Problem Set 3

Instructor: Dana Moshkovitz November 7, 2011

Due: November 22, 2011.

Question 1 - Sparse, unbiased, codes have many low density parity checks

Suppose that a code $C \subseteq \{0,1\}^n$ is: (i) *sparse*, in the sense that $|C| \leq n^2$ (rather than $|C| = 2^{\Omega(n)}$); (ii) $2/n^{0.1}$-*biased.*

Show that for a sufficiently large constant k, the number of parity checks in $C^{\perp}$ of weight k is:

$$\left(1 + o\left(n^{-1}\right)\right) \cdot \frac{\binom{n}{k}}{|C|}.$$

You may use the following fact about the Krawtchouk polynomials: for $\alpha \geq 1/2$ and sufficiently large k, for $(n - n^{\alpha})/2 \leq i \leq (n + n^{\alpha})/2$, it holds that $|P_k(i)| \leq 2n^{\alpha k}$.

Question 2 - Decoding BCH

Show an efficient algorithm for decoding BCH codes when the number of errors approaches half the distance.

Question 3 - List decoding algebraic geometry codes

In class we saw a toy example of an algebraic geometry code:

Let q be prime. Let $\mathbb{F} = GF(q^2)$ be a finite field. Let $S = \left\{ (x, y) \in \mathbb{F}^2 \;\middle|\; N(x) = Tr(y) \right\}$. The code contains a codeword per bivariate polynomial p of degree at most q over $\mathbb{F}$. The codeword is of length $|S| = q^3$. Position $(x, y) \in S$ of the codeword is $p(x, y)$.

Design and analyze an efficient list decoding algorithm for this code.