

Noise in Computation — Exercise 2 (submit July 17)

July 11, 2007

1. Prove the second part of Shannon’s Noisy Channel Coding Theorem for the case of the binary symmetric channel (BSC):

Theorem: If $R > 1 - H(p)$ where H is the binary entropy function, then for any sufficiently large n and for any pair of encoding and decoding functions $E : \{0, 1\}^{\lceil Rn \rceil} \rightarrow \{0, 1\}^n, D : \{0, 1\}^n \rightarrow \{0, 1\}^{\lceil Rn \rceil}$,

$$\Pr_{m \in \{0,1\}^{\lceil Rn \rceil}, \eta \sim \text{BSC}_p} [D(E(m) \oplus \eta) = m] \leq \exp(-n),$$

where m is selected uniformly at random from $\{0, 1\}^{\lceil Rn \rceil}$ and $\eta \sim \text{BSC}_p$ means $\eta \in \{0, 1\}^n$ is selected by setting each entry of it to 1 with probability p and to 0 with probability $1 - p$.

Hints:

- Argue that whp η has many ones (use the Chernoff bound).
 - Using volume arguments and the estimate $\binom{n}{pn} \approx 2^{H(p) \cdot n}$, show that there isn’t enough “space” in $\{0, 1\}^n$ to accommodate for $2^{\lceil Rn \rceil}$ large-radius balls on which D decodes correctly.
2. Let F_2 denote the two element field. In what follows all arithmetic operations are in F_2 . Let $H \in F_2^{(n-k) \times n}$ be a parity check matrix¹ for a $[n, k, d]_2$ -code, as defined in class. Consider the following decoding algorithm receiving as input a received word $w = (w_1, \dots, w_n) \in F_2^n$ and H . In what follows, e_i is the vector that has 1 in the i^{th} position and 0 everywhere else; $|y|$ denotes the weight of y , i.e., the number of ones in it.

Decode (w, H)

While (there exists $i \in \{1, \dots, n\}$ such that $|H \cdot (w + e_i)| < |H \cdot w|$) do

Set $w \leftarrow w + e_i$;

Return w

Bound the running time of the algorithm.

3. In this question we prove that the decoding algorithm correctly decodes noisy codewords of an expander-based LDPC code. Let $G = (V = (L, R), E)$ be the bipartite graph corresponding to the parity check matrix H from the previous question. Suppose G is a c -left regular², (γ, δ) -expander, for $\gamma > 3c/4$. This expansion means that for every $S \subset L, |S| \leq \delta n$ we have $|\Gamma(S)| \geq \gamma|S|$. Prove the following statement: Suppose w is $\delta/2$ -close to the code, i.e., $\Delta(w, w') \leq \delta n/2$ for some w' such that $H \cdot w' = \vec{0}$. Then Decode (w, H) returns w' . Hints:

¹Not to be confused with the entropy function H from Question 1.

²I.e., each vertex in L has c neighbors

- Use the unique-expansion lemma proved in class to argue the following:
- Throughout the operation of **Decode**, w remains within small distance of w' .
- As long as w is not a codeword, some bit will be flipped.