Handout2: The LFKN protocol

March 19, 2003

An *interactive proof* for a language L is a two player protocol involving a computationally unlimited prover P and a random polynomial time verifier V. Both share a common input x, and can exchange messages of polynomial length. The protocol needs to satisfy two properties:

- *Completeness.* If $x \in L$, then the prover has a strategy (a function from the history of messages so far to the next message that the prover sends) that causes the verifier to accept.
- *Soundness.* If $x \notin L$, then regardless of the provers strategy, the verifier accepts with probability at most 1/2 (probability taken over the coin tosses of V).

There is some analogy between interactive proofs and PCPs. Both contain a probabilistic verifier, and the IP prover is analogous to the PCP witness. A major difference is that the IP prover is *adaptive*, and hence may cheat more easily.

In late 1989, Lund, Fortnow, Karloff and Nisan proved an unexpected result, namely, that every co-NP language has an interactive proof. We shall present a later version of the LFKN protocol.

The number of rounds in the LFKN protocol grows as a function of the input length. The question of whether co-NP has an interactive proof with a constant number of rounds is open.

Homework (hand in by April 2).

Show that any nonzero multinomial with n variables, each of degree at most d, has at most ndp^{n-1} roots modulo prime p. (E.g., $x^3y^3 - xy^2 + x^2 - 5 = 0 \pmod{p}$ has at most $6p$ solutions.) Hint: by induction on n. You may assume the base case $n = 1$ for granted.

C. Lund, L. Fortnow, H. Karloff, N. Nisan, "Algebraic methods for interactive proof systems", *JACM, 39 (1992), 859-868.* (Preliminary version in STOC 1990.)