Handout7: A constant number of query bits

June 4, 2003

We describe the second inner PCP. It probes only a constant number of bits in the inner PCP witness, but is relatively inefficient in terms of randomness. The encoding scheme E for this inner verifier is the Hadamard code: linear functions (total degree 1) over $\{0,1\}^n$. The linearity test that is associated with this code has a simple analysis (for those familier with the discrete Fourier transform). The sum check protocol (which appears to inherently require a nonconstant number of probes) is avoided by extending the linear Hadamard code to a "quadratic code" that is even more redundent than the Hadamard code. Satisfiability can be checked by reading only a constant number of bits of the quadratic code.

Homework.

The linearity test is analysed using the discrete Fourier transform. A key aspect of the analysis is the fact that the Fourier coefficients of the convolution of two functions is simply the products of the respective Fourier coefficients. Prove this fact.

(**Remark**: this fact is true for Fourier transforms in general, and not only for discrete Fourier transform. Hence many textbooks and articles contain proofs of this fact, and you are welcome to consult them.)