Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

8. Exercise sheet
Hand in solutions until Sunday, 21 June 2009, 24:00h.

Exercise 8.1 (Modifying pseudorandom generators). (8 points)

Suppose you are given a pseudorandom generator f. In this exercise we will explore which modifications of such a generator still yield pseudorandom generators:

(i) Suppose you are given any (polynomial time computable) permutation h over strings of same length. Prove that $g_1(x) := f(h(x))$ and $g_2(x) := h(f(x))$ are both pseudorandom generators. 4

(ii) Consider the following two modifications to f: 4

- The generator h_1 is defined as follows: define $h_1(x) := 0$ if the number of 1's in x is exactly len$(x)/2$, and $h_1(x) = f(x)$ otherwise.
- The generator h_2 is defined as follows: define $h_2(x) := 0$ if the number of 1's in x is exactly len$(x)/3$, and $h_2(x) = f(x)$ otherwise.

Which of these is a pseudorandom generator? Hint: Stirling approximation.

Exercise 8.2 (From short to long – an example). (9 points)

We are given again and again the following generator $g\colon \mathbb{B}^3 \to \mathbb{B}^6$:

x	$g(x)$
000	001100
001	001110
010	010101
011	011011
100	101000
101	100101
110	110010
111	110011

In the last two sheets we have studied this generator in great detail. This time we will use it to construct a generator that produces longer outputs.

(i) Give a formal argument that the construction in class can be used to enlarge also this generator. 3

(ii) Provide the tables of the enlarged generators h_9, h_{12} that map 3 bits to 9 and 12 bits, respectively. 3

3 (iii) Assume you are given an algorithm A that distinguishes the output $h_{12}(U_3)$ from the uniform distribution U_{12} on 12 bits with distinguishing power δ. Provide a distinguisher B that distinguishes the output of the short generator g from the uniform distribution on 6 bits and estimate its distinguishing power.

Exercise 8.3 (From short to long – a different construction). (4 points)

4 In class we constructed out of a generator $f : \mathbb{B}^k \to \mathbb{B}^{k+1}$ a generator $g : \mathbb{B}^k \to \mathbb{B}^{k+\ell}$, by applying f iteratively on the last k bits. In this exercise we consider the same construction but instead of applying f to the last k bits, we apply f to the *first* k bits. Provide a *simple* proof that this construction works as well as the construction presented in class. Hint: Do not modify the proof presented in class, but instead modify f itself.

Exercise 8.4 (From short to long – yet another construction). (0+10 points)

Suppose you are given a pseudorandom generator f, given by the functions $f_i : \mathbb{B}^i \to \mathbb{B}^{i+1}$. That is for every bitlength i we have a function f_i that produces $i+1$ bits. For $x \in \mathbb{B}^k$, we define $f(x) := f_{\mathrm{len}(x)}(x)$. Consider now the following construction: Define $g(x) := g^\ell(x)$ to be the ℓ-fold application of f on x, where $g^0(x) := x$ and $g^i(x) := f(g^{i-1}(x))$.

+8 (i) Prove that for any fixed ℓ this construction yields a pseudorandom generator. Hint: Hybrids.

+2 (ii) Why is the construction presented in class preferable?