COS 522: Complexity Theory : Boaz Barak
Handout 7: Hardness amplification and error correcting codes.

Reading: Chapter 16

Overall plan Three results:

1. Mild average-case hardness to strong average-case hardness.
2. Worst-case hardness to mild average-case hardness.
3. Worst-case hardness to strong average-case hardness (in one shot).

Yao's XOR Lemma

Impagliazzo's Hardcore Lemma

Error correcting codes Definition, explicit constructions, encoding, decoding, local decoding.

Putting it all together

Getting to BPP = P Worst case to strong average case hardness.

List decoding List decoding of Reed-Solomon, Walsh-Hadamard.

Local list decoding Reed Muller.

Putting it all together

Homework Assignments

§1 (30 points) Exercise 17.2

§2 (30 points) Exercise 17.3

§3 (30 points) We say that a distribution X over $\{0,1\}^n$ has min entropy at least k if $\Pr[X = x] \leq 2^{-k}$ for every x in X's range. We say that a distribution X over $\{0,1\}^n$ is a *convex* combination of distributions $Y_1, \ldots, Y_m$ if there are non-negative numbers $\alpha_1, \ldots, \alpha_m$ summing to 1 such that $X = \sum_{i=1}^{m} \alpha_i Y_i$ when considering distributions as 2^n-dimensional vectors. Prove that every distribution over $\{0,1\}^n$ with min entropy at least k is a convex combination of distributions that are uniform over subsets of $\{0,1\}^n$ with size at least 2^k.

§4 (30 points) Exercise 17.10