Carnegie Mellon University Instructor: Venkatesan Guruswami
15-859Y: Coding Theory Term: Fall 2014

PROBLEM SET 1
Due by Monday, September 29

INSTRUCTIONS

- You are allowed to collaborate with up to two other students taking the class in solving problem sets. But here are some rules concerning such collaboration:

  1. You should think about each problem by yourself for at least 30 minutes before commencing any collaboration.
  2. Collaboration is defined as discussion of the lecture material and solution approaches to the problems. Please note that *you are not allowed to share any written material and you must write up solutions on your own*. You must clearly acknowledge your collaborator(s) in the write-up of your solutions.
  3. Of course, if you prefer, you can also work alone (see the last bullet item for some “credit” for doing so).

- Solutions typeset in LaTeX are encouraged.
- You should not search for solutions on the web. More generally, you should try and solve the problems without consulting any reference material other than the course notes and what we cover in class. If for some reason you feel the need to consult some source, *please acknowledge the source* and try to articulate the difficulty you couldn’t overcome before consulting the source and how it helped you overcome that difficulty. Alternatively, before turning to any such material, we encourage you to ask the instructor for hints or clarifications.
- Please start work on the problem set early. The problem set has **six** problems and is worth a total of 100 points. As a rough estimate, scoring around 85% of the points, or 75% of the points if you work by yourself, might correspond to an A level performance on this problem set.

---

1. (15 points) There are n people in a room, each of whom is given a black/white hat chosen uniformly at random (and independent of the choices of all other people). Each person can see the hat color of all other people, but not their own. Each person is asked if (s)he wishes to guess their own hat color. They can either guess, or abstain. Each person makes their choice without knowledge of what the other people are doing. They either win collectively, or lose collectively. They win if all the people who don’t abstain guess their hat color correctly *and* at least one person does not abstain. They lose if all people abstain, or if some person guesses their color incorrectly. It is trivial for the n people to win the game with probability at least $\frac{1}{2}$. Your goal below is to come up with a strategy that will allow the n people to win with optimal probability (when $n+1$ is a power of 2).

   (a) Lets say that a directed graph G is a subgraph of the n-dimensional hypercube if its vertex set is $\{0,1\}^n$ and if $u \to v$ is an edge in G, then u and v differ in at most one coordinate. Let $K(G)$ be the number of vertices of G with in-degree at least one, and out-degree zero. Show that the probability of winning the hat problem equals the maximum, over directed subgraphs G of the n-dimensional hypercube, of $K(G)/2^n$.

   (b) Using the fact that the out-degree of any vertex is at most n, show that $K(G)/2^n$ is at most $\frac{n}{n+1}$ for any directed subgraph G of the n-dimensional hypercube.

   (c) Show that if $n = 2^r - 1$, then there exists a directed subgraph G of the n-dimensional hypercube with $K(G)/2^n = \frac{n}{n+1}$.

2. ($1 + 2 + 3 + 4 + 5 = 15$ points) In this problem you will need to come up with some ways of constructing new codes from existing ones, and prove the following statements (recall that $[n, k, d]_q$ stands for an length n *linear code* over $\mathbb{F}_q$ of dimension k):

   (a) If there exists an $[n, k, d]_q$ code ($d \geq 2$), then there also exists an $[n-1, k, d' \geq d-1]_q$ code.

   (b) If there exists an $[n, k, d]_2$ code with d odd, then there also exists an $[n+1, k, d+1]_2$ code.

   (c) If there exists an $[n, k, d]_q$ code, then there also exists an $[n-d, k-1, d' \geq \lceil d/q \rceil]_q$ code. (Hint: Drop the d positions corresponding to the support of a minimum weight codeword.)

   (d) If there exists an $[n, k_1, d_1]_q$ code and an $[n, k_2, d_2]_q$ code, then there also exists a $[2n, k_1 + k_2, \min(2d_1, d_2)]_q$ code.

   (e) If there exists an $[n, k, d]_2$ code ($0 < d < n/2$), then for every $m \geq 1$, there also exists an $\left[n^m, k, \frac{n^m-(n-2d)^m}{2}\right]_2$ code.
   (Hint: Given an $n \times k$ generator matrix G for the code, consider the $n^m \times k$ generator matrix whose $(i_1, i_2, \ldots, i_m)$'th row is the sum of rows $i_1, i_2, \ldots, i_m$ of G. It is also more slick to use a ± 1 notation for binary alphabet via the translation $b \mapsto (-1)^b$ from $\{0, 1\}$ to $\{1, -1\}$, and track the bias $\mathbf{E}_{i \in \{1,\ldots,N\}}[x_i]$ of a string $x \in \{-1, 1\}^N$ as a proxy for its relative Hamming weight.)

3. (15 points) Let C_1 be an $[n_1, k_1, d_1]_2$ binary linear code, and C_2 an $[n_2, k_2, d_2]$ binary linear code. Let $C \subseteq \mathbb{F}_2^{n_1 \times n_2}$ be the subset of $n_1 \times n_2$ matrices whose columns belong to C_1 and whose rows belong to C_2 (view elements of C as binary vectors of length $n_1 n_2$ in some canonical way).

   Prove that C is an $[n_1 n_2, k_1 k_2, d_1 d_2]_2$ binary linear code.

4. ($3 + 7 + 5 + 10 = 25$ points) For $\tau \in [0, 1/2]$, define a binary code C of block length n to be τ-*covering* if every $\mathbf{r} \in \{0, 1\}^n$ is within Hamming distance τn from some codeword of C.

   (a) Prove that the rate of a τ-covering code must be at least $1 - h(\tau)$.

   (b) Prove that a random binary code of size $n^3 \cdot 2^{(1-h(\tau))n}$ is τ-covering with probability $1 - 2^{-\Omega(n)}$, thereby concluding the existence of τ-covering codes of rate $1 - h(\tau) + o(1)$.

   (c) Prove the following characterization for when a binary linear code is τ-covering:
   If H is a parity check matrix for an $[n, k]_2$ linear code C, then C is τ-covering if and only if for every $\mathrm{s} \in \mathbb{F}_2^{n-k}$, there is a set of at most τn columns of H which sum up to s (over $\mathbb{F}_2$).

   (d) Prove that there exist τ-covering binary **linear** codes C of rate $1 - h(\tau) + o(1)$.
   (Hint: (a) First prove that a random linear code of rate $1-h(\tau)+o(1)$ τ-covers *most* of the points in $\mathbb{F}_2^n$. This step will rely on pairwise independence of the nonzero codewords in a random linear code, and Chebyshev's tail inequality. (b) Then prove that some $O(\log n)$ translates (cosets) of such a linear code suffice to τ-cover the whole space.)

5. (15 points) A set of vectors $S \subseteq \mathbb{F}_q^n$ is called t-wise independent if for every set of positions I with $|I| = t$, the set S projected to I has each of the vectors in $\mathbb{F}_q^t$ appear the same number of times. (In other words, if one picks a vector $(s_1, \ldots, s_n)$ from S at random then any of the t random variables are uniformly and independently random over $\mathbb{F}_q$).

   Prove that any linear code C whose dual $C^\perp$ has distance $d^\perp$ is $(d^\perp - 1)$-wise independent.

6. (15 points) Let C be $[n,k]_2$ linear code with w_j denoting the number of codewords of C of Hamming weight j, for $0 \leq j \leq n$. (So $w_0 = 1$ and $\sum_{j=0}^{n} w_j = 2^k$.) Let $W(X) = \sum_{j=0}^{n} w_j X^j$ be the weight-enumerator polynomial of C.

   Suppose C is used for transmission on a discrete memoryless channel $(\mathcal{X} = \{0,1\}, \mathcal{Y}, \Pi)$ with maximum likelihood decoding at the receiver. That is, if $\mathbf{y} \in \mathcal{Y}^n$ is received, the decoding rule outputs a codeword $\mathbf{c} \in C$ for which $p(\mathbf{y}|\mathbf{c}) = \prod_{i=1}^{n} \Pi(y_i|c_i)$ is maximum.

   Prove that regardless of which codeword was transmitted, the resulting error probability P_{err} is at most $P_{\text{err}} \leq W(\zeta) - 1$ where $\zeta = \sum_{y \in \mathcal{Y}} \sqrt{\Pi(y|0)\Pi(y|1)}$.

   For BSC_p, using $\zeta = \sqrt{4p(1-p)}$ and the above bound on P_{err}, conclude the existence of linear codes of positive rate and exponentially small error probability for communication on the BSC_p for every fixed $p < 1/2$.