ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

Handout 25 | Information Theory and Coding
Solution 11 | December 7, 2010, SG1 – 15:15-17:00

Problem 1. (a) Let C be the set of all the codewords and assume that there is a codeword $x \in C$ such that the i-th bit of x is 1. Let C_0 and C_1 be the set of all the codewords which have 0 and 1 in the i-th position respectively. It is easy to see that $C_0 = x + C_1$ and the proof follows.

(b) Let G be the generator matrix of the code which has size $n \times k$. For $1 \leq i \leq n$, since the i-th row of G is non-zero, then there is a $u \in \{0,1\}^k$ such that $x = Gu$ is non-zeros at the i-th position and thus by part (a) half the codewords have 1 in the i-th position and half have 0.

(c) This follows easily from part (a).

Problem 2. (a) The number of n-dimensional vectors of weight at most e is equal to $\sum_{i=0}^{e} \binom{n}{i}$. Denote the set of all such vectors by E. For $y \in H$, if the decoder receives $x + y$, then it should decide that x was sent.

(b) Let the set of all the codewords be denoted by C and for $x \in C$ let S_x be the set of all the n-dimensional vectors that are decoded to x at the decoder. Clearly for two distinct codewords $x, y \in C$, S_x and S_y are disjoint. We have

$$| \cup_{x \in C} S_x| = \sum_{x \in C} |S_x| \geq M \sum_{i=0}^{e} \binom{n}{i}.$$

And on the other hand $| \cup_{x \in C} S_x||$ is at most 2^n (the number of all the n-dimensional vectors).

Problem 3. (a) Let G_i be the matrix made by removing the last $n - i$ columns of G (define $G_0 = 0$ and G_0 consider it to be full rank). We have

$$\mathbb{P}(G_i \text{ is full rank } | G_{i-1} \text{ is full rank }) = 1 - \frac{1}{2^{n-i-1}},$$

for $0 \leq i \leq k - 1$. This is because assuming G_{i-1} is full rank, G_i is full rank only if its i-th row is not contained in the row space of G_{i-1} which has 2^{i-1} elements (since G_{i-1} is full rank). The proof now follows by noting that,

$$\mathbb{P}(G_k \text{ is full rank }) = \prod_{i=1}^{k} \mathbb{P}(G_i \text{ is full rank } | G_{i-1} \text{ is full rank }).$$

(b) Let

$$y_\alpha = \prod_{i=1}^{n\alpha - 1} (1 - \frac{1}{2^{n-i}}).$$

Assuming $\alpha < 1$, we have

$$\lim_{n\to\infty} \ln y_\alpha = \lim_{n\to\infty} \sum_{i=0}^{n\alpha-1} \ln(1 - \frac{1}{2^{n-i}})$$
$$= \lim_{n\to\infty} \sum_{i=0}^{n\alpha-1} \frac{1}{2^{n-i}}$$
$$= 0.$$

Thus $\lim_{n\to\infty} y_\alpha = 1$ and with high probability G is full rank which means that the rate of the linear code based on G is $\frac{k}{n} = \alpha$.

Problem 4. (a) Firstly, observe that

$$\mathbb{P}(x = X(u)|G) = \mathbb{P}(v = x + uG|G) = 2^{-n}.$$

and the rest follows from the law of total probability.

(b) We have

$$\mathbb{P}(x = X(u), x' = X(u')) = \mathbb{P}(x = X(u)|x' = X(u'))\mathbb{P}(x' = X(u')),$$

and by using part (a),

$$\mathbb{P}(x = X(u), x' = X(u')) = \mathbb{P}(x = X(u)|x' = X(u'))2^{-n}.$$

As a result, it remains to show that

$$\mathbb{P}(x = X(u)|x' = X(u')) = 2^{-n}.$$

We have

$$\mathbb{P}(x = X(u)|x' = X(u')) = \mathbb{P}((u + u')G = x + x').$$

Now, let I be the set of indices of which the vector $u + u'$ is not zero (since u and u' are distinct, I is non-empty). Assuming $g_1, \cdots, g_k$ are the rows of G, we have

$$\mathbb{P}(x = X(u)|x' = X(u')) = \mathbb{P}(\sum_{i\in I} g_i = x + x').$$

Now the rest follows from the fact that since the vector $\sum_{i\in I} g_i$ is again a vector whose elements are i.i.d and $\{0, 1\}$ valued with uniform probability, the above probability is 2^{-n}.

(c) Recall the random coding proof of the fact that there exist codes which achieve capacity: In that proof, one generated M codewords $X(1), \cdots, X(M)$, each picked independently according to the distribution $p(x) = p(x_1)\cdots p(x_n)$, and p is chosen to maximize the mutual information (which is uniform here). The proof then proceeded to analyze the probability of error by assuming that $X(m)$ is the transmitted sequence, Y the received sequence and bounding the probability that for $m' \neq m$, the pair $(X(m'), Y)$ is jointly typical. What made the proof work was that for any m and $m' \neq m$, the codewords $X(m)$ and $X(m')$ were chosen independently; i.e., that the codewords were pairwise independent. The full independence of the M codewords was not necessary in the proof. Here we also have the pair-wise independence property (part (b)) as well so the proof follows similarly.