# Introduction to Computational Complexity - Assignment 4

To be submitted by 27/4/2008

In this assignment, you will complete the proof of Yao's XOR lemma:

**Lemma** (Yao's XOR Lemma)**.** *Let $p : \mathbb{N} \to \mathbb{N}$ be a polynomial and let $f : \{0,1\}^* \to \{0,1\}$ be a function such that for every family of polynomial size circuits $\{C_n\}$ it holds that*

$$\Pr_{x \in \{0,1\}^n} [C_n(x) = f(x)] \leq 1 - \frac{1}{p(n)}$$

*Let $t(n) = n \cdot p(n)$, and let $F(x^1, \ldots, x^{t(n)}) = \oplus_{i=1}^{t(n)} f(x^i)$ (where $|x^i| = n$). Then, for every polynomial $q : \mathbb{N} \to \mathbb{N}$ and for every family of polynomial size circuits $\{C_m\}$ it holds that*

$$\Pr_{x \in \{0,1\}^m} [C_m(x) = F(x)] \leq \frac{1}{2} + \frac{1}{q(m)}$$

The book gives a more general and quantatative version of the XOR lemma.

**Notation** For every two strings $x, y \in \{0,1\}^n$, we denote by $b(x,y)$ the inner product mod 2 of $x$ and $y$. That is,

$$b(x,y) = \sum_{i=1}^{n} x_i y_i \pmod 2$$

## 1 Reading Assignment - The direct product lemma

*Read Section 7.2.1.2 of the book.*

Section 7.2.1.2 discusses the proof of the XOR lemma, but contains only the proof of the direct product lemma:

**Lemma** (Direct Product Lemma)**.** *Let $p$ and $f$ be as in the XOR lemma. Let $t(n) = n \cdot p(n)$, and let $G(x^1, \ldots, x^{t(n)}) = \big(f(x^1), \ldots, f(x^{t(n)})\big)$. Then, for every polynomial $q : \mathbb{N} \to \mathbb{N}$ and for every family of polynomial size circuits $\{C_m\}$ it holds that*

$$\Pr_{x \in \{0,1\}^m} [C_m(x) = G(x)] \leq \frac{1}{q(m)}$$

As before, the book gives a more general and quantitative version of the direct product lemma. In the next two questions you will derive the XOR lemma from the direct product lemma.

## 2 From Direct Product to Selective XOR

In this question you will derive the following "selective XOR lemma" from the Direct Product lemma:

**Lemma** (Selective XOR Lemma)**.** *Let $p$, $f$, $t$, and $G$ be as in the Direct Product lemma. For every $x_1, \ldots, x_{t(n)}$ and every $r \in \{0,1\}^{t(n)}$, let $H(x^1, \ldots, x^{t(n)}, r) = b\big(G(x^1, \ldots, x^{t(n)}), r\big)$. Then, for every polynomial $q : \mathbb{N} \to \mathbb{N}$ and for every family of polynomial size circuits $\{C_m\}$ it holds that*

$$\Pr_{x \in \{0,1\}^m} [C_m(x) = H(x,r)] \leq \frac{1}{2} + \frac{1}{q(m)}$$

In order to prove this Lemma recall that in class we proved that for any one way function $f(x)$, the predicate $b(x,r)$ is a hard-core predicate of the one way function $f'(x,r) = (f(x),r)$. Actually, we proved something more general. Observe that throughout the proof of the theorem, we have not used at all the fact that the function $f$ is polynomial-time computable - we only used the fact that it is hard to invert. Thus, we claim the following stronger theorem - *verify for yourself that it indeed follows from the proof that was shown in class*:

**Theorem 2.1.** *Let $g : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ be a function such that for every polynomial $q : \mathbb{N} \to \mathbb{N}$ and for every family of polynomial size circuits $\{C_n\}$ it holds that*

$$\Pr_{x \in \{0,1\}^n} [C_n(x) = g(x)] \leq \frac{1}{q(n)}$$

*Now, for every $x \in \{0,1\}^n$ and $r \in \{0,1\}^{\ell(n)}$ define $h(x,r) = b(g(x),r)$. Then, for every polynomial $q : \mathbb{N} \to \mathbb{N}$ and for every family of polynomial size circuits $\{C_m\}$ it holds that*

$$\Pr_{x \in \{0,1\}^n, r \in \{0,1\}^{\ell(n)}} \left[C_{n+\ell(n)}(x,r) = h(x,r)\right] \leq \frac{1}{2} + \frac{1}{q(n)}$$

# 3 From Selective XOR to the Yao's XOR Lemma

In this question, you need to derive Yao's XOR lemma from the Selective XOR lemma.

**Hint** Let $F$ and $H$ be the functions from the Yao's XOR lemma and the Selective XOR lemma. You need to show that every circuit $C$ that inverts $F$ can be transformed to a circuit $C'$ that inverts $H'$. To see how it can be done, consider the following "thought experiment": Suppose that $C'$ had a "magic box" that generates pairs of the form $(x, f(x))$ where $x$ is uniformly distributed over $\{0,1\}^n$. In such a case, we could have constructed $C'$ as follows. On input $\left(x^1, \ldots, x^{t(n)}, r\right)$, where $\left|x^1\right| = \ldots = \left|x^{t(n)}\right| = n$ and $|r| = t(n)$, the circuit $C'$ would have used its magic box to create pairs $\left(y^1, f(y^1)\right), \ldots, \left(y^{t(n)}, f(y^{t(n)})\right)$. It would then define

$$z^i = \begin{cases} x^i & r_i = 1 \\ y^i & r_i = 0 \end{cases}$$

and output $C(z^1, \ldots, z^{t(n)}) \bigoplus_{i:r_i=0} f(y^i)$. Verify that this reduction indeed works.

You need to construct $C'$ without using the magic box. In order to do so, note that the pairs $\left(y^1, f(y^1)\right), \ldots, \left(y^{t(n)}, f(y^{t(n)})\right)$ can be fixed to some values.

**Extra hint** To see that the $\left(y^1, f(y^1)\right), \ldots, \left(y^{t(n)}, f(y^{t(n)})\right)$ can be fixed, recall Question 2 from Exercise 3.