1. Circuits classiques

Calcul quantique

1. Circuits classiques

Calcul: $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$(x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n) = (y_1, \dots, y_n)$

ex:

- $x \to \boxed{\text{NOT}} \to \bar{x}$ $\qquad f(x) = \bar{x} = 1 - x \pmod 2 = 1 \oplus x \pmod 2$

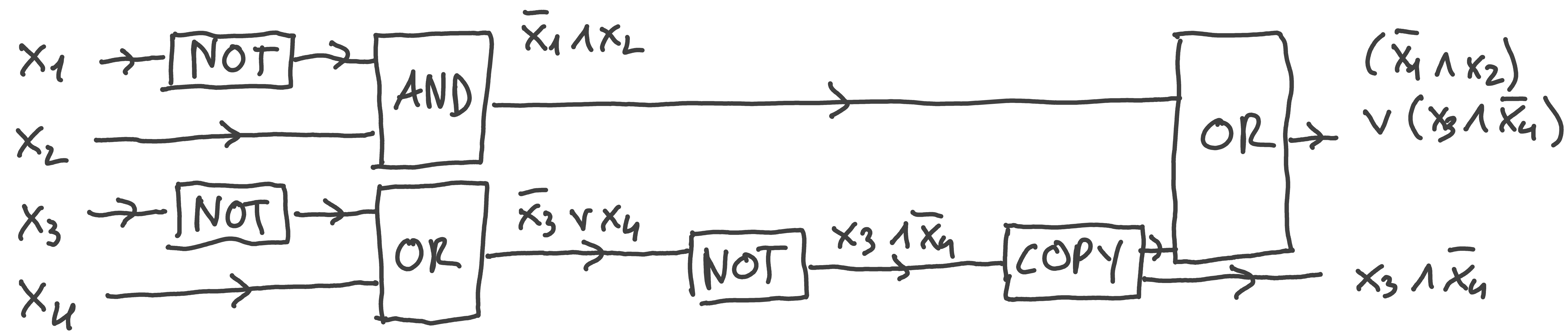
  $x \to \oplus \to 1 \oplus x$

- $x_1, x_2 \to \boxed{\text{AND}} \to x_1 \wedge x_2$ $\qquad f(x_1, x_2) = x_1 \wedge x_2 = x_1 \cdot x_2 \pmod 2$

- $x_1, x_2 \to \boxed{\text{OR}} \to x_1 \vee x_2$ $\qquad f(x_1, x_2) = x_1 \vee x_2 = x_1 + x_2 \pmod 2$

- $x \to \boxed{\text{COPY}} \to x, x$ $\qquad f(x) = (x, x)$

ex:



$$f(x_1, x_2, x_3, x_4) = (y_1, y_2), \quad \begin{cases} y_1 = (\bar{x}_1 \wedge x_2) \vee (x_3 \wedge \bar{x}_4) \\ y_2 = x_3 \wedge \bar{x}_4 \end{cases}$$

Circuit booléen: graphe acyclique, dirigé, n bits d'entrée & m bits de sortie

Thm de Emil-Post: Toute fct booléenne $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ peut être représentée par un graphe booléen. Ce graphe est réalisé grâce aux portes {NOT, AND, OR, COPY}.
Cet ensemble est un ensemble de portes universel.

Preuve: $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Il suffit de prouver pour chaque composante.
$f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ (une composante)

- $\vec{a}^{(1)}, \vec{a}^{(2)}, \dots, \vec{a}^{(k)} \in \mathbb{F}_2^n$ t.q. $f(\vec{a}^{(i)}) = 1 \quad \forall i,\ 1 \leq i \leq k$
  Si $\vec{b} \in \mathbb{F}_2^n$, $\vec{b} \neq \vec{a}^{(i)} \ \forall i \Rightarrow f(\vec{b}) = 0$

- $C_{\vec{a}}(x_1, \dots, x_n) = \begin{cases} 1, & \text{si } (x_1, \dots, x_n) = \vec{a} \\ 0, & \text{sinon} \end{cases}$ fct indicative

- $f(x_1, \dots, x_n) = C_{\vec{a}^{(1)}}(x_1, \dots, x_n) \vee \dots \vee C_{\vec{a}^{(k)}}(x_1, \dots, x_n)$

- $C_{\vec{a}}(x_1, \dots, x_n) = \phi_1(x_1) \wedge \dots \wedge \phi_n(x_n)$

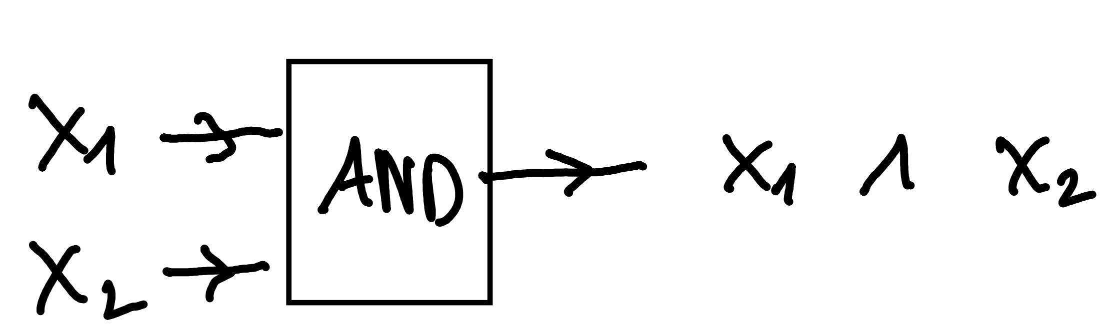
  avec $\phi_i(x_i) = \begin{cases} \bar{x}_i, & \text{si } a_i = 0 \\ x_i, & \text{si } a_i = 1 \end{cases}$

$C_a(x) = \begin{cases} 1, & \text{si } x = a \\ 0, & \text{si } x = \bar{a} = 1 \oplus a \end{cases}$, $\quad C_a(x) = \phi(x) = \begin{cases} \bar{x}, & \text{si } a = 0 \\ x, & \text{si } a = 1 \end{cases}$

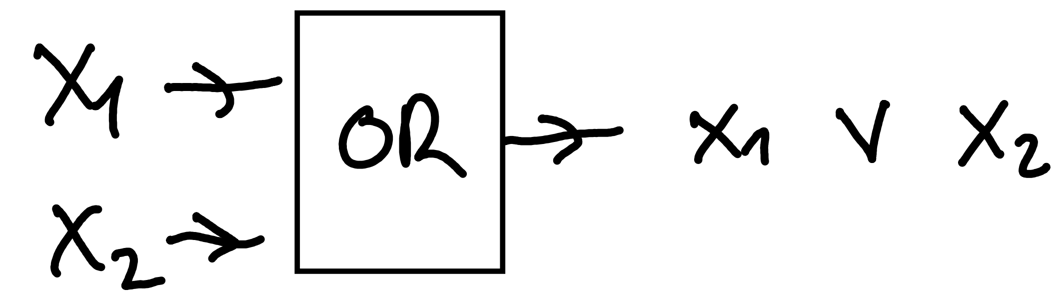
- $a = 0$: $\quad x = 0,\ C_0(x) = \bar{x} = 1, \quad a = x \Rightarrow C = 1$
  $\quad x = 1,\ C_0(x) = \bar{x} = 0 \quad a \neq x \Rightarrow C = 0$

- $a = 1$: $\quad x = 0,\ C_1(x) = x = 0, \quad a \neq x \Rightarrow C = 0$
  $\quad x = 1,\ C_1(x) = x = 1 \quad a = x \Rightarrow C = 1$

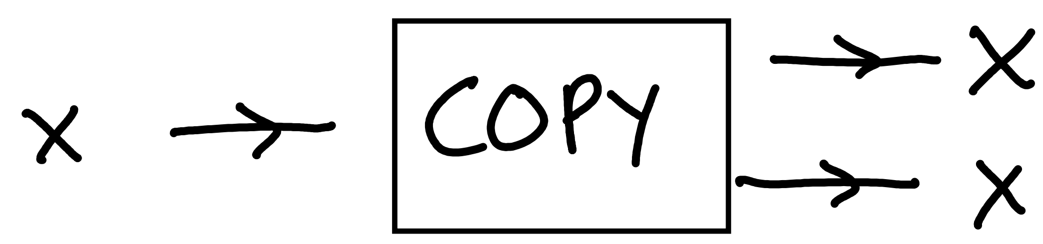
Porte réversible:

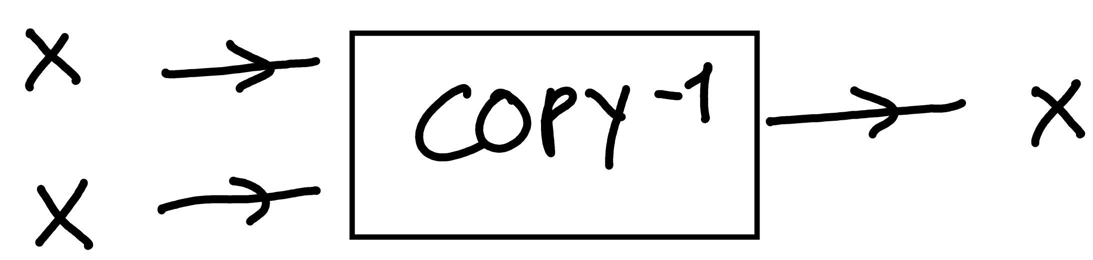


pas réversible

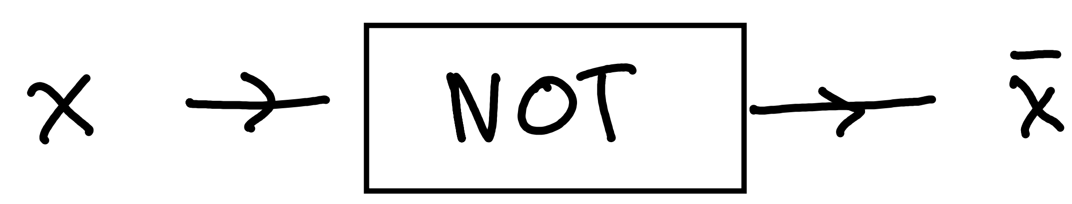


pas réversible





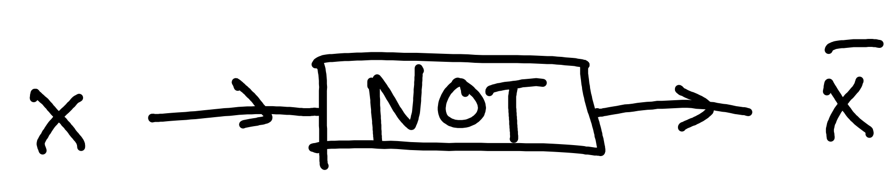
logiquement inversible mais l'inverse efface un bit et il y a dissipation de chaleur



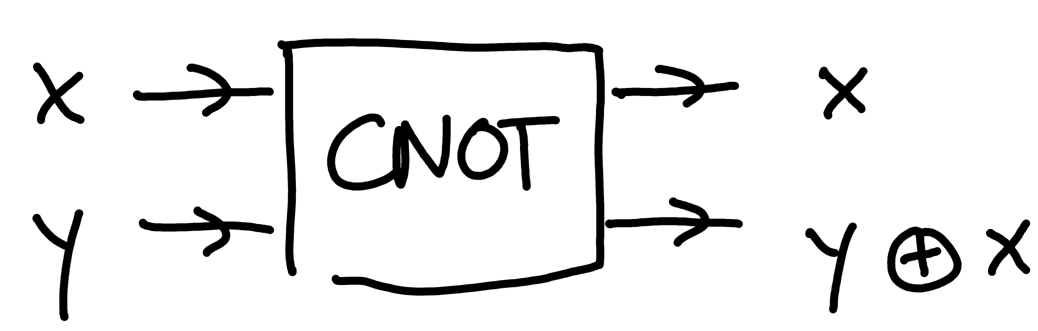
réversible

Thm: Une fct booléenne par un circuit booléen (graphe) qui contient uniquement des portes réversibles {NOT, CNOT, CCNOT}.
Cet ensemble est un autre ensemble de portes universel et sont réversibles.

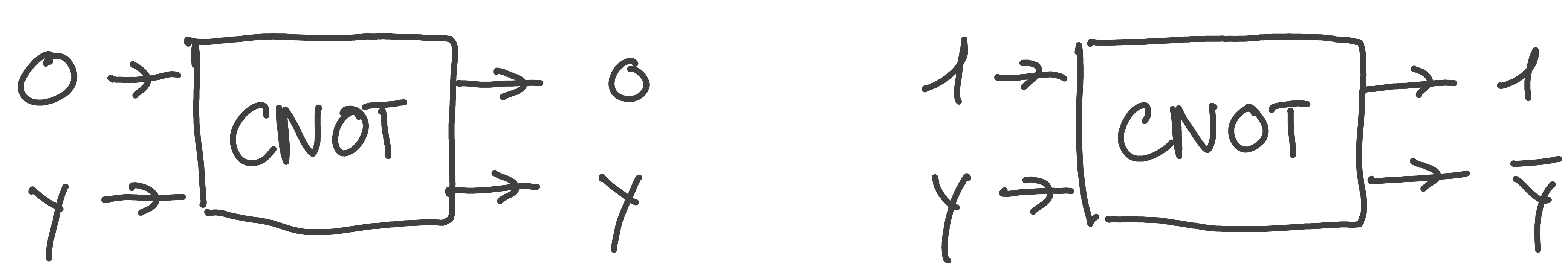
- NOT:



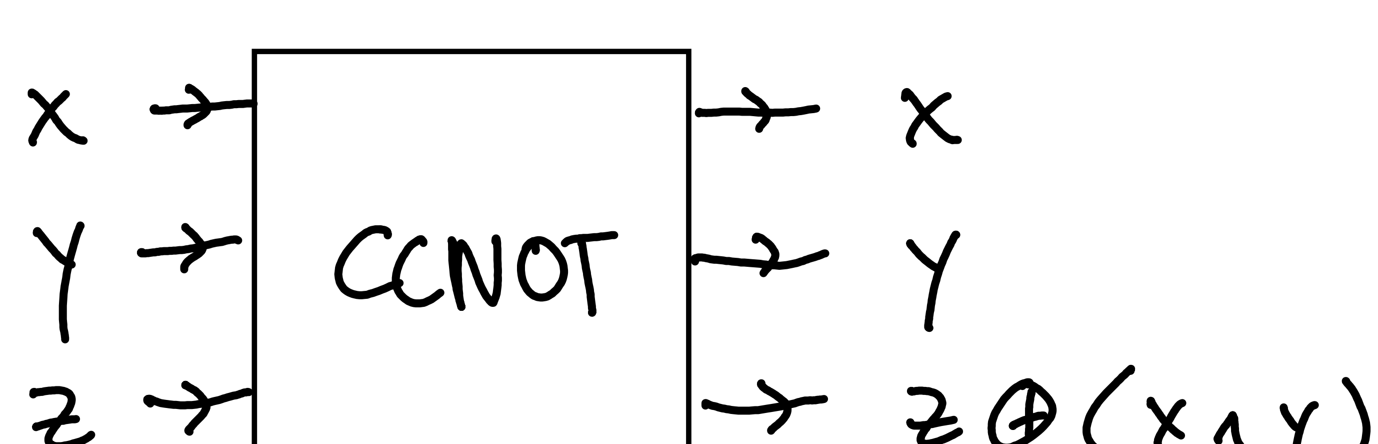
- CNOT:



$f(x,y) = (x, y \oplus x)$

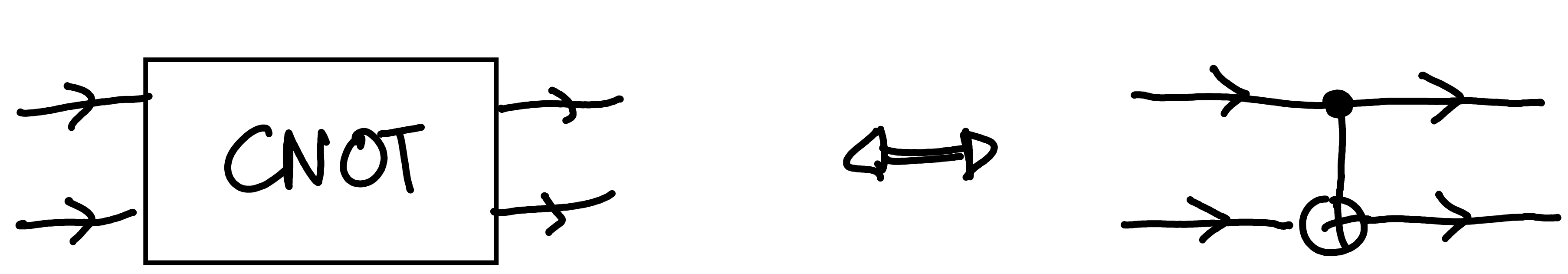


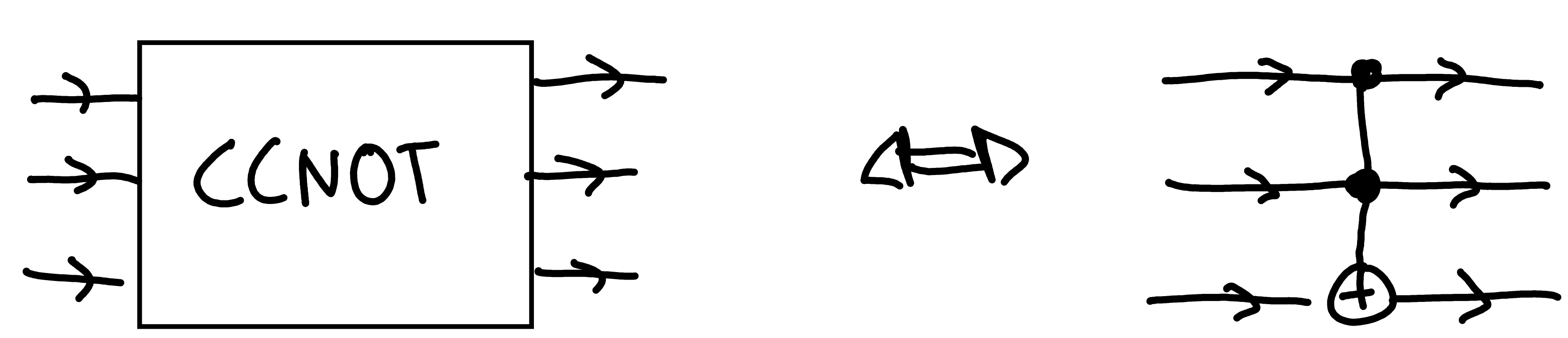
- CCNOT:



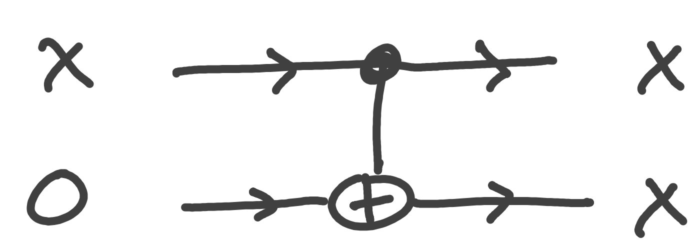
bits de contrôle

Notation:



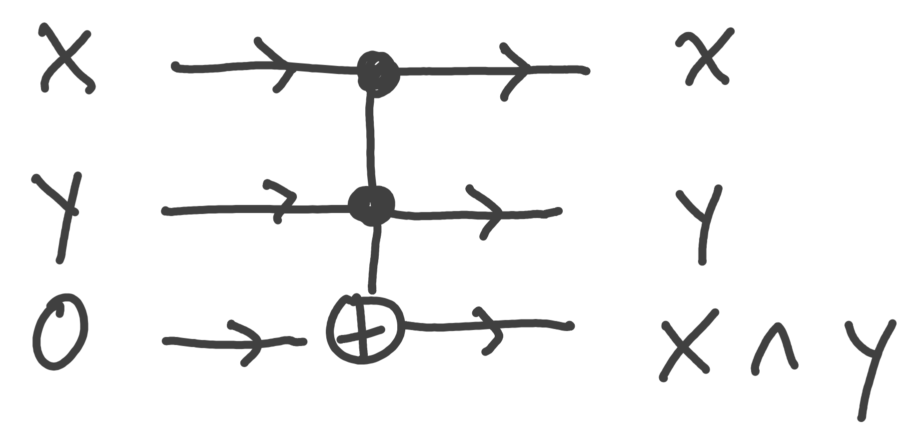


Preuve du thm : - COPY



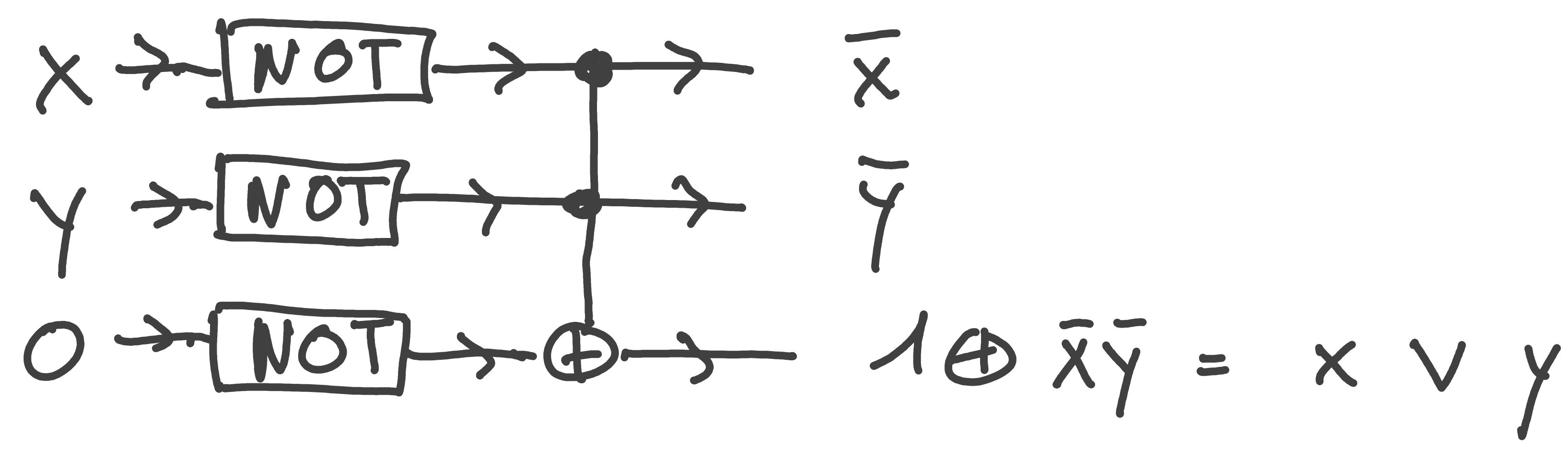
avec CNOT (réversible)

- AND



avec CCNOT (réversible)

- OR



$\Rightarrow$ tts les fcts booléennes peuvent êtres réalisées par un circuit booléen de manière réversibles