

# Qu'est ce que le calcul quantique ?

Géraud Sénizergues

cours donné à l'ENSEIRB, Bordeaux.

12/03/2024

## Dans ce cours

- 1 L'actualité
  - Décisions politiques
  - Exploits technologiques
- 2 Un peu d'histoire
- 3 La mécanique quantique
  - Cadre mathématique et postulats
  - Un modèle de calcul quantique
  - Impact sur la calculabilité/complexité
- 4 Cryptographie quantique
- 5 Les algorithmes quantiques
- 6 Les algorithmes répartis quantiques
- 7 Les réalisations physiques

## Après ce cours

### Pratique :

<https://mediapod.u-bordeaux.fr/video/41854-hello-quantum-world-comment-jai-execute-mon-premier-programme-quantique>

### Théorie :

Un peu **plus** (cours de **3 heures**) :

[https://dept-info.labri.fr/~ges/TALKS/talk\\_marseille\\_lis23.pdf](https://dept-info.labri.fr/~ges/TALKS/talk_marseille_lis23.pdf)

**Encore plus** (cours de **32 heures** et references) :

[https://dept-info.labri.fr/~ges/ENSEIGNEMENT/CALCULQ/cours\\_td\\_calculq.html](https://dept-info.labri.fr/~ges/ENSEIGNEMENT/CALCULQ/cours_td_calculq.html)

# L'actualité

# Rapport de I. Kerrenidis et alii



# Plans de recherche

France : Emmanuel Macron le 21/01/21,  $1,8 \cdot 10^9$  Euros, sur 5 ans  
Region aquitaine : Alain Rousset le 10/02/21,  $10 \cdot 10^6$  Euros pour 2020/23

Suisse : Entreprise Quantum-ID

Royaume-uni : en 2016  $300 \cdot 10^6$  euros, sur 5 ans.

Etats-unis :  $75 \cdot 10^6$  dollars publics. Entreprises IBM, Google, Quantinuum (EU-UK).

Canada : entreprise D-wave.

Chine :  $8 \cdot 10^9$  Euros (dixit Futura Tech)

# Entreprises francaises

**PASQAL**-lancée en Mars 2019- Saclay-proclame réaliser 1000 qbits en 2024

**QUANDELA**- lancée en 2017- Massy- issue du C2N (public)- recherches de Pascale Senellart-Mardon

**ALICE-and-BOB**- Paris- stages bac+4 -recrute un ingénieur génie logiciel

**ATOS**- Bordeaux - Logiciel quantique

# Recherche académique à Bordeaux

Groupe de Travail Quantique-2016-2023

Equipe de recherche Informatique Quantique-2023-...

## Equipe de Google

Deux équipes affirment avoir atteint la “suprématie quantique” :

Frank Arute et al.

Quantum supremacy using a programmable  
superconducting processor.

Nature, 574 :505-510, 2019.

## Equipe universitaire chinoise (Heihfei, Shangai, Beijing)

**Quantum computational advantage** using photons

Han-Sen Zhong, Hui Wang, ...Jian-Wei Pan

Science 18 Dec 2020 :

Vol. 370, Issue 6523, pp. 1460-1463

# Un peu d'histoire

## Calcul/Information classique et physique classique

- Brillouin 1956 : Science and [information theory](#)
- Landauer, Bennet, Toffoli [ $\sim$  1960] : calcul [réversible](#)
- Gandy 1980 : déduit la [thèse de Church-Turing](#) des lois de la physique [classique](#).

## Calcul/Information quantique et physique quantique

- Feynmann 1982 : faire calculer les lois de la mécanique quantique ...par des **systèmes quantiques**
- Deutsch 1985 : machine de Deutsch i.e. machine de Turing , mais **quantique**  
démontre l'existence d'une machine **universelle** quantique.
- Arrighi-Dowek 2012 : déduisent la **thèse de Church-Turing** des lois de la physique **quantique**.

# Physique “informationnelle”

J.A. Wheeler [directeur de thèse de Feynmann] : “**Everything is information**” changement de paradigme, voir [Gruska, 2007, poly de calcul quantique].

P. Höhn : **déduit** la formulation de la mécanique quantique (espaces de Hilbert, opérateurs linéaires hermitiens (resp. unitaires), amplitude de probabilité) d'axiomes “**informationels**” i.e. sur l'acquisition et la communication d'informations.

# La mécanique quantique

# Espace des états

Un système physique  $\mathcal{S}$  est décrit par un espace de Hilbert  $\mathcal{H}$ .  
Chaque état du système est décrit par un vecteur unitaire :

$$|\psi\rangle \in \mathcal{H}, \quad \langle\psi|\psi\rangle = 1.$$

Système  $\mathcal{S}$  formé de **deux** particules  $A_1, A_2$  :  
 $\mathcal{H}_1$  (resp.  $\mathcal{H}_2$ ) est l'espace de  $A_1$  (resp.  $A_2$ ).  
L'espace du système entier est

$$\mathcal{H} := \mathcal{H}_1 \otimes \mathcal{H}_2.$$

Système  $\mathcal{S}$  formé de **n sous-systèmes**  $\mathcal{S}_1, \dots, \mathcal{S}_n$  :

$$\mathcal{H} := \bigotimes_{j=1}^n \mathcal{H}_j.$$

# Evolution

Espace des états : sphère unité d'un espace de Hilbert  $\mathcal{H}$ .

Équation de Schrödinger :

$$i\hbar \frac{d}{dt} |\psi\rangle(t) = H(t) |\psi\rangle(t)$$

où  $H(t) \in \mathcal{L}(\mathcal{H})$ ,  $H(t) = H^*(t)$ .

Si  $H(t)$  est constant, il existe une application dérivable

$U : \mathbb{R} \times \mathbb{R} \rightarrow \mathcal{U}(\mathcal{H})$  telle que,  $\forall t \in \mathbb{R}$ ,  $U(t, t) = I$  et, pour tous  $(t_0, t) \in \mathbb{R} \times \mathbb{R}$  et  $|\psi_0\rangle \in \mathcal{H}$

$$|\psi\rangle(t) = U(t_0, t) |\psi_0\rangle$$

est l'unique solution de l'équation sur  $\mathbb{R}$  t.q.  $|\psi\rangle(t_0) = |\psi_0\rangle$ .

NB : il suffit de poser  $U(t_0, t) = \exp(-i \frac{t-t_0}{\hbar} H)$ .

# Evolution

Exemple 1 :

Etat initial :  $|\psi_0\rangle := |0\rangle$

Porte de Hadamard (opérateur unitaire)

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

Etat final :

$$|\psi_1\rangle = H \cdot |\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

# Evolution

Exemple 2 :

Etat initial :  $|\psi_0\rangle := |10\rangle = |0\rangle \otimes |1\rangle$

Porte cNOT (opérateur unitaire) cNOT :  $|x, y\rangle \mapsto |x, x \oplus y\rangle$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
 dans la base  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ .

Etat final :

$$|\psi_1\rangle = \text{cNOT} \cdot |\psi_0\rangle = |11\rangle$$

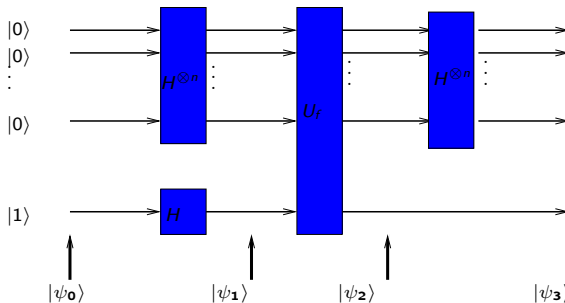
# Evolution

Exemple 3 :

Etat initial :

$$|\psi_0\rangle = |00\dots 0\rangle |1\rangle \in \mathcal{B}^{\otimes(n+1)}$$

Circuit  $\mathcal{C}$  :



Etat final :

$$|\psi_3\rangle = \mathcal{C} \cdot |\psi_0\rangle.$$

# Mesure

Observable  $\mathcal{M}$  : protocole de mesure d'une grandeur sur le système.

Opérateur **hermitien** associé

$$M \in \mathcal{L}(\mathcal{H}, \mathcal{H})$$

tel que

$$M^* = M.$$

Soit  $\mathcal{H}_\lambda = \text{Ker}(M - \lambda I)$ ,  $\text{pr}_\lambda$  la projection orthogonale sur le sous-espace propre  $\mathcal{H}_\lambda$ .

# Mesure

Résultat d'une mesure :

$\mu : \Omega \rightarrow \mathbb{R}$  est une **variable aléatoire**. Si le système est dans l'état  $|\psi\rangle$

$$\Pr\{\mu = \lambda\} = \|\text{pr}_\lambda |\psi\rangle\|^2$$

État après la mesure :

$$\frac{1}{\|\text{pr}_\lambda |\psi\rangle\|} \cdot \text{pr}_\lambda |\psi\rangle$$

la fonction d'onde **"s'effondre"**.

## Mesure et évolution de sous-systèmes

Système  $\mathcal{S}$  formé de deux sous-systèmes  $\mathcal{S}_1, \mathcal{S}_2$ , dont les espaces sont  $\mathcal{H}_1$  (resp.  $\mathcal{H}_2$ ).

Evolution : si  $U_1, U_2$  sont des évolutions possibles de  $\mathcal{S}_1, \mathcal{S}_2$ , alors  $U_1 \otimes U_2$  est une évolutions possible de  $\mathcal{S}_1, \mathcal{S}_2$ .

NB :  $U_1 \otimes U_2 = (U_1 \otimes I_2) \cdot (I_1 \otimes U_2)$

Mesure : la mesure de l'observable  $\mathcal{M}_1$  sur  $\mathcal{S}_1$  est représentée par l'endomorphisme

$$M_1 \otimes I_2$$

sur  $\mathcal{S}$ .

la mesure de l'observable  $\mathcal{M}_2$  sur  $\mathcal{S}_2$  est représentée par l'endomorphisme

$$I_1 \otimes M_2$$

sur  $\mathcal{S}$ .

## Circuits quantiques

un qbit : espace  $\mathcal{B} = \text{Vect}_{\mathbb{C}}(|0\rangle, |1\rangle) \simeq \mathbb{C}^2$ .

$n$  qbits : espace  $\mathcal{B}^{\otimes n}$ .

transition d'évolution : une application unitaire de la forme

$$I_{2^p} \otimes P \otimes I_{2^{n-p-r}}$$

pour un ensemble fini de portes  $P \in U(\mathcal{B}^{\otimes r})$  avec  $r \leq 3$ .

mesure : une famille de projecteurs orthogonaux  $(\text{pr}_j)_{j \in J}$  tels que

$$\sum_{j \in J} \text{pr}_j = I_{2^n}, \quad \text{pr}_j \circ \text{pr}_k = \text{pr}_k \circ \text{pr}_j$$

(i.e.  $\mathcal{H} = \bigoplus_{j=1}^{\ell} \text{Im } \text{pr}_j$  et  $k \neq j \Rightarrow \text{Im } \text{pr}_j \subseteq (\text{Im } \text{pr}_k)^{\perp}$  ).

résultat :  $\text{Pr}(\mu = j) = \|\text{pr}_j |\psi\rangle\|^2$

transition :  $|\psi\rangle \mapsto \frac{1}{\|\text{pr}_j |\psi\rangle\|} \text{pr}_j |\psi\rangle$

# Algorithme

Calcul de  $f : \mathbb{B}^n \rightarrow \mathbb{B}^n$

Étape 1 : calcul **classique** produit un circuit  $C_n$  sur  $n$  qbits

Étape 2 : on **initialise** l'ordinateur quantique dans l'état

$|b_1, b_2, \dots, b_n\rangle$

Étape 3 : Le circuit  $C_n$  fait **évoluer** l'état de  $|b_1, b_2, \dots, b_n\rangle$  à  $|\psi\rangle$ .

Étape 4 : On **mesure**  $|\psi\rangle \rightarrow (\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{R}^n$

on **décode**  $\rightarrow (b'_1, b'_2, \dots, b'_n) \in \mathbb{B}^n$

$$\Pr(\{(b'_1, b'_2, \dots, b'_n) = f(b_1, b_2, \dots, b_n)\}) \geq \frac{2}{3}.$$

# Impact sur la calculabilité/complexité

Calculabilité : aucun impact ([Bennett 70],[Deutsch 85]).

Complexité : peut être **réduite**

pourquoi ? :

1- **superposition** → grand nombre d'états :

sur  $n$  bits :  $2^n$  états possibles  $(b_1, b_2, \dots, b_n)$  ( $b_i \in \{0, 1\}$ )

sur  $n$  **q**bits :  $2^{2^n}$  états discrets possibles :

$$\frac{1}{2^{n/2}} \sum_{(b_1 b_2 \dots b_n) \in \{0,1\}^n} \alpha(b_1 b_2 \dots b_n) |b_1\rangle \otimes |b_2\rangle \dots |b_n\rangle$$

(où  $\alpha : \mathbb{B}^n \rightarrow \{1, -1\}$ ).

## Impact sur la calculabilité/complexité

2- **superposition** → parallélisme :

sur  $n$  bits :  $n$  opérations en parallèle possibles (XOR en parallèle par exemple)

sur  $n$  **q**bits :  $2^n$  opérations en parallèle possibles : Si  $f : \mathbb{B}^n \rightarrow \mathbb{B}$  et  $U_f : |\vec{b} \otimes c\rangle \mapsto |\vec{b} \otimes (c \oplus f(\vec{b}))\rangle$

$$\begin{aligned} U_f H^{\otimes(n+1)} |0^n\rangle |1\rangle &= \frac{1}{\sqrt{2^{n+1}}} U_f \left( \sum_{\vec{z} \in \mathbb{B}^n} |\vec{z}\rangle \right) \otimes (|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{\vec{z} \in \mathbb{B}^n} (-1)^{f(\vec{z})} |\vec{z}\rangle \otimes (|0\rangle - |1\rangle) \end{aligned}$$

## Impact sur la calculabilité/complexité

Définition :

Un état  $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$  est dit **intriqué** s'il n'est pas de la forme  $|u_1\rangle \otimes |u_2\rangle$  pour des vecteurs  $u_1 \in \mathcal{H}_1, u_2 \in \mathcal{H}_2$ .

3- **intrication**  $\rightarrow$  **corrélations** étroites entre les résultats de mesures de qbits différents.

en physique : “paradoxe” [Einstein-Podolsky-Rosen 1935].

en calcul quantique :

- jeux quantiques où une équipe de 2 joueurs quantiques avec des mémoires intriquées ont une stratégie **meilleure** que toute équipe de joueurs classiques
- les algorithmes : une mesure de  $k$  q-bits “**projette**” l'état global des  $n$  qbits, ce qui “**sélectionne**” l'état des  $(n-k)$  autres q-bits.

# Cryptographie quantique

# Protocole de Bennett-Brassard 1984

**But** : Alice et Bob disposent d'un canal authentifié.

A et B peuvent échanger des 0, 1 sur ce canal et aussi sur un canal public.

l'espion E peut écouter le canal.

A et B doivent se mettre d'accord sur une clé  $c \in \{0, 1\}^n$

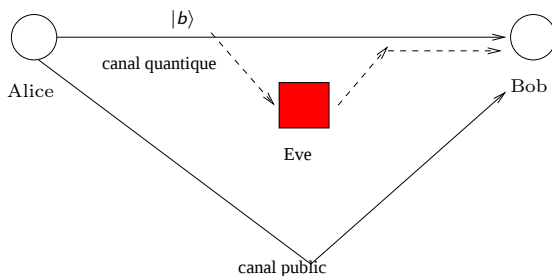
**Difficultés** :

1- A et B doivent **connaître la clé**.

2- sans qu'un adversaire **E ne puisse connaître** cette clé.

Pour A,B,E : connaître demande de **mesurer** le qbit, ce qui le modifie.

# Protocole de Bennett-Brassard 1984



Protocole de [Bennett-Brassard 1984] : sécurité fondée sur les lois de la physique quantique

Protocoles classiques (sécurité fondée sur une hypothèse de théorie de la complexité).

Exemple : RSA < “le problème de la factorisation d'un nombre entier est difficile”.

# Les algorithmes quantiques

# Algorithme de Grover

DONNÉE :  $f : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/2\mathbb{Z}$

RÉSULTAT : Un vecteur  $\vec{x} \in (\mathbb{Z}/2\mathbb{Z})^n$  tel que  $f(\vec{x}) = 1$ .

Donnée : la “boîte noire”  $U_f : \mathcal{B}^{\otimes n} \otimes \mathcal{B} :$

$$U_f |x\rangle |y\rangle := |x\rangle |y \oplus f(x)\rangle .$$

temps :  $O(\sqrt{N})$  où  $N = 2^n$ .

On peut trouver dans une base de donnée de taille  $N$  une réponse à la requête  $f(\vec{x}) = 1$ ? en temps  $O(\sqrt{N})$ .

Algos classiques (probabilistes) :  $\Omega(N)$ .

# Algorithme de Simon

DONNÉE :  $f : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/2\mathbb{Z}$

fortement périodique i.e.  $\exists D \subseteq (\mathbb{Z}/2\mathbb{Z})^n$  s.t.

$$\forall x, y \in (\mathbb{Z}/2\mathbb{Z})^n, \quad f(x) = f(y) \Leftrightarrow (x - y \in D)$$

RÉSULTAT : Une base de  $D$ .

Donnée : la “boîte noire”  $U_f$  :

$$U_f |x\rangle |y\rangle := |x\rangle |y \oplus f(x)\rangle.$$

Temps :  $O(n^3)$ .

Algos classiques (probabilistes) :  $\Omega(2^{n/2})$ .

# Algorithme de Simon

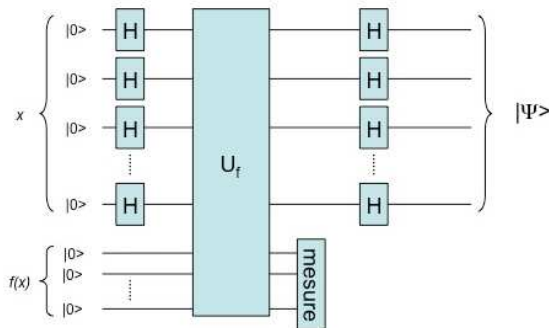


Figure – Le circuit.

# Algorithme de Shor

DONNÉE :  $n \in \mathbb{N}$  qui est composé.

RÉSULTAT : Une décomposition  $n = p \times q$  avec  $p \geq 2, q \geq 2$ .

Temps :  $O(\log(n)^2)$ .

Algos classiques (probabilistes) connus :  $O(2^{\sqrt{\log(n)}})$ .

Autres algorithmes : <https://quantumalgorithmzoo.org>  
(435 articles).

# Les algorithmes répartis

## Le problème

Alice et Bob calculent ensemble. Chacun a une part des données :

DONNÉES :  $D_A$  (vue par A),  $D_B$  (vue par B)

CALCULER :  $f(D_A, D_B)$

COMPLEXITÉ **de communication** : le nombre de (q)bits échangés par A,B au cours du calcul.

## Complexité de communication

Un exemple : ici A peut envoyer des qbits à B mais pas en sens opposé.

DONNÉES de A :  $x \in \mathbb{B}^{[0, 2N-1]}$

DONNÉES de B : un couplage  $C \subseteq [0, N_1] \times [N, 2N - 1]$

CALCULER : un couple  $((i, j), x_i \oplus x_j)$  tel que  $(i, j) \in C$ .

COMPLEXITÉ de communication quantique :  $O(\log(n))$   
complexité classique (probabiliste)  $\Omega(n)$ .

# Les réalisations physiques

## Réalisation de qbits

Exposé de Pascale Senellart, DR CNRS, médaille d'argent du CNRS :

<https://webcast.in2p3.fr/video/>

les — debuts — de — l'ordinateur — quantique

## Cryptographie quantique (ID Quantique)

ID Quantique : entreprise privée suisse. Produit et vend

- des **générateurs aléatoires** fondés sur la mesure d'un système quantique
- des boîtiers qui implémentent le **protocole cryptographique** de [Bennett-Brassard 1984]  
(utilisé pour les élections dans le canton de Genève en Octobre 2007)

## Calcul adiabatique (D-wave)

**D-wave** : entreprise privée canadienne.

Machines de 2000 qbits.

Implémente le “modèle adiabatique”.

Machine **non-universelle**. Résout des problèmes de minimisation de formes quadratiques.

Visite à Bordeaux en Février 2016.

## Circuits (IBM)

**IBM** :entreprise privée (US).

The “IBM Q Experience” launched in 2016, now consists of 15 publicly available quantum computers ranging from five to 53 qubits in size”.

Semble développer des systèmes hybrides calculateurs classiques-circuits quantiques.

# Circuits (Google)

Quantum supremacy, introduced by [Preskill, 2012] :

“The day when well controlled quantum systems can perform tasks surpassing what can be done in the classical world”.

What is needed to achieve it :

- 1- A **mathematical specification** of a computational problem with a **well defined solution**
- 2- A high-fidelity **programmable computational device** able to perform the task
- 3- A **scaling runtime difference** between the quantum and classical computational processes that can be made large enough as a function of problem size so that **it becomes impractical** for a supercomputer to solve the task using any known classical algorithm

# Circuits (Google)

## 1- 1.1 Problem :

INPUT : quantum circuit  $U$  on 53 qbits,

OUTPUT : sample  $30 \cdot 10^6$  vectors in  $\mathbb{B}^{53}$  with the probability law :

$$\Pr(x) = \frac{1}{53} \cdot |\langle x | U | 0^{53} \rangle|^2.$$

1.2 Test that the answer is a **solution** : statistical tests

1.3 Publish the values of  $U$  and the corresponding set of vectors  
(**everybody** can test)

2- Programmable device : Sycomor, 53 qbits, can implement “any” circuit on 53 qbits.

“**programmable**” : done on 10 different  $U$  of length 20 ( $U$  produced by a random process, with law the Haar-measure on  $U(2^{53})$ ).

Implements the quantum-circuit-model

## Circuits (Google)

3- **Scaling** runtime difference :

theory : non feasible on a classical computer (for a large number  $n$  of qbits)

experiment : **100 s** on Sycomor, **3 days** on IBM supercomputer.

# Echantillonnage de photons (equipe chinoise)

HARVARD UNIVERSITY  
17 Oxford Street  
Cambridge, MA 02138



**Tuesday, February 23, 2021, at 9:30 (Boston)**  
**14:30 (UK/Eire) 15:30 (C.Europe) 22:30 (China)**

[!NOTE EARLIER TIME!](#)

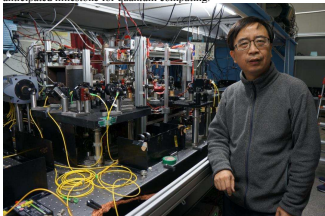
## Mathematical Picture Language Seminar

Zoom at: <https://harvard.zoom.us/j/779283357?pwd=MlRlVW1pYUlnZzQlZGt3blV2pCT1ZUQT09>

[From multi-photon entanglement to quantum computational advantage](#)

Jian-Wei Pan, University of Science and Technology of China

Abstract: By developing high-performance quantum light sources, the multi-photon interference has been scaled up to implement Boson sampling with up to 76 photons out of a 100-mode interferometer, which yields a Hilbert state space dimension of  $10^{30}$  and a rate that is  $10^{14}$  faster than using the state-of-the-art simulation strategy on supercomputers. Such a demonstration of quantum computational advantage is a much-anticipated milestone for quantum computing.



# Echantillonnage de photons (equipe chinoise)

## 1- 1.1 Problème :

ENTRÉE : une matrice  $A \in \mathbb{C}^{m \times n}$  dont les vecteurs colonnes sont unitaires et orthogonaux deux à deux, où  $m = 100$ ,  $n = 76$  qbits,  
SORTIE : échantillon de vecteurs d'entiers  $s = (s_1, s_2, \dots, s_m)$  tels que  $\sum_{i=1}^m s_i = n$  suivant la loi de probabilité :

$$\Pr(s_1, s_2, \dots, s_m) = \frac{|Perm(A_s)|^2}{s_1! s_2! \dots s_m!}$$

où  $A_s$  est la matrice formée de  $s_1$  fois la ligne 1 de  $A$ , ...,  $s_i$  fois la ligne  $i$  de  $A$ , ...,  $s_m$  fois la ligne  $m$  de  $A$ .

1.2 Tester que l'échantillon calculé est une **solution** : tests statistiques

1.3 **Publier** les échantillons.

## Echantillonnage de photons (équipe chinoise)

2- Système **Programmable** : circuit optique avec  $n$  entrées et  $m$  sorties :  $n$  photons (= qbits) sont envoyés sur  $m$  états de sortie, indépendamment pour les  $n$  photons ;  $A$  est la matrice de transition du système ; le résultat est obtenu par une mesure.  $k_i$  = nbre de photons terminant dans le  $i$ -ème état.

Nombre d'échantillon ? taille des échantillons ?

Implémente le modèle de calcul "bosonique-noninteractif" défini par [Aaronson et Arkhipov, 2010].

3- Temps d'exécution :

théorie : intractable pour un ordinateur classique (pour  $n, m$  grands) [Aaronson, Arkhipov, 2013].

Argument-clé : calculer le **permanent** d'une matrice  $n \times n$  est #P-complet.

Experimentation : pas de tentative d'expérience classique (pour le moment).