Homework 2

CS 6810—David Steurer

Spring 2016

1 NP-hardness of systems of quadratic equations

In some of the previous lectures, we used the problem of solving systems of quadratic equations over $\mathbb{F}_2$, denoted QuadEq, as an example of a typical NP-hard problem.

Show that (the decision version of) QuadEq is NP-hard by reduction from 3Sat.

2 Error correcting codes and probabilisitcally checkable proofs

In class, we motivated the use of error correcting codes for the proof of the PCP theorem by the claim that query efficient verifiers cannot reliably distinguish between proofs that are close in Hamming distance. In this exercise, you will show this claim.

Let V be a randomized algorithm that given oracle access to a string π makes at most q queries to it.

Let $x, \pi \in \{0,1\}^*$ be arbitrary bit strings. Let π' be a bit string obtained by flipping every entry of π with probability ε. (Note that the expected Hamming distance between π and π' is ε.)

Show that

$$\mathbb{P}\{V^{\pi}(x) = 1\} \geq \mathop{\mathbb{E}}_{\pi'} \mathbb{P}\{V^{\pi'}(x) = 1\} - q \cdot \varepsilon\,. \tag{1}$$

3 Distance to Walsh-Hadamard code and Fourier coefficients

In class, we introduced Fourier analysis to analyze a local tester for the Walsh-Hadamard code. This exercise asks you to prove a relationship between the Fourier coefficients of a function and its distance to the Walsh-Hadamard code.

Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Define the corresponding real-valued function $F\colon \mathbb{F}_2^n \to \mathbb{R}$ as

$$F(x) = (-1)^{f(x)}\,. \tag{2}$$

Let $\{\chi_x \mid x \in \mathbb{F}_2^n\}$ be the Fourier basis, that is, $\chi_x(r) = (-1)^{r^T x}$ for all $x, r \in \mathbb{F}_2^n$. Let $\{c_x \mid x \in \mathbb{F}_2^n\} \subseteq \mathbb{R}$ be the Fourier coefficients of F, so that

$$F = \sum_{x \in \mathbb{F}_2^n} c_x \cdot \chi_x\,. \tag{3}$$

Show that for all $x \in \mathbb{F}_2^n$,

$$c_x = 1 - 2\mathrm{dist}(f, \mathrm{WH}[x]) \tag{4}$$

Footnotes