Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

6. Exercise sheet
Hand in solutions until Sunday, 07 June 2009, 24:00h.

Exercise 6.1 (Playing fair revised). (4 points)

We are given a biased coin whose probability for flipping heads is $p_{\mathrm{H}} = 30\%$.

(i) Compute the information entropy of such a coin toss. $\boxed{1}$

(ii) What is the maximal entropy which can be expected of such a coin toss? $\boxed{2}$

(iii) What is the value of the entropy of a fair coin? Compare that to your previous results. $\boxed{1}$

Exercise 6.2 (Entropy of a day). (3 points)

Suppose that on some machine, clock time is measured in nanoseconds $1 = 10^{-9}$ seconds, and that we take the current time, modulo 24 hours, to be a random value. How many random bits would this provide? How many, if we take the time modulo one hour? Modulo one minute? $\boxed{3}$

Exercise 6.3 (Distinguishing distributions). (3 points)

Consider the example from the lecture: $\boxed{3}$

x	$g_3(x)$
000	001101
001	001011
010	011010
011	010110
100	101100
101	100110
110	110100
111	110010

Let $A(y) \in \{0,1\}$ be random, if the first four bits of y are half 0's and half 1's, otherwise let $A(y) = 1$, if $y_5 = \text{minority}(y_1, y_2, y_3, y_4)$, and else $A(y) = 0$. Compute the prediction power of this algorithm.

Exercise 6.4 (Probabilities). (4 points)

Consider the following generator $g\colon \mathbb{B}^3 \to \mathbb{B}^5$ and let $(X_1, \ldots, X_5) := g(U_3)$.

x	$g(x)$	x	$g(x)$
000	11100	100	00110
001	00101	101	11110
010	01011	110	01010
011	10101	111	01101

$\boxed{2}$ (i) Compute the distribution of the projection on the second to fourth bit, thus of (X_2, X_3, X_4).

$\boxed{2}$ (ii) Compute a table of the probabilities $W(b \leftarrow X_4(y))$ for all possible initial sections $y \in \mathbb{B}^3$ and all $b \in \mathbb{B}$.

Exercise 6.5 (Distinguishers and predictors). (10 points)

We are given 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

The algorithm $\mathcal{U}$ answers 1 if and only if at most four bits are 1, and 0 otherwise. The algorithm $\mathcal{P}$ returns the second bit.

$\boxed{3}$ (i) Show: $\mathcal{U}$ is a $\frac{7}{64}$-distinguisher between the output distribution $p = g(u_3)$ of the generator and the uniform distribution u_6 on 6 bits.

$\boxed{3}$ (ii) Show: $\mathcal{P}$ is a $\frac{1}{4}$-predictor for the sixth bit under p.

$\boxed{4}$ (iii) Find a predictor of higher quality and compute its prediction power.