EE 605: Error Correcting Codes (Autumn 2015)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Problem Set 1 Date: August 7, 2015

1. [5 points] Prove that the Hamming distance satisfies the triangle inequality, i.e. $d(\mathbf{u}, \mathbf{v}) \le d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$ for all n-tuples $\mathbf{u}, \mathbf{v}, \mathbf{w}$.

2. [5 points] Let p be a prime number. Prove that the set $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ is a field under integer addition and multiplication modulo p. Give an example to show that $\mathbb{F}_p$ is not a field if p is composite.

3. [5 points] Prove that for a binary block code with minimum distance d_{min}, the minimum distance decoder can correct upto $\lfloor \frac{d_{min}-1}{2} \rfloor$ errors.

4. [5 points] Prove that the n-repetition code and the $(n, n-1)$ single parity check code are the dual codes of each other.

5. [5 points] Prove that $\left(C^{\perp}\right)^{\perp} = C$ when C is a linear block code. *Hint:* $\dim C + \dim C^{\perp} = n$ *where* n *is codeword length.*

6. [5 points] Let the generator matrix of an (n, k) binary linear block code C be of the form $\begin{bmatrix} I_k & P \end{bmatrix}$ where I_k is the $k \times k$ identity matrix and P is a $k \times n-k$ matrix. Show that $\begin{bmatrix} P^T & I_{n-k} \end{bmatrix}$ is a parity check matrix for C.

7. [5 points] Let C be a linear block code with parity check matrix $\mathbf{H}$. Prove that

$$\mathbf{v} \in C \iff \mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$$

8. [5 points] Let C be a binary linear block code given by the vectors

$$\begin{gathered}
[0,0,0,0,0,0,0], [1,0,0,0,0,0,1], [0,1,0,0,1,0,0], [1,1,0,0,1,0,1], \\
[0,0,1,0,0,1,0], [1,0,1,0,0,1,1], [0,1,1,0,1,1,0], [1,1,1,0,1,1,1], \\
[0,0,0,1,0,0,1], [1,0,0,1,0,0,0], [0,1,0,1,1,0,1], [1,1,0,1,1,0,0], \\
[0,0,1,1,0,1,1], [1,0,1,1,0,1,0], [0,1,1,1,1,1,1], [1,1,1,1,1,1,0]
\end{gathered}$$

   (a) What is the dimension of $C^{\perp}$?
   (b) What is the minimum distance of $C^{\perp}$?

9. [5 points] The first row of a standard array is given below where the last four entries are missing. It is known that this standard array has 8 columns.

$$000000 \quad 110001 \quad 101010 \quad 000111 \quad * \quad * \quad * \quad *$$

   (a) Complete the standard array by giving all the remaining columns and rows.
   (b) If the code corresponding to this standard array is used over a binary symmetric channel with crossover probability p, what is the probability of decoding error?

10. [5 points] Consider a binary linear code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Suppose a codeword from this code is sent over a binary symmetric channel with crossover probability p. What is the probability that the received vector is a codeword?

11. [5 points] Let C_1, C_2 be binary linear block codes of same length n and dimensions k_1, k_2 respectively. Let d_i be the minimum distance of C_i for $i = 1, 2$. Consider the set of vectors in $\mathbb{F}_2^{2n}$

$$C_3 = \left\{ \begin{bmatrix} \mathbf{u} & \mathbf{v} \end{bmatrix} \middle| \mathbf{u} \in C_1, \mathbf{v} \in C_2 \right\}.$$

   (a) Show that C_3 is a linear block code.

   (b) What is the dimension of C_3? Explain your answer.

   (c) What is the minimum distance of C_3? Explain your answer.

   (d) Let G_i be a generator matrix of code C_i for $i = 1, 2$. Find a generator matrix for C_3 in terms of G_1 and G_2.

12. [5 points] Let C be an (n, k) binary linear block code having minimum distance d_{min} and weight enumerator $A(z)$. Let $\mathbf{G}$ be a generator matrix of C. Consider the length $3n$ code C_1 with generator matrix $\mathbf{G}_1 = \begin{bmatrix} \mathbf{G} & \mathbf{G} & \mathbf{G} \end{bmatrix}$. Answer the following in terms of the parameters of C. Explain your answers.

   (a) What is the dimension of C_1?

   (b) What is the minimum distance of C_1?

   (c) What is the weight enumerator of C_1?

13. [5 points] Construct the standard array for a binary linear block code with the following generator matrix if it is to be used over a binary symmetric channel with crossover probability $p < \frac{1}{2}$.

$$G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

   Construct the syndrome-error pattern lookup table for this code, i.e. a one-to-one mapping between the set of syndromes and set of correctable error patterns.

14. [5 points] Let C be a linear block code and $C^\perp$ be its dual code. A code is said to be *self-dual* if $C = C^\perp$. Prove that a linear self-dual code has even length n and dimension $\frac{n}{2}$.

15. [5 points] Let C be a linear block code and $C^\perp$ be its dual code. A code is said to be *self-orthogonal* if $C \subseteq C^\perp$.

   (a) Prove that each codeword in a binary self-orthogonal code C has even weight and $C^\perp$ contains the all-ones codeword $\mathbf{1} = 111\cdots1$.

   (b) Prove that if every codeword of a binary linear block code C has weight divisible by 4, then C is self-orthogonal.

16. [5 points] Find the smallest binary linear block code which contains the following codewords $\{100101, 110010, 010111, 001011\}$. Find a systematic[1] generator matrix for this code. What is the minimum distance of this code?

[1] A systematic generator matrix for an (n, k) linear block code has the $k \times k$ identity matrix in its first k columns.

17. [5 points] Let C_1 and C_2 be two linear block codes of same length n.
    (a) Show that $C_1 \cap C_2$ is a linear code.
    (b) Show that $C_1 \cup C_2$ is a linear code if and only if either $C_1 \subseteq C_2$ or $C_2 \subseteq C_1$.

18. [5 points] Let C_1 and C_2 be binary linear block codes of the same length n. If $C_1 \subseteq C_2$, show that $C_2^{\perp} \subseteq C_1^{\perp}$.

19. [5 points] Let C be an (n, k) binary linear block code with $k \geq 1$. Let $\mathbf{v} \in \mathbb{F}_2^n$ be a vector not in the dual code of C, i.e. $\mathbf{v} \notin C^{\perp}$. Show that $\mathbf{v}$ is orthogonal to exactly half of the codewords in C.

20. [5 points] Show that in every binary linear block code either all the codewords have even Hamming weight or exactly half of the codewords have even Hamming weight. *Hint:* $\sum_{i=1}^{n} v_i = 0$ for a codeword $\mathbf{v}$ of even weight or equivalently $\mathbf{v} \cdot \mathbf{1}^T = 0$ where $\mathbf{1}$ is the $1 \times n$ vector containing all ones.

21. [5 points] Show that in a binary linear block code, either all the codewords begin with 0, or exactly half begin with 0 and half with 1.

22. [5 points] Let C_1 be an (n, k_1) binary linear block code with minimum distance d_1 and let C_2 be an (n, k_2) binary linear block code with minimum distance d_2. Consider the following set of $2n$-tuples

$$C = \{(\mathbf{u}, \mathbf{u} + \mathbf{v}) | \mathbf{u} \in C_1, \mathbf{v} \in C_2\}.$$

    Prove that the set C is a binary linear block code with dimension $k = k_1 + k_2$ and minimum distance $d_{min} = \min\{2d_1, d_2\}$.

23. [5 points] Show that a binary block code can simultaneously correct $1, 2, 3, \ldots, a$ errors and detect $a + 1, a + 2, \ldots, b$ errors if and only if it has minimum distance at least $a + b + 1$. *Note: If a code is used for **only error detection**, it can detect upto $d_{min} - 1$ errors. If it is used for **only error correction**, it can correct upto $\lceil \frac{d_{min}-1}{2} \rceil$ errors.*