# ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

School of Computer and Communication Sciences

**Handout 24** Introduction to Communication Systems
Homework 11 December 7, 2010, SG1 – 15:15-17:00

---

**Problem 1.** (a) Consider a binary linear code with blocklength $n$. That is, each codeword is sequence of $n$ bits. Also consider the bit in the $i$-th position ($1 \leq i \leq n$). Show that either all codewords contain a 0 in the $i$-th position or half the codewords contain a 0 and half contain 1.

(b) Use part (a) to show that a linear code with a generator matrix with no zero columns imposes a linear input distribution.

(c) Show that for a binary linear code of blocklength $n$, the average number of ones per code word, averaged over all codewords can be at most $\frac{n}{2}$.

**Problem 2.** Consider a binary block code with $M$ codewords and blocklength $n$. That is, each codeword is sequence of $n$ bits. Suppose this code can correct up to (and including) $e$ errors.

(a) For a codeword $x$ consider the set $S$ of all binary sequences for which the decoder decides $x$. Show that

$$|S| \geq \sum_{i=0}^{e} \binom{n}{i}$$

(b) Show that the number of codewords M satisfies

$$M \leq \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}$$

This is known as the sphere packing bound.

**Problem 3.** Consider a binary linear code with a $k \times n$ generator matrix $G$ which is randomly generated as follows: each of the $k \times n$ elements of $G$ are either 0 or 1 with independent probability $\frac{1}{2}$.

(a) Prove that $\mathbb{P}(G \text{ is full-rank}) = \prod_{i=0}^{k-1}(1 - \frac{1}{2^{n-i}})$.

(b) Deduce that assuming $k = n\alpha$ where $\alpha < 1$, then with high probability the rate of the binary linear code with generator matrix $G$ chosen randomly as above, has rate equal to $\alpha$.

**Problem 4.** In this problem we aim to prove that random linear codes achieve the capacity of Binary Memoryless Symmetric (BMS) channels. The proof is quiet similar to the proof of the channel coding theorem done in the class. However there are several important steps to be justified. Let $W$ be a BMS channel. Recall that the uniform input distribution achieves the capacity of $W$ which we denote by $I(W)$. Assume the message we want to send is a binary $k$ dimensional vector denoted by $u$ and the encoding is done by using a $k \times n$ binary generator matrix $G$ (linear coding). So the codewords corresponding to $u$, denoted by $X(u)$ is $X(u) = uG$. For a given $\epsilon > 0$ our objective is to prove that as $n \to \infty$ there exits at least one $k \times n$ binary generator matrix $G$ that under jointly typical decoding, the error probability is less than $\epsilon$. For this, we assume that the each element of $G$ is chosen

to be 0 or 1 with independent probability $\frac{1}{2}$ and we ask you to show through the following steps that as long as the rate is less than $I(W)$, the average probability of error over this uniform choice of $G$ falls below $\epsilon$ as $n \to \infty$. For simplicity, we consider a slightly different but equivalent model here: assuming $G$ is randomly generated as above, the codewords are constructed by $X(u) = uG + v$, where $v$ is also a random vector whose elements are either 0 or 1 with independent probability $\frac{1}{2}$. The new model is equivalent to the old one since at the decoder we van subtract the vector $v$ from the received vector and proceed in the same manner (this follows from the BMS property of the channel). In the following consider the new model. Note that the randomness here is over the choice of $G$ as well as the choice of $v$.

(a) Let $u$ and $x$ be binary $k$ and $n$ dimensional vectors respectively. Prove that $\mathbb{P}(x = X(u)) = 2^{-n}$.

(b) Let $u$ and $u'$ be two distinct binary $k$ dimensional vectors. Also let $x$ and $x'$ be two binary $n$ dimensional vector. Prove that $\mathbb{P}(x = X(u), x' = X(u')) = 2^{-2n}$ and use part (a) to deduce that the two events are independent.

(c) Now try to use the above steps and the proof of the channel coding theorem explained in class to prove that for $\epsilon > 0$ and as long as the rate is less than $I(W)$, the average probability of error over the uniform choice of $G$ is less than $\epsilon$ for large enough $n$.