Essential Coding Theory — Madhu Sudan
6.896
Due: Wednesday, December 4, 2002

Problem Set 4

Instructions: See PS1.

1. (Decoding the CRT code:) Recall that the Chinese Remainder Theorem based code (CRT codes) with integer parameters $0 < k < n$ and n relatively prime integers $p_1 < p_2 < \cdots < p_n$ has as its message set, the set of integers $\mathbb{Z}_K = \{0, \ldots, K-1\}$ where $K = \prod_{i=1}^{k} p_i$ and encodes a message $m \in \mathbb{Z}_K$ as the n-tuple $\langle m(\mathrm{mod}\, p_1), \ldots, m(\mathrm{mod}\, p_n)\rangle$.

   (a) Applying reasoning analogous to the abstract decoding algorithm used to decode AG codes, show that an efficient solution to the following task yields an efficient decoding algorithm for the CRT code:

   > Given $r_1, \ldots, r_n$ and bounds L, U find $a \in \mathbb{Z}_L$ and $b \in \mathbb{Z}_U$ such that $a \cdot r_i = b(\mathrm{mod}\, p_i)$ for every $i \in [n]$.

   How many errors does your algorithm correct?

   For the curious: Show how the above task can be expressed as an integer programming problem in a *constant* (independent of n, k, p_i's) number of variables.

   (b) (Hard question) Using the fact that the algorithm above has nice "errors and erasures" correcting behavior, derive an algorithm to correct from $(n-k)/2$ errors.

2. (Johnson bound for large alphabets:) Let B be a bipartite graph with n vertices on the left and ℓ vertices on the right with the property that it has no $K_{m,2}$ (i.e., no induced subgraph that is a complete bipartite graph with m vertices on the left and 2 vertices on the right) and every right vertex has degree at least t. Show that if $t^2 > mn$, then $\ell \leq n(t-m)$.

   Assuming the above, show that an $[n, k, d+1]_q$ code C is also $(e.\ell)$-error-correcting for $e = n - \sqrt{n(n-d)}$ and $\ell = O(n)$. (recall defn. from Lecture 13.)

3. (Decoding Tanner codes:) Recall the codes described in Lecture 16, Section 6 introduced by Tanner. These are codes obtained by combining a (c, d)-regular (δ, γ)-bipartite expander with a constant sized error correcting code C' of minimum distance Δ. Consider the following decoding algorithm for this code, which proceeds in stages, with the ith stage as follows:

   - The iteration starts with a current assignment to left vertices.
   - If each right vertex sees a codeword of C', then output the current assignment and stop.
   - Else, in parallel each right vertex does the following: If the assignment to its neighbors is at distance at most $\epsilon\Delta$ from some codeword, then send a FLIP message to every left neighbor that is inconsistent with the nearest codeword of C'.
   - In parallel, every left vertex that receives at least one FLIP message from its neighbors, flips its current assignment.

Show that the above algorithm corrects a constant fraction of errors (provided $\gamma > 0$, and $\epsilon < O(1/c)$ and Δ is sufficiently large). Also give sufficient conditions for the rate of this code to be positive.

(Email madhu@mit.edu for hints!)

4. (Rate vs. list-decodability:)

   (a) Let $\mathcal{C}$ be an infinite family of codes of rate R such that every code of block length n in $\mathcal{C}$ is $(\tau n, n)$ list-decodable. Show that $R \leq 1 - H(\tau)$.

   (b) For any R, τ such that $R < 1 - H(\tau)$, prove that there exists an infinite family of codes $\mathcal{C}$ of rate $R < 1 - H(\tau)$ is $(\tau n, O(n))$-list decodable.