Collaboration policy: You are encouraged to discuss homework problems with your classmates. However, you should think about the problems before discussing them, and you must write up your own solutions. In particular, nobody should email partial or full solutions to anybody. Finally, you must acknowledge any collaboration by writing your collaborators’ names on the front page of the assignment.

Citation policy: Try to solve the problems without reading any published literature or websites, besides the class text and links off of the class web page. If, however, you do use a solution or part of a solution that you found in the literature or on the web, you must cite it. Furthermore, you must write up the solution in your own words.

1. (10 points) Show that if an \([n,k=Rn]\) binary code is \((\rho,L(n))\) list-decodable, where \(L(n)=2^{o(n)}\), then \(R \leq 1-H_2(\rho)+o(1)\).

Hint: You may use Lemma 4.8 in the text.

2. (10 points) Use concatenation to give, for infinitely many \(n\) and for any \(\epsilon \geq 1/\sqrt{n}\), an explicit \([n,k \geq \epsilon \sqrt{n},d \geq (1/2-\epsilon)n]\) binary code. Your construction should be completely explicit, in that it shouldn’t use any greedily-constructed code.

3. (15 points) Let \(\mathbb{Z}_M = \{0,1,\ldots,M-1\}\) denote the integers modulo \(M\). Let \(p_1 < p_2 < \ldots < p_n\) be distinct primes, and for \(k < n\) let \(K = \prod_{i=1}^k p_i\) and \(N = \prod_{i=1}^n p_i\). The Chinese remainder code is defined by the encoder \(C\) mapping \(m \in \mathbb{Z}_K\) to

\[
C(m) = (m \mod p_1, m \mod p_2, \ldots, m \mod p_n) \in \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_n}.
\]

(This is not a code in the usual sense because symbols at different positions lie in different alphabets. However, the notion of Hamming distance \(\Delta\) still makes sense. Also, if you’ve forgotten the Chinese remainder theorem, look it up before continuing.)

(a) Suppose \(m \neq m'\). Prove that

\[
\prod_{i:C(m)_i \neq C(m')_i} p_i > N/K.
\]

Conclude that \(\Delta(C(m),C(m')) > n-k\). Conclude also that for a received word \(r = (r_1, \ldots, r_n)\), there is at most one \(m \in \mathbb{Z}_K\) such that:

\[
\prod_{i:C(m)_i \neq r_i} p_i \leq \sqrt{N/K}.
\]  

(1)

Call such a codeword close.
(b) This part and the following adapt the Welch-Berlekamp decoder to Chinese remainder codes. Suppose $r$ is the received word as above and there exists a code-word $m$ satisfying (1). Show that there exists integers $y, z$ with $0 \leq y < \sqrt{NK}$ and $1 \leq z \leq \sqrt{N/K}$ such that $y \equiv rz \pmod{N}$.

(c) Show that if $y, z$ are any integers satisfying the above conditions, then $m = y/z$.

4. (15 points) Let $G$ be an $\ell$-left-regular $(D, (1-\epsilon)\ell)$-expander on left nodes $[N] = \{1, 2, \ldots, N\}$ and right nodes $[M]$, i.e., for every left-subset $S \subseteq [N]$ with $|S| \leq D$, $|\Gamma(S)| \geq (1-\epsilon)\ell|S|$. Consider the following parallel iterative decoder for the corresponding expander code $C_G$:

For $c \log N$ rounds, do the following for each variable node $v$:

If $v$ is adjacent to at least $2\ell/3$ unsatisfied check nodes, then flip its value.

Show that for a large enough choice of the constant $c$, the above algorithm corrects any pattern of $(1 - 3\epsilon)D$ errors.