Heads and tails, summer 2015

PROF. DR. JOACHIM VON ZUR GATHEN AND DR. DANIEL LOEBENBERGER

4. Exercise sheet
Hand in solutions until Sunday, 10 May 2015, 23:59:59

Exercise 4.1 (Tracing the proof of Yao's theorem). (15 points)

Recall the generator

$$f\colon \mathbb{B}^3 \longrightarrow \mathbb{B}^6$$

given by the following table:

x	$f(x)$
000	001101
001	001011
010	011010
011	010110
100	101100
101	100101
110	110100
111	110010

We apply Yao's construction to $X = f(U_3)$ on $\mathbb{B}^6$ and the distinguisher $\mathcal{A}$ from the lecture, with $\mathcal{A}(y) = 1$ if and only if $w(y) = 3$. For $0 \le i \le 6$ and any $y \in f(\mathbb{B}^3)$, we denote by

$$c_i(y) = \binom{6-i}{3-w(y_1,\ldots,y_i)}$$

the number of extensions $(z_{i+1}, \ldots, z_6)$ of $(y_1, \ldots, y_i)$ that lead to total Hamming weight 3.

(i) For $0 \le i \le 6$ express the expected value $e_i = \mathcal{E}_{\mathcal{A}}(Y_i)$ of $\mathcal{A}$ on the hybrid distributions $Y_i = \pi_i(X) \times U_{6-i}$ in terms of the c_i. [3]

(ii) Calculate for all $x \in \mathbb{B}^3$ and all $0 \le i \le 6$ the table of values of $c_i(f(x))$. [2]

(iii) For $0 \le i \le 6$ compute the table of expectations $e_i = \mathcal{E}_{\mathcal{A}}(Y_i)$. [4]

(iv) For $1 \le i \le 6$ compute the table of differences of expectations $e_i - e_{i-1}$. [1]

(v) Specify the predictor $\mathcal{P}$ for the sixth bit from Yao's construction as presented in the lecture. [2]

(vi) Prove that the specified predictor is exactly the minority bit predictor by giving its input/output behavior. [3]

Exercise 4.2 (Combinations of generators). (7 points)

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

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

3 (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 $h(x) = f_1(g(x))$.

1 (iii) If f_1 is pseudorandom, and g any polynomial time computable function, then the composition of f_1 with g is pseudorandom.

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.