

**Written Problems:** Do four of the following problems.

1. A *maximum a posteriori decoder* (MAPD) for a code  $C$  with respect to a channel  $S$  is defined as follows:  $D_{\text{MAPD}} : \Phi^n \rightarrow C$ , where  $D_{\text{MAPD}}(y)$  is the codeword  $c$  that maximizes the probability  $\Pr\{c \text{ is transmitted} \mid y \text{ is received}\}$ . To compute this probability, we need to know the *a priori* probability of transmitting  $c$ . Suppose that  $C$  is an  $(n, M)$  code over  $F^n$  (for some finite alphabet  $F$  of size  $q$ ), each codeword of  $C$  is equally likely to be transmitted and  $S$  is a memoryless channel. Prove that  $D_{\text{MLD}}$  and  $D_{\text{MAPD}}$  are equivalent; that is, that  $D_{\text{MLD}}(y) = D_{\text{MAPD}}(y)$  for all received  $y$  in  $\Phi^n$ . (*Hint:*  $\Pr\{A \mid B\} = \Pr\{A \cap B\} / \Pr\{B\}$ .)
2. In the  $q$ -ary symmetric channel with crossover probability  $p$ , the input and output alphabets are the same: an alphabet  $F$  of size  $q$ . Each symbol transmitted has a probability  $p$  of error, independent of the other transmitted symbols. If a transmission has an error, then each of the other  $q - 1$  symbols are equally likely to replace the original symbol. Suppose that an  $(n, M, d)$  code is transmitted over the  $q$ -ary symmetric channel. Prove that the nearest-neighbor decoder and the maximum likelihood decoder are equivalent for appropriate values of  $q$  and  $p$  (in class, we saw that this was true for  $q = 2$  when  $p < 1/2$ ).
3. Let  $C$  be a  $(7, 16)$  code over  $F = \{0, 1\}$  such that every word in  $F^7$  is at Hamming distance at most 1 from exactly one codeword of  $C$ . A codeword of  $C$  is transmitted over a binary symmetric channel with crossover probability  $p = 10^{-2}$ .
  - (a) Compute the rate of  $C$ .
  - (b) Show that the minimum distance of  $C$  equals 3.
  - (c) What is the probability of having more than one error in the received word?
  - (d) A nearest-neighbor decoder  $D$  is applied to the received words. Compute the decoding error probability  $P_{\text{err}}$  of  $D$ .
  - (e) Compare the value of  $P_{\text{err}}$  to the error probability when no coding is used: compute the probability of having at least one bit in error when an (uncoded) word of four bits is transmitted through the given BSC.
4. Let  $C$  be a linear  $[n, k, d]$  code over  $\mathbb{F}_q$ .
  - (a) Show that the number of distinct generator matrices of  $C$  is equal to the number of  $k \times k$  invertible matrices over  $\mathbb{F}_q$ .
  - (b) Show that the number of distinct generator matrices of  $C$  is  $\prod_{i=0}^{k-1} (q^k - q^i)$ . (*Hint:* Construct  $k \times k$  invertible matrices one row at a time.)
5. *Plotkin bound for linear codes.*
  - (a) Let  $(a_1, \dots, a_k) \in \mathbb{F}_q^k$  be a nonzero vector, and let  $g : \mathbb{F}_q^k \rightarrow \mathbb{F}_q$  be defined by  $g(x_1, \dots, x_k) = \sum_{i=1}^k a_i x_i$ . Show that each element of  $\mathbb{F}_q$  is the image under  $g$  of exactly  $q^{k-1}$  vectors in  $\mathbb{F}_q^k$ .
  - (b) Let  $C$  be a linear  $[n, k, d]$  code over  $\mathbb{F}_q$ , and let  $T$  be a  $q^k \times n$  array whose rows are the codewords of  $C$ . Show that each element of  $\mathbb{F}_q$  appears in every nonzero column in  $T$  exactly  $q^{k-1}$  times.
  - (c) Show that every linear  $[n, k, d]$  code over  $\mathbb{F}_q$  satisfies

$$d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}.$$

(*Hint:* Show that the average Hamming weight of the  $q^k - 1$  nonzero codewords in the code is at most the right side.)