# Exercice 1.

**Question 1 –** $\vdash A \to A$

$$\dfrac{\dfrac{}{A \vdash A}\ \text{ax}}{\vdash A \to A}\ \to_i$$

**Question 2 –** $A \to B, A \vee B \vdash B$

$$\dfrac{\dfrac{}{A \to B, A \vee B \vdash A \vee B}\ \text{ax} \qquad \dfrac{\dfrac{}{\Gamma \vdash A \to B}\ \text{ax} \qquad \dfrac{}{\Gamma \vdash A}\ \text{ax}}{\Gamma \vdash B}\ \to_e \qquad \dfrac{}{A \to B, A \vee B, B \vdash B}\ \text{ax}}{A \to B, A \vee B \vdash B}\ \vee_e$$

où :

$$\Gamma = \{A \to B, A \vee B, A\}$$

**Question 3 –** $A \to (B \to C), A \to B, A \vdash C$

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A \to (B \to C)}\ \text{ax} \qquad \dfrac{}{\Gamma \vdash A}\ \text{ax}}{\Gamma \vdash B \to C}\ \to_e \qquad \dfrac{\dfrac{}{\Gamma \vdash A \to B}\ \text{ax} \qquad \dfrac{}{\Gamma \vdash A}\ \text{ax}}{\Gamma \vdash B}\ \to_e}{\Gamma \vdash C}\ \to_e$$

où :

$$\Gamma = \{A \to (B \to C), A \to B, A\}$$

**Question 4 –** $A \wedge B \vdash B \wedge A$

$$\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\ \text{ax}}{A \wedge B \vdash B}\ \wedge_e^d \qquad \dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\ \text{ax}}{A \wedge B \vdash A}\ \wedge_e^g}{A \wedge B \vdash B \wedge A}\ \wedge_i$$

**Question 5 –** $A \vee B \vdash B \vee A$

$$\dfrac{\dfrac{}{A \vee B \vdash A \vee B}\ \text{ax} \qquad \dfrac{\dfrac{}{A \vee B, A \vdash A}\ \text{ax}}{A \vee B, A \vdash B \vee A}\ \vee_i^d \qquad \dfrac{\dfrac{}{A \vee B, B \vdash B}\ \text{ax}}{A \vee B, B \vdash B \vee A}\ \vee_i^g}{A \vee B \vdash B \vee A}\ \vee_e$$

**Question 6 –** $A \to \neg A \vdash \neg A$

$$\dfrac{\dfrac{\dfrac{}{A \to \neg A, A \vdash A}\ \text{ax} \qquad \dfrac{\dfrac{}{A \to \neg A, A \vdash A \to \neg A}\ \text{ax} \qquad \dfrac{}{A \to \neg A, A \vdash A}\ \text{ax}}{A \to \neg A, A \vdash \neg A}\ \to_e}{A \to \neg A, A \vdash \bot}\ \neg_e}{A \to \neg A \vdash \neg A}\ \neg_i$$

**Question 7 –** $\neg A \to A \vdash A$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg A \to A, \neg A \vdash \neg A \to A}\,\text{ax} \qquad \dfrac{}{\neg A \to A, \neg A \vdash \neg A}\,\text{ax}}{\neg A \to A, \neg A \vdash A}\,\to_e \qquad \dfrac{}{\neg A \to A, \neg A \vdash \neg A}\,\text{ax}}{\neg A \to A, \neg A \vdash \bot}\,\neg_e}{\neg A \to A \vdash A}\,\bot_c$$

**Question 8 –** $A \to B, A \to \neg B \vdash \neg A$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A}\,\text{ax} \qquad \dfrac{}{\Gamma \vdash A \to B}\,\text{ax}}{\Gamma \vdash B}\,\to_e \qquad \dfrac{\dfrac{}{\Gamma \vdash A}\,\text{ax} \qquad \dfrac{}{\Gamma \vdash A \to \neg B}\,\text{ax}}{\Gamma \vdash \neg B}\,\to_e}{\Gamma \vdash \bot}\,\neg_e}{A \to B, A \to \neg B \vdash \neg A}\,\neg_i$$

où :

$$\Gamma = \{A \to B, A \to \neg B, A\}$$

**Question 9 –** $A \vee B, \neg B \vdash A$

$$\dfrac{\dfrac{}{A \vee B, \neg B \vdash A \vee B}\,\text{ax} \qquad \dfrac{}{A \vee B, \neg B, A \vdash A}\,\text{ax} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma, \neg A \vdash B}\,\text{ax} \qquad \dfrac{}{\Gamma, \neg A \vdash \neg B}\,\text{ax}}{\Gamma, \neg A \vdash \bot}\,\neg_e}{\Gamma \vdash A}\,\bot_c}{A \vee B, \neg B \vdash A}\,\vee_e$$

où :

$$\Gamma = \{A \vee B, \neg B, B\}$$

**Question 10 –** $\neg A \vdash A \to B$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A}\,\text{ax} \qquad \dfrac{}{\Gamma \vdash \neg A}\,\text{ax}}{\Gamma \vdash \bot}\,\neg_e}{\neg A, A \vdash B}\,\bot_c}{\neg A \vdash A \to B}\,\to_i$$

où :

$$\Gamma = \{\neg A, A, \neg B\}$$

**Question 11 –** $A \to B \vdash A \to (A \wedge B)$

$$\dfrac{\dfrac{\dfrac{}{A \to B, A \vdash A}\,\text{ax} \qquad \dfrac{\dfrac{}{A \to B, A \vdash A}\,\text{ax} \qquad \dfrac{}{A \to B, A \vdash A \to B}\,\text{ax}}{A \to B, A \vdash B}\,\to_e}{A \to B, A \vdash A \wedge B}\,\wedge_i}{A \to B \vdash A \to (A \wedge B)}\,\to_i$$

# Exercice 2.

**Question 1** – $\neg(A \to B) \vdash B \to A$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \neg A, A \vdash B}\,\text{ax}}{\Gamma, \neg A \vdash A \to B}\,\to_i \qquad \dfrac{}{\Gamma, \neg A \vdash \neg(A \to B)}\,\text{ax}}{\Gamma, \neg A \vdash \bot}\,\neg_e}{\Gamma \vdash A}\,\bot_c}{\neg(A \to B) \vdash B \to A}\,\to_i$$

où :

$$\Gamma = \{\neg(A \to B), B\}$$

**Question 2** – $A \to B \vdash (A \wedge C) \to (B \wedge C)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A \to B}\,\text{ax} \qquad \dfrac{\dfrac{}{\Gamma \vdash A \wedge C}\,\text{ax}}{\Gamma \vdash A}\,\wedge_e^g}{\Gamma \vdash B}\,\to_e \qquad \dfrac{\dfrac{}{\Gamma \vdash A \wedge C}\,\text{ax}}{\Gamma \vdash C}\,\wedge_e^d}{\Gamma \vdash B \wedge C}\,\wedge_i}{A \to B \vdash (A \wedge C) \to (B \wedge C)}\,\to_i$$

où :

$$\Gamma = \{A \to B, A \wedge C\}$$

**Question 3** – $\neg B \to \neg A \vdash A \to B$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A}\,\text{ax} \qquad \dfrac{\dfrac{}{\Gamma \vdash \neg B \to \neg A}\,\text{ax} \qquad \dfrac{}{\Gamma \vdash \neg B}\,\text{ax}}{\Gamma \vdash \neg A}\,\to_e}{\Gamma \vdash \bot}\,\neg_e}{\neg B \to \neg A, A \vdash B}\,\bot_c}{\neg B \to \neg A \vdash A \to B}\,\to_i$$

où :

$$\Gamma = \{\neg B \to \neg A, A, \neg B\}$$

**Question 4** – $A \to B \vdash \neg B \to \neg A$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A \to B}\,\text{ax} \qquad \dfrac{}{\Gamma \vdash A}\,\text{ax}}{\Gamma \vdash B}\,\to_e \qquad \dfrac{}{\Gamma \vdash \neg B}\,\text{ax}}{\Gamma \vdash \bot}\,\neg_e}{A \to B, \neg B \vdash \neg A}\,\neg_i}{A \to B \vdash \neg B \to \neg A}\,\to_i$$

où :

$$\Gamma = \{A \to B, \neg B, A\}$$

**Question 5 –** $\vdash A \leftrightarrow A \vee (A \wedge B)$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$A \vdash A$}
\RightLabel{$\vee_i^g$}
\UnaryInfC{$A \vdash A \vee (A \wedge B)$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash A \rightarrow A \vee (A \wedge B)$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$A \vee (A \wedge B) \vdash A \vee (A \wedge B)$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$A \vee (A \wedge B), A \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash A \wedge B$}
\RightLabel{$\wedge_e^g$}
\UnaryInfC{$\Gamma \vdash A$}
\RightLabel{$\vee_e$}
\TrinaryInfC{$A \vee (A \wedge B) \vdash A$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash A \vee (A \wedge B) \rightarrow A$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\vdash A \leftrightarrow A \vee (A \wedge B)$}
\end{prooftree}
$$

avec :

$$\Gamma = \{A \vee (A \wedge B), A \wedge B\}$$

**Question 6 –** $A \rightarrow (B \rightarrow C) \vdash B \rightarrow (A \rightarrow C)$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash A \rightarrow (B \rightarrow C)$}
\RightLabel{$\rightarrow_e$}
\BinaryInfC{$\Gamma \vdash B \rightarrow C$}
\RightLabel{$\rightarrow_e$}
\BinaryInfC{$\Gamma \vdash C$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$A \rightarrow (B \rightarrow C), B \vdash A \rightarrow C$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$A \rightarrow (B \rightarrow C) \vdash B \rightarrow (A \rightarrow C)$}
\end{prooftree}
$$

où :

$$\Gamma = \{A \rightarrow (B \rightarrow C), B, A\}$$

**Question 7 –** $\vdash (A \rightarrow B) \rightarrow \neg(A \wedge \neg B)$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash A \rightarrow B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash A \wedge \neg B$}
\RightLabel{$\wedge_e^g$}
\UnaryInfC{$\Gamma \vdash A$}
\RightLabel{$\rightarrow_e$}
\BinaryInfC{$\Gamma \vdash B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash A \wedge \neg B$}
\RightLabel{$\wedge_e^d$}
\UnaryInfC{$\Gamma \vdash \neg B$}
\RightLabel{$\neg_e$}
\BinaryInfC{$\Gamma \vdash \bot$}
\RightLabel{$\neg_i$}
\UnaryInfC{$A \rightarrow B \vdash \neg(A \wedge \neg B)$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash (A \rightarrow B) \rightarrow \neg(A \wedge \neg B)$}
\end{prooftree}
$$

où :

$$\Gamma = \{A \rightarrow B, A \wedge \neg B\}$$

**Question 8 –** $\vdash ((A \wedge B) \rightarrow C) \leftrightarrow (A \rightarrow C) \vee (B \rightarrow C)$

$$
\begin{prooftree}
\AxiomC{$\mathcal{A}_1$}
\UnaryInfC{$\Gamma_1 \vdash (A \rightarrow C) \vee (B \rightarrow C)$}
\AxiomC{$\mathcal{A}_2$}
\UnaryInfC{$\Gamma_2 \vdash (A \rightarrow C) \vee (B \rightarrow C)$}
\RightLabel{te}
\BinaryInfC{$(A \wedge B) \rightarrow C \vdash (A \rightarrow C) \vee (B \rightarrow C)$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash ((A \wedge B) \rightarrow C) \rightarrow (A \rightarrow C) \vee (B \rightarrow C)$}
\AxiomC{$\mathcal{A}_3$}
\UnaryInfC{$\Gamma_3 \vdash C$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$(A \rightarrow C) \vee (B \rightarrow C) \vdash (A \wedge B) \rightarrow C$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash (A \rightarrow C) \vee (B \rightarrow C) \rightarrow ((A \wedge B) \rightarrow C)$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\vdash ((A \wedge B) \rightarrow C) \leftrightarrow (A \rightarrow C) \vee (B \rightarrow C)$}
\end{prooftree}
$$

avec :

$$
\begin{aligned}
\Gamma_1 &= \{(A \wedge B) \rightarrow C, A\} \\
\Gamma_2 &= \{(A \wedge B) \rightarrow C, \neg A\} \\
\Gamma_3 &= \{(A \rightarrow C) \vee (B \rightarrow C), A \wedge B\}
\end{aligned}
$$

L'arbre $\mathcal{A}_1$ est :

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, B \vdash (A \wedge B) \to C$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, B \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, B \vdash B$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\Gamma_1, B \vdash A \wedge B$}
\RightLabel{$\to_e$}
\BinaryInfC{$\Gamma_1, B \vdash C$}
\RightLabel{$\to_i$}
\UnaryInfC{$\Gamma_1 \vdash B \to C$}
\RightLabel{$\vee_i^d$}
\UnaryInfC{$\Gamma_1 \vdash (A \to C) \vee (B \to C)$}
\end{prooftree}
$$

L'arbre $\mathcal{A}_2$ est :

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2, A, \neg C \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2, A, \neg C \vdash \neg A$}
\RightLabel{$\neg_e$}
\BinaryInfC{$\Gamma_2, A, \neg C \vdash \bot$}
\RightLabel{$\bot_c$}
\UnaryInfC{$\Gamma_2, A \vdash C$}
\RightLabel{$\to_i$}
\UnaryInfC{$\Gamma_2 \vdash A \to C$}
\RightLabel{$\vee_i^g$}
\UnaryInfC{$\Gamma_2 \vdash (A \to C) \vee (B \to C)$}
\end{prooftree}
$$

L'arbre $\mathcal{A}_3$ est :

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_3 \vdash (A \to C) \vee (B \to C)$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_3, A \to C \vdash A \to C$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_3, A \to C \vdash A \wedge B$}
\RightLabel{$\wedge_e^g$}
\UnaryInfC{$\Gamma_3, A \to C \vdash A$}
\RightLabel{$\to_e$}
\BinaryInfC{$\Gamma_3, A \to C \vdash C$}
\AxiomC{\fbox{Similaire à l'arbre de preuve de $\Gamma_3, A \to C \vdash C$}}
\UnaryInfC{$\Gamma_3, B \to C \vdash C$}
\RightLabel{$\vee_e$}
\TrinaryInfC{$\Gamma_3 \vdash C$}
\end{prooftree}
$$

**Question 9 –** $A \vee B, \neg B \vee C \vdash A \vee C$

$$
\begin{prooftree}
\AxiomC{$\mathcal{A}$}
\UnaryInfC{$A \vee B, \neg B \vee C, B \vdash A \vee C$}
\AxiomC{\fbox{Similaire à $\mathcal{A}$}}
\UnaryInfC{$A \vee B, \neg B \vee C, \neg B \vdash A \vee C$}
\RightLabel{te}
\BinaryInfC{$A \vee B, \neg B \vee C \vdash A \vee C$}
\end{prooftree}
$$

L'arbre $\mathcal{A}$ est :

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma \vdash \neg B \vee C$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma, \neg B, \neg C \vdash B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma, \neg B, \neg C \vdash \neg B$}
\RightLabel{$\neg_e$}
\BinaryInfC{$\Gamma, \neg B, \neg C \vdash \bot$}
\RightLabel{$\bot_c$}
\UnaryInfC{$\Gamma, \neg B \vdash C$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma, C \vdash C$}
\RightLabel{$\vee_e$}
\TrinaryInfC{$\Gamma \vdash C$}
\RightLabel{$\vee_i^d$}
\UnaryInfC{$\Gamma \vdash A \vee C$}
\end{prooftree}
$$

où :

$$\Gamma = \{A \vee B, \neg B \vee C, B\}$$

**Question 10 –** $\vdash (A \to B) \leftrightarrow (\neg A \vee B)$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1 \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1 \vdash A \to B$}
\RightLabel{$\to_e$}
\BinaryInfC{$\Gamma_1 \vdash B$}
\RightLabel{$\vee_i^d$}
\UnaryInfC{$\Gamma_1 \vdash \neg A \vee B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$A \to B, \neg A \vdash \neg A$}
\RightLabel{$\vee_i^g$}
\UnaryInfC{$A \to B, \neg A \vdash \neg A \vee B$}
\RightLabel{te}
\BinaryInfC{$A \to B \vdash \neg A \vee B$}
\RightLabel{$\to_i$}
\UnaryInfC{$\vdash (A \to B) \to (\neg A \vee B)$}
\AxiomC{$\mathcal{A}_2$}
\UnaryInfC{$\Gamma_2 \vdash B$}
\RightLabel{$\to_i$}
\UnaryInfC{$\neg A \vee B \vdash A \to B$}
\RightLabel{$\to_i$}
\UnaryInfC{$\vdash (\neg A \vee B) \to (A \to B)$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\vdash (A \to B) \leftrightarrow (\neg A \vee B)$}
\end{prooftree}
$$

où :

$$\Gamma_1 = \{A \to B, A\}$$
$$\Gamma_2 = \{\neg A \lor B, A\}$$

L'arbre $\mathcal{A}_2$ est :

$$\dfrac{\dfrac{}{\Gamma_2 \vdash \neg A \lor B}\,\text{ax} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma_2, \neg A, \neg B \vdash \neg A}\,\text{ax} \quad \dfrac{}{\Gamma_2, \neg A, \neg B \vdash A}\,\text{ax}}{\Gamma_2, \neg A, \neg B \vdash \bot}\,\neg_e}{\Gamma_2, \neg A \vdash B}\,\bot_c \qquad \dfrac{}{\Gamma_2, B \vdash B}\,\text{ax}}{\Gamma_2 \vdash B}\,\lor_e$$

## Exercice 3. Admissibilité des règles pour la double négation

$\star$ Pour la règle d'introduction, on suppose disposer d'un arbre de preuve $\mathcal{A}$ pour $\Gamma \vdash A$ et on construit un arbre de preuve pour $\Gamma \vdash \neg\neg A$ :

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathcal{A}}{\Gamma \vdash A}}{\Gamma, \neg A \vdash A}\,\text{aff} \quad \dfrac{}{\Gamma, \neg A \vdash \neg A}\,\text{ax}}{\Gamma, \neg A \vdash \bot}\,\neg_e}{\Gamma \vdash \neg\neg A}\,\neg_i$$

$\star$ Pour la règle d'élimination, on suppose disposer d'un arbre de preuve $\mathcal{A}$ pour $\Gamma \vdash \neg\neg A$ et on construit un arbre de preuve pour $\Gamma \vdash A$ :

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \neg A \vdash \neg A}\,\text{ax} \quad \dfrac{\mathcal{A}}{\Gamma, \neg A \vdash \neg\neg A}}{\Gamma, \neg A \vdash \bot}\,\neg_e}{\Gamma \vdash A}\,\bot_c$$

## Exercice 4. Distributivité

**Question 1 –** $\vdash A \land (B \lor C) \leftrightarrow (A \land B) \lor (A \land C)$.

$$\dfrac{\dfrac{\dfrac{\mathcal{A}_1}{\Gamma_1 \vdash (A \land B) \lor (A \land C)}}{\vdash A \land (B \lor C) \to (A \land B) \lor (A \land C)}\,\to_i \qquad \dfrac{\dfrac{\dfrac{\mathcal{A}_2}{\Gamma_2 \vdash A} \quad \dfrac{\mathcal{A}_3}{\Gamma_2 \vdash B \lor C}}{\Gamma_2 \vdash A \land (B \lor C)}\,\land_i}{\vdash (A \land B) \lor (A \land C) \to A \land (B \lor C)}\,\to_i}{\vdash A \land (B \lor C) \leftrightarrow (A \land B) \lor (A \land C)}\,\land_i$$

Où :

$$\Gamma_1 = \{A \land (B \lor C)\}$$
$$\Gamma_2 = \{(A \land B) \lor (A \land C)\}$$

Où $\mathcal{A}_1$ est l'arbre :

$$\dfrac{\dfrac{\dfrac{}{\Gamma_1 \vdash A \land (B \lor C)}\,\text{ax}}{\Gamma_1 \vdash B \lor C}\,\land_e^d \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_1, B \vdash A \land (B \lor C)}\,\text{ax}}{\Gamma_1, B \vdash A}\,\land_e^g \quad \dfrac{}{\Gamma_1, B \vdash B}\,\text{ax}}{\Gamma_1, B \vdash A \land B}\,\land_i}{\Gamma_1, B \vdash (A \land B) \lor (A \land C)}\,\lor_i^g \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_1, C \vdash A \land (B \lor C)}\,\text{ax}}{\Gamma_1, C \vdash A}\,\land_e^d \quad \dfrac{}{\Gamma_1, C \vdash C}\,\text{ax}}{\Gamma_1, C \vdash A \land C}\,\land_i}{\Gamma_1, C \vdash (A \land B) \lor (A \land C)}\,\lor_i^d}{\Gamma_1 \vdash (A \land B) \lor (A \land C)}\,\lor_e$$

Où $\mathcal{A}_2$ est l'arbre :

$$\dfrac{\dfrac{}{\Gamma_2 \vdash (A\wedge B)\vee(A\wedge C)}\,\mathrm{ax} \qquad \dfrac{\dfrac{}{\Gamma_2, A\wedge B \vdash A\wedge B}\,\mathrm{ax}}{\Gamma_2, A\wedge B\vdash A}\,\wedge_e^g \qquad \dfrac{\dfrac{}{\Gamma_2, A\wedge B\vdash A\wedge C}\,\mathrm{ax}}{\Gamma_2, A\wedge C\vdash A}\,\wedge_e^g}{\Gamma_2\vdash A}\,\vee_e$$

Où $\mathcal{A}_3$ est l'arbre :

$$\dfrac{\dfrac{}{\Gamma_2 \vdash (A\wedge B)\vee(A\wedge C)}\,\mathrm{ax} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma_2, A\wedge B \vdash A\wedge B}\,\mathrm{ax}}{\Gamma_2, A\wedge B\vdash B}\,\wedge_e^d}{\Gamma_2, A\wedge B\vdash B\vee C}\,\vee_i^g \qquad \dfrac{\dfrac{\dfrac{}{\Gamma_2, A\wedge B\vdash A\wedge C}\,\mathrm{ax}}{\Gamma_2, A\wedge C\vdash C}\,\wedge_e^d}{\Gamma_2, A\wedge C\vdash B\vee C}\,\vee_i^d}{\Gamma_2\vdash B\vee C}\,\vee_e$$

**Question 2 –** $\vdash A\vee(B\wedge C)\leftrightarrow(A\vee B)\wedge(A\vee C)$.

$$\dfrac{\dfrac{\dfrac{\mathcal{A}_1}{\Gamma_1\vdash (A\vee B)\wedge(A\vee C)}}{\vdash A\vee(B\wedge C)\rightarrow(A\vee B)\wedge(A\vee C)}\,\rightarrow_i \qquad \dfrac{\dfrac{\mathcal{A}_2}{\Gamma_2\vdash A\vee(B\wedge C)}}{\vdash (A\vee B)\wedge(A\vee C)\rightarrow A\vee(B\wedge C)}\,\rightarrow_i}{\vdash A\vee(B\wedge C)\leftrightarrow(A\vee B)\wedge(A\vee C)}\,\wedge_i$$

où :

$$\Gamma_1 = \{A\vee(B\wedge C)\}$$
$$\Gamma_2 = \{(A\vee B)\wedge(A\vee C)\}$$

Où $\mathcal{A}_1$ est l'arbre :

$$\dfrac{\dfrac{\dfrac{}{\Gamma_1\vdash A\vee(B\wedge C)}\,\mathrm{ax} \qquad \dfrac{\dfrac{}{\Gamma_1, A\vdash A}\,\mathrm{ax}}{\Gamma_1, A\vdash A\vee B}\,\vee_i^g \qquad \dfrac{\dfrac{\dfrac{}{\Gamma_1, B\wedge C\vdash B\wedge C}\,\mathrm{ax}}{\Gamma_1, B\wedge C\vdash B}\,\wedge_e^g}{\Gamma_1, B\wedge C\vdash A\vee B}\,\vee_i^d}{\Gamma_1\vdash A\vee B}\,\vee_e \qquad \dfrac{\boxed{\text{Similaire à l'arbre de preuve de } \Gamma_1\vdash A\vee B}}{\Gamma_1\vdash A\vee C}}{\Gamma_1\vdash (A\vee B)\wedge(A\vee C)}\,\wedge_i$$

Où $\mathcal{A}_2$ est l'arbre :

$$\dfrac{\dfrac{\dfrac{}{\Gamma_2\vdash (A\vee B)\wedge(A\vee C)}\,\mathrm{ax}}{\Gamma_2\vdash A\vee B}\,\wedge_e^g \qquad \dfrac{\dfrac{}{\Gamma_2, A\vdash A}\,\mathrm{ax}}{\Gamma_2, A\vdash A\vee(B\wedge C)}\,\vee_i^g \qquad \dfrac{\mathcal{A}_3}{\Gamma_2, B\vdash A\vee(B\wedge C)}}{\Gamma_2\vdash A\vee(B\wedge C)}\,\vee_e$$

Où $\mathcal{A}_3$ est l'arbre :

$$\dfrac{\dfrac{\dfrac{}{\Gamma_2, B\vdash (A\vee B)\wedge(A\vee C)}\,\mathrm{ax}}{\Gamma_2, B\vdash A\vee C}\,\wedge_e^d \qquad \dfrac{\dfrac{}{\Gamma_2, B, A\vdash A}\,\mathrm{ax}}{\Gamma_2, B, A\vdash A\vee(B\wedge C)}\,\vee_i^g \qquad \dfrac{\dfrac{\dfrac{}{\Gamma_2, B, C\vdash B}\,\mathrm{ax} \quad \dfrac{}{\Gamma_2, B, C\vdash C}\,\mathrm{ax}}{\Gamma_2, B, C\vdash B\wedge C}\,\wedge_i}{\Gamma_2, B, C\vdash A\vee(B\wedge C)}\,\vee_i^d}{\Gamma_2, B\vdash A\vee(B\wedge C)}\,\vee_e$$

## Exercice 5. Lois de De Morgan.

**Question 1** – $\vdash \neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, A \vdash A$}
\RightLabel{$\vee_i^g$}
\UnaryInfC{$\Gamma_1, A \vdash A \vee B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, A \vdash \neg(A \vee B)$}
\RightLabel{$\neg_e$}
\BinaryInfC{$\Gamma_1, A \vdash \bot$}
\RightLabel{$\neg_i$}
\UnaryInfC{$\Gamma_1 \vdash \neg A$}
\AxiomC{$\boxed{\begin{array}{c}\text{Similaire à}\\ \text{l'arbre de}\\ \text{preuve de}\\ \Gamma_1 \vdash \neg A\end{array}}$}
\UnaryInfC{$\Gamma_1 \vdash \neg B$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\Gamma_1 \vdash \neg A \wedge \neg B$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash \neg(A \vee B) \rightarrow \neg A \wedge \neg B$}
\AxiomC{$\mathcal{A}$}
\UnaryInfC{$\Gamma_2 \vdash \bot$}
\RightLabel{$\neg_i$}
\UnaryInfC{$\neg A \wedge \neg B \vdash \neg(A \vee B)$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash \neg A \wedge \neg B \rightarrow \neg(A \vee B)$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\vdash \neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$}
\end{prooftree}
$$

où :

$$
\begin{aligned}
\Gamma_1 &= \{\neg(A \vee B)\} \\
\Gamma_2 &= \{\neg A \wedge \neg B, A \vee B\}
\end{aligned}
$$

L'arbre $\mathcal{A}$ est :

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2 \vdash A \vee B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2, A \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2, A \vdash \neg A \wedge \neg B$}
\RightLabel{$\wedge_e^g$}
\UnaryInfC{$\Gamma_2, A \vdash \neg A$}
\RightLabel{$\neg_e$}
\BinaryInfC{$\Gamma_2, A \vdash \bot$}
\AxiomC{$\boxed{\begin{array}{c}\text{Similaire à}\\ \text{l'arbre de}\\ \text{preuve de}\\ \Gamma_2, A \vdash \bot\end{array}}$}
\UnaryInfC{$\Gamma_2, B \vdash \bot$}
\RightLabel{$\vee_e$}
\TrinaryInfC{$\Gamma_2 \vdash \bot$}
\end{prooftree}
$$

**Question 2** – $\vdash \neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$

$$
\begin{prooftree}
\AxiomC{$\mathcal{A}_2$}
\UnaryInfC{$\Gamma_1 \vdash \neg A \vee \neg B$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash \neg(A \wedge B) \rightarrow \neg A \vee \neg B$}
\AxiomC{$\mathcal{A}_1$}
\UnaryInfC{$\Gamma_2 \vdash \bot$}
\RightLabel{$\neg_i$}
\UnaryInfC{$\neg A \vee \neg B \vdash \neg(A \wedge B)$}
\RightLabel{$\rightarrow_i$}
\UnaryInfC{$\vdash \neg A \vee \neg B \rightarrow \neg(A \wedge B)$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\vdash \neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$}
\end{prooftree}
$$

où :

$$
\begin{aligned}
\Gamma_1 &= \{\neg(A \wedge B)\} \\
\Gamma_2 &= \{\neg A \vee \neg B, A \wedge B\}
\end{aligned}
$$

$\mathcal{A}_1$ est l'arbre :

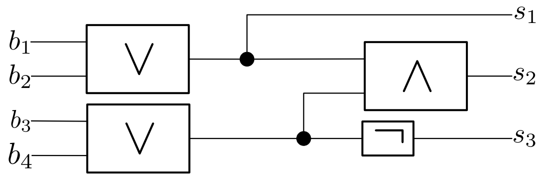
$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2 \vdash \neg A \vee \neg B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2, \neg A \vdash A \wedge B$}
\RightLabel{$\wedge_e^g$}
\UnaryInfC{$\Gamma_2, \neg A \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_2, \neg A \vdash \neg A$}
\RightLabel{$\neg_e$}
\BinaryInfC{$\Gamma_2, \neg A \vdash \bot$}
\AxiomC{$\boxed{\begin{array}{c}\text{Similaire à}\\ \text{l'arbre de}\\ \text{preuve de}\\ \Gamma_2, \neg A \vdash \bot\end{array}}$}
\UnaryInfC{$\Gamma_2, \neg B \vdash \bot$}
\RightLabel{$\vee_e$}
\TrinaryInfC{$\Gamma_2 \vdash \bot$}
\end{prooftree}
$$

$\mathcal{A}_2$ est l'arbre :

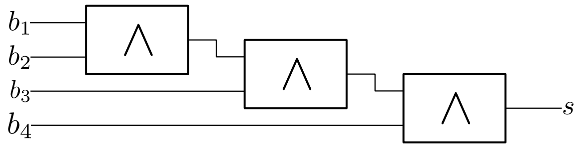
$$
\begin{prooftree}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, A, B \vdash A$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, A, B \vdash B$}
\RightLabel{$\wedge_i$}
\BinaryInfC{$\Gamma_1, A, B \vdash A \wedge B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, A, B \vdash \neg(A \wedge B)$}
\RightLabel{$\neg_e$}
\BinaryInfC{$\Gamma_1, A, B \vdash \bot$}
\RightLabel{$\neg_i$}
\UnaryInfC{$\Gamma_1, A \vdash \neg B$}
\RightLabel{$\vee_i^d$}
\UnaryInfC{$\Gamma_1, A \vdash \neg A \vee \neg B$}
\AxiomC{}
\RightLabel{ax}
\UnaryInfC{$\Gamma_1, \neg A \vdash \neg A$}
\RightLabel{$\vee_i^g$}
\UnaryInfC{$\Gamma_1, \neg A \vdash \neg A \vee \neg B$}
\RightLabel{te}
\BinaryInfC{$\Gamma_1 \vdash \neg A \vee \neg B$}
\end{prooftree}
$$

## Exercice 6. Circuits logiques

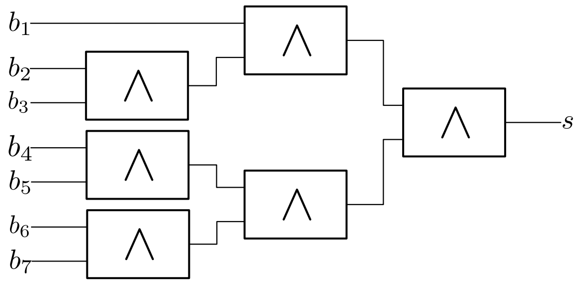
**Question 1 –** Le circuit suivant convient :




**Question 2.a –** Voici le circuit $\mathcal{C}_4$ :




Voici le circuit $\mathcal{D}_7$ :




**Question 2.b –** Les circuits $\mathcal{C}_k$ et $\mathcal{D}_k$ représentent la fonction $\boxed{f_k : (b_1, \ldots, b_k) \mapsto b_1 \wedge \ldots \wedge b_k}$. En d'autres termes, c'est le fonction $f_k : \mathcal{B}^k \to \mathcal{B}$ définie pour tout $b = (b_1, \ldots, b_k) \in \mathcal{B}^k$ par :

$$\begin{cases} f_k(b) = 1 & \text{si } b = (1, \ldots, 1), \\ f_k(b) = 0 & \text{sinon.} \end{cases}$$

On le montre facilement par récurrence sur $k$.

**Question 3 –** On note $N(\mathcal{C})$ le nombre de portes dans un circuit $\mathcal{C}$ et $P(\mathcal{C})$ sa profondeur.

**Question 3.a –** On a :

$$\begin{cases} N(\mathcal{C}_1) = 0 \\ N(\mathcal{C}_{k+1}) = 1 + N(\mathcal{C}_k) & \text{pour } k \geqslant 1 \end{cases}$$

Donc $\boxed{N(\mathcal{C}_k) = k - 1}$.

On a :

$$\begin{cases} P(\mathcal{C}_1) = 0 \\ P(\mathcal{C}_{k+1}) = \max(1, 1 + P(\mathcal{C}_k)) & \text{pour } k \geqslant 1 \end{cases}$$

Donc $\boxed{P(\mathcal{C}_k) = k - 1}$.

**Question 3.b** – On a :

$$\begin{cases} N(\mathcal{D}_1) = 0 \\ N(\mathcal{D}_k) = 1 + N(\mathcal{D}_e) + N(\mathcal{D}_{k-e}) & \text{pour } k \geqslant 1 \text{ où } e = \lfloor k/2 \rfloor \end{cases}$$

Par récurrence forte sur $k$, on obtient $\boxed{N(\mathcal{D}_k) = k - 1}$.

On a :

$$\begin{cases} P(\mathcal{D}_1) = 0 \\ P(\mathcal{D}_k) = 1 + \max\Big(P(\mathcal{D}_e), P(\mathcal{D}_{k-e})\Big) & \text{pour } k \geqslant 1 \text{ où } e = \lfloor k/2 \rfloor \end{cases}$$

Montrons par récurrence forte sur $k \geqslant 1$ que $\boxed{P(\mathcal{D}_k) = \lceil \log_2(k) \rceil}$ :

- L'égalité est vraie pour $k = 1$.
- Soit $k \geqslant 2$ et $e = \lfloor k/2 \rfloor$. On suppose la propriété vraie pour tout $\ell < k$.
  - Si $k$ est pair alors $\lfloor k/2 \rfloor = k/2 \in \mathbb{N}$ donc :

$$P(\mathcal{D}_k) = 1 + \max\Big(\lceil \log_2(k/2) \rceil, \lceil \log_2(k/2) \rceil\Big) = \lceil \log_2(k) \rceil$$

  - Si $k$ est impair alors $\lfloor k/2 \rfloor = (k-1)/2 \in \mathbb{N}$ donc :

$$P(\mathcal{D}_k) = 1 + \max\left(\left\lceil \log_2\left(\frac{k-1}{2}\right)\right\rceil, \left\lceil \log_2\left(\frac{k+1}{2}\right)\right\rceil\right) = \left\lceil \log_2(k+1) \right\rceil$$

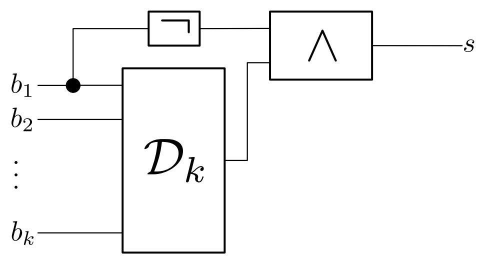
  Soit $\ell = \left\lceil \log_2(k+1) \right\rceil \geqslant 2$ alors $2^{\ell-1} < k+1 \leqslant 2^{\ell}$. Puisque $k$ est impair et $\ell \geqslant 2$, on a $k \neq 2^{\ell-1}$, donc $2^{\ell-1} < k \leqslant 2^{\ell}$ et $\ell = \left\lceil \log_2(k) \right\rceil$.

**Question 4** – On a $|\mathcal{B}^k| = 2^k$ et $|\mathcal{B}^n| = 2^n$ donc le nombre de fonctions $f : \mathcal{B}^k \to \mathcal{B}^n$ est $\boxed{2^{n2^k}}$.

**Question 5.a** – Si $f$ est de poids 0 alors elle est identiquement nulle. Ainsi, pour tout $(b_1, \dots, b_k)$, on a :

$$f(b_1, \dots, b_k) = \neg b_1 \wedge (b_1 \wedge \ldots \wedge b_k).$$

Le circuit suivant convient ($\mathcal{D}_k$ est le circuit défini par l'énoncé.) :




**Question 5.b** – Si $f$ est de poids 1 alors il existe un $k$-uplet $(a_1, \dots, a_k) \in \mathcal{B}^k$ tel que $f(a_1, \dots, a_k) = 1$ et $f(b) = 0$ pour tout $b \neq (a_1, \dots, a_k)$. Ainsi, pour tout $(b_1, \dots, b_k)$, on a :

$$f(b_1, \dots, b_k) = c_1 \wedge \ldots \wedge c_k. \qquad \text{où} \qquad c_i = \begin{cases} b_i & \text{si } a_i = 1 \\ \neg b_i & \text{sinon} \end{cases}$$

Pour construire un circuit représentant $f$, on procède comme suit :

- Pour chaque entrée $b_i$, on calcule le $c_i$ correspondant. Pour cela, il suffit d'appliquer une porte NON lorsque $a_i = 0$ et de ne pas appliquer de porte sinon.
- On applique le circuit $\mathcal{D}_k$ aux $c_i$.

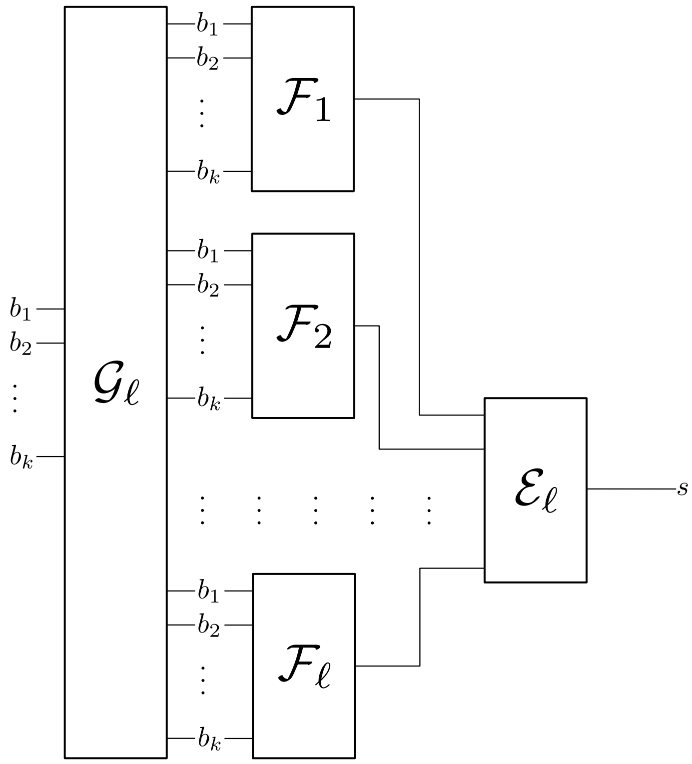
**Question 5.c –** Pour commencer, on construit un circuit $\mathcal{E}_\ell$ représentant la fonction $f : (b_1, \ldots, b_\ell) \mapsto b_1 \vee \ldots \vee b_\ell$. Pour cela on procède comme pour la construction de $\mathcal{D}_\ell$ en remplaçant les portes ET par des portes OU.

On construit ensuite un circuit $\mathcal{G}_\ell$ avec $k$ entrées et $\ell \times k$ sorties, qui duplique $\ell$ fois chacune de ses entrées. Pour construire ce circuit, il suffit d'utiliser des duplicateurs en série.

Soit $f : \mathcal{B}^k \to \mathcal{B}$ une fonction de poids $\ell \geqslant 1$. Il existe donc des $k$-uplets $b_1, \ldots, b_\ell$ tels que $f(b_1) = \ldots = f(b_\ell) = 1$ et $f(b) = 0$ pour tout $b \notin \{b_1, \ldots, b_\ell\}$. Notez qu'ici chaque $b_j$ appartient à $\mathcal{B}^k$. Pour tout $j$, on note $f_j$ la fonction de poids 1 telle que $f_j(b_j) = 1$ et $f_j(b) = 0$ pour tout $b \neq b_j$. Pour tout $b \in \mathcal{B}^k$, on a alors :

$$f(b) = f_1(b) \vee \ldots \vee f_\ell(b).$$

Pour chaque $j$, on construit à l'aide de la question précédente un circuit $\mathcal{F}_j$ pour calculer $f_j$, puis on combine les $\ell$ sorties obtenues à l'aide du circuit $\mathcal{E}_\ell$.




**Question 6 –** Il suffit de calculer chaque composante de la fonction indépendamment.

Soit $f : \mathcal{B}^k \to \mathcal{B}^n$ une fonction quelconque. Pour tout $i \in [\![1, n]\!]$, on note $f_i$ la fonction qui à tout $b \in \mathcal{B}^k$ associe la $i^{\text{ème}}$ composante de $f(b)$. On a donc $f : b \mapsto (f_1(b), \ldots, f_n(b))$.

Grâce à la question précédente, on peut construire $\mathcal{H}_i$ un circuit qui représente la fonction $f_i : \mathcal{B}^k \to \mathcal{B}$. Il suffit alors de juxtaposer les circuit $\mathcal{H}_1, \ldots, \mathcal{H}_n$ pour obtenir un circuit représentant la fonction $f$.

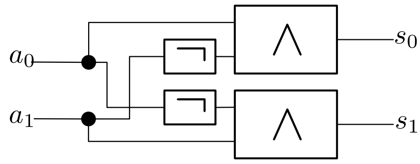
**Question 7 –** On a $2 \equiv -1 \pmod 3$ donc :

$$A = \sum_{i=0}^{k-1} a_i 2^i \equiv \sum_{i=0}^{k-1} (-1)^i a_i \pmod 3$$

**Question 8 –** Calculons $s_0$ et $s_1$ en fonction de $a_0$ et $a_1$ :

| $a_0$ | $a_1$ | reste modulo 3 | $s_0$ | $s_1$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 2 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 |

On a donc $\boxed{s_0 = a_0 \wedge \neg a_1 \text{ et } s_1 = \neg a_0 \wedge a_1}$. Le circuit $\mathcal{M}_1$ suivant convient :




**Question 9 –** Calculons $s_0$ et $s_1$ en fonction de $a_0, a_1, b_0, b_1$ :

| $a_0$ | $a_1$ | $b_0$ | $b_1$ | reste modulo 3 de $A + B$ | $s_0$ | $s_1$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 2 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 2 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 2 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | 2 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 2 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 |

On a donc :

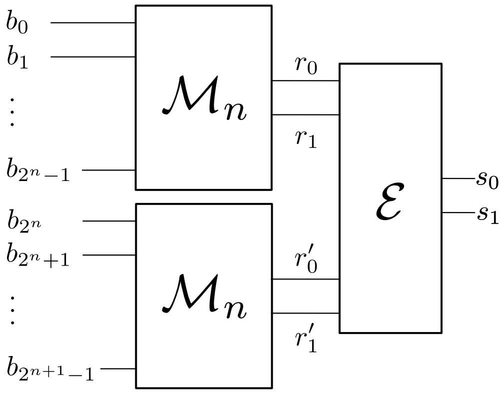
$$\begin{aligned}
s_0 =& (a_0 \wedge \neg a_1 \wedge \neg b_0 \wedge \neg b_1) \vee (\neg a_0 \wedge \neg a_1 \wedge b_0 \wedge \neg b_1) \vee (a_0 \wedge a_1 \wedge b_0 \wedge \neg b_1) \vee \\
& (\neg a_0 \wedge a_1 \wedge \neg b_0 \wedge b_1) \vee (a_0 \wedge \neg a_1 \wedge b_0 \wedge b_1) \\
s_1 =& (\neg a_0 \wedge a_1 \wedge \neg b_0 \wedge \neg b_1) \vee (a_0 \wedge \neg a_1 \wedge b_0 \wedge \neg b_1) \vee (\neg a_0 \wedge \neg a_1 \wedge \neg b_0 \wedge b_1) \vee \\
& (a_0 \wedge a_1 \wedge \neg b_0 \wedge b_1) \vee (\neg a_0 \wedge a_1 \wedge b_0 \wedge b_1)
\end{aligned}$$

**Question 10 –** Soit $n \geqslant 1$. Étant donné un nombre $B = \displaystyle\sum_{k=0}^{2^{n+1}-1} b_k 2^k$, on souhaite calculer le reste de $B$ modulo 3. On remarque que :

$$\begin{aligned}
B &= \left(\sum_{k=0}^{2^n-1} b_k 2^k\right) + 2^{2^n}\left(\sum_{k=0}^{2^n-1} b_{k+2^n} 2^k\right) \\
&\equiv \left(\sum_{k=0}^{2^n-1} b_k 2^k\right) + (-1)^{2^n}\left(\sum_{k=0}^{2^n-1} b_{k+2^n} 2^k\right) \pmod 3 \\
&\equiv \left(\sum_{k=0}^{2^n-1} b_k 2^k\right) + \left(\sum_{k=0}^{2^n-1} b_{k+2^n} 2^k\right) \pmod 3
\end{aligned}$$

Pour construire le circuit $\mathcal{M}_{n+1}$ :

- On applique le circuit $\mathcal{M}_n$ sur les entrées $(b_0, \ldots, b_{2^n-1})$ pour obtenir deux sorties $r_0, r_1$.
- On applique le circuit $\mathcal{M}_n$ sur les entrées $(b_{2^n}, \ldots, b_{2^{n+1}-1})$ pour obtenir deux sorties $r'_0, r'_1$.
- On applique le circuit $\mathcal{E}$ aux entrées $r_0, r_1, r'_0, r'_1$ pour obtenir $s_0, s_1$ qui représentent le reste de $B$ modulo 3.




**Question 11 –** Pour $n \geqslant 1$, soit $c_n$ le nombre de portes dans le circuit $\mathcal{M}_n$. On a :

$$c_{n+1} = 2c_n + a \qquad \text{pour } n \geqslant 1.$$

C'est une suite arithmético-géométrique :

$$c_n = a(2^{n-1} - 1) + 2^{n-1}c_1.$$

On obtient l'équivalent quand $n \to +\infty$ :

$$c_n \sim \frac{c_1 + a}{2} 2^n$$

avec $c_1 = 6$ le nombre de portes dans le circuit de la question 8.