

## 1 Mise en contexte

En cours nous avons vu plusieurs algorithmes quantiques avec une structure précise, produisant un résultat souvent déterministe (la réponse souhaitée). Dans ce projet, on s'intéressera à des circuits aléatoires. Ces circuits sont souvent utiles, par exemple comme circuit initial de certains algorithmes d'optimisation [1], ou lors de protocoles de certifications d'ordinateur quantique [2].

Les mesures finales d'un circuit quantique sont généralement non-déterministe, avec une certaine distribution de probabilité sur les résultats possibles. Ici, on s'intéresse au cas où les *circuits* eux-mêmes sont aléatoires, ajoutant une couche supplémentaire d'aléatoire. Ainsi, la *distribution de probabilité* finale d'un circuit devient elle-même une variable aléatoire, qu'on cherchera à caractériser. Plus précisément, on cherchera à montrer dans ce projet que, surprenamment, pour un circuit complètement aléatoire, la distribution de probabilité des résultats de mesures n'est pas distribuée uniformément. Les objectifs principaux de ce travail sont de

1. Comprendre ce qu'est la mesure de Haar
2. Comprendre le concept d'une distribution de probabilité aléatoire
3. Vérifier numériquement qu'un circuit quantique aléatoire produit généralement une distribution de probabilité loin d'une distribution uniforme.

Les questions commençant par un astérisque \* demandent du code.

Pour les questions impliquant du code, vous pouvez utiliser la librairie de votre choix pour réaliser des circuits quantiques. Cependant, je vous suggère d'utiliser la librairie Qiskit. Vous trouverez sur leur site plusieurs ressources pour vous aider à installer et utiliser cette librairie.

Les références suivantes [3, 4] pourraient vous être utiles.

## 2 Mesure de Haar

Lorsqu'on parle de circuits aléatoires, on a besoin de parler de distributions de probabilité sur les circuits eux-mêmes, c'est-à-dire une distribution de probabilité sur les transformations unitaires  $U$ . Une distribution utilisée souvent est la distribution de Haar [4].

**Question #1:** Décrire succinctement en quoi consiste la mesure de Haar pour un circuit quantique à 1 qubit (transformations unitaires  $U \in SU(2)$ ).

**Question #2:** Donner une paramétrisation d'un circuit à un qubit selon la mesure de Haar. C'est-à-dire, donnez une paramétrisation (donnez les  $\alpha, \beta, \gamma, \delta$ ) d'une transformation unitaire

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \quad (1)$$

Pour cette question, vous devez spécifier la distribution de probabilité pour chaque paramètre.

**Question #3:** Décrire succinctement en quoi consiste la mesure de Haar pour un circuit quantique à  $n$  qubits.

### 3 Circuits aléatoires à un qubit

Ici on s'intéresse à un circuit aléatoire à un qubit, et les résultats associés. En supposant qu'un qubit commence dans l'état  $|0\rangle$ , on s'intéresse dans cette section à la valeur moyenne de l'opérateur de Pauli  $Z$ ,

$$z \equiv \langle Z \rangle, \quad (2)$$

où les brackets font référence à la moyenne sur les multiples réalisations du même circuit (moyenne standard pour un opérateur). On met l'emphasis sur le fait que  $z$  est une variable aléatoire ici.

**Question #4:** Pour un circuit  $C$  donné, comment peut-on calculer  $z$  à partir de l'état final  $|\psi\rangle = U|0\rangle$  si vous avez accès à  $|\psi\rangle$  directement ?

**Question #5:** Pour un circuit  $C$  donné, comment peut-on calculer  $z$  si vous avez accès à une machine qui réalise le circuit  $C$  puis effectue des mesures dans la base de  $Z$  ?

**Question #6:** Montrez analytiquement que la moyenne et la variance de  $z$  sont donnés par  $\bar{z} = 0$  et  $\Delta z^2 = \bar{z}^2 - \bar{z}^2 = 1/3$ , où ici la barre sur  $z$  réfère à la moyenne les différentes réalisations de la transformation unitaire  $U$  prise selon la mesure de Haar.

Notez que pour la question ci-dessus,  $z^2 = \langle Z \rangle^2 \neq \langle Z^2 \rangle = 1$ .

On cherche maintenant à vérifier que la paramétrisation de  $U$  obtenue à la question # 2 est bien uniforme. On cherche donc à montrer que la moyenne et variance de  $z$  correspond bien au résultat de la question # 6. Pour ce faire, utilisez une librairie de simulation de circuits quantiques tels que la librairie qiskit.

**\*Question #7:** Montrer numériquement que votre paramétrisation de  $U$  de la question # 2 est bien uniforme. En plus de calculer la moyenne et la variance de  $z$ , donnez un histogramme du nombre d'occurrence en fonction de la valeur de  $z$  obtenue.

Pour la question ci-dessus, vous pouvez utiliser directement la fonction d'onde  $|\psi\rangle$  pour calculer  $z$ . Pour ce faire, la fonction `Statevector` de qiskit pourrait vous être utile. De plus, on cherche à générer explicitement une porte aléatoire  $U$ , pour cette question n'utilisez pas la fonction `random_unitary(2)` de qiskit qui nous donne directement une porte  $U$  aléatoire prise selon la mesure de Haar. (Par contre n'hésitez pas à utiliser cette fonction pour tester votre code.)

## 4 Circuits aléatoires à plusieurs qubits: simulations

Comme vu en classe, un état à  $n$  qubits peut être décrit comme un entier  $j \in [0, 2^n - 1]$  en notation binaire. Pour un circuit quantique donné, on a donc pour chaque état à  $n$  qubits  $j$  une probabilité associée  $p_j$ . Gardez en tête que cette probabilité  $p_j$  est aléatoire, et dépend du circuit  $C$  utilisé. Dans un premier temps, nous allons calculer les propriétés de ces  $p_j$  à l'aide de simulations nous donnant directement la fonction d'onde des qubits de sortie, et donc les  $p_j$ .

Pour un circuit  $C$  donné, on notera la *médiane* des probabilités par

$$p_{\text{med}} = \text{Mediane}(\{p_j\}) \quad (3)$$

Pour caractériser la distribution des  $p_j$ , on considère la mesure  $P_{\text{heavy}}$  suivante. Supposons qu'on mesure les qubits à la fin d'un circuit  $C$ , obtenant le résultat  $j$  (la probabilité d'obtenir ce  $j$  est de  $p_j$ ). À partir de ce  $j$ , on analyse la variable aléatoire  $p_j$  associée au résultat de la mesure. Plus précisément, on regarde si  $p_j$  est plus grand que  $p_{\text{med}}$ . En répétant ce scénario, on peut estimer

$$P_{\text{heavy}} = \mathbb{P}(p_j \geq p_{\text{med}}), \quad (4)$$

où la probabilité  $\mathbb{P}$  est calculée en répétant un tirage au sort des  $j$ . On met l'emphasis sur le fait que  $p_j$  joue deux rôles distincts ici:  $p_j$  est à la fois la probabilité de mesurer  $j$  et une fonction de  $j$  qui correspond à la variable aléatoire à caractériser.

**(\*)Question #8:** À partir d'un état quantique de sortie  $|\psi\rangle$ , décrivez (et codez) un algorithme permettant de calculer  $P_{\text{heavy}}$ .

**Question #9:** Montrez que pour un circuit avec un résultat déterministe (c'est-à-dire un seul  $p_j = 1$ ), on a  $P_{\text{heavy}} = 1$  peu importe le nombre de qubits.

**Question #10:** Montrez que pour un circuit donnant une distribution aléatoire uniforme des résultats  $j$ , on obtient  $P_{\text{heavy}} = 1/2$  peu importe le nombre de qubits. Pour simplifier le calcul de cette question, vous pouvez supposer que la distribution est quasiment uniforme, c'est-à-dire que pour la moitié des  $j$  vous avez  $p_j = 1/2^n + \epsilon$ , et pour l'autre moitié vous avez  $p_j = 1/2^n - \epsilon$ . On suppose que  $\epsilon \ll 1$  et  $n$  le nombre de qubits.

On dira qu'un résultat  $j$  est *lourd* si sa probabilité associée est plus grande que la médiane  $p_j > p_{\text{med}}$ . De manière similaire, on dira que la sortie d'un circuit est lourde si en moyenne les  $j$  obtenus sont lourds.

Dans le reste du projet, on cherche à montrer que le résultat d'un circuit quantique aléatoire est généralement lourd. Plus précisément, on cherche à montrer que

$$\bar{P}_{\text{heavy}} > 2/3, \quad (5)$$

où la barre fait référence à la moyenne sur les circuits.

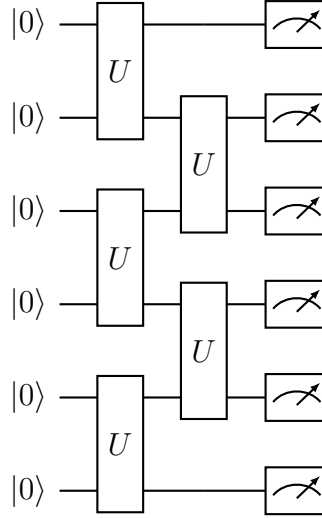
### 4.1 Circuit bruité

Dans la limite de grand bruit, l'état final du circuit tend généralement vers un état complètement mixte.

**Question #11:** Pour un état de sortie complètement mixte, montrez mathématiquement que  $P_{\text{heavy}} = 1/2$ .

## 4.2 Circuit parfait

On s'intéresse maintenant à un circuit du type.



Ici, toutes les portes  $U$  sont différentes et sont prises selon la mesure de Haar sur  $SU(4)$ , c'est-à-dire les portes à deux qubits. Dans qiskit, vous pouvez utiliser la fonction `random_unitary(4)` pour générer une porte à 2 qubits aléatoire. Ce circuit montre une "couche", mais pour les questions suivantes on s'intéressera à plusieurs couches, où le même schéma de portes logiques est répété plusieurs fois avant la mesure finale des qubits. On prendra toujours des transformations différentes à chaque couche.

**\*Question #12:** Estimez  $\bar{P}_{\text{heavy}}$  pour un circuit à 10 qubits et 5 couches de transformations unitaires .

Pour cette question vous pouvez utiliser la fonction `Statevector` de qiskit pour avoir directement accès aux  $p_j$ , sans devoir faire rouler votre algorithme sur les serveurs d'IBM.

**(Bonus)** Comment varie  $\bar{P}_{\text{heavy}}$  en fonction du nombre de qubits et du nombre de couches du circuit appliqués ?

## 5 Circuits aléatoires à plusieurs qubits: machine réelle

Dans la section précédente, vous avez simulé des circuits quantiques aléatoires et vérifié que leur sortie était, en moyenne, lourde. Ici, on s'intéresse à vérifier qu'une machine réelle produit bien les résultats attendus. Lors d'un calcul réel, on peut mesurer les qubits, obtenant un résultat  $j$  à chaque itération. Cependant, on a pas accès directement aux  $p_j$ . Une méthode serait donc d'estimer les  $p_j$  de la manière standard:

$$p_j = \frac{N_j}{N_{\text{tirages}}}, \quad (6)$$

où  $N_j$  est le nombre de fois où le résultat  $N_j$  a été obtenu et  $N_{\text{tirages}}$  est le nombre de répétitions de l'expérience.

**Question #13:** En pratique, quel est le problème avec cette méthode lorsque le nombre de qubits augmente (pour  $n \gtrsim 30$  par exemple)?

Pour évaluer  $\bar{P}_{\text{heavy}}$  sur une machine réelle, on s'aidera donc de simulations classiques. L'algorithme suivant permet d'estimer  $\bar{P}_{\text{heavy}}$  en combinant une machine quantique et un simulateur quantique.

---

**Algorithm 1** Estimé de  $\bar{P}_{\text{heavy}}$

---

```

Compteur  $\leftarrow 0$ 
for  $i = 1$  à  $N_{\text{circuits}}$  do
   $C \leftarrow$  circuit aléatoire
   $\{p_j\} \leftarrow$  Probabilités des résultats pour  $|\psi\rangle = C|0\rangle^{\otimes n}$  (calculé avec simulateur)
   $p_{\text{med}} \leftarrow$  Médiane( $\{p_j\}$ ) pour le circuit  $C$ 
  for  $k = 1$  à  $N_{\text{tirages}}$  do
     $l \leftarrow$  résultat de la mesure pour le circuit  $C$  appliqué sur une machine réelle
     $p_l \leftarrow$  probabilité d'obtenir  $l$  selon une simulation classique (parfaite) de  $C$ 
    if  $p_l \geq p_{\text{med}}$  then
      Compteur  $+= 1$ 
    end if
  end for
end for
return  $\frac{\text{Compteur}}{N_{\text{circuits}} \times N_{\text{tirages}}}$ 

```

---

**Question #14:** Montrez qu'en absence de bruit, c'est-à-dire si la machine effectue parfaitement le circuit désiré, l'algorithme plus haut donne un bon estimé de  $\bar{P}_{\text{heavy}}$  (dans la limite où  $N_{\text{circuits}}, N_{\text{tirages}}$  sont grand).

**Question #15:** Montrez que dans la limite de grand bruit, c'est-à-dire si l'état de sortie de la machine réelle est complètement mixte, l'algorithme suivant donne un estimé  $\bar{P}_{\text{heavy}} = 1/2$ .

**\*Question #16:** Implémentez l'algorithme plus haut pour un ordinateur quantique de votre choix et estimez  $\bar{P}_{\text{heavy}}$ . Afin de bien comparer au résultat idéal, on prendra  $n = 10$  qubits et 5 couches de circuit. Comparez le résultat obtenu à celui de la question #12.

**(Bonus) Question:** Comment varie votre estimé de  $\bar{P}_{\text{heavy}}$  en fonction du nombre de couches du circuit ? Expliquez ce résultat.

## 6 Livrables

Fournir la réponse à toutes les questions énoncées dans ce document (explicitées en caractères gras), ainsi que le code utilisé avec les illustrations correspondantes.

## References

- [1] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A Quantum Approximate Optimization Algorithm, November 2014.
- [2] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, October 2019.
- [3] Olivia Di Matteo. Quantum volume. *PennyLane Demos*, December 2020.
- [4] Olivia Di Matteo. Understanding the Haar measure. *PennyLane Demos*, March 2021.