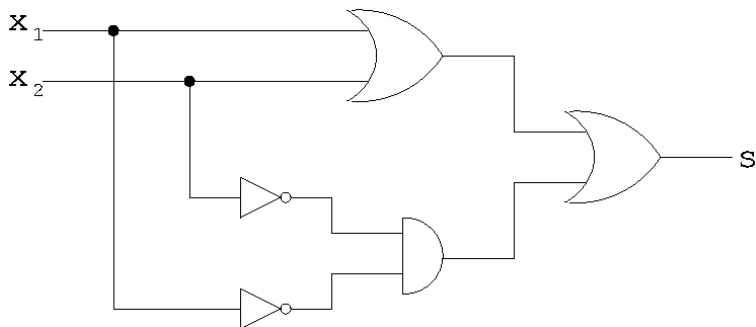


## Série 8

### 1 Que fait ce circuit?

a) On considère le circuit logique suivant:

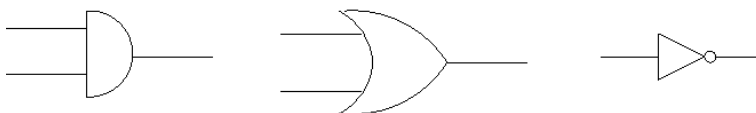


Ecrire la sortie  $s$  de ce circuit sous forme de proposition logique impliquant  $x_1$  et  $x_2$  et établir sa table de vérité:

$x_1$	$x_2$	$s$
0	0	
0	1	
1	0	
1	1	

### 2 Additionneur avec retenue en entrée

Au cours, vous avez vu comment réaliser, à l'aide des trois portes logiques ET, OU et NON suivantes:



un additionneur dont l'entrée soit 2 bits  $x_1$  et  $x_2$ , et dont la sortie soit 2 autres bits  $s$  et  $r$ , où

$$s = x_1 \oplus x_2 \quad \text{et} \quad r = \begin{cases} 1 & \text{si } x_1 = 1 \text{ et } x_2 = 1 \\ 0 & \text{sinon} \end{cases}$$

i.e.,  $s$  est l'addition modulo 2 des bits  $x_1$  et  $x_2$ , tandis que  $r$  est la retenue de cette addition (qui ne prend donc la valeur 1 que lorsque  $x_1 = 1$  et  $x_2 = 1$ ).

On vous demande de réaliser ici, à l'aide des mêmes portes ET, OU et NON, et de la porte additionnelle  $\oplus$ :



un additionneur complet dont l'entrée soit les 2 bits  $x_1$  et  $x_2$ , ainsi qu'une retenue  $r_1$  provenant d'une addition précédente, et dont la sortie soit 2 autres bits  $s$  et  $r_2$ , où

$$s = x_1 \oplus x_2 \oplus r_1 \quad \text{et} \quad r_2 = \begin{cases} 1 & \text{si } x_1 + x_2 + r_1 > 1 \\ 0 & \text{sinon} \end{cases}$$

*Indication:* Réécrivez tout d'abord les égalités ci-dessus à l'aide de symboles logiques.

### 3 Comparateur

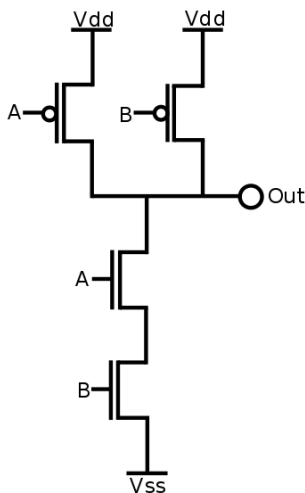
Réaliser un circuit logique avec les mêmes portes ET, OU et NON que ci-dessus, dont l'entrée soit 2 bits  $x_1$  et  $x_2$  et dont la sortie  $s$  soit le résultat du tableau de vérité ci-dessous:

$x_1$	$x_2$	$s$
0	0	1
0	1	1
1	0	0
1	1	1

Combien de portes logiques votre solution utilise-t-elle? Pouvez-vous minimiser ce nombre? (les places ont chères sur les microprocesseurs actuels!)

*Remarque:* Au vu de la table de vérité ci-dessus, la sortie de ce circuit est donc le résultat de la comparaison "est-ce que  $x_1 \leq x_2$ "? Mais notez que si on interprète 0=faux et 1=vrai, alors la sortie de ce circuit indique aussi si l'affirmation logique " $x_1$  implique  $x_2$ " (notée " $x_1 \implies x_2$ ") est vraie ou non.

### 4 Une porte logique construite avec des transistors



a)  $A$  et  $B$  sont les bits d'entrée de ce circuit. Quel est la sortie (Out) de celui-ci en fonction de  $A$  et  $B$ ?

*Remarque:* Sur le schéma ci-dessus, Vdd correspond une tension de 5V ("1") et Vss correspond à une tension de 0V ("0").

b) Montrer qu'on peut construire chacune des trois portes NON, ET et OU à l'aide de la porte logique ci-dessus.

## 5 Pour le plaisir: deviner deux nombres en une seule évaluation\*

Soient  $a_1, a_2 \in \{0, 1\}$  fixés ; considérons la fonction  $f : \{0, 1\}^2 \rightarrow \{0, 1\}$  définie par

$$f(x_1, x_2) = a_1 x_1 \oplus a_2 x_2, \quad x_1, x_2 \in \{0, 1\}$$

On aimerait apprendre les valeurs de  $a_1$  et  $a_2$  en effectuant un nombre minimum d'évaluations de la fonction  $f$ . Classiquement, ce problème se résout avec deux évaluations de  $f$ , à savoir  $f(1, 0) = a_1$  et  $f(0, 1) = a_2$ . Mais avec un algorithme quantique, une seule évaluation suffit!

Pour cela, on considère un système à deux qubits, initialement dans l'état  $|0\rangle \otimes |0\rangle$ <sup>1</sup>, aussi noté  $|0, 0\rangle$ . Puis on applique à chacun de ces qubits la transformation de Hadamard définie dans le cours:

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

pour obtenir ainsi l'état

$$H|0\rangle \otimes H|0\rangle = |+\rangle \otimes |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle)$$

Ensuite, on applique la porte oracle  $O_f$  à cet état, dont l'effet est le suivant:

$$O_f \left( \frac{1}{2} (|0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle) \right) = \frac{1}{2} \left( (-1)^{f(0,0)} |0, 0\rangle + (-1)^{f(0,1)} |0, 1\rangle + (-1)^{f(1,0)} |1, 0\rangle + (-1)^{f(1,1)} |1, 1\rangle \right)$$

Et finalement, on réapplique à chaque qubit la transformation de Hadamard vue précédemment.

A vous maintenant de montrer qu'en mesurant l'état de sortie des deux qubits (! long calcul !), il est possible de deviner la valeurs des deux nombres  $a_1$  et  $a_2$  (avec donc un seul appel à l'oracle  $O_f$ ).

---

<sup>1</sup>La notation  $|\phi\rangle \otimes |\psi\rangle$  est ce qu'on appelle formellement un *produit tensoriel*, mais pour les besoins du présent exercice, vous pouvez interpréter ça comme un simple produit.