Quantum info in TCS
Lecture 6: Coding over quantum channel

Suppose a quantum channel $\mathcal{N}_{A\to B}$ is connected Alice to Bob. Alice wants to transmit "information" to Bob over this channel. The information Alice can transmit can be either classical or quantum.

1 Sending classical information over classical channels

Consider a *classical* channel where Alice sends $x \in \{0,1\}$ and Bob receives $x \oplus z$ where z is Bernoulli(p).

Multiple independent use of channel With one use of the channel, Alice cannot do anything non-trivial. So we consider n independent uses of the channel. Alice has m bits and encode it into a binary string of n bits and transmits it over the channel. Bob receives the noisy version and attempts to recover the original m bits

Repetition code As an example, suppose Alice has one bit $b \in \{0,1\}$. She encodes this into n bits by repetition and transmits it over the channel. Bob does majority voting for decoding. If more than half of the received bits are 1 he decodes the bit as one, otherwise as zero.

Rate vs probability of error There are two important parameters of every code.

1. **Rate**: it is the number of bits transmitted per channel use, i.e., m/n. For repetition code, the rate is $1/n$.
2. **Probability of error:** It is the probability that Bob cannot decode *any* transmitted bits. For repetition code, it is $\sum_{i=0}^{(n-1)/2}(1-p)^{n-i}p^i$, which converges to zero if $p < \frac{1}{2}$.

Formal definition of a code Fix the number of bits to be transmitted m and the number of channel uses n. The code consists of two functions $f : \{0,1\}^m \to \{0,1\}^n$ for encoding and $g : \{0,1\}^n \to \{0,1\}^m$ for decoding. Alice encodes m bits $b_1, \cdots, b_m$ into a codeword of length n using $x = f(b_1, \cdots, b_m)$ and transmits x over n uses of the channel. Bob receives y at the output of the channel and decodes the bits as $\hat{b}_1, \cdots, \hat{b}_m = g(y)$.

Shannon channel coding

Theorem 1.1. *There exists a sequence of codes $(f_n, g_n)_{n\geq 1}$ such that the probability of error goes to zero and the rate is converging to $1 - h_2(p)$.*

Here $h_2(x) := -x\log(x) - (1-x)\log(1-x)$ is the binary entropy function. A few remarks about channel coding:

1. $1 - h_2(p) = I(X : Y)$ where X is uniformly distributed bit and Y is the output of the channel when X is transmitted.
2. The optimal decoder for BSC is minimum distance decoder. It is not computationally efficient
3. We can generalize this theorem to any channel.

Random coding A code is characterized by the set of all codewords. We consider a random code where all codewords are chosen independently at random. Let $x(1), \cdots, x(2^{nR}) \in \{0,1\}^n$ be the random codewords for $R = 1 - h_2(p) - \delta$ for a fixed $\delta > 0$. The decoder works as follows. Fix $\epsilon > 0$. If there is a unique i such that $|x(i) \oplus y|$[1] is between $(1-\epsilon)np$ and $(1+\epsilon)np$ then the decoded value would be i. Otherwise, the decoder output 1. To analyze the probability of error, assume that the codeword $x(1)$ is transmitted over the channel. Then, by law of large number $|x(1) \oplus y|$ is between $(1-\epsilon)np$ and $(1+\epsilon)np$ with high probability. We need to show that with high probability there is not $i \neq 1$ such that $|x(i) \oplus y|$ is between $(1-\epsilon)np$ and $(1+\epsilon)np$. By union bound, we have

$$\Pr[\exists i \neq 1 : (1-\epsilon)np < |x(i) \oplus y| < (1+\epsilon)np] \leq \sum_{i=2}^{2nR} \Pr[(1-\epsilon)np < |x(i) \oplus y| < (1+\epsilon)np] \quad (1)$$

$$= (2^{nR} - 1)\Pr[(1-\epsilon)np < |x(2) \oplus y| < (1+\epsilon)np] \quad (2)$$

Note that $x(2) \oplus y$ has uniform distribution. Therefore,

$$\Pr[(1-\epsilon)np < |x(2) \oplus y| < (1+\epsilon)np] = \frac{\#\{x : (1-\epsilon)np \leq |x| \leq (1+\epsilon)np\}}{2^n} \approx 2^{-n(1-h_2(p))} \quad (3)$$

By our choice of R, the second type of probability of error goes to zero as well.

[1] $|x|$ is the number of 1 in a binary string x