Please discuss the following problems among the students in your group. Some of the groups will be selected to present sample solutions at the group presentation on Wednesday.

Day Two

Problem 1

Consider the linear code $\mathbb{C}$ of length 10 and dimension 9 over $\mathbb{F}_{11}$ whose parity-check matrix is given by

$$\mathbf{H} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

(Note that $\mathbb{F}_{11}$ is a fancy way of saying that one is computing with integers where addition and multiplication are modulo 11.)

This code is used for ISBNs (International Standard Book Numbers). Actually, in that case, the first nine symbols (the information symbols) are confined to lie in $\{0, 1, 2, \ldots, 9\}$, whereas the last symbol (check symbol) lies in $\{0, 1, 2, \ldots, 9, \mathrm{X}=10\}$.

(a) Wikipedia says that the parity-check matrix for the ISBN code is

$$\mathbf{H}' = \begin{pmatrix} 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Why is there no contradiction with the above definition?

(b) Show that $\mathbb{C}$ has minimum (Hamming) distance two.

(c) Show that there is a decoder for $\mathbb{C}$ which can detect one single error or the transposition of two codeword positions.

Remark: The above is the description of the ISBN-10 standard, which uses codewords of length 10. There is also the newer ISBN-13 standard, which uses 13 symbols, a different parity-check matrix, and modulo-10 arithmetic.

Problem 2

Consider the transmission of a binary codeword of length n over a binary symmetric channel (BSC) with cross-over probability ε, where $0 \leq \varepsilon \leq 1$. (A BSC with cross-over probability ε is a memoryless channel that flips a transmitted bit with probability ε.)

Let Z_i, $i = 1, \ldots, n$, be independent discrete random variables that tell us if a bit flip happened at time i, i.e., when a bit flip happened at time i then $z_i = 1$, otherwise $z_i = 0$. The probability mass function of Z_i is therefore $P_{Z_i}(0) = 1 - \varepsilon$ and $P_{Z_i}(1) = \varepsilon$. Furthermore, let

$$Z = Z_1 + \cdots + Z_n \quad (\text{in } \mathbb{Z})$$

be the total number of bit flips and let

$$Z' = Z/n$$

be the relative number of bit flips.

(a) What are $\mathrm{E}[Z_i]$ and $\mathrm{Var}[Z_i]$ for $i = 1, \ldots, n$?

(b) What are $\mathrm{E}[Z]$ and $\mathrm{Var}[Z]$?

(c) What are $\mathrm{E}[Z']$ and $\mathrm{Var}[Z']$?

(d) Let $\varepsilon = 0.1$. For $n = 10$, $n = 1000$, and $n = 100000$, compute the the mean $\mathrm{E}[Z']$ and standard deviation $\sqrt{\mathrm{Var}[Z']}$.

(e) The smaller the standard deviation (or the variance) of a random variable is, the more we can expect that the value taken on in a random experiment will be near the expected value. What does this and the above calculations imply about the relative number of errors when using longer and longer block lengths n?

Calvin, the coding theorist:

Problem 3

(a) Let the binary linear code $\mathbb{C}_2$ of length $n = 2$ be defined by the parity-check matrix

$$\mathbf{H}_2 = \begin{pmatrix} 1 & 1 \end{pmatrix}.$$

List all the codewords of $\mathbb{C}_2$. Using the natural embedding map $\mathbb{F}_2 \to \mathbb{R}$, where $0 \mapsto 0$ and $1 \mapsto 1$, draw the codewords in $\mathbb{R}^2$. Show that $\mathrm{conv}(\mathbb{C}_2)$ is characterized as follows:

$$\mathrm{conv}(\mathbb{C}_2) = \left\{ (\omega_1, \omega_2) \in \mathbb{R}^2 \;\middle|\; \begin{array}{c} 0 \le \omega_1 \le 1 \\ 0 \le \omega_2 \le 1 \\ -\omega_1 + \omega_2 \ge 0 \\ +\omega_1 - \omega_2 \ge 0 \end{array} \right\}.$$

(b) Let the binary linear code $\mathbb{C}_3$ of length $n = 3$ be defined by the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

List all the codewords of $\mathbb{C}_3$. Using the natural embedding map $\mathbb{F}_2 \to \mathbb{R}$, where $0 \mapsto 0$ and $1 \mapsto 1$, draw the codewords in $\mathbb{R}^3$. Show that $\mathrm{conv}(\mathbb{C}_3)$ is characterized as follows:

$$\mathrm{conv}(\mathbb{C}_3) = \left\{ (\omega_1, \omega_2, \omega_3) \in \mathbb{R}^3 \;\middle|\; \begin{array}{c} 0 \le \omega_1 \le 1 \\ 0 \le \omega_2 \le 1 \\ 0 \le \omega_3 \le 1 \\ -\omega_1 + \omega_2 + \omega_3 \ge 0 \\ +\omega_1 - \omega_2 + \omega_3 \ge 0 \\ +\omega_1 + \omega_2 - \omega_3 \ge 0 \\ -\omega_1 - \omega_2 - \omega_3 \ge -2 \end{array} \right\}.$$

Note: It turns out that the first three inequalities are not needed here, i.e., the last four inequalities describe $\mathrm{conv}(\mathbb{C}_3)$ completely. However, when generalizing these results to $n \ge 4$, the inequalities of the type $0 \le \omega_i \le 1$, $i = 1, \ldots, n$, are needed.

(c) Consider again the code in Part (a). Let

$$\mathcal{S}_2 \triangleq \big\{ \mathbf{x} \in \mathbb{F}_2^2 \;\big|\; w_{\mathrm{H}}(\mathbf{x}) \text{ is odd} \big\}.$$

Show that

$$\mathrm{conv}(\mathbb{C}_2) = \left\{ (\omega_1, \omega_2) \in \mathbb{R}^2 \;\middle|\; \begin{array}{c} 0 \le \omega_i \le 1 \text{ for } i = 1, 2 \\ \|\boldsymbol{\omega} - \mathbf{s}\|_1 \ge 1 \text{ for all } \mathbf{s} \in \mathcal{S}_2 \end{array} \right\},$$

where the natural embedding map is used for the components of the vector $\mathbf{s}$ and where $\|\mathbf{a}\|_1 \triangleq \sum_i |a_i|$ denotes the ℓ_1-norm of a vector.

(d) Consider again the code in Part (b). Let

$$\mathcal{S}_3 \triangleq \big\{ \mathbf{x} \in \mathbb{F}_2^3 \;\big|\; w_{\mathrm{H}}(\mathbf{x}) \text{ is odd} \big\}.$$

Show that

$$\mathrm{conv}(\mathbb{C}_3) = \left\{ (\omega_1, \omega_2, \omega_3) \in \mathbb{R}^3 \;\middle|\; \begin{array}{c} 0 \le \omega_i \le 1 \text{ for } i = 1, 2, 3 \\ \|\boldsymbol{\omega} - \mathbf{s}\|_1 \ge 1 \text{ for all } \mathbf{s} \in \mathcal{S}_3 \end{array} \right\},$$

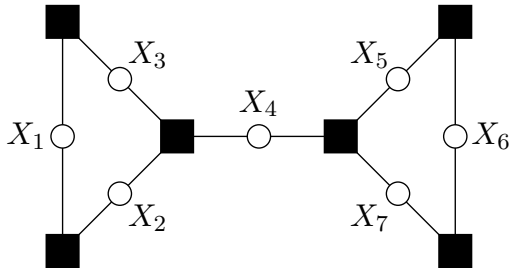
where the natural embedding map is used for the components of the vector $\mathbf{s}$ and where $\|\mathbf{a}\|_1 \triangleq \sum_i |a_i|$ denotes the ℓ_1-norm of a vector.

Problem 4

Consider the binary linear code $\mathbb{C}$ defined by the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

This code is also defined by the following Tanner graph:



(a) Show that the rank of $\mathbf{H}$ is 5.
Note: This implies that a suitably chosen row of $\mathbf{H}$ can be removed without changing $\mathbb{C}$.

(b) List all the codewords of $\mathbb{C}$. What are the code parameters n and k?

(c) Verify that

$$\boldsymbol{\omega} \triangleq \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$$

is a pseudo-codeword, i.e., show that $\boldsymbol{\omega}$ is in the fundamental polytope $\mathcal{P}(\mathbf{H})$.
Hint: You need to show that

$$\begin{aligned} (\omega_1, \omega_2) &\in \operatorname{conv}(\mathbb{C}_2), \\ (\omega_1, \omega_3) &\in \operatorname{conv}(\mathbb{C}_2), \\ (\omega_2, \omega_3, \omega_4) &\in \operatorname{conv}(\mathbb{C}_3), \\ (\omega_4, \omega_5, \omega_7) &\in \operatorname{conv}(\mathbb{C}_3), \\ (\omega_5, \omega_6) &\in \operatorname{conv}(\mathbb{C}_2), \\ (\omega_6, \omega_7) &\in \operatorname{conv}(\mathbb{C}_2), \end{aligned}$$

where $\mathbb{C}_2$ and $\mathbb{C}_3$ were defined in Problems 3(a) and 3(b), respectively.

(d) With the help of the last Parts (b) and (c), show that $\operatorname{conv}(\mathbb{C}) \subsetneq \mathcal{P}(\mathbf{H})$.

(e) Give an LLR vector $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_7)$ such that linear programming decoding decides for

$$\boldsymbol{\omega} \triangleq \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right).$$

Comment: for this $\boldsymbol{\lambda}$, the LP decoding result and the (blockwise) ML decoding result will obviously differ because (blockwise) ML decoding always gives back a codeword.