Génération d'aléa Quantique et intrication

ANOMAN Don Jean Baptiste

Sous la direction de: Monsieur ARNAULT François
Équipe Cryptis , Axe Matis

8 mars 2019


Nord-
Pas-de-Calais-
Picardy
OnTheWorldMap.com
Normandy
Île-de-
France
Alsace-
Champagne-
Ardenne-
Lorraine
Brittany
Pays de la
Loire
Centre-
Val de Loire
Bourgogne-
Franche-
Comté
Aquitaine-
Limousin-
Poitou-
Charentes
OnTheWorldMap.com
Limoges
Auvergne-
Rhône-Alpes
Languedoc-
Roussillon-
Midi-Pyrénées
Provence-
Alpes-
Côte d'Azur
Corsica
Copyright © Ontheworldmap.com

Plan

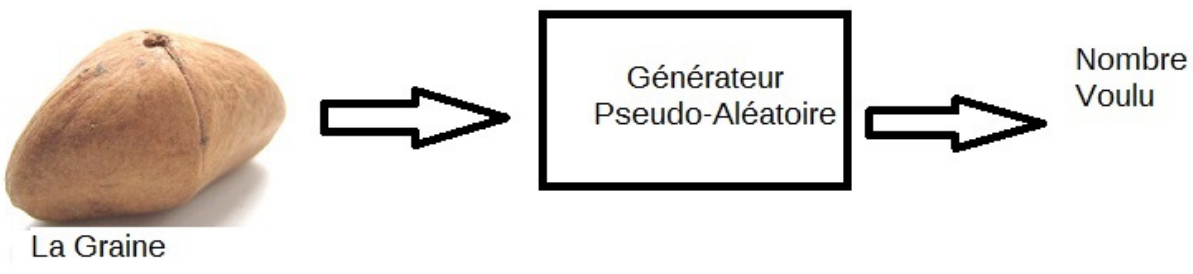
- Motivations et contexte
- La physique quantique et ses apports
- Nos travaux réalisés :
  - Les généralisations directes
  - Les autres angles de production d'aléa
- Perspectives

Motivation et contexte

- Grande importance de l'aléa
  - En cryptographie (algo de chiffrement, clés de session...)
  - Et bien d'autres domaines (la simulation ...)

Comment produire de l'aléa ?

- Pour répondre à ce besoin : La physique classique
  - les générateurs pseudo-aléatoires



Génération de nombre aléatoire en C et C++

Motivation et contexte

- **Inconvénient Majeur** :
  Déterministes $\Rightarrow$ Imprévisibles (temporairement) $\neq$ aléatoires

- Une solution sûre :
  La physique quantique, **l'aléa est intrinsèque**.

La physique quantique et ses apports

Le monde du quantique

La physique quantique et ses apports

Définition

Formalisme expliquant les interactions à l'échelle atomique et subatomique.

La physique quantique et ses apports

1er Postulat

Pour un système quantique :

- $\mathbb{H}$, un $\mathbb{C}-$ espace vectoriel
- "ket" $|h\rangle$ un vecteur de $\mathbb{H}$

La physique quantique et ses apports

Exemple Des Qubits

Les bits normaux : 0 ou 1

La physique quantique et ses apports

Exemple Des Qubits

Les bits normaux : 0 ou 1

Les qubits : éléments de $\mathbb{C}^2$ *de base*

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Ils s'écrivent $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

avec $\alpha, \beta \in \mathbb{C}$; $|\alpha|^2 + |\beta|^2 = 1$ *; vecteurs de norme 1*

La physique quantique et ses apports

3ème Postulat

Les mesures quantiques (projectives) sont définies par des Matrices diagonalisables dans une base orthonormale.

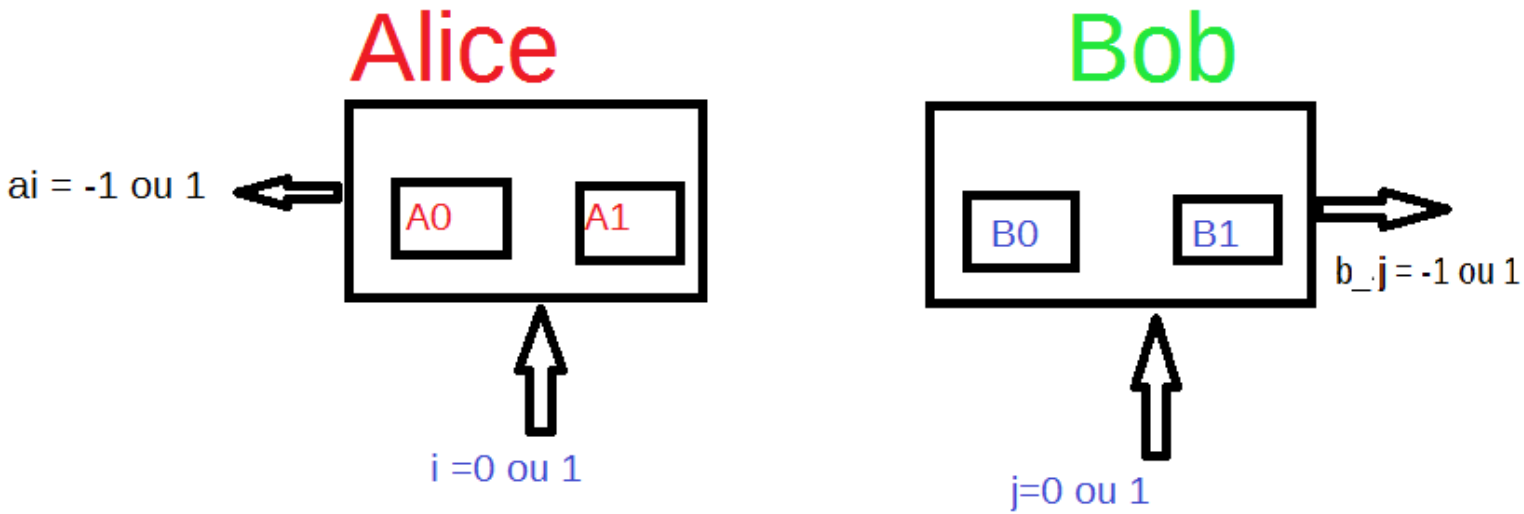
Exemple

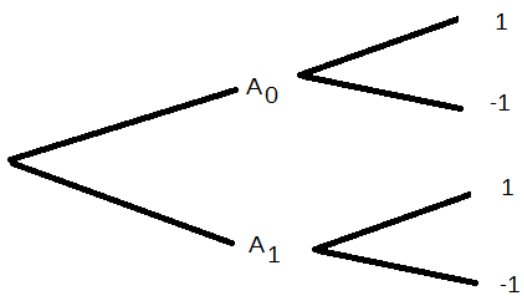
Dans la base canonique $(|0\rangle, |1\rangle)$

- *Soit l'observable* $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Processus déterministe ou manque d'information ?

Le jeu de Bell





$$I = a_0 b_0 + a_0 b_1 + a_1 b_0 - a_1 b_1$$

Outil important : Inégalité de Bell nommée CHSH

Cas déterministe

Inégalité CHSH (Clauser, Horne, Shimony, Holt) 1969

Dans le cadre classique la quantité

$$I = a_0 b_0 + a_0 b_1 + a_1 b_0 - a_1 b_1$$

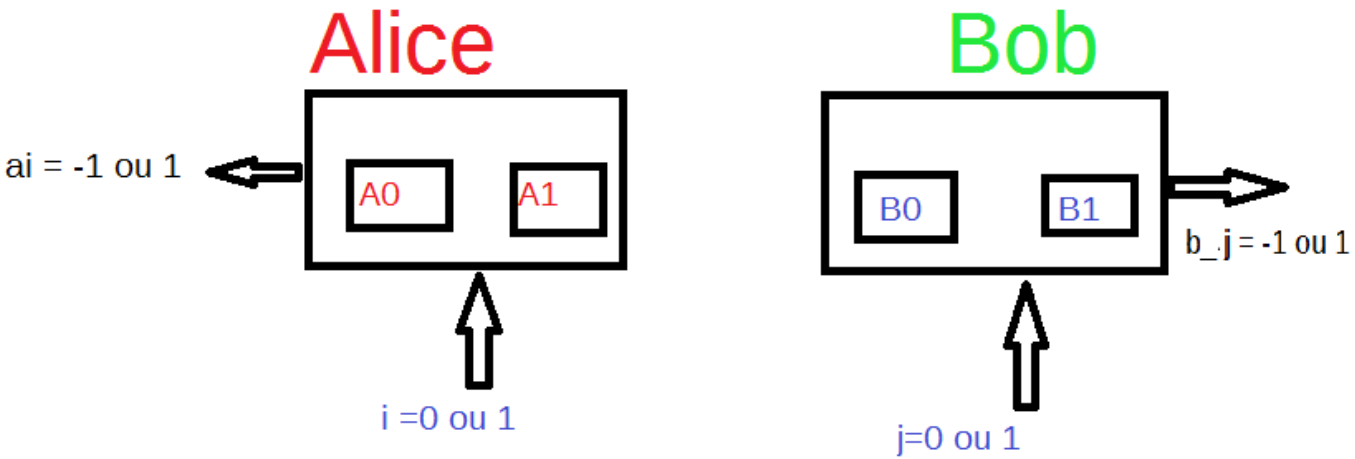
est telle que

$$|I| = 2$$

$$|E(I)| = |E(a_0 b_0) + E(a_0 b_1) + E(a_1 b_0) - E(a_1 b_1)| \leq 2$$

La physique quantique et ses apports

État du système $\{A \quad B\}$: $|\beta_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$



En Physique quantique : $I = 2\sqrt{2} > 2$

La physique quantique et ses apports

Les mêmes causes produisent des **effets différents**

Utilité : Production quantique d'aléa sûr

$$H(AB|XY) = -\sum_{a,b,x,y} p(ab \cap xy) * log_2(p(ab|xy))$$

Quantité d'information potentiellement recueillie par un attaquant.

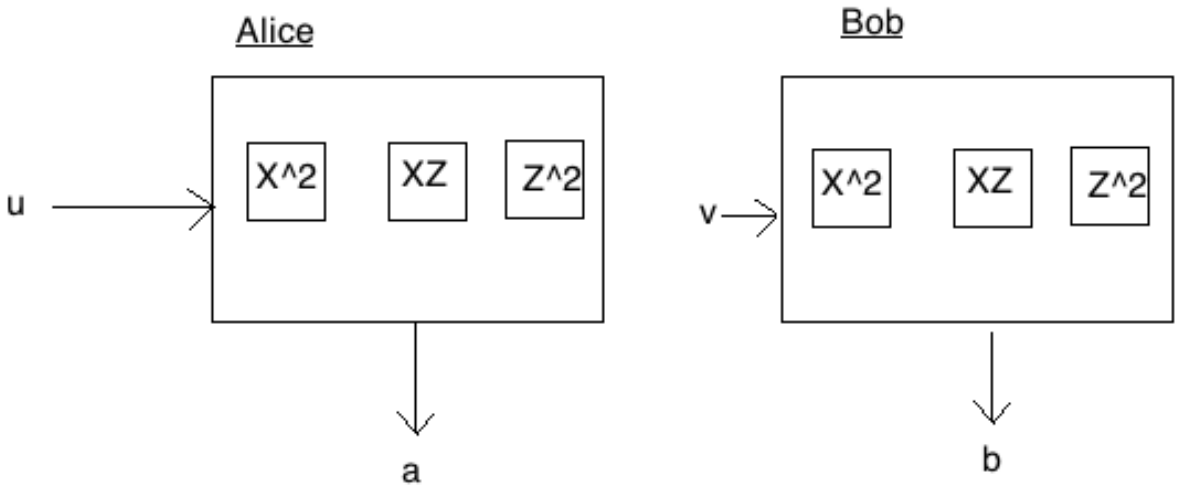
Minorée par

$$f(I) \leq H(AB|XY)$$

avec $f(I) = 1 - log_2(1 + \sqrt{2 - I^2/4})$

Généralisation directe

État du système $\{A \quad B\} : |\Psi\rangle = \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle + \omega|22\rangle)$



Utilisation des

- Inégalités homogènes de Bell développées par monsieur François ARNAULT.
- Des ditters (dont on a prouvé la praticabilité)

Pas de violation conséquente de l'inégalité mais débouché sur le poster suivant

Random number with only one qutrit

{ ARNAULT François with ANOMAN Don }

Motivation, Classical Setting and Bell inequalities' constraints

We aim to produce randomness using a single quantum system, and certify it by quantum only behaviour [2]. In this sense, we imagine the following theoretical setting which produces randomness that could be certified by **Homogeneous Bell Inequalities** [3].
Assume a physical system and a single ternary measurement apparatus whose outcomes are denoted $1; \omega; \omega^2$ (with $\omega^3 = 1$) for commodity. We also set a transformation V, between the system and the device, which could represent a change of orientation for the apparatus, with the property $V^3 = \mathrm{Id}$. Thus according to the number of time we apply the transformation V it gives rise to a different measurement :

$$0 \text{ time} \mapsto A_0; \quad 1 \text{ time} \mapsto A_1; \quad 2 \text{ times} \mapsto A_2;$$

Classical systems

Supposing the system has a classical behaviour, the elements of reality a_i associated to the measurements A_i verify inequalities:
$Im(B) \leq \sqrt{3}/2$ with B a **Homogeneous Bell expression** among the following expressions

$$\begin{array}{ccc} (\omega + x + x^2) & (1 + \omega x + x^2) & (1 + x + \omega x^2) \\ -(\omega^2 + x + x^2) & -(1 + \omega^2 x + x^2) & -(1 + x + \omega^2 x^2) \end{array}$$

or those obtained multiplying them by ω and ω^2. Here x stands for $\omega^2 a_1/a_0 = \omega^2 a_2/a_1$. We thus make isotropic assumption

Quantum Setting

The system is a qutrit.
Here the transformation V has this form:

$$V = \frac{\omega - \omega^2}{3} \begin{pmatrix} \omega & 1 & 1 \\ 1 & \omega & 1 \\ 1 & 1 & \omega \end{pmatrix} \quad \text{hence} \quad V^2 = \frac{1}{\omega - \omega^2} \begin{pmatrix} \omega & 1 & 1 \\ 1 & \omega & 1 \\ 1 & 1 & \omega \end{pmatrix}.$$

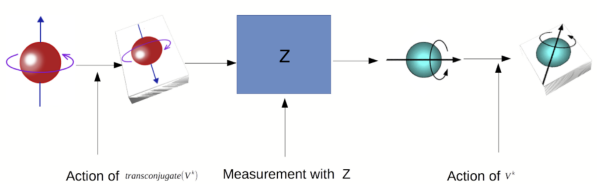
Observables associated to measurements in the three possible configurations are:

$$A_i := V^i Z V^{\dagger i} \quad (\text{with } 0 \leq i \leq 2)$$

$$A_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} = Z; \quad A_1 = \begin{pmatrix} 0 & 0 & \omega \\ \omega^2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \omega ZX; \quad A_2 = \begin{pmatrix} 0 & \omega^2 & 0 \\ 0 & 0 & 1 \\ \omega & 0 & 0 \end{pmatrix} = \omega^2 ZX^2; \quad \text{with} \quad \omega A_1^2 = A_0 A_2$$

Action

1. One chooses a measurement number "k" in the set $\{0, 1, 2\}$.
2. We then apply "k" times the transformation $V^\dagger$ on the particle at the input of the apparatus making Z measurement. After measurement, we also apply "k" times the transformation V

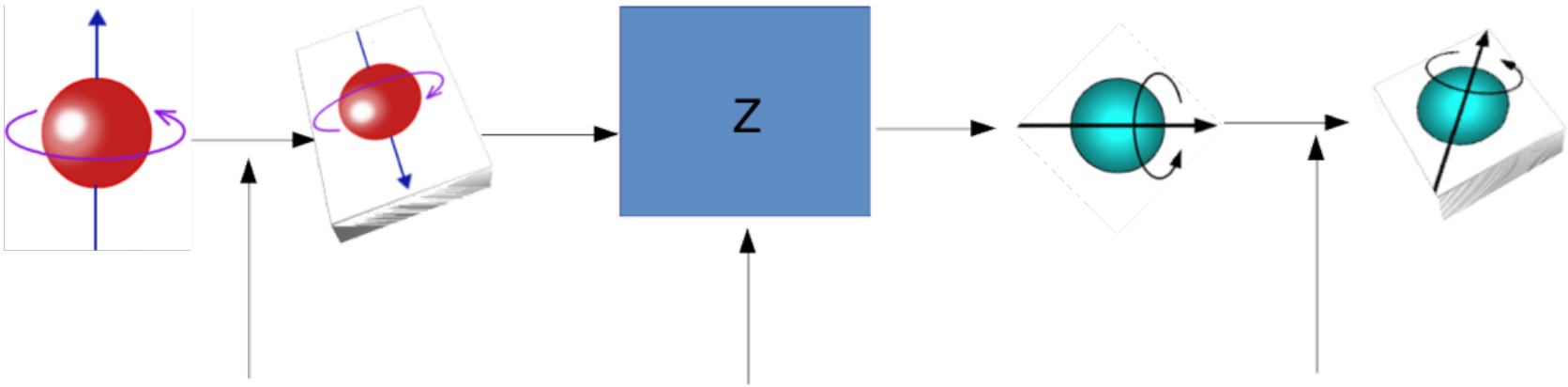


Quantum violations of Bell inequalities

In the **quantum case** we use the Bell Expression $B = (1 + \omega x + x^2)$ which can be written with quantum observable : $B = A_0^2 + \omega A_0 A_2 + A_2^2$. The operator B is such that its eigenvalues have module $\sqrt{3}$ and arguments respectively $(-\frac{23\pi}{18}, \frac{\pi}{18}, \frac{11\pi}{18})$. Thus the greatest imaginary part is given by the first eigenvalue that gives **violation factor of** $2sin(-\frac{23\pi}{18}) \simeq 1.53$.

References

[1] S. Pironio, A. Acín, S.Massard, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, " Random Numbers Certified by Bell's Theorem", arXiv:0911.3427v3 (2010).
[2] M. Um, X. Zhang, J. Zhang, Y. Wang, S. Yangchao, D.-L. Deng, and K. Kim, "Experimental certification of random numbers via quantum contextuality", Nature Scientific Reports 3, 1627 (2013).
[3] François ARNAULT , "A complete set of multidimensional Bell inequalities", J.Phys. A : Math. Theor. 45 (2012) 255304 (18pp)


Z
Action of $transconjugate(V^k)$
Measurement with Z
Action of V^k

- Volonté de la lier à la génération d'aléa avec les polynômes homogènes de Bell
- Étude d'une approche nouvelle de l'intrication (Concurrence)

MERCI POUR VOTRE ATTENTION!!!