Handout4: the degree h test

April 9, 2003

On April 16 and 23 there is no class because of passover. On April 30 I will be away, but perhaps there will be a class (if Adi Shamir will be available to talk about IP=PSPACE, which is an extension of the LFKN result). On May 7 there is no class because of Indepedence Day.

Tomorrow, April 10 at 14:00, Avi Wigderson will give a talk in the advanced student seminar on derandomized low degree tests, with applications to PCPs. It is recommended that you come.

We analyse the basic degree-h test. We give a full proof (extending that of [BFL,FGLSS]) that $O(hm)$ repetitions of the basic degree test suffice in order to reject when a function is far from being degree h. As Arora and Safra show, in fact $O(m)$ repetitions suffice. We indicate some of the ideas that they use, and in particular, the use of a procedure of Berlekamp and Welsh to solve the following problem.

Let $\mathcal{F}$ be a finite field, and let $S = \{(x_i, y_i)\}$ for $1 \leq i \leq n \leq |\mathcal{F}|$ be a set of pairs specifying points $x_i \in \mathcal{F}$ and values $y_i \in F$. We assume that all x_i are distinct. For a parameter t, we are interesting in finding a degree d polynomial $q(x)$ such that for at least t pairs in S, $q(x_i) = y_i$. Observe that if $2t > n + d$, then if such a polynomial q exists then it must be unique.

Homework (hand it in by May 14).

In the procedure of Berelekamp and Welsh, suppose that the set S is such that no degree d polynomial agrees with t of the n pairs (for given n, t, d that satisfy $2t > n + d$). Here are a few things that might go wrong:

1. The system of linear equations has no solutions.
2. The system of linear equations does have a solution, but e' does not divide p' as formal polynomials.
3. e' does divide p', but the resulting polynomial q' does not agree with S on t pairs.

For each of the options above, either show an example when it happens, or prove that it cannot happen.