Handout3: $NP \subset PCP(\log n, (\log n)^c)$

March 26, 2003

The PCP theorem says that $NP \subset PCP(\log n, 1)$. We build gradually towards the proof of this theorem As an intermediate step, we show that $NP \subset PCP(\log n, (\log n)^c)$.

The proof has some ingredients that we met in the LFKN "sum-check" protocol, and some new ingredients.

The PCP witness for 3SAT is composed of two components. One is a redundent encoding A of a satisfying assignment. This encoding is based on low degree multinomials. The other is answers prepared in advance to all possible queries in a sum-check protocol for an arithmetization of the 3CNF formula.

The verification procedure consists of two components. One is a *low degree test* that checks that A is indeed a low degree multinomial (up to a negligible number of outliers). The other is a sum-check protocol. The final expression obtained from the sum-check protocol is evaluated by substituting in three random values from A.

Homework (hand in by April 9).

For a 3CNF formula with n clauses and n variables, what is the number of bits (as a function of n) in the PCP witness for the protocol described in class? Explain your answer. Try to identify components of the protocol where one may hope to get improvements that would lead to shorter PCP witnesses. (You just need to try to identify parts with possible slackness, rather than actually show how to do better.)