

Problem Set #1

Due date: Friday February 9, 2007

1. One version of the (7, 4) Hamming code has generator matrix

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

- (a) List all of the codewords. How many codewords are there of each possible weight? What is the minimum distance of the code?
- (b) Find a parity-check matrix for this code.
- (c) This code is used on a binary symmetric channel with crossover probability  $p < 1/2$ . Decode the following received vectors:  $r = 1010101$ ,  $r = 1011101$ ,  $r = 1010010$ ,  $r = 1111111$ .
- (d) Find the probability of a decoding error as a function of  $p$ .
2. (a) Show that the Hamming codes over a finite field of  $q$  elements have, for integer  $m \geq 2$ , block length  $n = (q^m - 1)/(q - 1)$  and dimension  $k = n - m$ .
- (b) Construct generator and parity-check matrices for the (4, 2) ternary Hamming code.
- (c) Construct generator and parity-check matrices for the (6, 4) Hamming code over  $F_5$ .
3. A *metric* on a set  $X$  is a function  $d : X \times X \rightarrow \mathbb{R}$  satisfying, for all  $x, y, z \in X$ ,
- (a)  $d(x, y) \geq 0$  (with equality if and only if  $x = y$ ),
- (b)  $d(x, y) = d(y, x)$  and
- (c)  $d(x, z) \leq d(x, y) + d(y, z)$ .

Prove that Hamming distance is a metric on  $F^n$  for any finite field  $F$ .

4. Let  $p$  be a prime and let  $a$  be any integer. Show that  $a^p \equiv a \pmod{p}$ . [*Hint*: consider the order of  $a \pmod{p}$  in the cyclic group  $\mathbb{Z}_p$ .]
5. (In this problem you will prove the familiar result from linear algebra that the sum of the rank and the nullity of a linear mapping gives the dimension of the mapping's domain.)

Let  $V$  and  $W$  be finite-dimensional vector spaces over a field  $F$ , and let  $T : V \rightarrow W$  be a linear mapping, i.e., a function with domain  $V$  and co-domain  $W$  satisfying  $T(a_1v_1 + a_2v_2) = a_1T(v_1) + a_2T(v_2)$  for all scalars  $a_1, a_2 \in F$  and vectors  $v_1, v_2 \in V$ . Let  $\text{img}_T(V) \subseteq W$  denote the image of  $V$  under  $T$ , and let  $\text{ker}_T(V) \subseteq V$  denote the kernel of  $T$ , i.e., the subset of  $V$  that is mapped to the zero vector by  $T$ .

- (a) Show that  $\text{img}_T(V)$  and  $\text{ker}_T(V)$  are vector spaces.
- (b) Show that  $\dim(\text{img}_T(V)) + \dim(\text{ker}_T(V)) = \dim(V)$ . [*Hint*: Suppose that  $\text{img}_T(V)$  has basis  $w_1, \dots, w_a$  and  $\text{ker}_T(V)$  has basis  $v_1, \dots, v_b$ . Show that

$$T^{-1}(w_1), \dots, T^{-1}(w_a), v_1, \dots, v_b$$

is a basis for  $V$ , where  $T^{-1}(w_i)$  is any element in the pre-image of  $w_i$  under  $T$ .]

6. Let  $C$  be a linear  $(n, k)$  code over a field  $F$ . Show that the dual code  $C^\perp$  has dimension  $n - k$ . [Hint: Use a generator matrix for  $C$  to define a linear mapping between two vector spaces and apply the rank-nullity theorem. You may also need to use the property that the row-rank and column-rank of a matrix are equal.]
7. Let  $C$  be a linear  $(n, k)$  code over a finite field  $F$  and let  $H$  be a parity-check matrix for  $C$ . Show that two vectors  $v, w \in F^n$  are elements of the same coset of  $C$  if and only if  $vH^T = wH^T$ .
8. A linear code  $C_2$  is a *linear subcode* of a linear code  $C_1$  if  $C_2 \subseteq C_1$ . Show that if  $C_2$  is a linear subcode of  $C_1$ , then  $C_1^\perp$  is a linear subcode of  $C_2^\perp$ .
9. Let  $C$  be a binary linear  $(n, k)$  code. Let  $M_C$  be a codebook matrix for  $C$ , i.e., a  $2^k \times n$  matrix whose rows consist of the  $2^k$  distinct codewords of  $C$ , taken in some arbitrary order.
- Show that each column of  $M$  is either identically zero, or has an equal number of zeros and ones.
  - Show that the total weight of  $C$ , i.e., the number of ones in  $M$ , is no greater than  $n2^{k-1}$ .
  - Show that, among the nonzero codewords, the average codeword weight is no greater than  $\frac{n2^{k-1}}{2^k - 1}$ . Explain why the *minimum* nonzero weight cannot exceed the *average* nonzero weight, and conclude that any binary  $(n, k)$  code  $C$  has a minimum distance  $d_{\min}(C)$  that satisfies

$$d_{\min}(C) \leq \frac{n2^{k-1}}{2^k - 1}.$$

- Give conditions on  $C$  for which this bound is met with equality.
- Show that the code  $(3m, 2)$  code with generator matrix

$$G = \left[ \begin{array}{cccccccccccc} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \end{array} \right],$$

in which every row has weight  $2m$ , has maximum possible minimum distance among all two-dimensional codes of length  $3m$ .

10. Let  $N(k, d)$  denote the length of the shortest binary linear code of dimension  $k$  and minimum distance  $d$ .
- Show that

$$N(k, d) \geq d + N(k - 1, \lceil d/2 \rceil).$$

[Hint: If  $C$  is an  $[N(k, d), k, d]$  code, then without loss of generality, a generator matrix for  $C$  can be written as

$$G = \left[ \begin{array}{cccc|cccc} 1 & 1 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ \hline & & & & & & & \end{array} \right]$$

where  $G_1$  has  $k - 1$  rows and  $N(k, d) - d$  columns. Show that  $G_1$  has rank  $k - 1$  and suppose  $G_1$  generates a code  $C_1$  of minimum distance  $d_1$ . Use the property that if  $(u, v) \in C$ , where  $v \in C_1$ , then  $(\bar{u}, v) \in C$  to show that  $2d_1 \geq d$ .]

- Show, by iterating this bound, that

$$N(k, d) \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil.$$

This bound is the *Griesmer bound*.