ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 28 | Information Theory and Coding
Solutions to Homework 11 | Dec. 11, 2017

PROBLEM 1. Let x and x' be two different codewords in the extended Hamming code. Let z and z' be the parts of x and x' that come from the Hamming code (i.e., z is all but the last bit of x, and z' that of x'), and p and p' be the bits appended to z and z' to get x and x'. Since x and x' are different then so are z and z': if $z = z'$ then $p = p'$ and x and x' would have been the same. Thus, $d_H(z, z') \geq 3$ since z and z' are different Hamming codewords. On the other hand, if $d_H(z, z') = 3$, then z and z' must have different parity: if they both had an even number of 1's or both had an odd number of 1's they would have differed in an even number of places and $d_H(z, z')$ would have been an even number. Thus, if $d_H(z, z') = 3$ then $p \neq p'$ and we have $d_H(x, x') = 4$. If $d_H(z, z') \geq 4$ then clearly $d_H(x, x') \geq 4$. We thus see that the minimum distance of the new code is 4.

Consider the following procedure to decode

> Given a sequence y, compare it to all the codewords and find the number of positions in which y differs from them. If there is a unique codeword for which this number is smallest, declare that codeword. If not, declare 'errors were detected'.

If the minimum distance d of a code is an even number, $d = 2j$, then if a sequence y differs from the transmitted codeword x by up to $j - 1$ places, then y will be close to the transmitted codeword than to any other and the decoder will correctly decode x. If however, y differs from x in j places, then no other codeword will be closer to y, but there might be a codeword x' which also differs from y in j places. In such a case the decoder will not be able to correct but detect the errors. In particular, if $d = 4$, then all single errors are corrected and all double errors are detected (may even be corrected).

PROBLEM 2.

(a) Note first that the sum of two even-weight codewords is of even weight, the sum of two odd-weight codewords is of even weight and the sum of an odd-weight codeword with an even-weight codeword is of odd weight.

If the code contains no odd-weight codeword then we are done. Otherwise let x be an odd-weight codeword. Then the mapping $y \mapsto x + y$ is a bijection between even-weight and odd-weight codewords, and we conclude that there must be an equal number of odd-weight and even-weight codewords.

(b) The same proof above applies: either all codewords have a zero at the nth digit, or there is a codeword x with has a 1 in its nth digit. The mapping $y \mapsto x + y$ gives a bijection between codewords who have a zero at the nth digit and codewords which have a 1 at the nth digit. In the first case, when all codewords have a zero at the nth digit, one can improve the code by simply deleting the nth digit from each codeword: no matter what the message is, the same symbol would have been transmitted, giving no additional information.

(c) To find the average number of 1's per codewords, one would find the total number of 1's in all codewords, and divide this sum by the number of codewords. Suppose there are M codewords. Arrange the codewords in rows, and count the total number of 1's by going over columns one by one. Since each column contains at most $M/2$ ones, and there are N columns, the total number of 1's is less than or equal to $MN/2$. Dividing by M we see that the average number of 1's per codeword is at most $N/2$.

PROBLEM 3. Recall that the minimum distance is also given by the weight of the minimum weight codeword. Now observe that there exists a codeword x of weight w iff $xH = 0$ where H is the parity-check matrix with n rows. This is equivalent to saying that some w rows of H are linearly dependent. We then know that there exist d rows that are linearly dependent. However, no combination of $d-1$ rows or less are dependent since this case would give rise to a codeword of weight less or equal to $d-1$. This concludes the proof.

PROBLEM 4.

(a) At the first step, we can choose any non-zero column vector with r coordinates. This will be the first row of our $n \times r$ parity-check matrix. Now suppose we have chosen i rows so that no $d-1$ are linearly dependent. They are all non-zero rows. There are at most

$$\binom{i}{1} + \cdots + \binom{i}{d-2}$$

distinct linear combinations of these i rows taken $d-2$ or fewer at a time.

(b) The total number of r-tuples (include the all-zero one) is 2^r. We can then choose a new row different from the previous ones, linearly independent from the previous ones, and keep the property that every $d-1$ rows are independent.

(c) We can iterate the procedure and we keep doing so as long as

$$1 + \binom{i}{1} + \cdots \binom{i}{d-2} < 2^r$$

where the first term counts the all-zero vector. At the last step, we can do so iff

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

(d) Multiply both sides of the previous inequality by $M = 2^k$ gives the result since $r = n - k$.

PROBLEM 5. Let S_0 be the set of codewords at Hamming distance n from $\mathbf{x}_0$ and S_1 be the set of codewords at Hamming distance n from $\mathbf{x}_1$. For each $\mathbf{y}$ in S_0, note that $\mathbf{x}_1 + \mathbf{y}$ is at distance n from $\mathbf{x}_1$, and thus $\{\mathbf{x}_1 + \mathbf{y} : \mathbf{y} \in S_0\} \subset S_1$. Similarly, $\{\mathbf{x}_1 + \mathbf{y} : \mathbf{y} \in S_1\} \subset S_0$. These two relationships yield $|S_0| \leq |S_1|$ and $|S_1| \leq |S_0|$, leading to the conclusion that $|S_0| = |S_1|$.