Modèles de calcul, fiche de TD numéro 3

Friday, October 15, 2004

# Boolean functions

### Question 0

An easy warm-up: show that any boolean function can be expressed using the boolean connectives AND, OR and NOT.

### Question 1

Show that the two connectives AND and NOT are sufficient.

### Question 2

The connectives NOR and NAND are defined by

$$\text{NOR}(x, y) = \neg(x \vee y)$$

and

$$\text{NAND}(x, y) = \neg(x \wedge y).$$

Can any boolean function be expressed using NOR only ? What about NAND ?

### Question 2

Are there other binary connectives which can express all boolean functions (without using the constant functions TRUE and FALSE)?

### Question 3

A boolean function is called *monotone* if it satisfies the following property: if an input is changed from FALSE to TRUE then the output cannot change from TRUE to FALSE (note that these functions should perhaps be called *monotone nondecreasing*).

Show that a function is monotone iff it can be expressed using only the AND and OR connectives, and the constant functions TRUE and FALSE.

# Boolean circuits

### Question 4

Design a circuit which computes the sum of two integers $x = \overline{x_{n-1} \cdots x_0}$ and $y = \overline{y_{n-1} \cdots x_0}$ written in binary, using the "naive" method. Evaluate its size and depth.

### Question 5

Let us assume that $n$ is a power 2. Design a circuit of smaller depth using the following recursive method: compute the two sums $\overline{y_{n-1} \cdots y_{n/2}} + \overline{x_{n-1} \cdots x_{n/2}}$ and $1 + \overline{y_{n-1} \cdots y_{n/2}} + \overline{x_{n-1} \cdots x_{n/2}}$. Select the correct result depending on the actual value of the carry.

Evaluate again the size and depth of your circuit.

### Question 6

Let $(C_n)$ be a circuit family of depth $O((\log n)^k)$ for some constant $k$. What can you say about the size of $(C_n)$ ?

NC$^k$ is the class of functions $f : \{0,1\}^* \to \{0,1\}^*$ that are computable by circuits of polynomial size and depth $O((\log n)^k)$. What have you just shown about the complexity of integer addition ?

### Question 7

Show that integer addition is in AC$^0$, i.e., that it can be computed by a circuit family of polynomial size and constant depth, made of NOT gates and of AND/OR gates of *unbounded fan-in*.

Hint: at stage $i$ the incoming carry $c_i$ is equal to 1 if a carry was generated at some stage $j < i$ and propagated all the way from $j$ to $i$.

What class of functions is obtained if we remove the polynomial size constraint from the definition of $AC^0$ ?

### Question 8

Let $s(C)$ be the size of a circuit $C$, and let $i(C)$ be the number of inputs (we recall that the size is defined as the number of gates, including input gates). Show that

$$s(C) \leq 3(s(C) - i(C))$$

if none of the input gates is an output gate. We conclude that counting the input gates does not make a big difference in the size of a circuit.

**Question 9**

One might also take the number $e(C)$ of edges (or "wires") into account in the definition of the size of a circuit. This would not make a big difference either since we have the inequality (prove it!)

$$s(C) - o(C) \leq e(C) \leq 2(s(C) - i(C)),$$

where $o(C)$ is the number of output gates.

**Question 10**

Show that $d(C) \leq s(C) - i(C)$ and $s(C) \leq o(C).(2^{d(C)+1} - 1)$ where $d(C)$ is the depth of $C$.

**Question 11**

In this question we allow identity gates in our circuits (gates with one input $x$ which output $I(x) = x$). Show that any boolean circuit $C$ is equivalent to a circuit $C'$ such that all gates have outdegree at most two and $s(C') \leq 3s(C)$. What can we say about the depth of $C'$ ?

**Question 12**

Let $C$ be a circuit of OR, AND and NOT gates, with $n$ inputs $x_1, \ldots, x_n$. Explain how $C$ can be transformed into an equivalent circuit $C'$ with OR/AND gates only, and inputs $x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n$. What is the effect of this transformation on the size and depth of the circuit?