Étant données deux formules logiques A et B, on note $A \leftrightarrow B$ la formule $(A \to B) \wedge (B \to A)$. On pourra utiliser sans restriction les 13 règles de la logique classique ainsi que la règle du tiers-exclus :

$$\frac{\Gamma, \neg B \vdash A \qquad \Gamma, B \vdash A}{\Gamma \vdash A}\ \text{te}$$

Exercice 1.

Prouver les séquents suivants :

1. $\vdash A \to A$
2. $A \to B, A \vee B \vdash B$
3. $A \to (B \to C), A \to B, A \vdash C$
4. $A \wedge B \vdash B \wedge A$
5. $A \vee B \vdash B \vee A$
6. $A \to \neg A \vdash \neg A$
7. $\neg A \to A \vdash A$
8. $A \to B, A \to \neg B \vdash \neg A$
9. $A \vee B, \neg B \vdash A$
10. $\neg A \vdash A \to B$.
11. $A \to B \vdash A \to (A \wedge B)$

Exercice 2.

Prouver les séquents suivants :

1. $\neg(A \to B) \vdash B \to A$
2. $A \to B \vdash (A \wedge C) \to (B \wedge C)$
3. $\neg B \to \neg A \vdash A \to B$
4. $A \to B \vdash \neg B \to \neg A$
5. $\vdash A \leftrightarrow A \vee (A \wedge B)$
6. $A \to (B \to C) \vdash B \to (A \to C)$
7. $\vdash (A \to B) \to \neg(A \wedge \neg B)$
8. $\vdash ((A \wedge B) \to C) \leftrightarrow (A \to C) \vee (B \to C)$
9. $A \vee B, \neg B \vee C \vdash A \vee C$
10. $\vdash (A \to B) \leftrightarrow (\neg A \vee B)$

Exercice 3. Admissibilité des règles pour la double négation

Montrer que les règles d'introduction et d'élimination de la double négation sont admissibles :

$$\frac{\Gamma \vdash A}{\Gamma \vdash \neg\neg A}\ \neg\neg_i \qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ \neg\neg_e$$

Exercice 4. Distributivité

Prouver les séquents suivants :

1. $\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$.
2. $\vdash A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$.

Exercice 5. Lois de De Morgan

Prouver les séquents suivants :

1. $\vdash \neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$
2. $\vdash \neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$

Exercice 6. Système LK

Dans cet exercice, on remplace les règles de la logique classique vues en cours par les règles du ***système LK*** listées ci-dessous. Dans le système LK, un séquent est noté $\Gamma \vdash \Delta$ où :

- ⋆ Γ et Δ sont des multi-ensembles, c'est à dire qu'ils peuvent contenir plusieurs fois la même formule.
- ⋆ L'interprétation intuitive de la phrase « $A_1, \ldots, A_n \vdash B_1, \ldots, B_n$ est prouvable » est :

$$A_1 \wedge \ldots \wedge A_n \qquad \text{permet de démontrer} \qquad B_1 \vee \ldots \vee B_n$$

Les éléments de Γ correspondent donc à une conjonction et ceux de Δ à une disjonction.

Axiomes :

$$\frac{}{\bot \vdash}\ \bot_g \qquad\qquad \frac{}{A \vdash A}\ \text{ax}$$

Règles structurelles :

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ \text{aff}_g \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\ \text{aff}_d \qquad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ \text{contr}_g \qquad \frac{\Gamma \vdash A, A, \Delta}{\Gamma \vdash A, \Delta}\ \text{contr}_d$$

Règles des connecteurs logiques :

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\ \wedge_g \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\ \wedge_d \qquad \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\ \vee_g \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\ \vee_d$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta}\ \to_g \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\ \to_d \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ \neg_g \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ \neg_d$$

Règle de coupure :

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ \text{coupure}$$

1. Prouver que $\bot'_g$ et ax' sont admissibles :

$$\frac{}{\Gamma, \bot \vdash \Delta}\ \bot'_g \qquad\qquad \frac{}{\Gamma, A \vdash A, \Delta}\ \text{ax}'$$

2. Prouver les séquents (vous pouvez utiliser ax' et $\bot'_g$) :

   (a) $\vdash A \to (B \to A)$
   (b) $\vdash \neg\neg A \to A$
   (c) $\vdash A \vee \neg A$
   (d) $\neg A \vee \neg B \vdash \neg(A \wedge B)$
   (e) $\neg(A \wedge B) \vdash \neg A \vee \neg B$
   (f) $\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$
   (g) $A \to B, A \to C, B \wedge C \to D \vdash A \to D$

Exercice 7. Circuits logiques [Centrale 2001 + École de l'air 2003]

Dans cet exercice, on appelle ***ensemble des booléens*** l'ensemble $\mathcal{B} = \{0, 1\}$. Les opérateurs $\neg$, $\wedge$ et $\vee$ sont assimilés à des fonctions. Ainsi :

$$\neg : \mathcal{B} \to \mathcal{B} \qquad\qquad \wedge : \mathcal{B}^2 \to \mathcal{B} \qquad\qquad \vee : \mathcal{B}^2 \to \mathcal{B}$$

Les opérateurs binaires $\wedge$ et $\vee$ sont des opérateurs infixes, c'est à dire qu'on écrira $b_1 \wedge b_2$ à la place de $\wedge(b_1, b_2)$. On écrira également $\neg b$ à la place de $\neg(b)$.

b	0	1
$\neg b$	1	0

Soit $k \in \mathbb{N}^*$. Étant données deux fonctions booléennes $g_1, g_2 : \mathcal{B}^k \to \mathcal{B}$, on note $(g_1 \wedge g_2)$ la fonction booléenne de $\mathcal{B}^k \to \mathcal{B}$ définie pour tout $b \in \mathcal{B}^k$ par $(g_1 \wedge g_2)(b) = g_1(b) \wedge g_2(b)$. De manière similaire, $\neg g_1$ et $g_1 \vee g_2$ désignent des fonctions de $\mathcal{B}^k \to \mathcal{B}$.

b_1	0	0	1	1
b_2	0	1	0	1
$b_1 \wedge b_2$	0	0	0	1
$b_1 \vee b_2$	0	1	1	1

Une ***fonction logique*** avec $k \in \mathbb{N}^*$ entrées et $n \in \mathbb{N}^*$ sorties est une application de $\mathcal{B}^k$ dans $\mathcal{B}^n$. Par exemple, $\neg$ est une fonction logique avec une entrée et une sortie, et $\wedge, \vee$ sont des fonctions logiques avec deux entrées et une sortie. Notre but est de représenter graphiquement les fonctions logiques. Pour cela, on dispose de quatre briques de base appelées les ***portes logiques*** :

→ La première porte s'appelle un ***duplicateur***. Elle comporte une entrée b et deux sorties s_1 et s_2 telles que $s_1 = s_2 = b$. Comme son nom l'indique, cette porte duplique son entrée.

→ La porte NON possède une entrée et une sortie. Elle représente la fonction $\neg$.

→ Les portes ET et OU possèdent deux entrées et une sortie. Elles représentent les fonctions $\wedge$ et $\vee$.

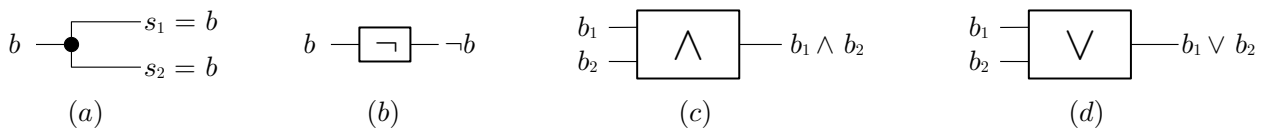
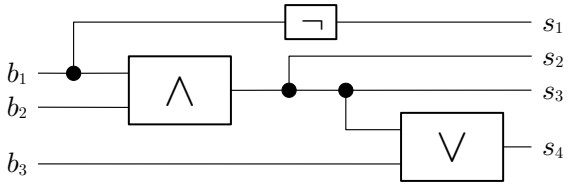


FIGURE 1 – (a) Un duplicateur – (b) La porte NON – (c) La porte ET – (d) La porte OU

Sur tous les schémas du sujet, les entrées des portes sont situées à gauche et les sorties à droite. Un ***circuit logique*** est un assemblage orienté de portes logiques. La sortie (resp. entrée) d'une porte peut être reliée à l'entrée (resp. sortie) d'une autre porte ou bien être une sortie (resp. entrée) globale du circuit. Un circuit est nécessairement acyclique ce qui signifie qu'en suivant l'orientation des portes (de gauche à droite), il n'existe pas de boucle dans le circuit. Par exemple, le circuit de la figure 2 représente la fonction :

$$f : \begin{cases} \mathcal{B}^3 \to \mathcal{B}^4 \\ (b_1, b_2, b_3) \mapsto (s_1, s_2, s_3, s_4) = (\neg b_1, b_1 \wedge b_2, b_1 \wedge b_2, (b_1 \wedge b_2) \vee b_3) \end{cases}$$



	s_1	s_2	s_3	s_4
b_1	2	3	4	5
b_2	×	2	3	4
b_3	×	×	×	1

FIGURE 2 – Un circuit logique de profondeur 5 avec 6 portes.

La ***profondeur*** d'un circuit est le nombre maximal de portes se trouvant entre une entrée et une sortie. Le tableau ci-dessus donne le nombre de portes entre chaque entrée et chaque sortie pour le circuit de la figure 2. Dans ce tableau une × signifie que l'entrée et la sortie en question ne sont pas reliées. La profondeur du circuit est donc égale à 5.

1. Donner un circuit représentant la fonction :

$$g : \begin{cases} \mathcal{B}^4 \to \mathcal{B}^3 \\ (b_1, b_2, b_3, b_4) \mapsto (s_1, s_2, s_3) = (b_1 \vee b_2, (b_1 \vee b_2) \wedge (b_3 \vee b_4), \neg(b_3 \vee b_4)) \end{cases}$$

Conjonction k-aire

Définissons deux circuits notés $\mathcal{C}_k$ et $\mathcal{D}_k$:

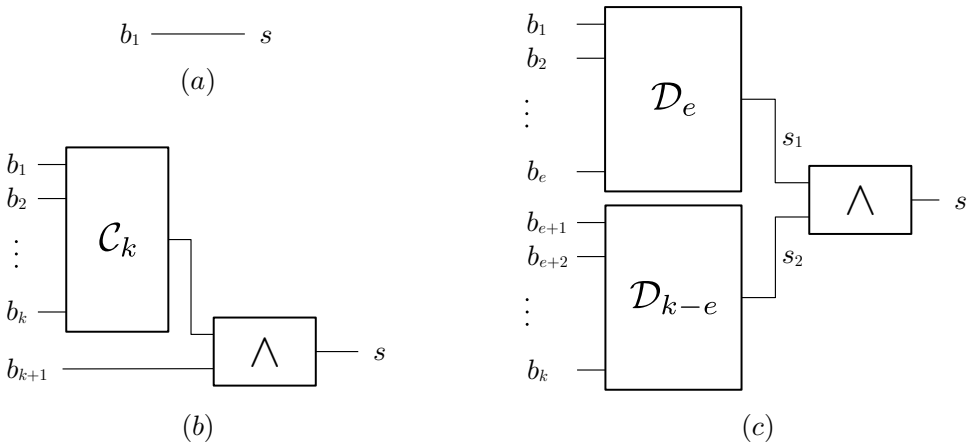


FIGURE 3 – (a) Le circuit $\mathcal{C}_1 = \mathcal{D}_1$
(b) Le circuit $\mathcal{C}_{k+1}$ pour $k \geqslant 1$
(c) Le circuit $\mathcal{D}_k$ pour $k \geqslant 2$ où on a posé $e = \lfloor k/2 \rfloor$

Le circuit $\mathcal{C}_k$ est défini récursivement :

- ⋆ $\mathcal{C}_1$ est le circuit sans porte qui renvoie directement son entrée.
- ⋆ Pour $k \geqslant 1$, $\mathcal{C}_{k+1}$ consiste à appliquer le circuit $\mathcal{C}_k$ aux k premières entrées, puis à appliquer une porte ET entre la sortie de $\mathcal{C}_k$ et la $(k+1)^{\text{ème}}$ entrée.

Le circuit $\mathcal{D}_k$ est construit à l'aide d'une stratégie de type diviser pour régner :

- ⋆ $\mathcal{D}_1$ est le circuit sans porte qui renvoie directement son entrée.
- ⋆ Pour construire $\mathcal{D}_k$ avec $k \geqslant 2$, on pose $e = \lfloor k/2 \rfloor$ puis :
  - On applique $\mathcal{D}_e$ aux e premières entrées pour obtenir une sortie s_1.
  - On applique $\mathcal{D}_{k-e}$ aux $(k-e)$ autres entrées pour obtenir une sortie s_2.
  - On applique une porte ET entre s_1 et s_2.

2. (a) Dessiner les circuits $\mathcal{C}_4$ et $\mathcal{D}_7$.
   (b) Montrer que les circuits $\mathcal{C}_k$ et $\mathcal{D}_k$ représentent la même fonction f_k que l'on précisera.
3. (a) Déterminer le nombre exact de portes logiques dans le circuit $\mathcal{C}_k$ ainsi que sa profondeur. Justifier.
   (b) Même question pour $\mathcal{D}_k$.

Universalité

Le but de cette partie est de montrer que toute fonction $f : \mathcal{B}^k \to \mathcal{B}^n$ peut être représentée par un circuit logique.

4. Quel est le nombre de fonctions $f : \mathcal{B}^k \to \mathcal{B}^n$?

On étudie d'abord le cas $n = 1$. Étant donnée une fonction $f : \mathcal{B}^k \to \mathcal{B}$, on appelle ***poids*** de f le nombre d'éléments $b \in \mathcal{B}^k$ tels que $f(b) = 1$. Par exemple, $\neg$ et $\wedge$ sont de poids 1 et $\vee$ est de poids 3.

5. (a) Montrer que toute fonction $f : \mathcal{B}^k \to \mathcal{B}$ de poids 0 est représentable par un circuit logique.
   (b) Soit $f : \mathcal{B}^k \to \mathcal{B}$ une fonction de poids 1. Construire un circuit représentant f.
   (c) Soit $f : \mathcal{B}^k \to \mathcal{B}$ une fonction logique de poids quelconque. À l'aide des questions précédentes, construire un circuit représentant f.
6. Monter que toute fonction $f : \mathcal{B}^k \to \mathcal{B}^n$ peut être représentée par un circuit logique.

Calcul du reste modulo 3

Soit $k \in \mathbb{N}^*$. Dans cette partie, tout entier $N \in [\![0, 2^k - 1]\!]$ est représenté par la suite de ses bits dans son écriture en base 2. Ainsi, le k-uplet $a = (a_0, a_1, \ldots, a_{k-1}) \in \mathcal{B}^k$ représente l'entier $A = \sum_{i=0}^{k-1} a_i 2^i$. On souhaite concevoir un circuit dont les k entrées sont $a_0, a_1, \ldots, a_{k-1}$ et dont les deux sorties représentent le reste de A modulo 3.

7. Soit $A = \sum_{i=0}^{k-1} a_i 2^i$ un entier. Montrer que A est égal modulo 3 à $B = \sum_{i=0}^{k-1} (-1)^i a_i$.
8. Concevoir un circuit $\mathcal{M}_1$ disposant de deux entrée a_0 et a_1, deux sorties s_0 et s_1, et tel que $a_0 - a_1$ soit égal à $s_0 + 2s_1$ modulo 3 (c'est-à-dire que le nombre $s_1 s_0$ est, en base 2, le reste modulo 3 de $a_1 a_0$).
9. Concevoir un circuit logique, noté $\mathcal{E}$, disposant de quatre entrées a_0, a_1, b_0, b_1 et de deux sorties s_0, s_1, tel que $S = s_0 + 2s_1$ soit congru modulo 3 à $A + B$, en notant $A = a_0 + 2a_1$ et $B = b_0 + 2b_1$. On pourra se contenter ici de donner des formules logiques qui expriment s_0 et s_1 en fonction de a_0, a_1, b_0, b_1, sans dessiner le circuit $\mathcal{E}$.
10. Supposons disposer d'un circuit $\mathcal{M}_n$ à 2^n entrées $a_0, \ldots, a_{2n-1}$ et deux sorties s_0, s_1 tel que $S = s_0 + 2s_1$ soit congru à $A = \sum_{k=0}^{2^n-1} a_k 2^k$ modulo 3. À l'aide de $\mathcal{M}_n$ et $\mathcal{E}$, concevoir un circuit $\mathcal{M}_{n+1}$ qui résout le problème pour un nombre à 2^{n+1} bits en entrée.
11. Déterminer un équivalent lorsque n tend vers $+\infty$ du nombre de portes utilisées dans le circuit $\mathcal{M}_n$, en fonction de n et du nombre a de portes utilisées dans le circuit $\mathcal{E}$.