KUNGL TEKNISKA HÖGSKOLAN
Datavetenskap och kommunikation
Johan Håstad

4 mars 2010

Theoreticians Toolkit, 2009/10

The purpose of this document is to keep track of what happened at the lectures and to some extent give a pointer to what will happen in the next few lectures.

1 Lectures that have taken place

F1, 2/11 Overview of course.

F2, 10/11 The probabilistic method. Constructing a graph without a large independent set nor a large clique. The second moment method for proving existence of objects.

F3, 17/11 (Ola Svensson lecturing) Constructing a dense graph of large girth. Chernoff bounds.

F4, 24/11 Constructing k-wise independent spaces of random variables. Upper and lower bounds on the size of the space. Application to derandomizing an algorithm for Max-3Sat. The method of conditional expectations.

F5, 1/12 Almost k-wise independent ensambles of small size. Key technique: vandermonde matrices and that linear algebra over finite fields of $GF[2^l]$ is just linear algebra over $GF[2]$.

F6, 8/12 Lovasz local lemma as applied to k-sat with few occurrences.

F7, 15/12 (Ola) Corrected Lovasz local lemma argument, discussion of old homework problems. Definition of extractors.

F8, 12/1 Constructing extractors using pairwise independent hash functions.

F9, 19/1 Schwartz-Zippel (non-zero polynomial likely to be non-zero on random point). co-NP can be done by an interactive proof. Introduction to Reed-Solomon codes.

F10, 26/1 Error correcting codes. The Hamming code and Reed Solomon codes. Decoding of Reed-Solomon codes in the case of unique decodability.

F11, 2/2 List decoding of Reed-Solomon codes. Efficient and explicit construction of binary codes with constant rate and relative distance.

F12, 9/2 Expander graphs, definition and application to hardness of bounded occurrence Max-Sat and error correcting codes.

F13, 16/2 Finished application of expander codes. Discussed walks on expanders and the role of the second eigenvalue. Initial discussion of a good pseudorandom generator.

F14, 23/2 A good generator from a one-way permutation using the Goldreich-Levin predicate. An overview of the Nisan-Wigdersson generator.

F15, 2/3 The concept of a lattice with some example. How to find a short vector; the LLL-algorithm.

2 Topics that might be covered

Ola will lecture for the last two lectures.

Inapproximability An n^c inapproximability resuly for clique.

Linear programming Some application of LP to approximability.