KTH Computer Science
and Communication

Homework V, Theoreticians Toolkit 2009/2010

Due on Tuesday February 16 at 15.15. Solutions to many homework problems, including problem one on this set, is available on the internet, either in exactly the same formulation or with some minor perturbation. It is *not acceptable* to copy such solutions. It is hard to make strict rules on what information from the internet you may use and hence whenever in doubt contact Johan Håstad. You are, however, allowed to discuss problems in groups with up to three students, but solutions should be handed in individually. On this problem set the second problem is about finding information and here you should feel free to use any source.

1 (30 p) Consider a code with words of length n coding $n/3$ symbols over the alphabet $\{0, 1, 2\}$. We want to construct such a code with good minimal distance.

Your task is to try three approaches.

1. Prove existence by a volume argument. Guess a minimal distance and make sure you can pack a suitable number of balls of a suitable diameter.
2. Prove existence by a picking a random subset of cardinality $3^{n/3}$ of $\{0, 1, 2\}^n$ as your code and calculate the expected minimal distance of such a set.
3. Prove existence by a picking a random linear space of dimension $n/3$ in $\{0, 1, 2\}^n$ as your code and calculate the expected minimal distance of such a set.

Aim for a full solution to the problem in the last two cases in that you should find the minimal distance up to a factor of $(1 + o(1))$. You are expected to prove that your answer is indeed the minimal distance with high probability proving both upper and lower bounds.

2 (20p) This is a problem of finding information about a research problem, in this case the list decodability of Reed-Solomon codes. Say that a triplet (n, k, e) is *feasible* if, in a k-dimensional Reed-Solomon code of length n there is an efficient (polynomial time) algorithm to find all words that differ from a received word in at most e positions.

What triplets (n, k, e) are known to be feasibly, what triplets are known not to be feasible and for what triplets is the question open?

You just need to write a short note stating the results but you should include references to original papers where the results were proved.

3 (20p) Considering the following problem. Each of n people in a room is given a hat that is black or white each with probability one half independently for each person. Each person sees the colors of all hats but his/her own and the task is to guess the color of this unseen hat. Each person is supposed make a guess in writing which can be "black", "white" or "no guess". The guesses are all made in parallel and the group wins if somebody makes a guess and everybody that does make a guess is correct.

The group may not communicate during the experiment but can make any agreement before they get their hats. An obvious strategy is to fix one person who always guesses while the others make no guess; a strategy that succeeds with probability $\frac{1}{2}$. Determine a better strategy and to get a full credit determine asymptotically the probability of winning with the optimal strategy.

Hint: If there are three people the following strategy is interesting: If you see two hats of the same color guess that your hat has the opposite color.