ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 27 Information Theory and Coding
Homework 11 Dec 5, 2017

PROBLEM 1. Consider appending an overall parity check to the codewords of Hamming code: Each codeword of a Hamming code is extended by 1 bit which is 0 if the codeword contains an even number of 1's and 1 if the codeword contains an odd number of 1's. For example, for the (7,4,3) Hamming code discussed in class, the codeword 0000000 becomes 00000000, the codeword 1110000 becomes 11100001, the codeword 1111111 becomes 11111111, etc. Show that this new code has minimum distance 4, can correct 1 error, and can detect 2 errors. This class of $(2^m, 2^m - m - 1, 4)$ codes are known as the "extended Hamming codes."

PROBLEM 2.

(a) Show that in a binary linear code, either all codewords contain an even number of 1's or half the codewords contain an odd number of 1's and half an even number.

(b) Let $x_{m,n}$ be the nth digit in the mth codeword of a binary linear code. Show that for any given n, either half or all of the $x_{m,n}$ are zero. If all of the $x_{m,n}$ are zero for a given n, explain how the code could be improved.

(c) Show that the average number of ones per codeword, averaged over all codewords in a linear binary code of blocklength N, can be at most $N/2$.

PROBLEM 3. Show that, if H is the parity-check matrix of a code of length n, then the code has minimum distance d iff every $d-1$ rows of H are linearly independent and some d rows are linearly dependent.

PROBLEM 4. In this problem we will show that there exists a binary linear code which satisfies the Gilbert–Varshamov bound. In order to do so, we will construct a $n \times r$ parity-check matrix H and we will use Problem 3.

(a) We will choose rows of H one-by-one. Suppose i rows are already chosen. Give a combinatorial upper-bound on the number of distinct linear combinations of these i rows taken $d-2$ or fewer at a time.

(b) Provided this number is strictly less than $2^r - 1$, can we choose another row different from these linear combinations, and keep the property that any $d-1$ rows of the new $(i+1) \times r$ matrix are linearly independent?

(c) Conclude that there exists a binary linear code of length n, with at most r parity-check equations and minimum distance at least d, provided

$$1 + \binom{n-1}{1} + \cdots + \binom{n-1}{d-2} < 2^r. \tag{1}$$

(d) Show that there exists a binary linear code with $M = 2^k$ distinct codewords of length n provided $M \sum_{i=0}^{d-2} \binom{n-1}{i} < 2^n$.

PROBLEM 5. The weight of a binary sequence of length N is the number of 1's in the sequence. The Hamming distance between two binary sequences of length N is the weight of their modulo 2 sum. Let $\mathbf{x}_1$ be an arbitrary codeword in a linear binary code of block length N and let $\mathbf{x}_0$ be the all-zero codeword. Show that for each $n \leq N$, the number of codewords at distance n from $\mathbf{x}_1$ is the same as the number of codewords at distance n from $\mathbf{x}_0$.