Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

9. Exercise sheet
Hand in solutions until Sunday, 28 June 2009, 24:00h.

Exercise 9.1 (A property of pseudorandom generators). (3 points)

Prove that no pseudorandom generator will assign a noticable probability mass to any string, i.e. prove that if f is a pseudorandom generator then for every positive polynomial p and all sufficiently large n and any given x_0, we have that $\text{prob}(f(U_k) = x_0) \leq \frac{1}{p(n)}$ $\boxed{3}$

Exercise 9.2 (Combinations of generators). (7 points)

Assume you are given generators $f_1, f_2 : \mathbb{B}^k \to \mathbb{B}^\ell$ and $g : \mathbb{B}^\ell \to \mathbb{B}^n$. Proof or refute the following conjectures:

(i) If f_1 and f_2 are both pseudorandom, so is the concatenation of f_1 and f_2, i.e. the function $h(x) := f_1(x)f_2(x)$. $\boxed{2}$

(ii) If f_1 and g are both pseudorandom, so is the composition of f_1 with g, i.e. the function $h : \mathbb{B}^k \to \mathbb{B}^n$ defined by $h(x) = g(f_1(x))$. $\boxed{3}$

(iii) If f_1 is pseudorandom, and g any polynomial time computable function, then the composition of f with g is pseudorandom. $\boxed{1}$

(iv) If f_1 is any polynomial time computable function and g is pseudorandom, then the composition of f_1 with g is pseudorandom. $\boxed{1}$

Exercise 9.3 (Another Modification). (4 points)

Refute the conjecture that for every pseudorandom generator $g : \mathbb{B}^k \to \mathbb{B}^n$ also the generator $h(x) := g(x) \oplus x0^{n-k}$ is pseudorandom. Hint: Let f be a pseudorandom generator and consider the generator g defined on stings on same length such that $g(x_1, x_2) = (x_1, f(x_2))$. Don't forget to argue that in this case also g is pseudorandom. $\boxed{4}$

Exercise 9.4 (Nisan-Wigderson generator). (12+4 points)

Let D be the design presented in the text: $k = 9$, $n = 12$, $s = 3$, $t = 1$ und $S_1 = \{1,2,3\}$, $S_2 = \{4,5,6\}$, $S_3 = \{7,8,9\}$, $S_4 = \{1,4,7\}$, $S_5 = \{2,5,8\}$, $S_6 = \{3,6,9\}$, $S_7 = \{3,5,7\}$, $S_8 = \{1,6,8\}$, $S_9 = \{2,4,9\}$, $S_{10} = \{1,5,9\}$, $S_{11} = \{2,6,7\}$, $S_{12} = \{3,4,8\}$. Let furthermore be $f \colon \mathbb{B}^3 \to \mathbb{B}$ the function with $f^{-1}(1) = \{001, 010, 100\}$.

$\boxed{2}$ (i) Determine f_D for the arguments 010101000, 000111000.

$\boxed{2}$ (ii) Find a natural number $s \in \mathbb{N}$, such that f is not $(\frac{3}{4}, s)$-hard, and give a corresponding circuit.

$\boxed{2}$ (iii) Find a positive real number $\varepsilon < \frac{3}{4}$ and a natural number $s' < s$ such that f is not (ε, s')-hard, and give a corresponding circuit.

Let $\mathcal{P}$ be the predictor for bit 6 with $\mathcal{P}(y_1, \ldots, y_5) = \left(\sum_{i=1}^{5} y_i\right) \operatorname{rem} 2$.

$\boxed{+4}$ (iv*) Prove that there are 344 matrices in $\mathbb{B}^{3\times 3}$ for which the number of lines (columns and rows) with ones only is even.

$\boxed{3}$ (v) Prove that $\mathcal{P}$ is a $\frac{11}{64}$-predictor for the sixth bit under f_D. You may use the result of (iv*).

$\boxed{3}$ (vi) Design an algorithm $\mathcal{A}$ which approximates f with

$$\left|\operatorname{prob}(\mathcal{A}(X) = f(X)) - \frac{1}{2}\right| \geq \frac{11}{64}.$$