LABORATOIRE D'INFORMATIQUE FONDAMENTALE D'ORLEANS

Université d'ORLÉANS

M2 informatique + GPEX Minerve

TD programmation quantique : fonctions booléennes, qubit, mesure, circuits, problème de Bernstein-Vazirani

Nicolas OLLINGER et Ioan TODINCA

1 Fonctions booléennes et portes quantiques

Rappelons que toute fonction booléenne classique $f : \{0,1\}^n \to \{0,1\}^m$ peut être simulée par un circuit quantique de taille similaire

$$\begin{array}{rccc} U_f & : & \mathbb{C}^{\{0,1\}^{m+n}} & \to & \mathbb{C}^{\{0,1\}^{m+n}} \\ & & |x,y\rangle & \mapsto & |x, f(x) \oplus y\rangle \end{array}$$

pour toutes suites de bits $x = x_1, \ldots, x_n$ et $y = y_1, \ldots, y_m$.

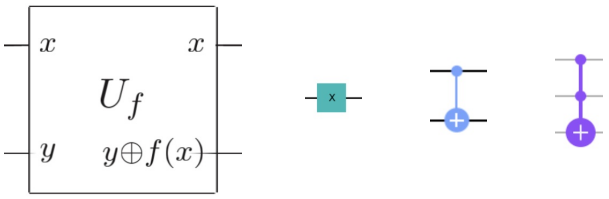


FIGURE 1 – Circuit U_f pour fonction f booléenne, en utilisant les portes NOT, CNOT et CCNOT.

L'objectif de cet exercice est d'implémenter certaines fonctions booléennes avec des portes quantiques. Nous utiliserons les portes NOT, CNOT et CCNOT, également appelées (surtout en Qiskit) portes X, CX et CCX. La dernière est souvent nommée porte de Toffoli.

Proposer les circuits U_f pour les fonctions booléennes suivantes :

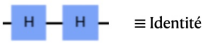
1. NOT : $f_{\text{NOT}}(x_1) = \neg x_1$
2. AND : $f_{\text{AND}}(x_1, x_2) = x_1 \wedge x_2$, que l'on pourrait également écrire $f_{\text{AND}}(x_1, x_2) = x_1 x_2$,
3. OR : $f_{\text{OR}}(x_1, x_2) = x_1 \vee x_2$
4. XOR : $f_{\text{XOR}}(x_1, x_2) = x_1 \oplus x_2$
5. La fonction de Bernstein-Vazirani, $f_s : \{0,1\}^n \to \{0,1\}$ dépendant d'une suite fixée $s = s_1, \ldots, s_n$ de n bits, définie par

$$f_s(x_1, x_2, \ldots, x_n) = x_1 s_1 \oplus x_2 s_2 \cdots \oplus x_n s_n$$

6. n-OR : $f_{\text{OR}_n}(x_1, x_2, \ldots, x_n) = x_1 \vee x_2 \vee \cdots \vee x_n$

2 Qubits, mesure, premiers circuits

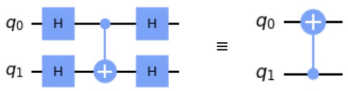
1. Considérer chacun des qubits suivants : $|0\rangle$, $|1\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
   (a) Donner les mesures possibles, avec leurs probabilites respectives.
   (b) Proposer, pour chacun de ces qubits, un circuit pour le construire à partir de $|0\rangle$.
2. Considérons maintenant l'état à deux qubits $|\phi\rangle = \frac{|00\rangle+|11\rangle}{2}$, appelé état de Bell.
   (a) Donner les mesures possibles sur les deux qubits, avec leurs probabilites respectives
   (b) Proposer un circuit pour construire cet état.
   (c) On mesure uniquement le premier qubit. Que devient le deuxième ? [1]
3. Les portes Hadamard jouent un rôle majeur en algorithmique quantique.
   (a) Montrer que $H \cdot H = \mathrm{Id}$:



   (b) Calculer $H^{\otimes n}\left(|0\rangle^{\otimes n}\right)$ et étudier ce circuit.
   (c) Montrer que $H|x\rangle \mapsto \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle$.
   (d) Montrer que $H^{\otimes n}|x\rangle \mapsto \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\bullet y}|y\rangle$ avec $x \bullet y = \bigoplus_i x_i y_i$.
4. Pour toute fonction booléenne $f : \{0,1\}^n \to \{0,1\}$ il existe un circuit U_f qui prend en entrée $n+1$ qubits qui, pour tout entrée $|x\rangle|y\rangle$ calcule $|x\rangle|y \oplus f(x)\rangle$. Montrer qu'en ajoutant une porte X et une porte H de part et d'autre du circuit sur le fil de $|y\rangle$, on obtient un circuit qui sur l'entrée $|x\rangle$ calcule $(-1)^{f(x)}|x\rangle$ à l'aide d'un qubit auxiliaire à $|0\rangle$.

3 Problème de Bernstein-Vazirani

1. Rappeler le problème de Bernstein-Vazirani.
2. Montrer que, en ajoutant des portes H sur chauqe qubit, avant et après une porte CX, cela a l'effet de « renverser » la porte, en permutant le rôle des deux qubits.



3. En utilisant la remarque précédente, montrer que l'algorithme de Bernstein-Vazirani calcule bien la suite cachée s.

1. N'hésitez pas à chercher ce que Einstein a qualifie de *"spooky action at a distance"*, pour deux qubits enchêvetrés comme ici. Vous pouvez aller plus loin en creusant le sujet de la controverse Bohr - Einstein sur le sujet, dont la résolution a été courronée par le prix Nobel de physique en 2022, attribué entre autres au Français Alain Aspect.