Massachusetts Institute of Technology
6.5630: The Evolution of Proofs in Computer Science
Professor Yael Tauman Kalai

Problem Set

We saw in class how to use the GKR protocol to construct a PCP for NP.

1. It may seem tempting to try to construct such a PCP from any succinct interactive proof by having the PCP contain the prover's answers to all possible verifier messages.
   (a) Why does this not always work?
   (b) Which two properties of the GKR protocol did we use to construct a PCP (with polynomial blowup)?
2. Recall that the PCP we constructed in class includes the low-degree extension of the witness (which the verifier needs in order to verify the proof). As mentioned in class the verifier needs to add a "low degree test."
   (a) What goes wrong if no such test is added. Show an attack by constructing a malicious PCP that convinces the PCP verifier that an unsatisfiable φ is in 3SAT.
   (b) A common low-degree test is the one due to Rubinfield and Sudan. This test verifies that a multi-variate polynomial $W^* : \mathbb{F}^m \to \mathbb{F}$ is ϵ-close to a polynomial of *total degree* d.[1] Recall that in the GKR protocol we have the guarantee that this a true polynomial of degree $|H| - 1$ in each variable (since it is computed by the honest verifier). This guarantee is stronger than the guarantee provided by the low-degree test, which only provides ϵ-closeness and only guarantees that the total degree is at most $d = m \cdot (|H| - 1)$. Why are the guarantees given by the low-degree test sufficient to guarantee soundness?
3. Show how to convert the GKR protocol to an interactive argument for NP using Merkle Hashing, *without* going through PCPs. Give one advantage of this scheme over the Kilian-Micali protocol we saw in class.

[1] In this test the verifier chooses a random line in $\mathbb{F}^m$, reads $d+2$ random points on this line, and checks that they interpolate to a polynomial of degree d. For a good survey on low-degree tests see https://www.wisdom.weizmann.ac.il/ oded/PDF/pt-low.pdf.

6.5630 Advanced Topics in Cryptography

Fall 2023