

CS222: Homework 4. Due January 9

Note: in the assignment, you may wish to recall the following Chernoff bound: Let $Y = X_1 + X_2 \dots + X_n$ be the sum of n independent 0/1 random variables with $E[Y] = \mu$. Then for $\epsilon < 1$,

$$\Pr(|Y - \mu| > \epsilon\mu) < 2e^{-\epsilon^2\mu/3}.$$

1. Alice wants to send Bob the result X of a fair coin flip over a binary symmetric channel that flips each bit with probability $0 < p < 1/2$. To avoid errors in transmission, she encodes heads as a sequence of $2k + 1$ zeroes and tails as a sequence of $2k + 1$ ones.

- A. Consider the case where $k = 1$, so heads is encoded as 000 and tails as 111. For each of the eight possible sequences of three bits that can be received, determine the probability that X was heads conditioned on Bob receiving that sequence.
- B. Argue that for general k , Bob minimizes the probability of error by deciding that X was heads if at least $k + 1$ of the bits are 0. (For partial credit, just prove this for $k = 1$.)
- C. Give a formula for the probability that Bob makes an error that holds for general k and $p < 1/2$. Evaluate the formula for $p = 0.1$ and k ranging from 1 to 6.
- D. Give a bound on the probability that Bob makes an error that holds for general k and $p < 1/2$ using Chernoff bounds.

2. Consider the following channel: the sender can send a symbol from the set $\{0, 1, 2, 3, 4\}$. The channel introduces errors; when the symbol j is sent, the receiver receives $j + 1 \pmod 5$ with probability $1/2$, and receives $j - 1 \pmod 5$ with probability $1/2$. The errors are mutually independent when multiple symbols are sent.

We can define (k, n) encoding and decoding functions for this channel. The encoding function En maps numbers from $\{0, \dots, k - 1\}$ into sequences from $\{0, 1, 2, 3, 4\}^n$, and the decoding function De maps sequences from $\{0, 1, 2, 3, 4\}^n$ into a number in $\{0, \dots, k - 1\}$.

There are $(2, 1)$ encoding and decoding functions with zero probability of error. The encoding function maps 0 to 0 and 1 to 1. When a 0 is sent, the receiver will receive either a 1 or 4, so the decoding function maps 1 and 4 back to 0. When a 1 is sent, the receiver will receive either a 2 or 0, so the decoding function maps 2 and 0 back to 1. This guarantees that no error is made. Hence at least one bit can be sent without error per channel use.

- A. Show that there are $(5, 2)$ encoding and decoding functions with zero probability of error. Argue that this means that on average more than one bit of information can be sent per use of the channel.
- B. Show that if there are (k, n) encoding and decoding functions with zero probability of error, then $n \geq \log k / (\log_2 5 - 1)$.

3. I have encoded a message using Reed-Solomon codes. My encoding works as follows. Each letter corresponds to a number: a to 1, b to 2, etc. To simplify matters, I do all work modulo 29, which is prime. My message is a four-letter word, and I used the four letters as the coefficients of a polynomial. (If my word was "aaaa", my polynomial would be $1 + x + x^2 + x^3$.) Below I provide the values $P(1), \dots, P(6)$, at most one of which is in error. Determine the message.

$$P(1) = 15, P(2) = 13, P(3) = 22, P(4) = 24, P(5) = 1, P(6) = 22.$$

4. Recall the decoding algorithm for Tornado codes on a bipartite graph: find a check node on the right for which only neighboring message node message node on the left is missing; solve for that message node; and repeat. Prove that the the order in which you recover the message nodes does not matter. That is, regardless of what order you handle the message nodes, at the end you will always recover the same set of message nodes.

5. 15 prisoners are offered the following deal to secure their release. Each of their foreheads will be marked with either a black or white mark, each independently with probability $1/2$ for all prisoners. This will be done so that each person can see the mark on everyone else's foreheads, but not their own. They will be asked to either write down a guess about the color of the mark on their own forehead, or abstain. The prisoners cannot communicate with each other in any way, and in particular they cannot see what other people have guessed or if others have abstained. The prisoners will all be released if at least one person correctly guesses the color on their forehead and nobody guesses a color incorrectly. That is, at least one person must not abstain, and everyone who fails to abstain must answer correctly.

The players can decide their strategy before the day of marking. Suggest a strategy should they use to maximize their probability of being released? (Note: the bigger the probability, the better the credit you get.)

(Hint 1: you better try to come up with something that is right better than $1/2$ of the time! Think of the case of 3 players first, and then 7. This problem does actually relate to error-correcting codes in a subtle way. Why 3, 7, and 15?)

(Hint 2, from Adam: Consider any strategy for the players. Think of an assignment of black/white marks to the players' foreheads as a string in $\{0,1\}^{15}$, and let W and L denote the sets of assignments that correspond to a win or loss for the players, respectively. Note that a player's action under the strategy cannot depend on the mark on his/her forehead. How does this fact allow us to upper bound $|W|$ in terms of $|L|$? Then figure out how to choose W and L so that this bound would be tight if there were actually a strategy where the sets of assignments corresponding to wins and losses were given by your choices for W and L . (Think about the coding theory lectures here.) Finally, try to find a strategy for the players for which the sets of assignments corresponding to wins and losses match your choices for W and L .)

6. Give a Shannon-style proof of that the capacity of the binary erasure channel (each bit is erased with probability p) is at least $1 - p - \epsilon$ for any $\epsilon > 0$. Specifically, show that if one chooses $2^{(1-p-\epsilon)n}$ random codewords and one is sent uniformly at random over the erasure channel, the probability of error can be made less than ϵ for n sufficiently large. You should follow as much as possible the notes for the binary symmetric error channel.

Now suppose that after each time a bit was sent, there was *feedback*, so that both the receiver and the sender knew whether the bit was successfully received or not. Explain how to achieve, on average, sending 1 bit of information on average for every $1/(1-p)$ transmission with feedback, and why no more can be achieved. Explain why this means that feedback does not help (meaningfully) in this setting.