## Heads and Tails, summer 2009

PROF. DR. JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER

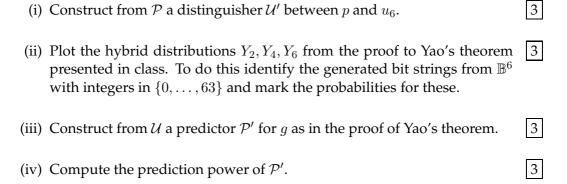
## 7. Exercise sheet Hand in solutions until Sunday, 12 June 2009, 24:00h.

Exercise 7.1 (Distinguishers from predictors and vice versa). (12 points)

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

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. We have shown that  $\mathcal U$  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. We also know that  $\mathcal P$  is a  $\frac{1}{4}$ -predictor for the sixth bit under p.



Exercise 7.2 (Distinguishers and Predictors).

(6 points)

3

3

3

3

We consider the following generator  $g: \mathbb{B}^3 \to \mathbb{B}^6$ :

x	g(x)
000	101100
001	011010
010	010101
011	111000
100	001011
101	000111
110	110110
111	100001

The algorithm  $\mathcal{U} \colon \mathbb{B}^6 \to \mathbb{B}$  answers 1 if and only if not more than four bits are 1, and 0 else. The algorithm  $\mathcal{V} \colon \mathbb{B}^5 \to \mathbb{B}$  answers 1, if the sum of the 5 bits is even, and 0 otherwise.

- (i) Prove:  $\mathcal U$  is a  $\frac{7}{64}$ -distinguisher between the generator's random variable  $X=g(U_3)$  and the random variable  $U_6$  of the uniform distribution on six bits.
- (ii) Prove: V is a  $\frac{1}{4}$ -predictor for the sixth bit produced by g.

Exercise 7.3 (And again: Distinguishers and Predictors). (6 points)

We consider the function  $g: \{0,1\}^3 \to \{0,1\}^6$ , which is given by the following truth table.

x	y = g(x)
000	110001
001	110010
010	101100
011	101100
100	011010
101	011001
110	000111
111	000111

Let  $\mathcal{U}$  be an algorithm with the input  $y \in \{0,1\}^6$ . The reply will be  $y_5$ , if  $y_1 + y_2 + y_3 + y_4 < 3$ , and  $y_5 \oplus 1$  else.

- (i) Prove:  $\mathcal{U}$  is a  $\frac{3}{8}$ -distinguisher between the distribution of the generator  $g(u_3)$  and the uniform distribution  $u_6$ .
- (ii) Construct out of this distinguisher a predictor as in the proof of Yao's theorem and compute its prediction power.