Y(x) \left[ \frac{1}{2} \log_2(2\pi\sigma^2) + \log_2(e) \cdot \frac{(x-\mu)^2}{2\sigma^2} \right] dx \\
 &= \int_{\mathbb{R}} f_Y(x) \log_2 \frac{1}{f_X(x)} dx
 \end{aligned} \tag{1}$$

Complete the proof based on (1).

**Solution.** See Slide IDC 6-54. Other than the fundamental inequality, you can also use Jensen's inequality, or log-sum inequality (or the non-negativity of divergence) to prove the result.

2. (50%) Let the generator polynomial of a polynomial code of length  $n = 5$  be  $g(X) = X^3 + X + 1$ . List all the code polynomials of this polynomial code via

$$c(X) = a(X)g(X).$$

What is the minimum pairwise Hamming distance of this code?

Hint:

$$d_{\min} = \min_{\mathbf{c}_i, \mathbf{c}_j \in \mathcal{C}, \mathbf{c}_i \neq \mathbf{c}_j} d_H(\mathbf{c}_i, \mathbf{c}_j) = \min_{\mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}} w_H(\mathbf{c})$$

**Solution.**  $c(X) = (a_0 + a_1X)(1 + X + X^3)$  implies

| $c(X)$                                                    | $(a_0 + a_1X)(1 + X + X^3)$    |
|-----------------------------------------------------------|--------------------------------|
| $0 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4$ | $(0 + 0 \cdot X)(1 + X + X^3)$ |
| $0 + 1 \cdot X + 1 \cdot X^2 + 0 \cdot X^3 + 1 \cdot X^4$ | $(0 + 1 \cdot X)(1 + X + X^3)$ |
| $1 + 1 \cdot X + 0 \cdot X^2 + 1 \cdot X^3 + 0 \cdot X^4$ | $(1 + 0 \cdot X)(1 + X + X^3)$ |
| $1 + 0 \cdot X + 1 \cdot X^2 + 1 \cdot X^3 + 1 \cdot X^4$ | $(1 + 1 \cdot X)(1 + X + X^3)$ |

The minimum pairwise Hamming distance is the smallest Hamming weight of non-zero codewords, which is 3.