



KTH Computer Science
and Communication

Homework III, Theoreticians Toolkit 2009

Due on Tuesday Dec 22 at 15.15. Solutions to many homework problems, including this one, will be 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.

- 1 (20+5+10 p) Let us color integers with three colors, red, blue and green. A set S is well colored if all three colors occur in S . The translate $S + t$ of a set S is the set of all points of the form $s + t$ and $s \in S$.

We say that a set S is *n-well colored* if it, and all its translates by any integer t such that $S + t \subseteq [n]$ (the integers from 0 to $n - 1$) are well colored. It is infinitely well colored if all its integer translates are well colored.

Prove that any set S of size at least 22 can be n -well colored for any n . This gives you a score of 20 points. For a bonus score of 5 points prove that any such S can be infinitely well colored.

For a different bonus of 10 points show how to efficiently¹ find such a coloring, given S and n .

- 2 (20p) In class we proved how to get a set T of size $O((k \log n)^2 \epsilon^{-2})$ of n bit strings such that when picking a random element from T , any xor of size at most k is at most ϵ biased. The construction was completely efficient and explicit using finite fields. Another natural way to construct such a set T is to pick a random set of cardinality t and hope it does the job.

For what value of t can you prove that the probability that a random T of cardinality t has the property with probability at least $1/2$? Only an upper bound is needed together with a heuristic argument² that is tight.

In this problem we are only looking for an asymptotic size as a function of n , k and ϵ and we do not care about constant factors.

¹In expected time which is polynomial in n .

²You may here assume that events that are not independent are independent.