Vers l'avantage quantique ?

Étude mathématique du Boson Random Sampling

Victor Niaussat

Équipe Projet INRIA PARADYSE Lille - Lab. P.Painleve CNRS

Encadrant: Stephan De Bièvre

Sommaire

Sommaire

Contexte

Université de Lille

cnrs

inria

Laboratoire Paul Painlevé

Equipe Paradyse

centralelille

Introduction

Nous sommes partis de l'article de Hangleiter and Eisert 2022 : *Computational advantage of quantum random sampling*.

L'avantage quantique est le fait de résoudre un problème irréalisable pour un ordinateur classique avec un ordinateur quantique.

L'article nous présente différents problèmes qui pourraient atteindre l'avantage quantique dont le Boson Random Sampling

Est-ce que le Boson Random Sampling pourrait atteindre un avantage quantique ?

Sommaire

Décrire n photons avec un espace de Fock

État de Fock: n nombre de photons, m nombre de modes, s_i nombre de photons dans le mode i

$$|S\rangle = |s_1 \dots s_m\rangle$$

Ensemble des tuples avec n photons et m modes optiques:

$$\Phi_{m,n} = \{S = (s_1, s_2, \dots, s_m) : \sum_{j=1}^{m} s_j = n\}$$

$\{|S\rangle \, , S = (s_1, s_2, \dots, s_m) \in \Phi_{m,n}\}$ forme une base de l'espace de Fock.

Superposition quantique, mesure et règle de Born

Principe de superposition: un même état quantique peut posséder plusieurs valeurs pour une certaine quantité physique observable.

$$|\psi\rangle = \sum_{S\in\Phi_{m,n}} \alpha_S \, |S\rangle$$

Mesure: Mesurer le nombre de photons dans $|\psi\rangle \sim$ Mesurer aléatoirement $|R\rangle$ dans la combinaison linéaire :

$$|\psi\rangle = \sum_{S\in\Phi_{m,n}} \alpha_S \, |S\rangle \xrightarrow{\text{mesure}} |R\rangle \in \Phi_{m,n}$$

Règle de Born: La probabilité pour que le résultat de la mesure du nombre de photons dans chaque mode soit $R = (r_1, r_2, \ldots, r_m)$ est :

$$p_\psi(R) = |\langle R|\psi\rangle| = |\alpha_R|^2$$

Opérateur d'échelle

Opérateur d'annihilation et de création:

$$\begin{aligned} a_i \left| s_1 \dots s_n \right\rangle &= \sqrt{s_i} \left| s_1 \dots s_i - 1 \dots s_n \right\rangle \\ {a_i}^\dagger \left| s_1 \dots s_n \right\rangle &= \sqrt{s_i + 1} \left| s_1 \dots s_i + 1 \dots s_n \right\rangle \end{aligned}$$

Relation de commutation:

$$\begin{aligned} \left[a_i, a_j^\dagger\right] &= a_i a_j^\dagger - a_j^\dagger a_i = \delta_{ij} \\ \left[a_i^\dagger, a_j^\dagger\right] &= \left[a_i, a_j\right] = 0 \end{aligned}$$

Tout état $\left| S \right\rangle$ peut être écrit avec les opérateurs de création:

$$\left| s_1, \dots, s_m \right\rangle = \prod_{i=1}^{m} \frac{(a_i^\dagger)^{s_i}}{\sqrt{s_i!}} \left| 0, \dots, 0 \right\rangle$$

Évolution dans le temps d'un état ou d'un opérateur

Représentation de Schrödinger

L'état $|\psi_t\rangle$ évolue selon l'équation de Schrödinger:

$$\begin{aligned} i\hbar \frac{d}{dt} |\psi_t\rangle &= H |\psi_t\rangle \\ \text{avec } |\psi_0\rangle &= |\varphi\rangle \end{aligned}$$

La solution de cette équation est:

$$|\psi_t\rangle = \exp\left(-\frac{iHt}{\hbar}\right) |\varphi\rangle = U_t |\varphi\rangle$$

Opérateur d'évolution: U_t unitaire

Représentation d'Heisenberg

La valeur moyenne d'un opérateur A

$$\langle A \rangle_{\psi_t} = \langle \psi_t | A | \psi_t \rangle = \langle \varphi | U_{-t} A U_t | \varphi \rangle$$

Un opérateur A évolue avec le temps:

$$A \longrightarrow U_{-t} A U_t$$

L'opérateur évolue selon l'équation de Heisenberg:

$$\frac{dA}{dt} = \frac{1}{i\hbar} [H, A]$$

Sommaire

Modèle de l'interféromètre

Soit U une matrice unitaire de taille $m \times m$. L'interféromètre réalise une transformation linéaire de l'opérateur de création:

$$b_j^\dagger := \sum_{i=1}^{m} U_{ji} a_i^\dagger$$

Pour un état $|\psi_{in}\rangle$ d'entrée, on obtient un état de sortie $|\psi_{out}\rangle$ avec un opérateur unitaire $\varphi(U)$ relié à U qui agit sur les états :

$$|\psi_{out}\rangle = \varphi(U)\,|\psi_{in}\rangle$$

Probabilité de sortie

La probabilité de mesurer $|T\rangle = |t_1 t_2 \dots t_m\rangle$ avec une entrée $|S\rangle = |s_1 s_2 \dots s_m\rangle$ dans la transformation unitaire $\varphi(U)$ a été démontré pour la première fois par Sheel :

Lemme (Scheel 2004)

$$P_U(S,T) = |\langle T|\, \varphi(U)\, |S\rangle|^2 = \frac{|\mathrm{Perm}(U_{S,T})|^2}{\prod_{j=1}^{m}(s_j!)\prod_{i=1}^{m}(t_i!)}$$

$$\mathrm{Perm}(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)}.$$

Physique de l'interféromètre

L'interféromètre est ici un réseau d'éléments optiques les plus simples qui sont les déphaseurs (*phase-shifters*) et les séparateurs de faisceaux (*beamsplitters*):

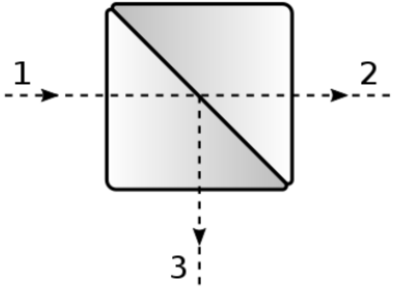


Figure: Beamsplitter

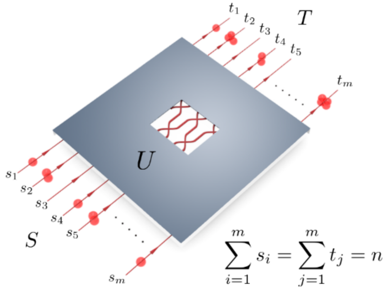


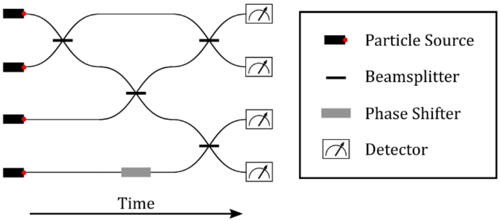
Figure: Circuit linéaire optique

Système de l'interféromètre

Théorème (Reck et al. 1994)

U une matrice unitaire de taille $m \times m$. On peut réaliser un circuit linéaire optique représentant cette matrice U avec $O(m^2)$ beamsplitters et phase-shifters.

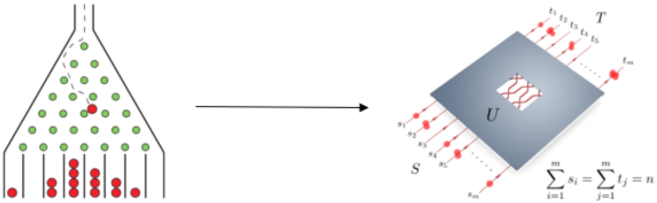
- Une source de photon
- Des beamsplitters et des phase-shifters
- Un détecteur de photon



Analogie avec le Galton Board

On peut voir le Boson random sampling comme une planche de Galton:

- Les boules sont des photons
- Les clous sont des beamsplitters et phase-shifters
- L'ensemble des clous est la matrice U unitaire
- La loi normale est la densité de probabilité avec les permanents



Intérêt du Boson random sampling : vers l'avantage quantique ?

La principale raison de l'intérêt croissant pour le Boson random sampling est qu'on pense fortement qu'il permet de faire un avantage quantique.

Théorème

L'approximation du permanent $|\mathrm{Perm}(X)|^2$ *est un problème* $\#P$*-difficile.*

Theorem (Aaronson and Arkhipov 2013)

Le problème exact du Boson Random Sampling n'est pas efficacement solvable par un ordinateur classique, à moins que $P^{\#P} = BPP^{NP}$ *et que la hiérarchie polynomiale s'effondre au troisième niveau.*

" Simuler classiquement et efficacement le Boson random sampling $\longrightarrow$ c'est comme si $P = NP$ "

Sommaire

Complexité P et NP

Definition (P)

Un langage $L \subset \{0,1\}*$ est dans la classe P s'il existe un algorithme classique $\mathcal{A}$ qui, étant donné $x \in \{0,1\}^*$ en entrée, décide si $x \in L$ en temps d'exécution polynomial en $|x|$:

$$x \in L \iff \mathcal{A}(x) = 1$$

Definition (NP)

Un langage $L \subset \{0,1\}^*$ est dans la classe NP s'il existe un polynôme $p : \mathbb{N} \to \mathbb{N}$ et un algorithme classique en temps polynomial$\mathcal{V}$ (appelé le vérificateur de L) tel que pour tout $x \in \{0,1\}^*$,

$$x \in L \iff \exists y \in \{0,1\}^{p(|x|)} : \mathcal{V}(x,y) = 1$$

.

Définitions supplémentaire

Definition (X-hard)

Soit X une classe de complexité. On dit qu'un problème et X-difficile (ou X-hard) si on peut le ramener à un problème de complexité X par une réduction polynomiale, c'est à dire qu'il existe une fonction $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ qui permet de passer du problème difficile au problème de classe X.

Definition (X-complet)

Soit X une classe de complexité. On dit qu'un problème et X-complet si il est à la fois X et X-hard.

Definition (Exposant de complexité)

Soit X et Y deux classes de complexité. On dit qu'un problème est dans la classe X^Y (nous écrivons une classe de complexité X en exposant d'une autre classe Y) si le problème est dans X ayant accès à ce que l'on peut appeler un oracle (boîte noire) ayant accès à un algorithme résolvant des problèmes arbitraires dans la classe Y

Complexité P et NP

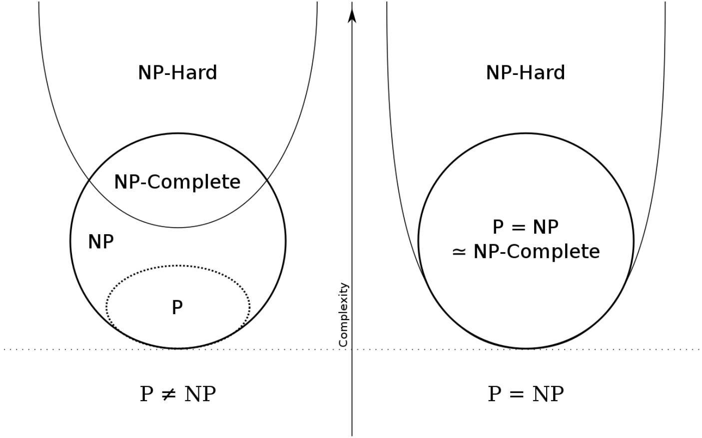


Figure: Diagramme d'Euler

Complexité $\#P$

Definition

La classe de fonctions $\#P$ est la classe de toutes les fonctions $f : \{0,1\}^* \longrightarrow \mathbb{N}$ pour lesquelles il existe un algorithme classique en temps polynomial $\mathcal{A}$ et un polynôme $p : \mathbb{N} \longrightarrow \mathbb{N}$ tel que

$$f(x) = Card\Big(\{y \in \{0,1\}^{p(|x|)} : \mathcal{A}(x,y) = 1\}\Big)$$

.

Definition (Hiérarchie polynomiale)

La hiérarchie polynomiale est l'ensemble des classes $(\Sigma_i^P)_{i\in\mathbb{N}}$ tel que :

$$\Sigma_0^P = P$$

$$\forall i \in \mathbb{N}^*, \Sigma_{i+1}^P = NP^{\Sigma_i^P}$$

On sait qu'une égalité entre classes d'un même niveau ou de niveaux consécutifs dans la hiérarchie impliquerait un " effondrement" de la hiérarchie à ce niveau.

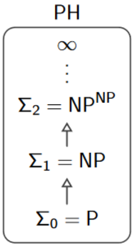


Figure: Hiérarchie polynomiale

Theorem (Théorème de Toda (1991))

$$\bigcup_{i\in\mathbb{N}} \Sigma_i^P = PH \subset P^{\#P}$$

Le théorème dit, en d'autres termes, que pour tout problème dans la hiérarchie polynomiale, il existe une réduction polynomiale à un problème de comptage.

Stratégie : Montrer que si le BRS est possible, alors on trouve une égalité entre un niveau de la hiérarchie polynomiale et la classe $P^{\#P}$

Sommaire

Theorem (Aaronson & Arkhipov (2011))

Le problème exact du Boson Random Sampling n'est pas efficacement solvable par un ordinateur classique, à moins que $P^{\#P} = BPP^{NP}$ et que la hiérarchie polynomiale s'effondre au troisième niveau.

Ce théorème semble compliqué mais il nous dit que si il existe un algorithme classique qui puisse simuler l'échantillonage aléatoire de Boson, alors c'est comme si $P = NP$.

Theorem (1983 Stockmeyers)

Soit une fonction $f : \{0,1\}^n \to \{0,1\}$ booléenne et

$$p = Pr_{x \in \{0,1\}^n}[f(x) = 1] = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} f(x)$$

.

Alors, $\forall c \leq 1 + 1/poly(n)$, il existe un algorithme de classe $FBPP^{NP}$ qui approxime p avec une erreur multiplicative c

Lier la probabilité d'acceptation au calcul du permanent

Theorem

L'approximation du permanent $|\mathrm{Perm}(X)|^2$ est un problème $\#P$-difficile.

Soit $\mathcal{O}$ un algorithme randomisé $\mathcal{O}$ réalisant le Boson random sampling

$$
\begin{aligned}
p_A &= \Pr_r[\mathcal{O}(X,r) = 1_n] \\
&= |\langle 1_n| \varphi(U) |1_n\rangle| \\
&= |\mathrm{Perm}(U_{n,n})|^2 = |\mathrm{Perm}(Y)|^2 \\
&= \varepsilon^{2n} |\mathrm{Perm}(X)|^2
\end{aligned}
$$

Alors, approximer p_A avec un facteur multiplicatif g est un problème $\#P$-difficile.

D'après le théorème de Stockmeyer, il est possible d'approximer p_A d'un facteur multiplicatif g à l'aide d'un algorithme de classe $FBPP^{NP^{\mathcal{O}}}$.

Lier la probabilité d'acceptation au calcul du permanent

Theorem ((1983) Sipser, Gacs, Lautemann)

$$BPP \subset \Sigma_2^P \implies BPP^{NP} \subset (\Sigma_2^P)^{NP} = \Sigma_3^P$$

$$\begin{aligned}
\text{(Possibilité du BRS)} &\implies \text{Les problèmes d'approximation } \#P - \text{difficile sont dans } BPP^{NP} \\
\text{(+ Théorème de Toda)} &\implies PH \subset P^{\#P} \subset BPP^{NP} \\
\text{(+ Théorème de Sipser)} &\implies PH = BPP^{NP} = \Sigma_3^P \\
\text{(+ Égalité à un niveau HP)} &\implies PH \text{ s'effondre à } \Sigma_3^P
\end{aligned}$$

Sommaire

État du travail

Ce qui a été fait:

- Définir le formalisme mathématique de l'optique quantique
- Décrire l'interféromètre
- Décrire le modèle du Boson random sampling et son intérêt pour montrer l'avantage quantique
- Définir et démontrer la complexité des problèmes
- Montrer le théorème d'Aaronson et Arkhipov pour le problème du calcul exact

Le BRS demeure tout de même un défi à la fois expérimental et théorique car:

- Demande des ressources considérables
- Possède des interférences
- La validation expérimentale est trop complexe

References I

Aaronson, Scott and Alex Arkhipov (Feb. 2013). “The Computational Complexity of Linear Optics”. In: *Theory of Computing* 9. Number: 4 Publisher: Theory of Computing, pp. 143–252. DOI: 10.4086/toc.2013.v009a004. URL: https://theoryofcomputing.org/articles/v009a004/ (visited on 11/12/2022).

Hangleiter, Dominik and Jens Eisert (Nov. 2022). *Computational advantage of quantum random sampling*. arXiv:2206.04079 [cond-mat, physics:quant-ph]. DOI: 10.48550/arXiv.2206.04079. URL: http://arxiv.org/abs/2206.04079 (visited on 11/10/2022).

Reck, Michael et al. (July 1994). “Experimental realization of any discrete unitary operator”. en. In: *Physical Review Letters* 73.1, pp. 58–61. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.73.58. URL: https://link.aps.org/doi/10.1103/PhysRevLett.73.58 (visited on 11/17/2022).

Scheel, Stefan (June 2004). *Permanents in linear optical networks*. arXiv:quant-ph/0406127. DOI: 10.48550/arXiv.quant-ph/0406127. URL: http://arxiv.org/abs/quant-ph/0406127 (visited on 11/23/2022).

Merci pour votre attention