# Informatique quantique IFT6155

# Circuits réversibles

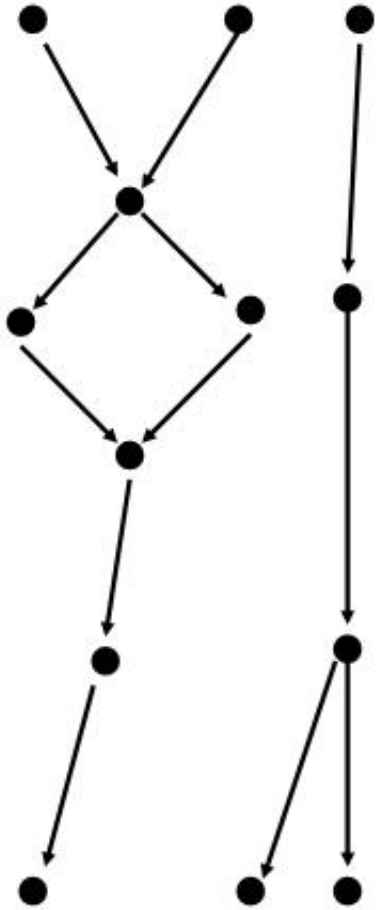
# Calcul de fonctions

Toute opération quantique est unitaire et donc réversible. Dans ce chapitre nous allons réviser les notions de base de la théorie des circuits et introduire la notion de circuit réversible. Leur compréhension est essentielle à l'élaboration de circuits quantiques. Le calcul réversible est aussi étudié dans le contexte de la thermodynamique du calcul.

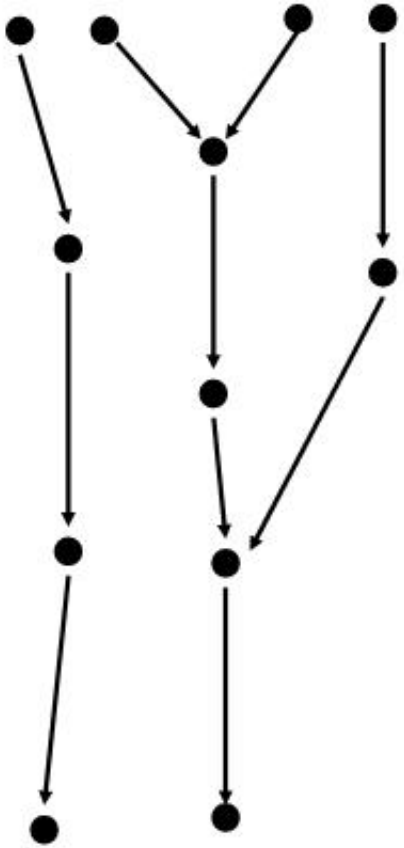
# Graphes de configuration

Chaques noeud représente un état de la machine et chaque arc représente une étape élémentaire de calcul. Les trois graphes sont acycliques.

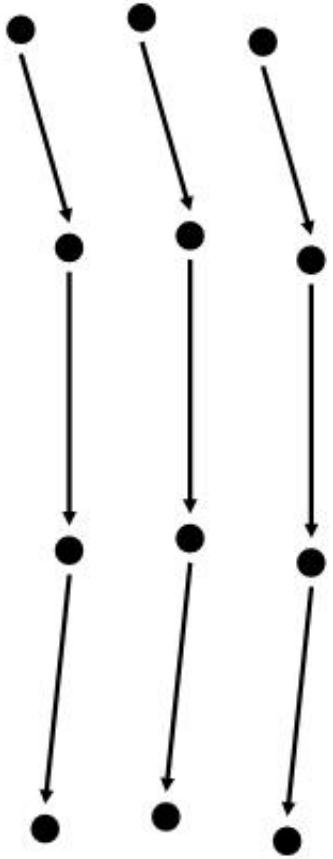
Probabiliste et
Non-déterministe



Déterministe

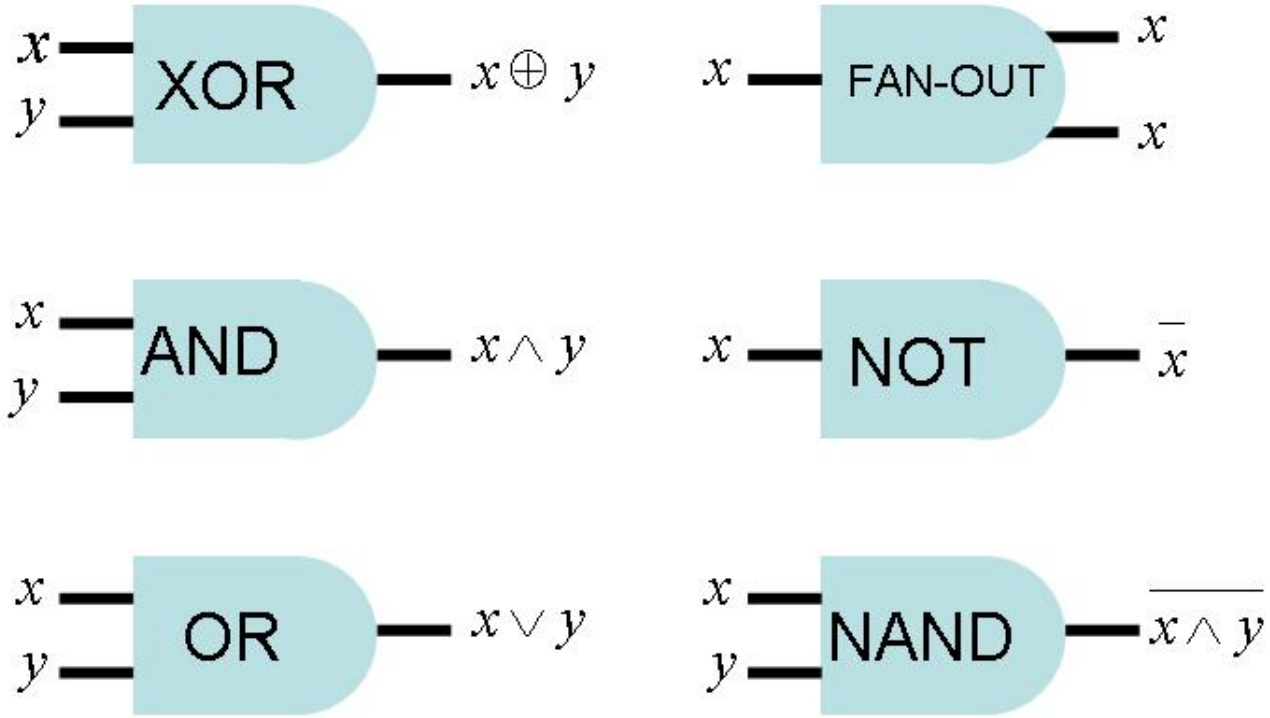


Réversible



# Circuits classiques

Dans un circuit classique on peut retrouver les portes suivantes:




Un circuit est une interconnexion de portes sans cycles où on retrouve en entrée les bits de $x$ et des constantes et en sortie les bits de $y = f(x)$.

# Universalité

Avec la création de bit et le FAN-OUT, la porte NAND (notée $*$) est universelle pour les circuits classiques. Tout circuit avec un nombre fini de fils d'entrée et de sortie peut être implanté en utilisant des constantes, le FAN-OUT et le NAND avec un nombre fini (constant) de portes.

Par exemple:

$$\begin{aligned} \bar{x} &= x * 1 \\ x \wedge y &= (x * y) * 1 \\ x \vee y &= (x * 1) * (y * 1) \\ x \oplus y &= (((x * 1) * y) * 1) * ((x * (y * 1)) * 1) \end{aligned}$$

# Uniformité

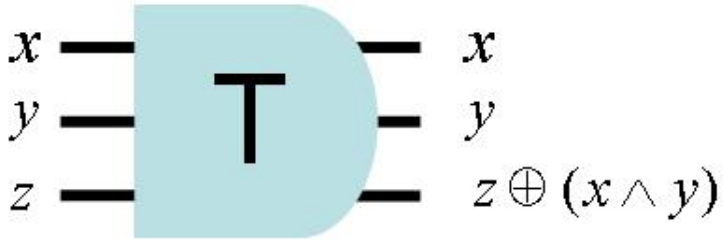
Pour calculer une fonction nous devons avoir un circuit pour chaque taille d'input. A chaque fonction on peut associer une famille de circuits et vice versa.

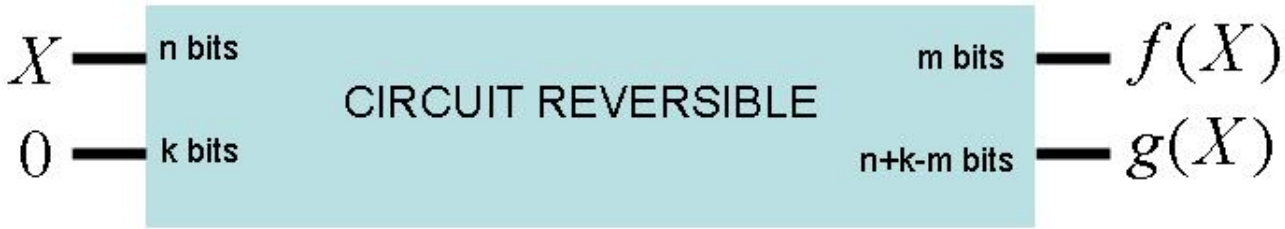
Si aucune restriction n'est faite sur la structure des circuits, alors certaine famille de circuits vont calculer des fonctions qui ne sont pas calculables au sens de Turing.

On dira qu'une famille de circuit $S = \{s_1, s_2, \ldots\}$ est uniforme si il existe un algorithme polynomial prenant comme entrée $1^n$ et retournant $s_n$.

# Circuits réversibles



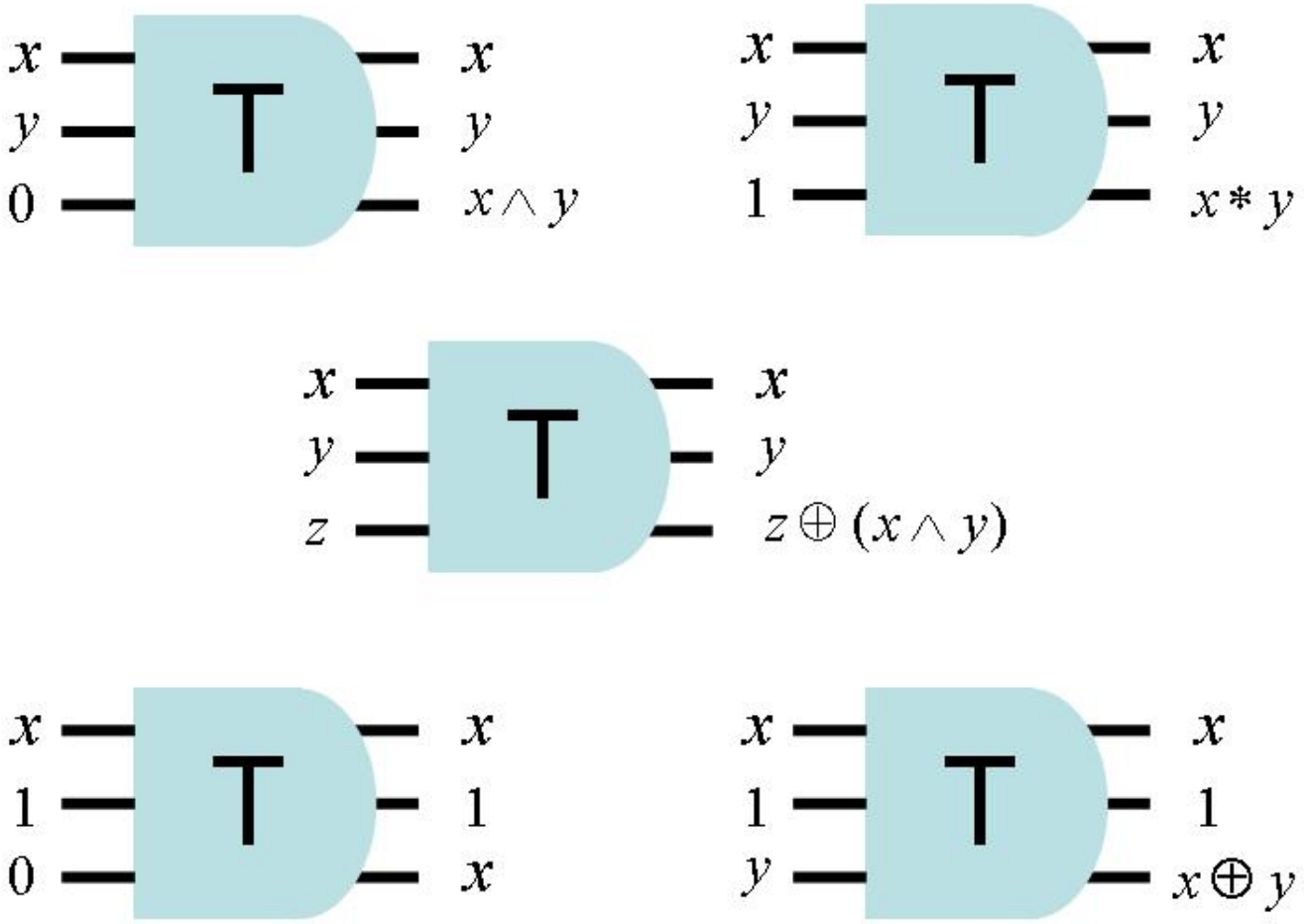


# Circuits réversibles

Un circuit est une interconnexion de portes, NOT,CNOT,T sans cycle où on retrouve en entrée les bits de $x$ et des zéros et en sortie les bits de $y = f(x)$ ainsi que des bits inutiles $g = g(x)$. Le nombre de fils est appelé largeur et le nombre de porte la taille.

# Universalité

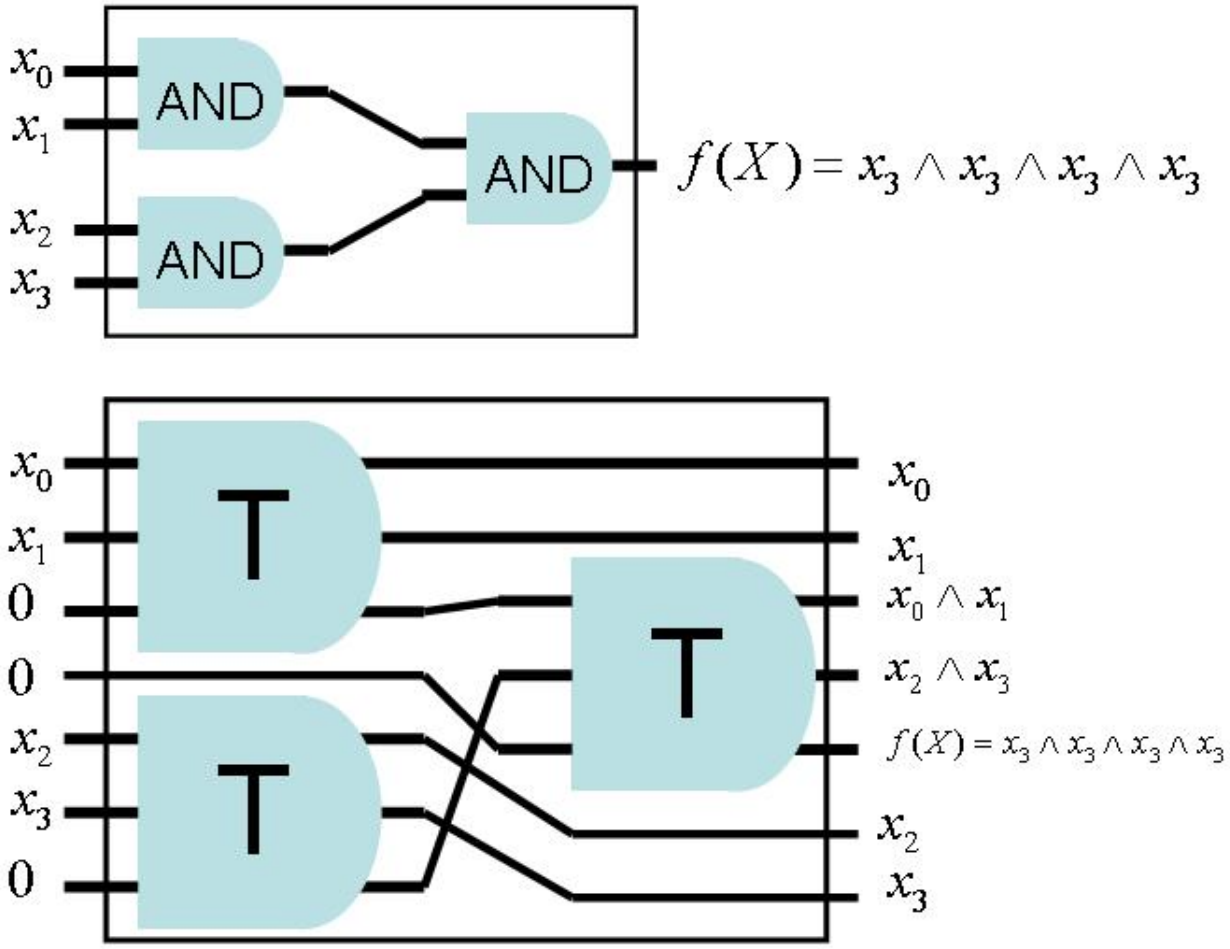


# Universalité

La porte de Toffoli, avec l'initialisation de valeur constante, est universelle.

Chacune des portes élémentaire d'un circuit classique peut être remplacée par une ou plusieur portes de Toffoli. La largeur du circuit devient donc proportionnelle au nombre de portes.

# Classique versus réversible

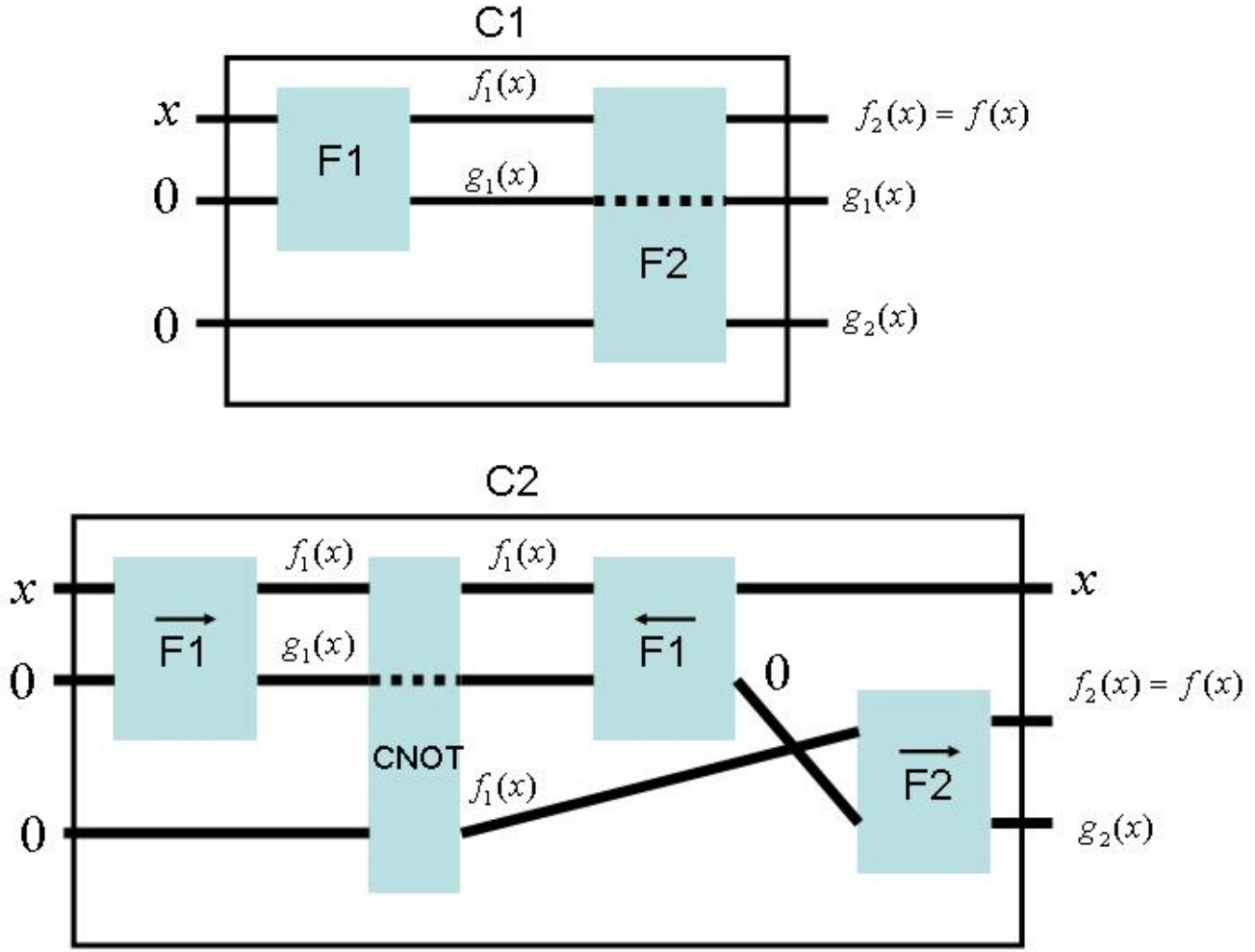


# Minimiser la largeur

La largeur des circuits construits à partir de circuits classiques de façon naïve est proportionnelle à leur taille. Dans bien des cas, ce n'est pas raisonnable. Bennett a inventé une technique qui permet de réutiliser la mémoire, diminuant considérablement la largeur du circuit tout en gardant sa taille raisonnable.

Divisons le circuit $F$ calculant $f$ en deux circuits $F_1$ et $F_2$ tels que $f_2(f_1(x)) = f(x)$. On peux recycler les bits résiduels.

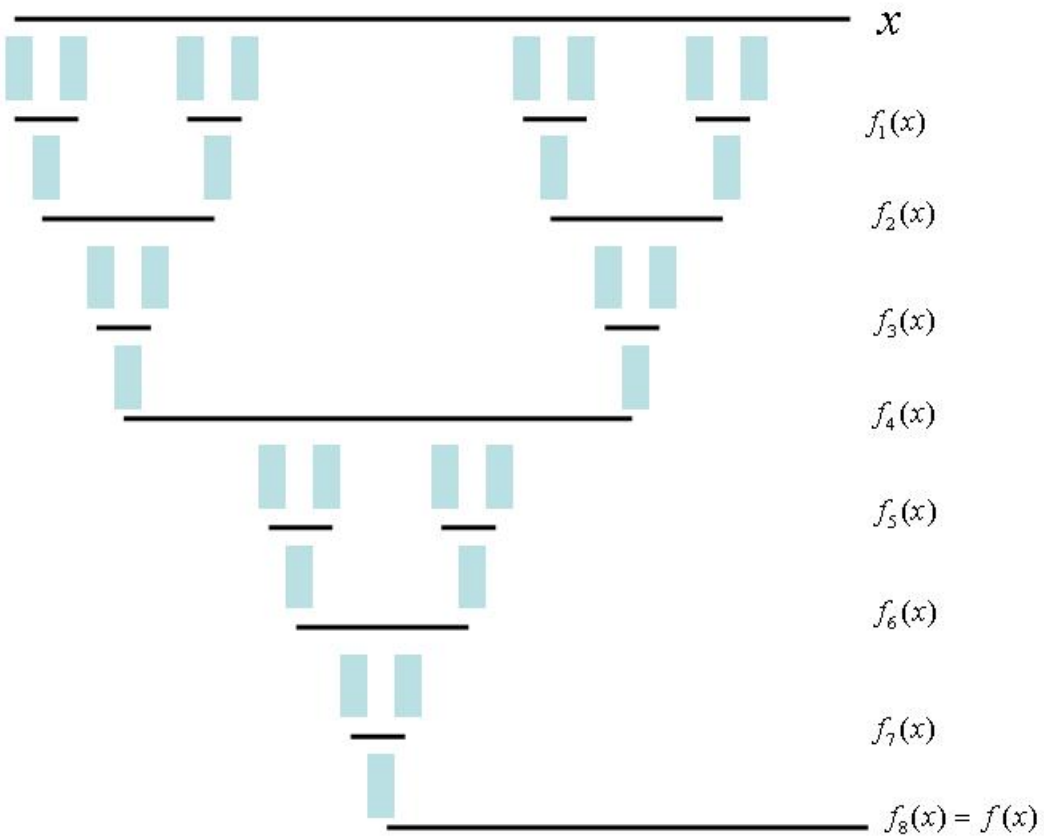
# Minimiser la largeur




Avantage significatif en largeur si $F_1$ et $F_2$ sont grands. Par contre la taille augmente.

# Minimiser la largeur

Soit le circuit classique $F$ de taille $t$; construisons le circuit réversible $F'$ en divisant $F$ en 8 circuits réversibles.




Taille de $F'$: $27t/8$

Largeur de $F'$: $4t/8$

# Minimiser la largeur

En général si $F$ est de taille $T = 2^t$ et de largeur maximale $l$ la technique de Bennett nous donnera $F'$ de taille $3^t$ et de largeur $lt$.

On peut pousser l'analyse et obtenir le résultat suivant.

**Théorème [LS90]** Soit $\mathcal{F}$ une famille de circuits classiques de taille $t(n)$ et de largeur $l(n)$. Pour tout $\epsilon$ il existe il existe une famille de circuits réversibles de taille $\Omega(t(n)^{1+\epsilon})$ et de largeur $\Omega(l(n)(1 + \log(\frac{t(n)}{l(n)})))$.

# Circuit propre

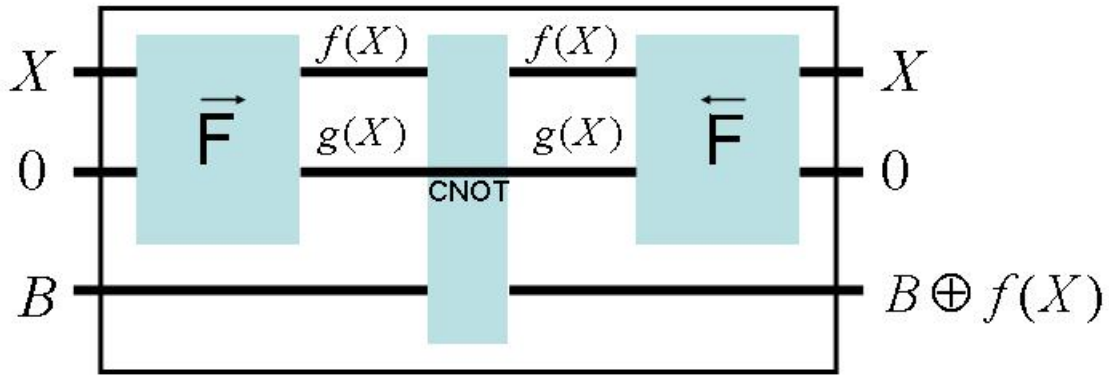
Un des intérêts des circuits réversibles est qu'en théorie une opération réversible peut être réalisée en dissipant une quantité arbitrairement faible d'énergie.

Effacer un bit ou remplacer un bit de valeur inconnue par un bit de valeur connue dissipe aussi de l'énergie.

Il serait donc intéressant de se débarasser de ces bits résiduels.

Des circuit réversibles propres seront essentiels pour la réalisation de circuits quantiques.

# Circuit propre


Si $f : \{0,1\}^n \to \{0,1\}^k$ est calculable par un circuit réversible de $p$ portes et de largeur $w$ alors il est calculable proprement par un circuit réversible de $2p + k$ portes et de largeur $w + k$.