



KTH Computer Science  
and Communication

## Homework VII, 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 first problem is about finding information and here you should feel free to use any source.

- 1** (20 p) We claimed in class that if  $f$  is one-way permutation and  $x$  and  $r$  are random strings in  $\{0, 1\}^n$  then the set of bits defined by  $x_0 = x$ ,  $x_i = f(x_{i-1})$  and  $b_i = (r, x_i)$  (the inner product of  $r$  and  $x_i$ ) gives a good pseudorandom generator. The key technical step that we skipped is the claim that if we have a polynomial time algorithm  $A$  that given  $y = f(x)$  and  $r$  can compute  $(x, r)$  and be correct with probability  $\frac{1+\delta}{2}$ , then there is a different algorithm  $B$  than runs in time polynomial in  $n$  and  $\delta^{-1}$  that can compute  $x$  given  $y$  and be correct with some non-negligible probability (such as  $\delta/2$ ).

Find the proof of this statement in the literature and rewrite it with your own words. The original theorem is due to Goldreich and Levin.

- 2** (25 p) The task of this problem is to find the exact expression for a real number,  $\theta$ , in the interval  $[\frac{1}{2}, 1]$ , when you are only given a numeric approximation,  $\tilde{\theta}$ , with  $n$  bits such that  $|\theta - \tilde{\theta}| \leq 2^{-n}$ .

- 2a** (10 p) Suppose you that  $\theta$  is a rational number with denominator at most  $t$ , i.e.  $\theta = p/q$  where  $q \leq t$ . For how large value of  $t$  (as a function of  $n$ ) can you find the exact rational expression for  $\theta$  and how much time does it take?

**Hint:** You may either use continued fractions or find a short vector in the lattice spanned by the vectors  $b_1 = (\tilde{\theta}, \epsilon)$  and  $b_2 = (1, 0)$  for a suitable  $\epsilon$ .

- 2b** (15 p) Suppose instead that  $\theta$  is the solution of second degree equations  $ax^2 + bx + c = 0$  with  $a$ ,  $b$  and  $c$  integers all bounded by  $t$  in absolute value. Can you, given the approximation  $\tilde{\theta}$ , find the coefficients  $a$ ,  $b$  and  $c$ ? Again you should do it efficiently and for a reasonably large value of  $t$ .