Handout5: parallelization of probes

May 21, 2003

We have explained last week the concepts of outer and inner verifiers. A key ingredient for inner verifiers is to have the number of probes made by the inner verifier constant (though each probe may read a character composed of many bits). In our proof that $NP \in PCP(\log n, (\log n)^{O(1)})$ the number of queries was polylogarithmic in n. Today we explain how to modify the PCP so that it probes only a constant number of locations, where each probe corresponds to multiple queries of the previous PCP.

Among the techniques that we use are the following. A PCP witness is encoded in a table A using a coding scheme E that is based of multinomials of total degree d. In addition, there is an auxiliary table B that gives for every line in $\mathcal{F}^m$ a univariate polynomial of degree d that supposedly describes A on this line. On top of that, there is another auxiliary table C that gives for (some) sets of l points in $\mathcal{F}^m$ a degree $d(l-1)$ polynomial that supposedly describes A on the degree $l-1$ curve that passes through the l points. Using only four probes (in fact, three probes suffice) one can simultaneously get the values of A on l points.

Homework.

1. Write down explicitly the procedure given in class that for arbitrary points $x_1, \ldots, x_l \in \mathcal{F}^m$ uses four probes (two to A, one to B, and one to C) and deduces from them all values $A(x_1), \ldots, A(x_l)$.

2. Let p the multinomial of total degree d that is closest to A. It is clear that if $A = p$ and B and C are prepared consistently with p, then the procedure really gives the value of A on the l points. Prove that if $\Delta(A,p) = \epsilon$ and if $A(x_i) \neq p(x_i)$ for some $1 \leq i \leq l$, then the procedure rejects with probability at least
$$1 - \frac{d(l-1)}{|\mathcal{F}| - l} - \frac{d}{|\mathcal{F}| - 1} - \epsilon$$

(Note: the handout as given in class required showing that the procedure rejects with probability at least $1 - 2\sqrt{\epsilon'} - \frac{d(l-1)}{|\mathcal{F}|-l}$, where $\epsilon' = \epsilon + d/(|\mathcal{F}| - 1)$. Either answer is okay.)