15-859V: Introduction to coding theory — Spring 2010
Carnegie Mellon University — V. Guruswami

PROBLEM SET 1
Due by Wednesday, February 17

INSTRUCTIONS

- Problem sets can be turned in groups of two people; i.e., a single write-up for each two person team suffices. You can form different groups for different problem sets. In fact this is encouraged so that you interact with several students from the class. 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 strongly preferred.
- You are *strongly urged* to 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 (such as a textbook or sources on the web), *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 consulting any such material, I'd encourage you to ask me for a hint, preferably by posting a comment on the blog post dedicated to this problem set, so all students can take advantage of any hints.
- Please use the comments section of the blog also to ask for any clarifications or questions about the problems.
- 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 $3/4$'th of the points, or $2/3$'rd of the points if you turn in solutions solo, suffices for an A on this problem set.

---

1. ($6 + 6 = 12$ points) Exercise 5 from Notes 1 (giving example of self-dual codes) and Exercise 2 from Notes 2 (Varshamov's improved bound for linear codes).

2. ($8 + 5 = 13$ points) For integers n, d, w, with $d \leq 2w \leq n$, let $A(n, d, w)$ be the largest possible size of a subset $S \subseteq \{\mathbf{x} \in \{0,1\}^n \mid \mathrm{wt}(\mathbf{x}) = w\}$ such that for every $\mathbf{x} \neq \mathbf{y} \in S$, the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is at least d.

   (a) Prove that $A(n, d) \leq \frac{2^n A(n,d,w)}{\binom{n}{w}}$.

   (b) Show that
   $$A(n, d, w) \geq \frac{\binom{n}{w}}{\sum_{j=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{w}{j}\binom{n-w}{j}} .$$

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.

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

4. ($5 + 8 + 5 + 12 = 30$ 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 $n^3 \cdot 2^{n-h(\tau)n}$ is τ-covering with probability $1 - 2^{-\Omega(n)}$. Conclude 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 $\mathbf{s} \in \mathbb{F}_2^{n-k}$, there is a set of at most τn columns of H which sum up to $\mathbf{s}$ (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) Suppose $\mathcal{F}$ is a non-empty collection of $[n, k]_2$ binary linear codes such that every nonzero element of $\mathbb{F}_2^n$ belongs to the same number of codes in $\mathcal{F}$.
Prove that for large enough n there are codes in this collection that asymptotically meet the Gilbert-Varshamov bound, i.e., their relative distance is at least $h^{-1}(1 - k/n) - o(1)$.

(b) This problem uses the algebra of the extension field $\mathbb{F}_{2^m}$. This field is isomorphic to the quotient $\mathbb{F}_2[X]/(h(X))$ where $h \in \mathbb{F}_2[X]$ is any polynomial of degree m that is irreducible over $\mathbb{F}_2$. For the problem, you do not need to do anything about $\mathbb{F}_{2^m}$ besides the field axioms and the fact that $\mathbb{F}_{2^m}$ also has the structure of a vector space of dimension m: i.e., there is there is a bijection $\sigma : \mathbb{F}_{2^m} \to \mathbb{F}_2^m$ such that $\sigma(x + y) = \sigma(x) + \sigma(y)$ for all $x, y \in \mathbb{F}_{2^m}$.

i. For $\alpha \in \mathbb{F}_{2^m}$, $\alpha \neq 0$, consider the map $L_\alpha : \mathbb{F}_2^m \to \mathbb{F}_2^{2m}$ defined as

$$L_\alpha(\mathbf{x}) = (\mathbf{x}, \sigma(\alpha \cdot \sigma^{-1}(\mathbf{x}))$$

where $\cdot$ denotes multiplication in the field $\mathbb{F}_{2^m}$.
Prove that L_α defines the encoding of a $[2m, m]_2$ binary linear code (call it C_α).

ii. Prove that there exists $\alpha \neq 0$ such that C_α asymptotically meets the Gilbert-Varshamov bound, i.e., has relative distance $h^{-1}(1/2) - o_m(1)$.

(c) (**Extra credit;** For fun/brownie points only!) By counting the total number of self-dual codes and the number of self-dual codes containing any even weight vector other than the all 0's or all 1's vector, and using Part (5a), conclude that there exist self-dual codes of relative distance $h^{-1}(1/2) - o(1) \approx 0.11$. To compare, what was the relative distance of the self-dual codes you constructed in Problem 1?

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 $p < 1/2$.