Essential Coding Theory — Madhu Sudan
CS 229r - Spring 2017
Due: Wednesday, February 22, 2017

Problem Set 2

Instructions

Collaboration: Collaboration is allowed and encouraged, but you must write everything up by yourselves. You must list all your collaborators.

References: Consulting references is OK. However, in general, try not to run to reference material to answer questions. Try to think about the problem to see if you can solve it without consulting *any* external sources. If this fails, you may look up any reference material. Cite all references (in addition to listing all collaborators). Explain why you needed to consult any of the references, if you did consult any.

"Not to be turned in" Problems . If a problem is marked "not to be turned in", you don't have to. But you must include a statement saying you know how to solve the problem. If you are unsure, write up your solution and turn it in. These problems won't count for your grades, but are good review exercises.

Submission: Submit your solutions on Canvas. If you do not have a canvas account, or are not taking this course for credit, but want to submit solutions to the psets anyway, please contact me (madhu) right away and I'll try to find a solution for you.

Problems

1. **(Need not be turned in)** (Finite field as vector spaces)
   (a) Let q be a prime power and t be a positive integer and let $\mathbb{F}_{q^t}$ be a field of size q^t. Show that there is a unique copy of $\mathbb{F}_q$ contained in $\mathbb{F}_{q^t}$, i.e., q elements that are closed under addition and multiplication and this form a field. (This allows us to talk about multiplication of an element of $\mathbb{F}_q$ with an element of $\mathbb{F}_{q^t}$ below.)
   (b) Show that there is a bijection $\Phi : \mathbb{F}_{q^t} \to \mathbb{F}_q^t$ that is $\mathbb{F}_q$-linear (i.e., for every $\alpha, \beta \in \mathbb{F}_q \subseteq \mathbb{F}_{q^t}$ and $\gamma, \delta \in \mathbb{F}_{q^t}$ it is the case that $\Phi(\alpha\gamma + \beta\delta) = \alpha\Phi(\gamma) + \beta\Phi(\delta)$).
   (c) Conclude that if $C \subseteq \mathbb{F}_{q^t}^n$ is a linear code over $\mathbb{F}_{q^t}$ then $C \circ \Phi \subseteq \mathbb{F}_q^{tn}$ is a linear code over $\mathbb{F}_q$, where $C \circ \Phi = \{(\Phi(u_1), \ldots, \Phi(u_n)) | (u_1, \ldots, u_n) \in C\}$.
2. (GV bound by Partitioning) Recall that linear codes $C_1, \ldots, C_M \subseteq \{0,1\}^n$ form a *partition* if (i) All codes are of the same size (soe $|C_i| = |C_j|$ for all $i, j \in [M]$); (ii) They cover $\{0,1\}^n$, i.e.,

$\cup_{i\in[M]} C_i = \{0,1\}^n$; and (iii) They have the minimal possible intersection i.e., $C_i \cap C_j = \{0^n\}$ for all $i \neq j$.

(a) Prove that if $C_1, \ldots, C_M$ form a partition, and d is such that $\sum_{i=1}^{d-1} \binom{n}{i} < M$ then there exists $i \in [M]$ such that $\Delta(C_i) \geq d$.

(b) (The Wozencraft ensemble): Let $n = 2t$, and let Φ be linear bijection from $\mathbb{F}_{2^t}$ to $\mathbb{F}_2^t$. For $\alpha \in \mathbb{F}_{2^t}$ let $C_\alpha \subseteq \mathbb{F}_{2^t}^2$ be the code with codewords $\{(\beta, \alpha \cdot \beta) | \beta \in \mathbb{F}_{2^t}\}$ and $\mathbb{F}_\infty = \{(0,\beta) | \beta \in \mathbb{F}_{2^t}\}$. Further, let $\tilde{C}_\alpha = C_\alpha \circ \Phi$. Show that $\{\tilde{C}_\alpha\}_{\alpha \in \mathbb{F}_{2^t} \cup \{\infty\}} \subseteq \{0,1\}^n$ form a partition. Conclude that for infinitely many n there is a code of length n with rate $1/2$ and relative distance approaching $H^{-1}(1/2)$.

(c) Prove that for most α, the code C_α has relative distance approaching $H^{-1}(1/2)$.

(d) Extend Part (b) to get codes of rate $1/\ell$ and distance approaching $H^{-1}(1 - 1/\ell)$ for (constant) every positive integer ℓ.

(e) (Extra credit:) Extend the notion of a partition to a notion of 'uniform cover" so as to build codes of rate $1 - 1/\ell$ and distance $H^{-1}(1/\ell)$.

3. (q-ary Plotkin bound). The q-ary Plotkin bound says that if $\{C_i = (n_i, k_i, d_i)_q\}$ is an infinite family of codes with $k_i/n_i \geq R$ and $d_i/n_i \geq \delta$ then $R \leq 1 - (q/(q-1))\delta$. Your goal is to prove this bound below.

(a) Prove that there exist vectors $\eta_1, \ldots, \eta_q \in \mathbb{R}^{q-1}$ such that $\langle \eta_i, \eta_j \rangle = 1$ if $i = j$ and $-1/(q-1)$ otherwise.

(b) Use the above to show that if $c_1, \ldots, c_K \in [q]^n$ have pairwise distance at least $(q-1)/q \cdot n$, then $K \leq 2(q-1)n$. (Conclude that if $\delta \geq (q-1)/q$ then $R = 0$.)

(c) Show that if there exists an $(n,k,d)_q$ code then there exists an $(n-1, k-1, d)_q$ code.

(d) Combine the above to infer the Plotkin bound.

4. (**Need not be turned in.**) (The Johnson bound.)

(a) Prove that if $w, c_1, \ldots, c_L \in \{0,1\}^n$ are words such that $\Delta(w, c_i) \leq \tau n$ and $\Delta(c_i, c_j) \geq \delta n$ for every $i \neq j$ and $\tau = 1/2(1 - \sqrt{1-2\delta})$ then $L \leq 2n$. (Hint: You may use the usual transformation to vectors in $\{-1,+1\}^n$ and convert statements about Hamming distance into statements about inner products. Suppose the vector w is transformed to $W \in \{-1,+1\}^n$ this way and vectors $c_1, \ldots, c_L$ to $C_1, \ldots, C_L$. Show that under the given condition on τ and δ, you can "shift" the origin to some point αW (for $\alpha \in [0,1]$) such that the from the new origin end points of the vectors $C_1, \ldots, C_L$ have pairwise non-positive inner product.)

(b) Prove the q-version of the above.

(c) Prove that your bound on the relationship between τ and δ is tight.

5. (Concatenated codes and Justesen codes).

(a) Use the Wozencraft ensemble to construct, in time poly(n), binary codes of length n, rate $1/4$ of relative distance approaching $1/2(H^{-1}(1/2))$. (Your code should be linear and your algorithm should construct the entire generator matrix in polynomial time.)

(b) Now we will show that concatenating with an ensemble of codes also works almost as well: Let $C_1, \ldots, C_N$ be $(n, k, d)_2$ codes such that most $(N - o(N))$ codes have distance $d - o(d)$. Suppose B is in $(N, K, D)_{2^k}$ code. Show that the concatenation of B with $(C_1, \ldots, C_N)$, which is obtained by encoding a message of B by the encoder of B, and then encoding the ith symbol of the encoding by the encoder for C_i, is a code of distance $D \cdot d - o(N \cdot d)$.

(c) Conclude that there is a strongly explicit code, one which has a generator matrix $G = [G_{ij}]$ with G_{ij} being computable in time $\operatorname{poly}\log(n)$ given i and j, of rate $1/4$ with relative distance approaching $1/2H^{-1}(1/2)$.