

Informatique quantique IFT6155

Circuits quantiques

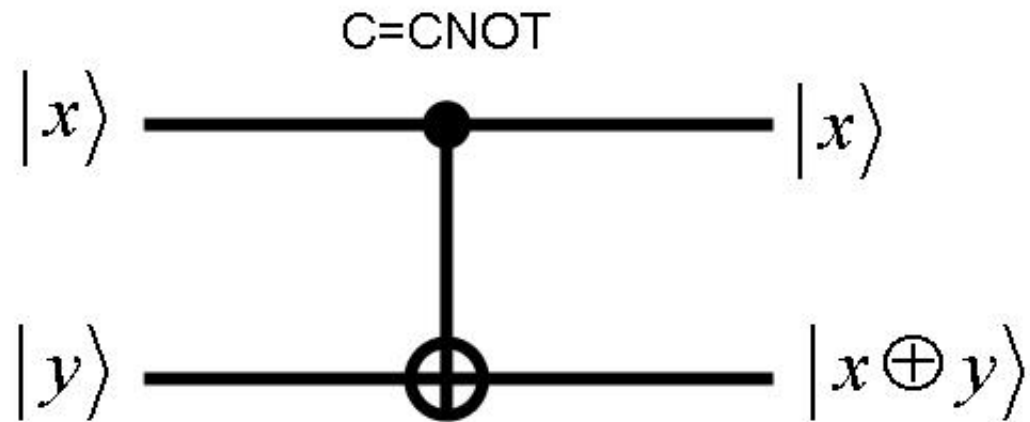
Calcul de fonctions

Tout algorithme quantique doit être divisé en opérations élémentaires. Les opérations impliquant un seul qubit sont en général simples, alors nous nous donnerons la possibilité d'utiliser n'importe quelle opération unitaire sur un seul qubit.

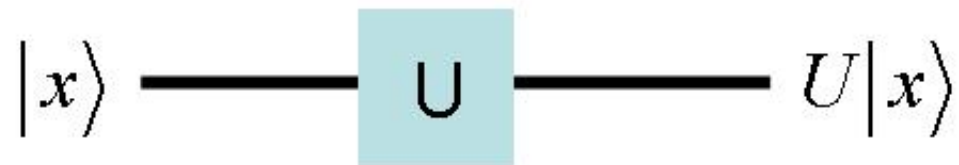
Nous utiliserons aussi une porte à deux qubits, le “non contrôlé” ou CNOT. Nous verrons au cours de ce chapitre que cet ensemble simple nous permet de faire tout ce dont nous avons besoin.

Nous étudierons plus loin l'universalité de ces portes et de certains ensembles finis de portes quantiques.

Calcul de fonctions



U, un qubit



Porte à un qubit

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$S_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

$$S_\theta |0\rangle \rightarrow |0\rangle$$

$$S_\theta |1\rangle \rightarrow e^{i\theta} |1\rangle$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$S |0\rangle \rightarrow |0\rangle$$

$$S |1\rangle \rightarrow i |1\rangle$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$T |0\rangle \rightarrow |0\rangle$$

$$T |1\rangle \rightarrow e^{i\pi/4} |1\rangle$$

Porte à un qubit

$$S_x S_y = S_{x+y}$$

$$S = S_{\pi/2}$$

$$T = S_{\pi/4}$$

$$T^2 = S$$

$$H = (X + Z)/\sqrt{2}$$

Les opérateurs de Pauli

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X |0\rangle \rightarrow |1\rangle$$

$$X |1\rangle \rightarrow |0\rangle$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Y |0\rangle \rightarrow i |1\rangle$$

$$Y |1\rangle \rightarrow -i |0\rangle$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z |0\rangle \rightarrow |0\rangle$$

$$Z |1\rangle \rightarrow -|1\rangle$$

Les opérateurs de Pauli

$$X = X^\dagger \quad Y = Y^\dagger \quad Z = Z^\dagger$$

$$X = iZY$$

$$Y = iXZ$$

$$Z = iYX$$

$$HXH = Z \quad HYH = -Y \quad HZH = X$$

Notation

Nous utiliserons une notation abrégée pour exprimer les opérateurs agissant sur un ou plusieurs qubits d'un registre à n qubits.

Si U agit sur $\mathcal{H}_2$ alors $U_{[i]} = I^{\otimes i-1} \otimes U \otimes I^{\otimes n-i}$.

Si U agit sur $\mathcal{H}_2 \otimes \mathcal{H}_2$ alors $U_{[i,j]}$ agit dans l'ordre sur les qubit i et j sans toucher les autres qubits.

Cette définition peut se généraliser à un nombre arbitraire de qubits.

CNOT

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$C |00\rangle \rightarrow |00\rangle$$

$$C |01\rangle \rightarrow |01\rangle$$

$$C |10\rangle \rightarrow |11\rangle$$

$$C |11\rangle \rightarrow |10\rangle$$

$$C |a\rangle |b\rangle = |a\rangle |a \oplus b\rangle \quad C_{[2,1]} |a\rangle |b\rangle = |a \oplus b\rangle |b\rangle$$

$$C = C^\dagger$$

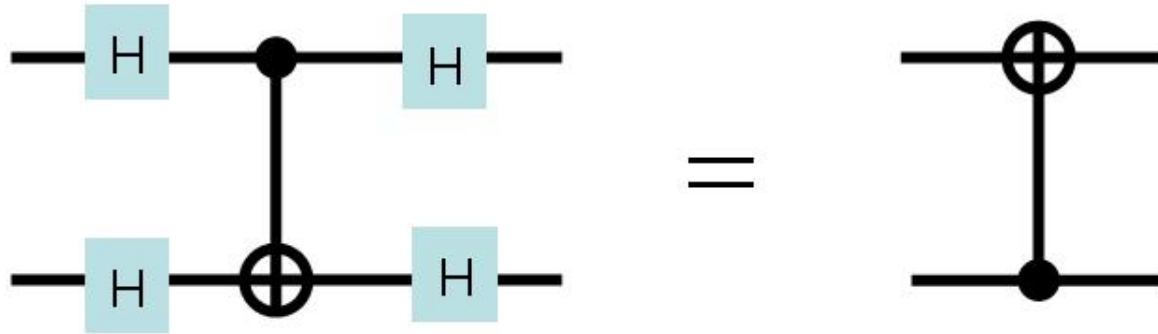
$$\forall |\psi\rangle \in \mathcal{H}_2, C |0\rangle |\psi\rangle = |0\rangle |\psi\rangle$$

$$\forall |\psi\rangle \in \mathcal{H}_2, C |1\rangle |\psi\rangle = |1\rangle (X |\psi\rangle)$$

$$C |1\rangle (H |0\rangle) = |1\rangle (H |0\rangle)$$

$$C |1\rangle (H |1\rangle) = -|1\rangle (H |1\rangle)$$

$$C_{[2,1]} = H^{\otimes 2}CH^{\otimes 2}$$



CNOT

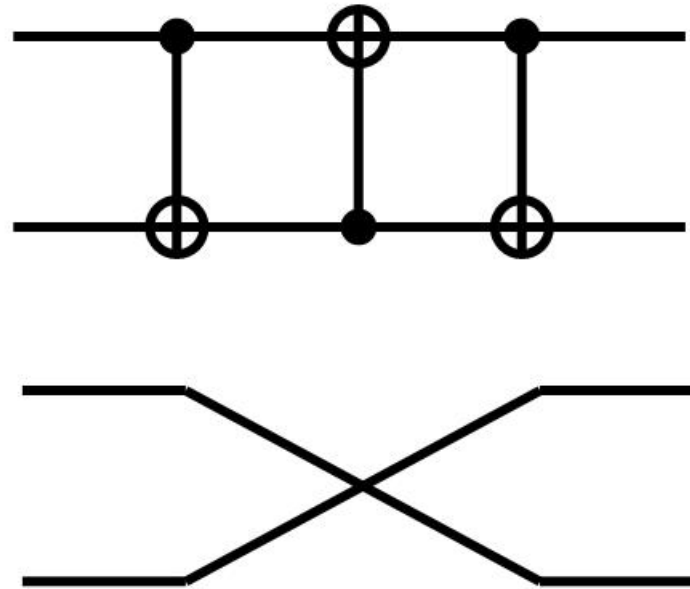
$$H |a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a |1\rangle)$$

$$H^{\otimes 2} C H^{\otimes 2} |a\rangle |b\rangle$$

$$\begin{aligned} &= H^{\otimes 2} C \frac{1}{2}(|0\rangle + (-1)^a |1\rangle)(|0\rangle + (-1)^b |1\rangle) \\ &= H^{\otimes 2} C \frac{1}{2}(|00\rangle + (-1)^b |01\rangle + (-1)^a |10\rangle + (-1)^{a+b} |11\rangle) \\ &= H^{\otimes 2} \frac{1}{2}(|00\rangle + (-1)^b |01\rangle + (-1)^a |11\rangle + (-1)^{a+b} |10\rangle) \\ &= H^{\otimes 2} \frac{1}{2}(|0\rangle + (-1)^{a+b} |1\rangle)(|0\rangle + (-1)^b |1\rangle) \\ &= |a \oplus b\rangle |b\rangle \\ &= C_{[2,1]} |a\rangle |b\rangle \end{aligned}$$

SWAP

$$P_{12} = CC'C$$

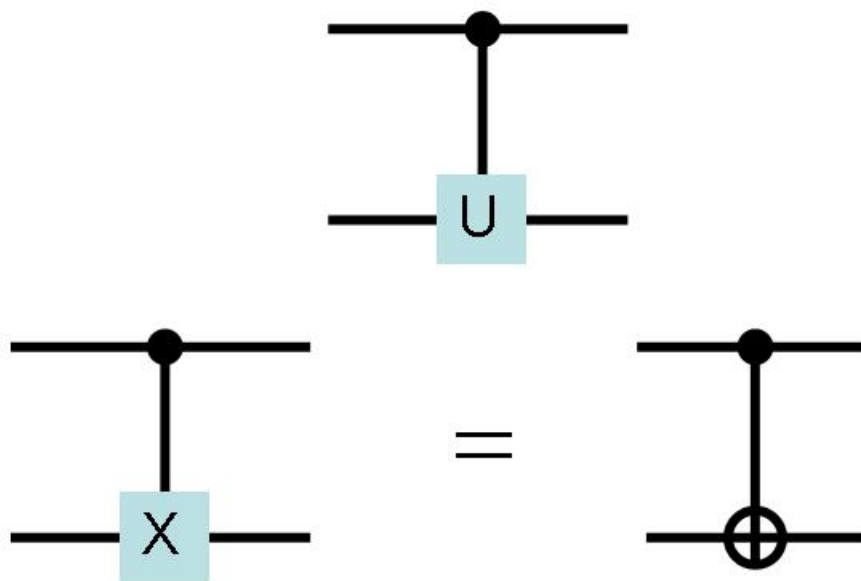


SWAP

$$P_{12} |\psi\rangle |\phi\rangle$$

$$\begin{aligned} &= P_{12} (\alpha |0\rangle + \beta |1\rangle)(\delta |0\rangle + \gamma |1\rangle) \\ &= CC_{[2,1]} C (\alpha |0\rangle + \beta |1\rangle)(\delta |0\rangle + \gamma |1\rangle) \\ &= CC_{[2,1]} C (\alpha\delta |00\rangle + \alpha\gamma |01\rangle + \beta\delta |10\rangle + \beta\gamma |11\rangle) \\ &= CC_{[2,1]} (\alpha\delta |00\rangle + \alpha\gamma |01\rangle + \beta\delta |11\rangle + \beta\gamma |10\rangle) \\ &= C (\alpha\delta |00\rangle + \alpha\gamma |11\rangle + \beta\delta |01\rangle + \beta\gamma |10\rangle) \\ &= (\alpha\delta |00\rangle + \alpha\gamma |10\rangle + \beta\delta |01\rangle + \beta\gamma |11\rangle) \\ &= (\delta\alpha |00\rangle + \delta\beta |01\rangle + \gamma\alpha |10\rangle + \gamma\beta |11\rangle) \\ &= |\phi\rangle |\psi\rangle \end{aligned}$$

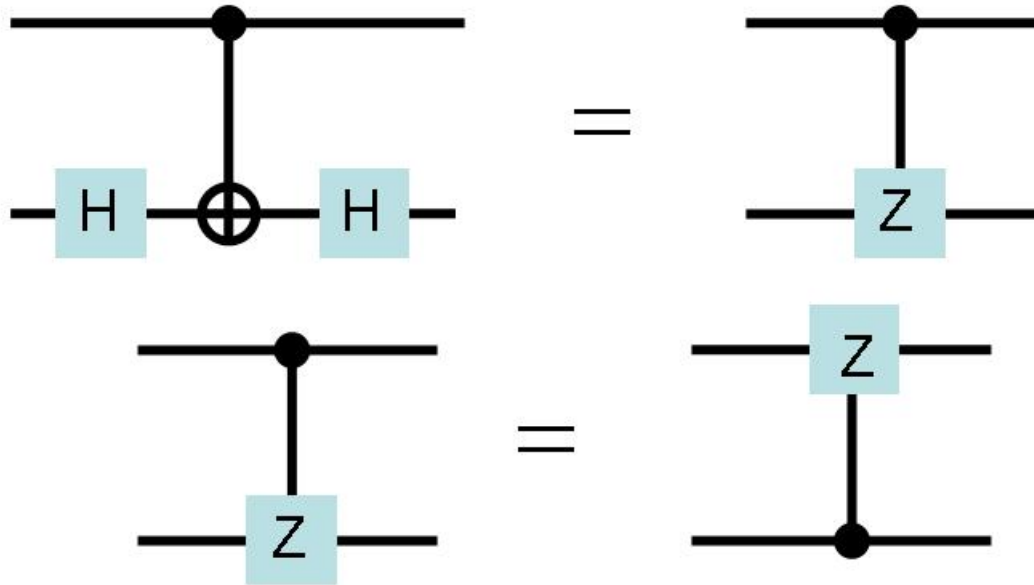
$C-U$



$$C-U |a\rangle |b\rangle = |a\rangle (U^a |b\rangle)$$

$$C-X = C$$

$C-Z$



$$\begin{aligned}
 H_{[2]} C H_{[2]} |0\rangle |b\rangle &= H_{[2]} C |0\rangle (H |b\rangle) \\
 &= H_{[2]} |0\rangle (H |b\rangle) \\
 &= |0\rangle |b\rangle \\
 H_{[2]} C H_{[2]} |1\rangle |b\rangle &= H_{[2]} C |1\rangle (H |b\rangle) \\
 &= H_{[2]} |1\rangle (X H |b\rangle) \\
 &= |1\rangle (H X H |b\rangle) \\
 &= |1\rangle (Z |b\rangle)
 \end{aligned}$$

Opérateurs de rotation

$$R_x(\theta) = e^{-i\theta X/2} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) X = \begin{pmatrix} \cos(\theta/2) & i \sin(\theta/2) \\ i \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_y(\theta) = e^{-i\theta Y/2} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Y = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_z(\theta) = e^{-i\theta Z/2} = \cos\left(\frac{\theta}{2}\right) I - i \sin\left(\frac{\theta}{2}\right) Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

Pour x, y et z nous avons $R(a)R(b) = R(a + b)$.

$$R_x(0) = R_y(0) = R_z(0) = I$$

$$X R_y(\theta) X = R_y(-\theta)$$

Décomposition d'opérateur

Théorème: Tout opérateur unitaire U sur $\mathcal{H}_2$, il existe α, β, δ et γ tels que

$$U = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma)$$

Preuve: L'opérateur U est formé par quatre nombres complexes (8 nombre réel). Puisque $UU^\dagger = I$ quatre équations doivent être satisfaites. Il reste donc 4 variables libres. Pour que chacune des équations soit satisfaite on doit avoir

$$U = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos(\gamma/2) & -e^{i(\alpha-\beta/2+\delta/2)} \sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)} \sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)} \cos(\gamma/2) \end{pmatrix}$$

d'où

$$U = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma)$$

Décomposition d'opérateur

Théorème:

Pour tout U sur $\mathcal{H}_2$ il existe A_1, A_2 et A_3 sur $\mathcal{H}_2$ et α tels que

$$A_1 A_2 A_3 = I \quad U = e^{i\alpha} A_1 X A_2 X A_3$$

Preuve:

Posons α, β, δ et γ tels que $U = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma)$. Posons

$$\begin{aligned} A_1 &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) \\ A_2 &= R_y\left(\frac{-\gamma}{2}\right) R_z\left(\frac{-\delta - \beta}{2}\right) \\ A_3 &= R_z\left(\frac{\delta - \beta}{2}\right) \end{aligned}$$

Clairement

$$\begin{aligned} A_1 A_2 A_3 &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(\frac{-\gamma}{2}\right) R_z\left(\frac{-\delta - \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\ &= R_z(\beta) R_y(0) R_z\left(\frac{-\delta - \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\ &= R_z(\beta) R_z\left(\frac{-\delta - \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\ &= R_z(0) \\ &= I \end{aligned}$$

Puisque $XX = I$ et $XR_y(a)X = R_y(-a)$, nous avons

$$A_1 X A_2 X A_3$$

$$\begin{aligned}
 &= A_1 X R_y \left(\frac{-\gamma}{2} \right) R_z \left(\frac{-\delta - \beta}{2} \right) X A_3 \\
 &= A_1 X R_y \left(\frac{-\gamma}{2} \right) X X R_z \left(\frac{-\delta - \beta}{2} \right) X A_3 \\
 &= A_1 R_y \left(\frac{\gamma}{2} \right) R_z \left(\frac{\delta + \beta}{2} \right) A_3 \\
 &= R_z(\beta) R_y \left(\frac{\gamma}{2} \right) R_y \left(\frac{\gamma}{2} \right) R_z \left(\frac{\delta + \beta}{2} \right) R_z \left(\frac{\delta - \beta}{2} \right) \\
 &= R_z(\beta) R_y(\delta) R_z(\gamma)
 \end{aligned}$$

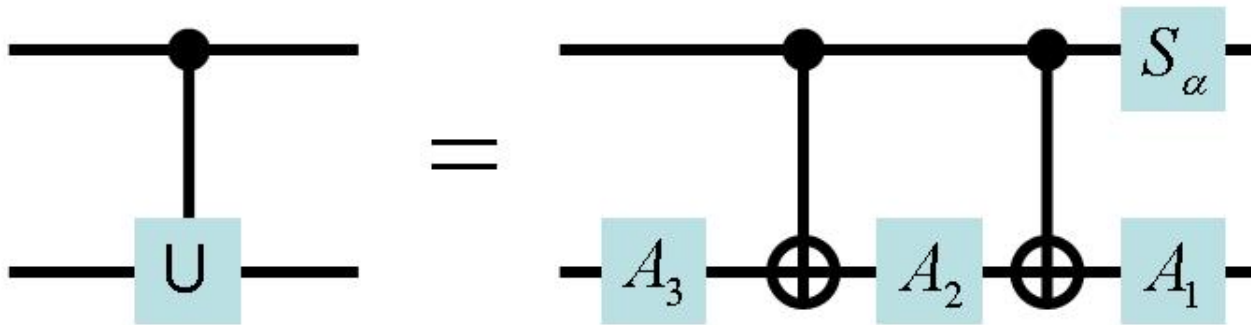
et donc

$$e^{i\alpha} A_1 X A_2 X A_3 = e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\gamma) = U$$

QED

$$C-U$$

Si $U = e^{i\alpha} A_1 X A_2 X A_3$ et $A_1 A_2 A_3 = I$ alors

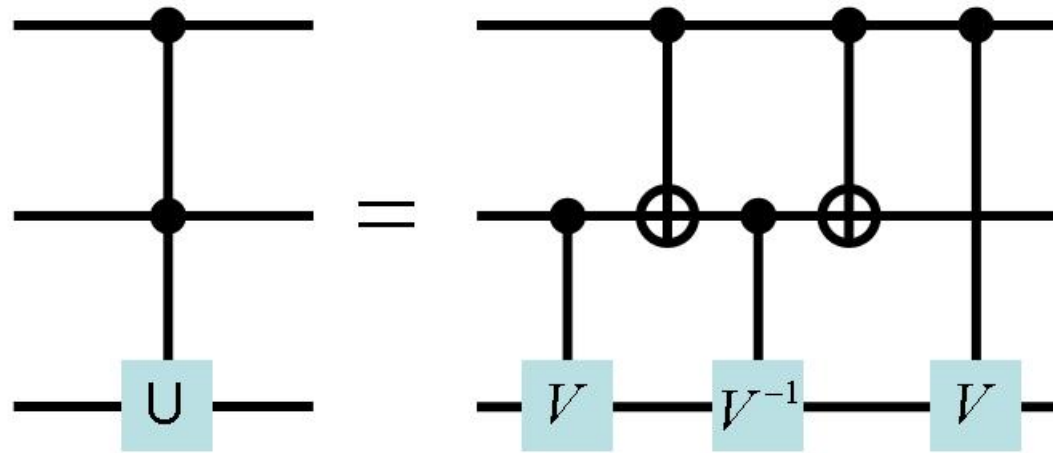


$$S_{\alpha[1]} A_{1[2]} C A_{2[2]} C A_{3[2]} |0\rangle |b\rangle = |0\rangle (A_1 A_2 A_3 |b\rangle) = |0\rangle |b\rangle$$

$$S_{\alpha[1]} A_{1[2]} C A_{2[2]} C A_{3[2]} |1\rangle |b\rangle = e^{i\alpha} |1\rangle (A_1 X A_2 X A_3 |b\rangle) = |1\rangle (U |b\rangle)$$

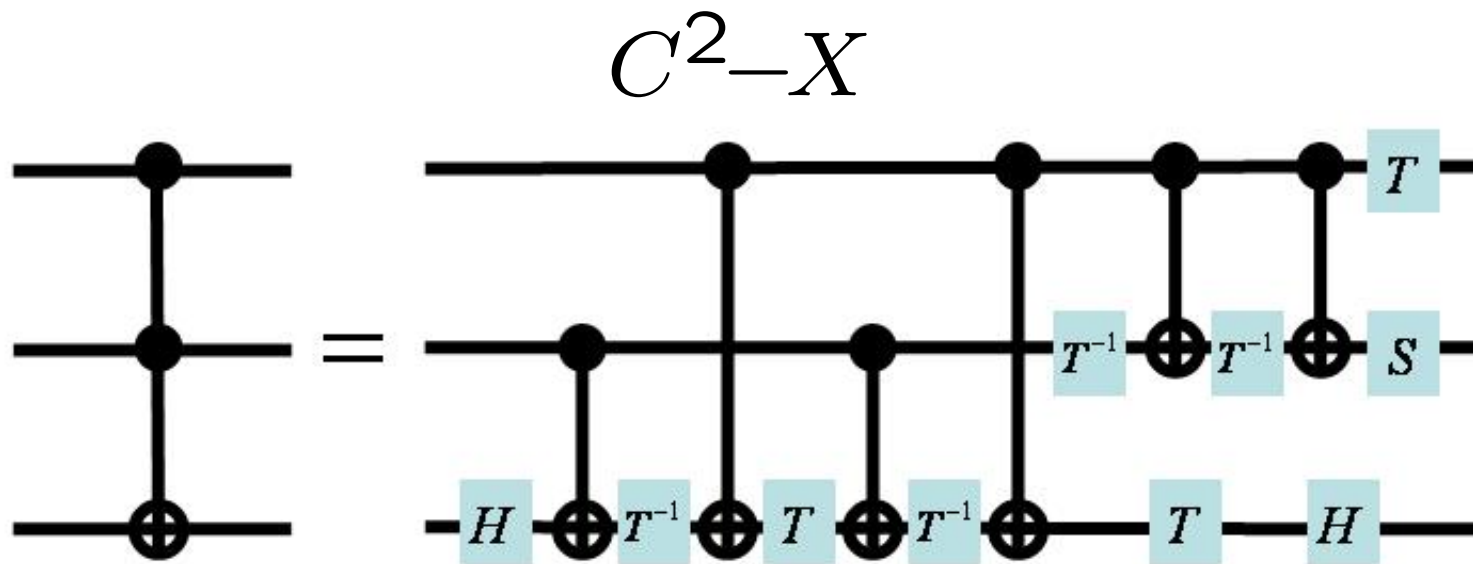
$$C^2-U$$

$$C^2-U |a\rangle |b\rangle |c\rangle = |a\rangle |b\rangle (U^{ab} |c\rangle) \quad V^2 = U$$



$$\begin{aligned} |00\rangle |a\rangle &\rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \rightarrow |00\rangle |a\rangle \\ |01\rangle |a\rangle &\rightarrow |01\rangle (V |a\rangle) \rightarrow |01\rangle (V |a\rangle) \rightarrow |01\rangle |a\rangle \rightarrow |01\rangle |a\rangle \rightarrow |01\rangle |a\rangle \\ |10\rangle |a\rangle &\rightarrow |10\rangle |a\rangle \rightarrow |11\rangle |a\rangle \rightarrow |11\rangle (V^\dagger |a\rangle) \rightarrow |10\rangle (V^\dagger |a\rangle) \rightarrow |10\rangle |a\rangle \\ |11\rangle |a\rangle &\rightarrow |11\rangle (V |a\rangle) \rightarrow |10\rangle (V |a\rangle) \rightarrow |10\rangle (V |a\rangle) \rightarrow |11\rangle (V |a\rangle) \rightarrow |11\rangle (V^2 |a\rangle) \end{aligned}$$

Notez que C^2-X est la porte de Toffoli et peut être implantée en effectuant 8 C et 12 portes à un qubit.



On peut implanter le C^2-X avec 6 portes C et 10 portes à un qubit.

Universalité classique

Tout circuit classique peut être implanté sur un ordinateur quantique en utilisant $C-X$ et des portes à un qubit.

En général à partir d'un circuit classique calculant f on obtient un circuit réversible calculant F

$$f_r(x, b, 0) = (x, f(x) \oplus b, 0)$$

en utilisant la porte de Toffoli quantique on obtient une transformation unitaire U_f telle que

$$U_F |x\rangle |b\rangle |0\rangle = |x\rangle |f(x) \oplus b\rangle |0\rangle$$

et donc une transformation F telle que

$$F |x\rangle |b\rangle = |x\rangle |f(x) \oplus b\rangle$$

et la taille du circuit calculant F est proportionnelle à la taille du circuit classique calculant f .

Quelques identités

$$CX_{[1]}C = X_{[1]}X_{[2]}$$

$$CY_{[1]}C = Y_{[1]}X_{[2]}$$

$$CZ_{[1]}C = Z_{[1]}$$

$$CX_{[2]}C = X_{[2]}$$

$$CY_{[2]}C = Z_{[1]}Y_{[2]}$$

$$CZ_{[2]}C = Z_{[1]}Z_{[2]}$$

$$R_z[1]C = CR_z[1]$$

$$R_x[2]C = CR_x[1]$$