Hugo SALOU
M1 ENS Lyon

Tutorial n° 1.

2. Linear algebra

A. 1. $(A^\dagger)^\dagger = \overline{(\overline{A}^T)}^T = \overline{\overline{(A^{TT})}} = \overline{\overline{A}} = A$

2. $(AB)^\dagger = \overline{(AB)}^T = \overline{(B^T A^T)} = \overline{B}^T \overline{A}^T = B^\dagger A^\dagger$.
identique pour $(Av)^\dagger = v^\dagger A^\dagger$.

3. $\langle A^\dagger u, v\rangle = (A^\dagger u)^\dagger v = u^\dagger A^{\dagger\dagger} v = u^\dagger A v = \langle u, Av\rangle$.

B. 1. Si A est hermitienne, $AA^\dagger = AA = A^\dagger A$ donc A normale.
Si A est unitaire, $AA^\dagger = AA^{-1} = \mathbb{1} = A^{-1}A = A^\dagger A$ donc A normale.

2. $(UV)^\dagger = V^\dagger U^\dagger = V^{-1}U^{-1} = (UV)^{-1}$ donc UV est unitaire.

3. $(G+H)^\dagger = \overline{G+H}^T = (\overline{G}+\overline{H})^T = \overline{G}^T + \overline{H}^T = G^\dagger + H^\dagger = G+H$
donc $G+H$ est hermitienne

4. $(vv^\dagger)^2 = v\underbrace{v^\dagger v}v^\dagger = \langle v,v\rangle vv^\dagger = \|v\|^2 vv^\dagger = vv^\dagger$
car v est unitaire

$(vv^\dagger)^\dagger = v^{\dagger\dagger} v^\dagger = vv^\dagger$ donc $vv^\dagger$ est bien une matrice de projection.

Soit $\lambda \in \mathbb{C}$ et u un vecteur.

On a : $P^2 u = Pu$.

$Pu = \lambda u \implies P(Pu) = \overbrace{P(\lambda u)}^{\lambda^2 u} = \lambda u$
$\implies \lambda^2 = \lambda$

D'où $\lambda = 0$ ou $\lambda = 1$.

3. Quantum random access code.

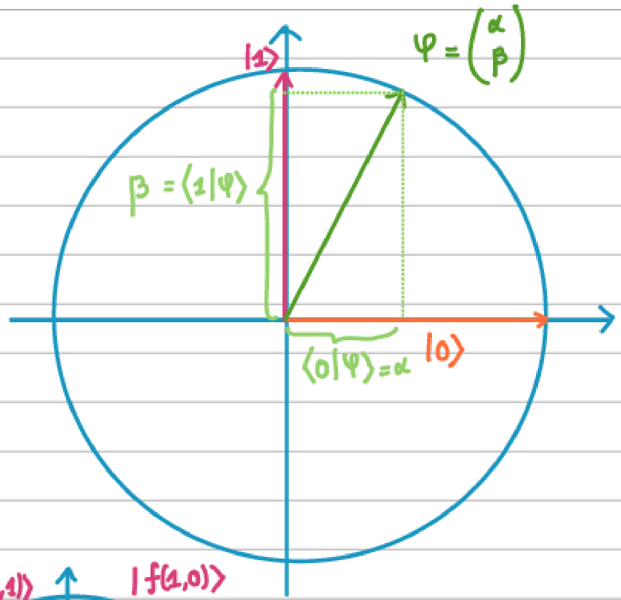
1. On a $f : \{0,1\}^2 \to \{0,1\}$ donc on a nécessairement une collision.
Sans perdre en généralité, supposons $f(0,x) = f(1,x)$.

D'où, pour obtenir le 1er bit, on a :
$f(0,x) \underset{q_0}{\rightsquigarrow} 0$ et $f(1,x) \underset{q_1}{\rightsquigarrow} 1$.

Nécessairement, $q_0 + q_1 = 1$ et $q_0 \geq p$, $q_1 \geq p$,

d'où $p \leq \frac{1}{2}$.

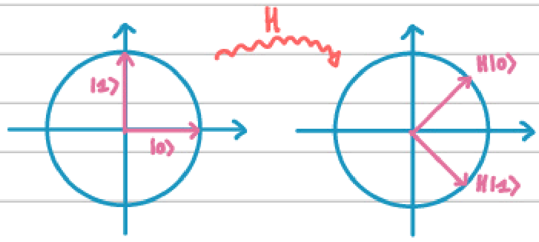
2.



Appliquer une matrice unitaire correspond à une rotation ou une symétrie de ce cercle unitaire (et du vecteur φ dedans).

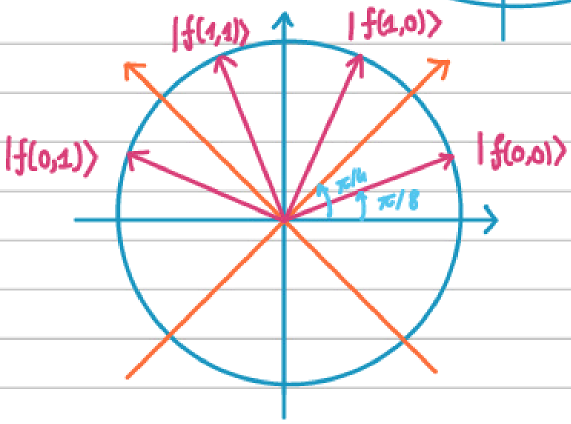
Exemple avec la matrice de Hadamard

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



C'est une symétrie sur l'axe x puis une rotation de $45°$.

3.



$U_1 = \mathbb{1}$ et $U_2 = R_{\pi/4}$.

La probabilité de succès est de $\cos^2(\pi/8) \simeq 0{,}86$.

4. Tensor products

1.

$$A \otimes B = \begin{pmatrix} 0 & e^{2i\pi/3} & 0 & e^{i\pi/3} \\ e^{-2i\pi/3} & 0 & -1 & 0 \\ 0 & -1 & 0 & e^{-i\pi/3} \\ e^{i\pi/3} & 0 & e^{i\pi/3} & 0 \end{pmatrix} ; \quad B \otimes A = \begin{pmatrix} 0 & 0 & e^{2i\pi/3} & e^{i\pi/3} \\ 0 & 0 & -1 & e^{-i\pi/3} \\ e^{-2i\pi/3} & -1 & 0 & 0 \\ e^{-i\pi/3} & e^{i\pi/3} & 0 & 0 \end{pmatrix}$$

2.

a) $$A \otimes (\lambda B) = \begin{pmatrix} a_{11}(\lambda B) & a_{21}(\lambda B) & \cdots \\ a_{12}(\lambda B) & a_{22}(\lambda B) & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} (a_{11}\lambda)B & (a_{21}\lambda)B & \cdots \\ (a_{12}\lambda)B & (a_{22}\lambda)B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} = \lambda A \otimes B$$

d) $$(A \otimes B)^{\dagger} = \begin{pmatrix} a_{11}B & a_{21}B & \cdots \\ a_{12}B & a_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}^{\dagger} = \begin{pmatrix} \overline{a}_{11}B^{\dagger} & \overline{a}_{12}B^{\dagger} & \cdots \\ \overline{a}_{21}B^{\dagger} & \overline{a}_{22}B^{\dagger} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

$$= A^{\dagger} \otimes B^{\dagger}$$

Tutorial 2

II. Warm-up calculations.

1) Measurements and probabilities

$\mathbb{P}(|\varphi\rangle \text{ is measured as } |b\rangle) = |\langle b|\varphi\rangle|^2$

Q1. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state
measuring $|\varphi\rangle$ leads to 0 with prabability 1/2
measuring $|\varphi\rangle$ leads to 1 with prabability 1/2

Q2. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state
measuring $|\varphi\rangle$ leads to 0 with prabability 1/2
measuring $|\varphi\rangle$ leads to 1 with prabability 1/2

Q3. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state
measuring $|\varphi\rangle$ leads to 0 with prabability 1
measuring $|\varphi\rangle$ leads to 1 with prabability 0

Q4. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state
measuring $|\varphi\rangle$ leads to 0 with prabability 1/2
measuring $|\varphi\rangle$ leads to 1 with prabability 1/2

Q5. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state
measuring $|\varphi\rangle$ leads to 00 with prabability 1/2
measuring $|\varphi\rangle$ leads to 01 with prabability 0
measuring $|\varphi\rangle$ leads to 10 with prabability 0
measuring $|\varphi\rangle$ leads to 11 with prabability 1/2

Q6. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state
measuring $|\varphi\rangle$ leads to 00 with prabability 1/2
measuring $|\varphi\rangle$ leads to 01 with prabability 0
measuring $|\varphi\rangle$ leads to 10 with prabability 0
measuring $|\varphi\rangle$ leads to 11 with prabability 1/2

Q7. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state
measuring $|\varphi\rangle$ leads to 00 with prabability 1/4
measuring $|\varphi\rangle$ leads to 01 with prabability 1/2
measuring $|\varphi\rangle$ leads to 10 with prabability 0
measuring $|\varphi\rangle$ leads to 11 with prabability 1/4

Q8. $\| |\varphi\rangle \| = 1$ thus $|\varphi\rangle$ is a state

measuring $|\varphi\rangle$ leads to 00 with probability $1/4$
measuring $|\varphi\rangle$ leads to 01 with probability $1/2$
measuring $|\varphi\rangle$ leads to 10 with probability $1/8$
measuring $|\varphi\rangle$ leads to 11 with probability $1/8$

2) Partial measurements.

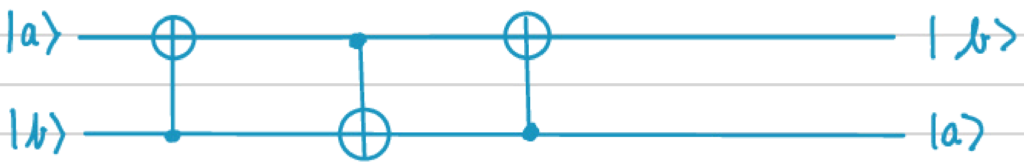
$$\sqrt{2}\,\langle 1|\psi\rangle = \langle 1|0\rangle\cdot\langle 1|\varphi\rangle + \langle 1|1\rangle\langle 1|\psi\rangle$$
$$= \langle 1|\psi\rangle$$
$$=$$

$$|\psi'\rangle := H\otimes 1\,|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle|\varphi\rangle + |-\rangle|\psi\rangle\Big) = \frac{1}{2}\Big(|0\rangle(|\varphi\rangle+|\psi\rangle) + |1\rangle(|\varphi\rangle-|\psi\rangle)\Big)$$

We have that
$$\mathbb{P}(\text{measuring } |1\rangle) = \| |\varphi\rangle - |\psi\rangle \|_2^2 \times \frac{1}{4}$$
$$= (\langle\varphi| - \langle\psi|)(|\varphi\rangle - |\psi\rangle)\times\frac{1}{4}$$
$$= \frac{1}{4}\Big(\langle\varphi|\varphi\rangle + \langle\psi|\psi\rangle - \langle\varphi|\psi\rangle - \langle\psi|\varphi\rangle\Big)$$
$$= \frac{1}{4}\Big(2 - \langle\varphi|\psi\rangle - \overline{\langle\varphi|\psi\rangle}\Big)$$
$$= \frac{1}{2}\Big(1 - \mathrm{Re}(\langle\varphi|\psi\rangle)\Big).$$

3) Gates

Q1.

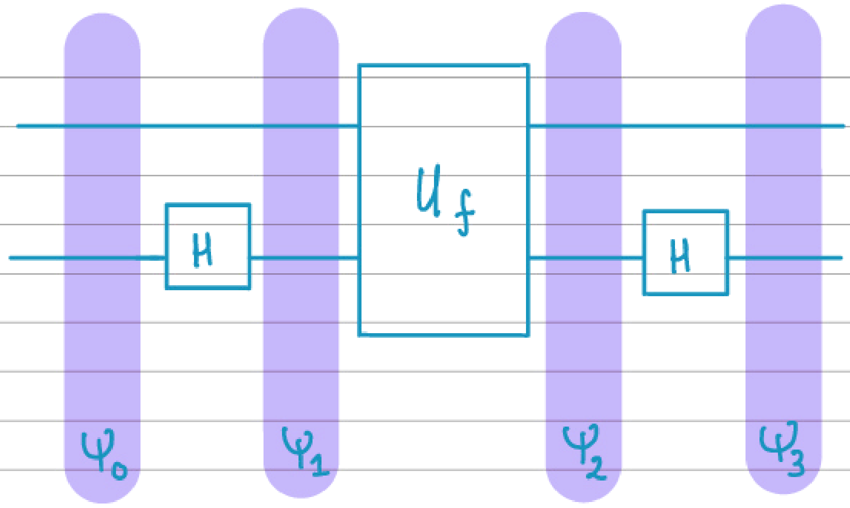


$|a\oplus b\rangle$
$|b\rangle$

$|a\oplus b\rangle$
$|b\oplus(a\oplus b)\rangle$
$\shortparallel$
$|a\rangle$

$|a\oplus b\oplus a\rangle = |b\rangle$
$|a\rangle$

Q2.



$$|\varphi_0\rangle = |a\rangle|b\rangle$$

$$|\varphi_1\rangle = (\mathbb{1} \otimes H)\,|a\rangle|b\rangle = \frac{1}{\sqrt{2}}|a\rangle\big(|0\rangle + (-1)^b|1\rangle\big)$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{2}} U_f |a\rangle|0\rangle + \frac{(-1)^b}{\sqrt{2}} U_f |a\rangle|1\rangle$$

$$= \frac{1}{\sqrt{2}}|a\rangle|0\oplus f(a)\rangle + \frac{(-1)^b}{\sqrt{2}}|a\rangle|1\oplus f(a)\rangle$$

$$= \frac{1}{\sqrt{2}}|a\rangle\Big(|f(a)\rangle + (-1)^b|\overline{f(a)}\rangle\Big)$$

$$|\varphi_3\rangle = (\mathbb{1} \otimes H)|\varphi_2\rangle = \frac{1}{2}|a\rangle\Big(\big(|0\rangle + (-1)^{f(a)}|0\rangle\big) + (-1)^b\big(|0\rangle + (-1)^{\overline{f(a)}}\big)\Big)$$

Par étude des cas $b=0$ et $b=1$, on a bien que

$$|\varphi_3\rangle = |a\rangle\,(-1)^{f(a)\cdot b}\,|b\rangle.$$

III. Superdense coding.

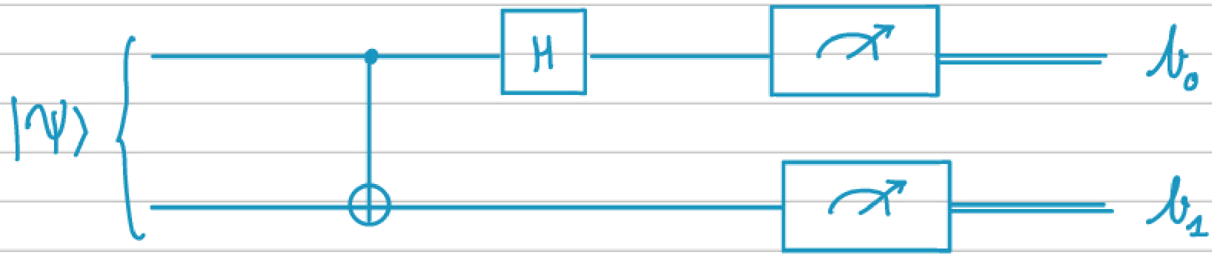
Q1. Two bits

Q2.
00 ⇝ $|00\rangle + |11\rangle \to |00\rangle + |11\rangle \to |00\rangle + |11\rangle$
01 ⇝ $|00\rangle + |11\rangle \to |10\rangle + |01\rangle \to |10\rangle + |01\rangle$
10 ⇝ $|00\rangle + |11\rangle \to |00\rangle + |11\rangle \to |00\rangle - |11\rangle$
11 ⇝ $|00\rangle + |11\rangle \to |10\rangle + |01\rangle \to -|10\rangle + |01\rangle$

Tous ces états sont orthogonaux ; ils forment une base

$$\mathcal{B} = \left\{ \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|10\rangle + |01\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\}.$$

Il suffit d'appliquer une matrice de passage de $\mathcal{B}$ dans $\mathcal{B}_{\text{Computationnelle}} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.



Tutorial #3.

2. Some properties of circuits

2.1. Do circuits commute?

Q1. $A = \mathbb{1}_2 \otimes A'$ and $B = B' \otimes \mathbb{1}_2$ commute: $AB = BA = B' \otimes A$

Q2. $A = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{X} \otimes \mathbb{1}_2$ and $B = H \otimes \mathbb{1}_2$ do not commute: $AB \neq BA$.

2.2. Are circuits ambiguous?

Q1. This is exactly 2.1/Q1.

Q2. Let $|\phi\rangle = \alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|11\rangle$.

When measuring the first qubit and then the second, we obtain that:

$$\Pr[1^{st} \text{ qubit is measured as } 0] = |\alpha|^2 + |\gamma|^2$$

$$\Pr[\text{measuring } 00] = \Pr[1^{st} \text{ qubit} \rightsquigarrow 0] \times \Pr[2^{nd} \text{ qubit} \rightsquigarrow 0 \mid 1^{st} \text{ qubit} \rightsquigarrow 0].$$

$$= (|\alpha|^2 + |\gamma|^2) \times \frac{|\alpha|^2}{|\alpha|^2 + |\gamma|^2} = |\alpha|^2$$

we can do the same for all the other cases.

When measuring the 2^{nd} qubit and then the 1^{st} qubit, we have:

$$\Pr[2^{nd} \text{ qubit} \rightsquigarrow 0] = |\alpha|^2 + |\beta|^2$$

and $\Pr[\text{measuring } 00] = \Pr[2^{nd} \text{ qubit} \rightsquigarrow 0] \times \Pr[1^{st} \text{ qubit} \rightsquigarrow 0 \mid 2^{nd} \text{ qubit} \rightsquigarrow 0]$

$$= (|\alpha|^2 + |\beta|^2) \times (|\alpha|^2 / (|\alpha|^2 + |\beta|^2))$$

$$= |\alpha|^2.$$

Q3. Let $|\phi\rangle = \alpha|\psi_0\rangle \otimes |0\rangle + \beta|\psi_1\rangle \otimes |1\rangle$.

We have that:

$$\Pr[|\phi\rangle \overset{\text{last}}{\rightsquigarrow} 0] = |\alpha|^2 \quad + \Pr[|\phi\rangle \overset{\text{last}}{\rightsquigarrow} 1] = |\beta|^2$$

$$(U \otimes \mathbb{1})|\phi\rangle = \alpha(U|\psi_0\rangle) \otimes |0\rangle + \beta(U|\psi_1\rangle) \otimes |1\rangle.$$

$$\Pr[(U\otimes\mathbb{1})|\phi\rangle \overset{\text{last}}{\rightsquigarrow} 0] = |\alpha|^2 \quad + \Pr[(U\otimes\mathbb{1})|\phi\rangle \overset{\text{last}}{\rightsquigarrow} 1] = |\beta|^2$$

3. The CHSH Game.

Q1. We have $A : \{0,1\} \to \{0,1\}$ and $B : \{0,1\} \to \{0,1\}$ two deterministic functions. With $A(x) = x$ and $B(y) = y$, we have a probability of success of $3/4$.

We know that the probability of success for any deterministic strategy is in $\{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1\}$. Suppose that we have a strategy with a success rate $> \frac{3}{4}$, i.e. $= 1$, that is,

$$\forall x, y, \qquad A(x) \oplus B(y) = x \wedge y.$$

This means $A(0) \oplus B(0) = A(1) \oplus B(0) = A(0) \oplus B(1) = 0$

By disjunction, we have no case such that this is true.

We can conclude that $\frac{3}{4}$ is the optimal success rate for a deterministic strategy.

Q2. (a)

$$\underbrace{\max_{n \in \mathbb{N}} \ \max_{\lambda \text{ a random on } [n]} \ \max_{(A_k, B_k)_{k \in [n]}} \sum_{k=0}^{n} \Pr[\lambda = k] \times \text{SuccessRate}(A_k, B_k)}_{\text{Success Rate(Shared Randomness)}}$$

(b) Success Rate(Shared Randomness) $\geq \max_{A,B}$ Success Rate $(A,B) = 3/4$.

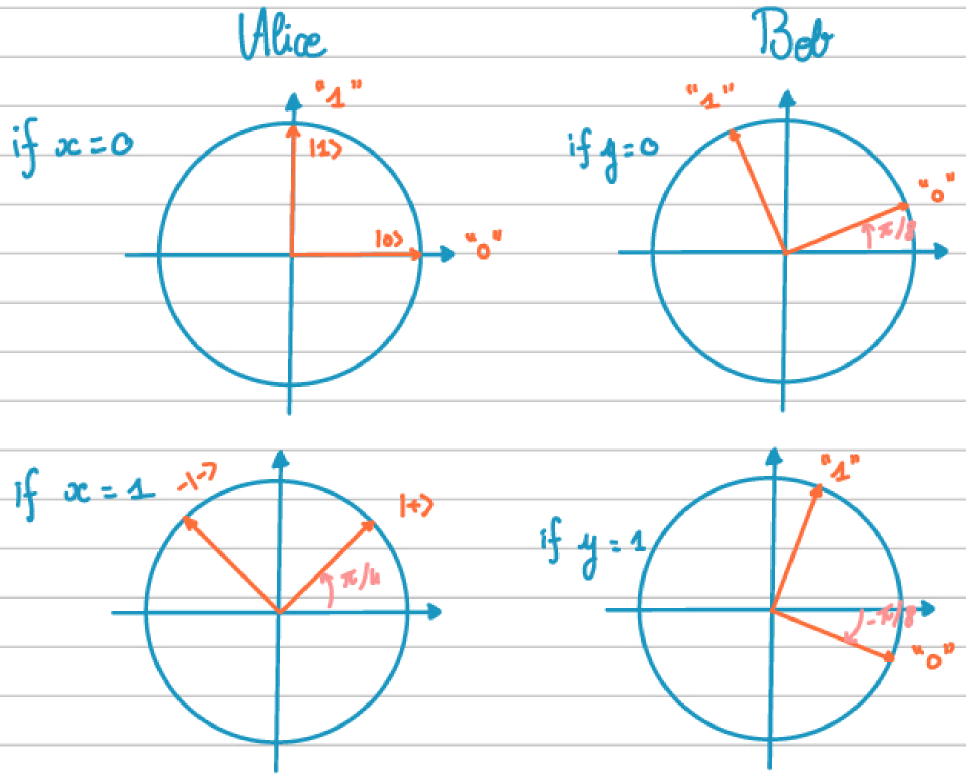
We have that

Fix $n \in \mathbb{N}$, λ a random variable over $[n]$ and $(A_k, B_k)_{k \in [n]}$.

$$\sum_{k=0}^{n} Pr[\lambda = k] \times \text{Success Rate}(A_k, B_k) \leq \sum_{k=0}^{n} Pr[\lambda = k] \cdot 3/4 = \frac{3}{4} \underbrace{\sum_{k=0}^{n} Pr[\lambda = k]}_{1} = \frac{3}{4}$$

Thus, Success Rate (Probabilistic Strategy).

Q3. We make the following measurments :



Success Rate $= \cos^2 \frac{\pi}{8} \approx 0.85$

TD n° 5

II From order-finding to factoring

Q1.

$$x \in [\![1, \ell-1]\!] \text{ inversible } \Leftrightarrow \exists k \in [\![1, \ell-1]\!],\ xk = 1$$

$$\overset{\text{Bézout}}{\Longleftrightarrow} \gcd(x, \ell) = 1$$

$$\Longleftrightarrow x \in \{1, \ldots, \ell-1\}$$

D'où, $\mathbb{Z}_\ell^\times = [\![1, \ell-1]\!]$ and thus $|\mathbb{Z}_\ell^\times| = \ell-1$.

Q2. $|\mathbb{Z}_N^\times| = |\mathbb{Z}_p^\times \times \mathbb{Z}_q^\times| = |\mathbb{Z}_p^\times| \times |\mathbb{Z}_q^\times| = (p-1)(q-1)$

Q3. Take $x \leftarrow \mathcal{U}([\![0, N]\!])$.

$$\Pr[x \in \mathbb{Z}_N^\times] = \frac{|\mathbb{Z}_N^\times|}{|\mathbb{Z}_N|} = \frac{p-1}{p}\,\frac{q-1}{q}$$

$$= 1 - \frac{1}{q} - \frac{1}{p} + \frac{1}{pq} \sim 1 - 2^{-\lambda/2}.$$

Q4. Soit k l'ordre de x.

$$(-x)^{2k} = \left((-1)^k x^k\right)^2 = (-1)^2 = 1.$$

On a donc $|\{x \in \mathbb{Z}_N^\times \mid \omega(x) \text{ impair}\}| \leq |\{x \in \mathbb{Z}_N^\times \mid \omega(x) \text{ pair}\}|$.

d'où $\Pr[x \text{ a un ordre impair}] \geq \frac{1}{2}$.

Q5.

$$x^r - 1 = \overbrace{(x^{r/2} - 1)}^{\neq 1, N}\overbrace{(x^{r/2} + 1)}^{\neq 1, N} = N$$

d'où on a un diviseur non-trivial de N.

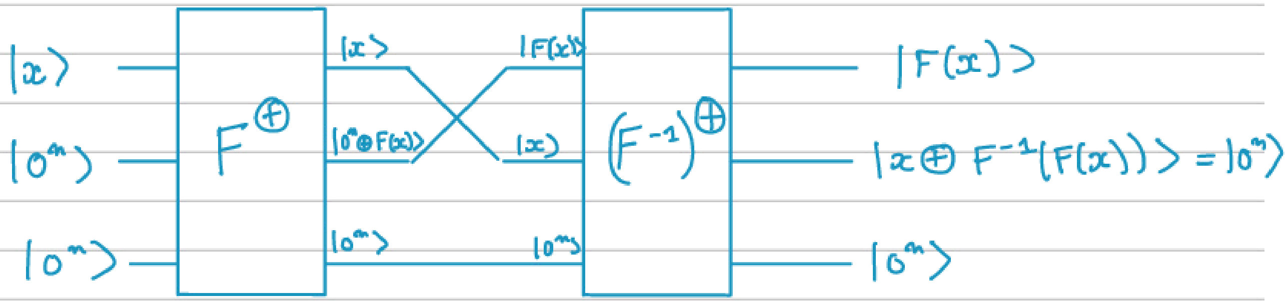
Q6. Run Shor while obtaining even order on random x, return $\gcd(x, N)$ or repeat.

Expected Run Time $\mathcal{O}\left(\underbrace{\frac{1}{1-\varepsilon}}_{\substack{\text{proba que} \\ x^{r} \pm 1 \neq 1, N}} \times \underbrace{2}_{} \right)$ appels à Shor

↳ proba even-order

III Modular exponentiation.

Q1.



Q2. $F(x) := ax \bmod N$ $\qquad F^{-1}(x) := a^{-1} x \bmod N$

Q3. Exponentiation rapide.

Si impair
| $y \leftarrow y \times y \times x$
Sinon
| $y \leftarrow y \times y$

TD n° 6

II. Amplitude amplification

Q1. $\Pr[\text{output} \in f^{-1}(1)] = p$ thus $\Pr[(\text{output}[k] \in f^{-1}(1)) \cap (\forall i < k, \text{output}[i] \notin f^{-1}(1))]$
$= p \cdot (1-p)^{k-1}$

We have a geometric law $\mathcal{G}(p)$ so $\mathbb{E}[\#\text{steps}] = 1/p$.

Q2. We write $\mathcal{A}$ in a universal set of gates, like $\{\text{NOT}, H, \text{CCNOT}\}$, and we compute

$$\mathcal{A} = U_1 \cdots U_n \quad \rightsquigarrow \quad \mathcal{A}^{-1} = \mathcal{A}^\dagger = U_n^\dagger \cdots U_n^\dagger.$$

Q3. $$|U\rangle = \sum_{i=1}^{2^n} \alpha_i |i\rangle = \sum_{i \in f^{-1}(0)} \alpha_i |i\rangle + \sum_{i \in f^{-1}(1)} \alpha_i |i\rangle$$

Define $$|G\rangle = \frac{\sum_{i \in f^{-1}(1)} \alpha_i |i\rangle}{\left(\sum_{i \in f^{-1}(1)} |\alpha_i|^2\right)^{1/2}} = \frac{1}{\sqrt{p}} \sum_{i \in f^{-1}(1)} \alpha_i |i\rangle$$

and
$$|B\rangle = \frac{1}{\sqrt{1-p}} \sum_{i \in f^{-1}(0)} \alpha_i |i\rangle$$

Q4. $$Z_f |G\rangle = \sum_{i \in f^{-1}(1)} \frac{\alpha_i}{\sqrt{p}} Z_f |i\rangle = \sum_{i \in f^{-1}(1)} \frac{\alpha_i}{\sqrt{p}} (-1)^{f(i)} |i\rangle = -\sum_{i \in f^{-1}(1)} \frac{\alpha_i}{\sqrt{p}} Z_f |i\rangle = -|G\rangle$$

Similarly, $Z_f |B\rangle = |B\rangle$.

This means Z_f is a "reflection through $|B\rangle$".

We have $$\mathcal{A} R \mathcal{A}^{-1} |U\rangle = \mathcal{A} R \mathcal{A}^{-1} \mathcal{A} |0^m\rangle$$
$$= \mathcal{A} R |0^m\rangle$$
$$= \mathcal{A}(2 |0^m\rangle \overbrace{\langle 0^m | 0^m\rangle}^{1} - |0^m\rangle)$$
$$= \mathcal{A} |0^m\rangle$$
$$= |U\rangle.$$

Let $|V\rangle$ be an orthogonal state to $|U\rangle$.

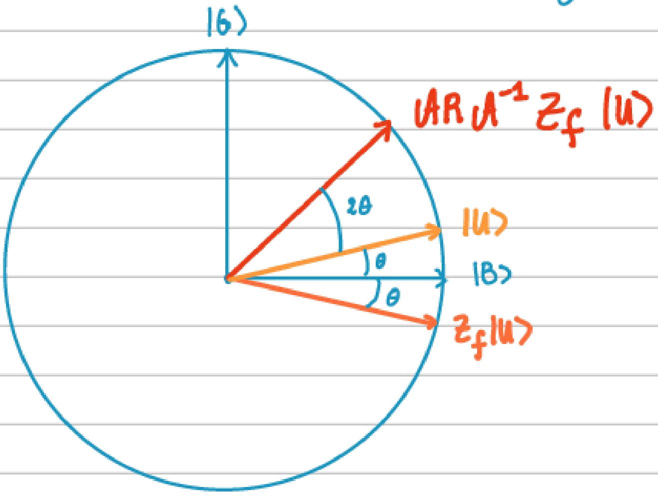
$\mathcal{A}^{-1} |V\rangle$ is orthogonal to $\mathcal{A}^{-1} |U\rangle = |0^m\rangle$

Thus $\mathcal{A}^{-1}|v\rangle = \sum_{i\neq 0^m} \beta_i |i\rangle$ for some $\beta_i \in \mathbb{C}$

Then $R\mathcal{A}^{-1}|v\rangle = \sum_{i\neq 0^m} \beta^i R|i\rangle = -\sum_{i\neq 0^m} \beta_i |i\rangle = -\mathcal{A}^{-1}|v\rangle$

and thus $\mathcal{A}R\mathcal{A}^{-1}|v\rangle = -|v\rangle$.

$\mathcal{A}R\mathcal{A}^{-1}$ is the "reflection through $|\mathcal{U}\rangle$."



Q5. After k calls, we have an angle $(2k+1)\theta$.

We want $(2k+1)\theta \approx \pi/2$ thus

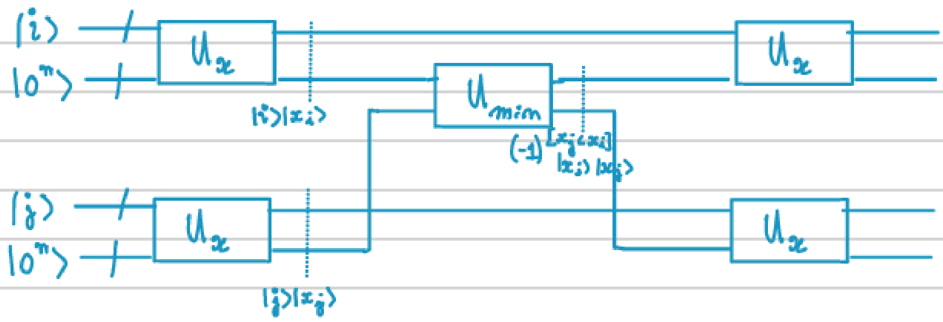
$$k \approx \pi/4\theta$$
$$\approx \pi/4 \sin^{-1}(\sqrt{p})$$
when p small $\approx \pi/4\sqrt{p}$

So, when p is small, we have $O(\sqrt{1/p})$ calls instead of $O(1/p)$.

Q6 Grover's algorithm is when $\mathcal{A} = H^{\otimes n}$, then $\Pr[\text{output} \in f^{-1}(1)] = \#f^{-1}(1)/2^n$.

III List-min

$$U_{min}|x_i\rangle|x_j\rangle = (-1)^{[x_i < x_j]}|x_i\rangle|x_j\rangle$$



a) The worst case is $x_1 > \cdots > x_N$.

The number of calls to Grover's algorithm is $O\left(\sum_{k=1}^{N} \sqrt{N/k}\right) = O(N)$

as $\sum_{k=1}^{n} \frac{1}{\sqrt{k}} = O(\sqrt{N})$

by comparing with an integral.

b) Let j be of rank r. Then $Pr[\, j$ chosen by the algorithm $] = 1/r$.

By induction on the size of the list, we have that:

- for $N = r = 1$, we have $Pr[\, 1$ chosen $] = 1$.

- $Pr[\, j$ chosen in the $N+1$-list$]$

$$= \frac{1}{N+1} + \sum_{i=1}^{N+1} Pr[\, j \text{ is chosen after } i \mid i \text{ is chosen}] \times \frac{1}{N+1}$$

$$= \frac{1}{N+1} + \frac{1}{N+1} \sum_{i=1}^{N+1} P(j, N-i)$$

$$= \frac{1}{N+1} + \frac{1}{N+1} \sum_{i=1}^{N-1} \frac{1}{r} = \frac{1}{N+1}\left(1 + \frac{N+1-r}{r}\right) = \frac{1}{r}$$

c) $\mathbb{E}[\#\text{ Queries}] \leq C \sum_{r=1}^{N} P(r, N) \sqrt{N/r} = C\sqrt{N} \sum_{r=1}^{N} \frac{1}{r\sqrt{r}} \leq G(\sqrt{N})$.

d) So, by Markov, $Pr[Q \geq t\, \mathbb{E}[Q]] \leq 1/t$

thus after $3\, G(\sqrt{N})$ calls, $Pr[\text{success}] \geq \frac{2}{3}$.

IV Bloch ball and sphere

TD n° 8

I. Parity check matrix

1) "⇒" As H is a parity check then $\ker(H^T) = C$ and thus $\text{rank}(H) = \text{rank}(H^T)$
$= n - \dim(\ker H^T)$
$= n - k$

We have $(\text{im } G) = C = (\ker H^T)$ thus $GH^T = 0$.

"⇐" If $GH^T = 0$ and $y \in C = (\text{im } G)$ then $y = xG$ for some $x \in \mathbb{F}_2^k$.

Then, $yH^T = xGH^T = 0$ thus $y \in \ker H^T$

and so $C \subseteq \ker H^T$ and $\dim(\ker H^T) = n - (n-k) = k = \dim C$.

We can conclude $C = \ker H^T$ and thus H is a parity check.

2) We have $G = \text{span}(11011, 10101)$ and

we can use $H^T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ and it works!

<u>Note</u>: We can note that $H = \left(\mathbb{1}_3 \middle| \begin{matrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{matrix} \right)$ and we can always do that (and to G too), thus we can use Gauss's pivot algorithm to get H.

III Computations around Shor's code.

1) $|\bar{0}\rangle = \frac{1}{2\sqrt{2}} \left(|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3} \right)^{\otimes 3}$ $\quad |\bar{1}\rangle = \frac{1}{2\sqrt{2}} \left(|0\rangle^{\otimes 3} - |1\rangle^{\otimes 3} \right)^{\otimes 3}$

2) (a) If $E = \mathbb{1}^{\otimes 9}$ then the whole circuit is equivalent to $\mathbb{1}^{\otimes 9}$.

(b) If $E = X \otimes \mathbb{1}^{\otimes 8}$ then the X error is propagated and corected.

(c) If $E = Z \otimes \mathbb{1}^{\otimes 8}$ then the Z error is propagated and corected.

(d) If $E = XZ \otimes \mathbb{1}^{\otimes 8}$ then the XZ error is propagated and corrected.

3) We have that $XZ \propto Y$ and thus we can correct any error on the first qubit (as $X, Y, Z, \mathbb{1}$ generates all unitary matrices).

IV Stabilizer codes

1) We consider $(|000\rangle, |111\rangle)$ which forms a basis of $\mathcal{C}_S$.

2) "$\Rightarrow$" $H \subseteq S$

"$\Leftarrow$" $g = h_1 \cdots h_k$, $\forall i\, h_i \in H$,

$$\begin{aligned} h_1 \cdots h_k |\psi\rangle &= h_1 \cdots h_{k-1} |\psi\rangle \\ &\vdots \\ &= h_1 |\psi\rangle \\ &= |\psi\rangle. \end{aligned}$$

3) If $-\mathbb{1} \in S$, then for any $u \in \mathcal{C}_S$, $-\mathbb{1} u = -u = u$ thus $u = 0$.

4) Reordering the elements, assume $g_1 g_2 \neq g_2 g_1$ then $g_1 g_2 = -g_2 g_1$

$\forall u \in \mathcal{C}_{\langle g_1 \cdots g_l \rangle}$ $g_1 g_2 u = g_2 g_1 u = u$

and thus $-u = u$ and thus $u = 0$.

<u>Lemma</u>: Take $a, b \in \{\mathbb{1}, X, Y, Z\}$, then either

$$[a,b] := ab - ba = 0 \quad \text{or} \quad \{a,b\} := ab + ba = 0$$

proof. $XY = -YX$, $XZ = -ZX$, $YZ = -ZY$, etc.

Note Let S be a stabilizer subgroup.

Define $N(S) := \{ x \in G_n \mid \forall y \in S, \underbrace{[x,y] = 0}_{xy = yx} \}$.

Then, for $\mathcal{E} \subseteq G_n$,

$\mathcal{E}$ can be corrected iff $\forall x, y \in \mathcal{E}$, $x^\dagger y \in N(S) \setminus S$.

And logical operators $\cong N(S) / S$.

5) Shor: $|\bar{0}\rangle \propto (|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3})^{\otimes 3}$ and $|\bar{1}\rangle \propto (|0\rangle^{\otimes 3} - |1\rangle^{\otimes 3})^{\otimes 3}$

If $\mathcal{C}_S$ is a $[n, k, d]_2$ - stabilizer code, then S is generated by $n-k$ stabilizers. # logical qubits We want to find 8 stabilizers.

physical logic

We can use $Z_1 Z_2, Z_2 Z_3, Z_4 Z_5, Z_5 Z_6, Z_7 Z_8, Z_8 Z_9, X_1 \cdots X_6, X_4 \cdots X_9$

1 1 1

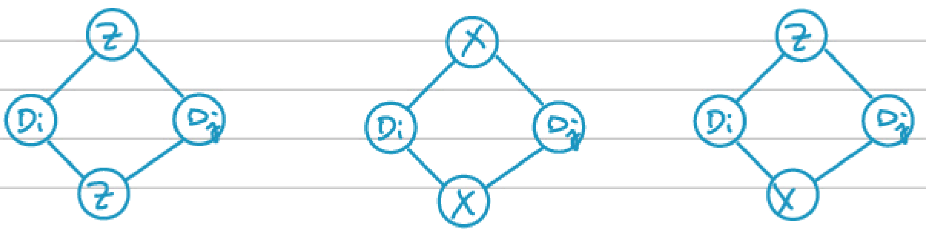
QEC Zoo

Philippe Faist FUB.

TD n° 9

2. The Surface Code.

Q1. From the drawing, we have that



commutes.

Q2a. For any $S, T \in G_n$, we have $[S,T] := ST - TS = 0$

<u>or</u> $\{S,T\} := ST + TS = 0$.

Q2b. $B^\dagger A|\psi\rangle = B^\dagger A \hat{S}|\psi\rangle = -\hat{S} B^\dagger A|\psi\rangle$

Thus $B^\dagger A|\psi\rangle$ is an eigenvector of $\hat{S}$ with eigenvalue -1.

However, $\mathcal{C}$ is a "proper" subspace of $\hat{S}$ with eigenvalue 1.

By the Spectral Theorem, we have that the two proper spaces associated with two different eigen values are orthogonal.

Thus, $B^\dagger A|\psi\rangle \perp \mathcal{C}$.

Q2c. Take $|\varphi\rangle, |\psi\rangle \in \mathcal{C}$ with $|\varphi\rangle \perp |\psi\rangle$.

Either $B^\dagger A = \mathbb{1}$ and then $\langle\phi|B^\dagger A|\psi\rangle = \langle\varphi|\psi\rangle = 0$

Either $B^\dagger A$ is a stabilizer and then $\langle\varphi|B^\dagger A|\psi\rangle = \langle\varphi|\psi\rangle = 0$.

Q3a. Write $|\psi\rangle = |d_1\rangle \cdots |d_9\rangle$ and $|d_1\rangle = \alpha|0\rangle + \beta|1\rangle$
$|d_4\rangle = \gamma|0\rangle + \delta|1\rangle$.

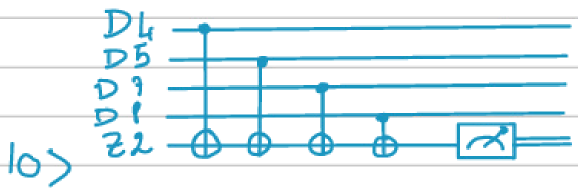
$$\hat{S}^{Z1}|\psi\rangle = |\psi\rangle \iff (Z|d_1\rangle)(Z|d_4\rangle) = |d_1\rangle|d_4\rangle$$

$$\iff (\alpha|0\rangle - \beta|1\rangle)(\gamma|0\rangle - \delta|1\rangle) = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$$

$$\iff \alpha\delta = 0 \text{ and } \beta\gamma = 0$$

$$\iff S^{Z1} = 0.$$

Q3b.



Q3c.

TD n° 10

II Entropies for counting

0) Chain rule:

$$H(X|Y) = -\sum_{x,y} p_{x,y} \log\left(p_{xy}/p_y\right)$$
$$= -\sum_{x,y} p_{x,y} \log p_{xy} + \sum_y \underbrace{\Big(\sum_x p_{x,y}\Big)}_{p_y} \log p_y$$
$$= H(X,Y) - H(Y)$$

1) $$\sum_{j=1}^{N} H(X_j \mid X_1, \dots, X_{j-1}) = \sum_{j=1}^{N} \left(H(X_1,\dots,X_j) - H(X_1,\dots,X_{j-1})\right)$$

"telescopic" sum

$$= H(X_1, \dots, X_N) - H(\ )$$
$$= H(X_1, \dots, X_N)$$

2) $$\sum_{j=1}^{M} H(X_{S_j}) = \sum_{j=1}^{M} H\left((X_l)_{l\in S_j}\right)$$
$$= \sum_{j=1}^{N} \sum_{l\in S_j} H\left(X_l \mid X_{\{i\in S_j \mid i<l\}}\right)$$
$$\geq \sum_{j=1}^{N} \sum_{l\in S_j} H(X_l \mid X_1, \dots, X_{l-1})$$
$$\geq k \sum_{l=1}^{n} H(X_l \mid X_1, \dots, X_{l-1})$$
$$= k H(X_1, \dots, X_N).$$

3) Consider $(X_1, X_2, X_3) \in A$ chosen uniformly over A.

Then $$2 H(X_1, X_2, X_3) \leq H(X_1,X_2) + H(X_2,X_3) + H(X_1,X_3)$$

and $H(X_1, X_2, X_3) = -\sum_{a \in A} p_a \log p_a = \log |A|$

thus

$$\log |A| \leq \frac{1}{2}\left(H(A_{12}) + H(A_{13}) + H(A_{23})\right)$$
$$\leq \frac{1}{2}\left(\log |A_{12}| + \log |A_{13}| + \log |A_{23}|\right)$$
$$\leq \frac{1}{2} \times 3 \log n \leq \log n^{3/2}$$

and finally $|A| \leq n^{3/2}$.

III From divergences to entropies.

$$D(P \| Q) = \mathop{\mathbb{E}}_{X \sim P}\left[\log\left(p_X / q_X\right)\right] = \sum_{x \in \mathcal{X}} p_x \log\left(p_x / q_x\right).$$

1)
$$-D(P_{XY} \| 1_X \otimes P_Y) = -\sum_{\substack{x \in \mathcal{X} \\ y \in \mathcal{Y}}} p_{xy} \log\left(p_{xy} / p_y\right)$$
$$= H(X|Y)$$

$$D(P_{XY} \| P_X \otimes P_Y) = -\sum_{\substack{x \in \mathcal{X} \\ y \in \mathcal{Y}}} p_{xy} \log\left(p_{xy} / p_x p_y\right)$$
$$= I(X:Y).$$

2) $D(\rho \| \sigma) = \mathrm{Tr}\left(\rho\left(\log \rho - \log \sigma\right)\right)$

Cannal quantique $\mathcal{H}$ un espace de Hilbert ("$\mathcal{H} = \mathbb{C}^n$")

$\mathcal{L}(\mathcal{H})$

Un cannal quantique $\Phi : \mathcal{L}(\mathcal{H}) \longrightarrow \mathcal{L}(\mathcal{H}')$ linéaire qui preserve les états (et qui est donc CPTP)

$\hookrightarrow$ Φ trace preserving $\iff \forall x \in \mathcal{L}(\mathcal{H}),\ tr(\Phi(x)) = tr\, x$
$\hookrightarrow$ Φ completely positive $\iff \forall n \in \mathbb{N} \quad \Phi \otimes Id_n \geq 0.$

Pour $n \in \mathbb{N}$,

$$\mathcal{M}_n(\mathcal{L}(\mathcal{H})) := \{(x_{ij})_{i,j \in [\![1,n]\!]} \mid \forall i,j,\ x_{ij} \in \mathcal{L}(\mathcal{H})\}.$$

$$Id_n \otimes \Phi : \mathcal{M}_n(\mathcal{L}(\mathcal{H})) \longrightarrow \mathcal{M}(\mathcal{L}(\mathcal{H}'))$$
$$X = (x_{ij})_{ij} \longmapsto (\Phi(x_{ij}))_{ij}$$

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

$$X \geq 0 \iff \mathrm{Spec}(X) \subseteq \mathbb{R}^+ \iff \exists Y \in \mathcal{M}_n(\mathcal{L}(\mathcal{H})),\ X = Y^\dagger Y.$$

Pour $\rho \in \mathcal{D}(\mathcal{H})$ et $\sigma \in \mathcal{D}(\mathcal{H}')$ où $\dim \mathcal{H}' =: m$

alors $\sigma \otimes \rho \in \mathcal{M}_m(\mathcal{L}(\mathcal{H}))$

et $Id_m \otimes \Phi(\sigma \otimes \rho) = \sigma \otimes \Phi(\rho) \geq 0.$

2) Avec $\Phi : x \longmapsto tr(x)\, \rho_0$ où $\rho_0 \in \mathcal{D}(x')$,

on a donc

$$D(\Phi(\rho) \,\|\, \Phi(\sigma)) = D(\rho_0 \,\|\, \rho_0) = tr(\rho_0(\log \rho_0 - \log \rho_0)) = 0$$

Si U est unitaire, alors $\Phi : x \mapsto U x U^\dagger.$

$(\mathcal{L}(\mathcal{H}), \langle -,- \rangle_{HS})$ où $\langle x, y \rangle = tr(x y^\dagger)$.
↳ Hilbert-Schmidt

Si Φ est un canal, alors Φ^* est unital & completely positive.

Traces partielles

Pour deux systèmes A, B joints,

$$\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) = \underset{⚠}{\underline{span}} \{ x_A \otimes x_B \mid x_A \in \mathcal{L}(\mathcal{H}_A), x_B \in \mathcal{L}(\mathcal{H}_B) \}.$$

trace partielle
$$tr_B : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \longrightarrow \mathcal{L}(\mathcal{H}_A)$$
$$x_A \otimes x_B \longmapsto tr(x_B)\, x_A$$

Ainsi, $tr(tr_B(x_A \otimes x_B)) = tr(x_A)\, tr(x_B) = tr(x_A \otimes x_B)$.

tr_B est un canal quantique qui donne la marginale sur A de l'état biparti ρ_{AB}.

$$H(A|B) = -D(\rho_{AB} \| \mathbb{1}_A \otimes tr_B(\rho_{AB}))$$

3) $\rho_A = tr_B(\rho_{AB}) = tr_B(\mathbb{1}_A/_d \otimes \mathbb{1}_B/_d) = \underbrace{tr\left(\frac{\mathbb{1}_B}{d}\right)}_{1} \mathbb{1}_A/d = \mathbb{1}_A/d$

De même, $\rho_B = \mathbb{1}_B/d$.

$$I(A:B) = D(\rho_{AB} \| \rho_A \otimes \rho_B) = D\left(\frac{\mathbb{1}_{AB}}{d^2} \middle\| \frac{\overbrace{\mathbb{1}_A \otimes \mathbb{1}_B}^{\mathbb{1}_{AB}}}{d^2}\right) = 0$$

ρ_{AB} produit $\Longrightarrow I(A:B) = 0$

$$H(A|B) = -D(\rho_{AB} \| \mathbb{1}_A \otimes \rho_B) = -D\left(\frac{\mathbb{1}_{AB}}{d^2} \middle\| \frac{\mathbb{1}_{AB}}{d}\right)$$
$$= -tr\left(\frac{\mathbb{1}_{AB}}{d^2}\left(\log(\mathbb{1}_{AB}/d^2) - \log(\mathbb{1}_{AB}/d)\right)\right)$$

$$= -\frac{1}{d^2}\sum_{i=1}^{d^2}\left(\log\frac{1}{d^2} - \log\frac{1}{d}\right) = -\log(1/d)$$
$$= \log d$$

$$\rho_{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}| = \frac{1}{d}\sum_{i,j} |ii\rangle\langle jj|$$
$$= \frac{1}{d}\sum_{ij} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B$$

$$\rho_A = tr_B\left(\frac{1}{d}\sum_{ij} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B\right)$$
$$= \frac{1}{d}\sum_{ij} tr(|i\rangle\langle j|_B)\, |i\rangle\langle j|_A$$
$$= \frac{\mathbb{1}_A}{d}$$

et $\rho_B = \mathbb{1}_B / d$

$$I(A:B)_{|\Psi_{AB}\rangle\langle\Psi_{AB}|} = D(|\Psi\rangle\langle\Psi| \,\|\, \mathbb{1}_{AB}/d^2)$$
$$= tr\left[|\Psi\rangle\langle\Psi|_{AB}\left(\log(|\Psi\rangle\langle\Psi|) - \log(\mathbb{1}_{AB}/d^2)\right)\right]$$
$$= -tr\left[|\Psi\rangle\langle\Psi|_{AB} \log(\mathbb{1}_{AB}/d^2)\right]$$
$$= -tr\left[\frac{1}{d}\left(\sum |ii\rangle\langle jj|\right)\sum \log(1/d^2)\, |kl\rangle\langle lk|\right]$$
$$= -\frac{1}{d} tr\left[\sum \log\frac{1}{d^2} |ii\rangle\langle ii|\right] = 2\log d$$

$H(A|B) = \dots = -\log d \quad < 0$ Quantique ! Intrication !

$$\left(H(A|B) \in [-\log d, \log d] \qquad I(A:B) \in [0, 2\log d] \right)$$

4) $H(A|BC) = -D(\rho_{ABC} \| \mathbb{1}_A \otimes \rho_{BC})$

$$\underset{\text{DPI}}{\leq} -D(\rho_{AB} \| \mathbb{1}_A \otimes \rho_B) = H(A|B).$$

TD 11

I Continuity of the entropy

1) $\rho - \sigma = (\rho-\sigma)_+ - (\rho-\sigma)_-$ donc $\rho + (\rho-\sigma)_+ = (\rho-\sigma)_- + \sigma = V$

$$\Delta(\rho,\sigma) = tr((\rho-\sigma)_+) + tr((\rho-\sigma)_-)$$

$$= 2\, tr\, V - tr\,\rho - tr\,\sigma$$

Let (t_i) be the eigenvalues of V ((r_i) for ρ, (s_i) for σ).

$$t_i \geq \max(r_i, s_i)$$

$$2t_i - r_i - s_i \geq |r_i - s_i|$$

$$\Delta(\rho,\sigma) = \sum_i (2t_i - r_i - s_i) \geq \sum_i |r_i - s_i|$$

2. $S(\rho) = -tr(\rho \log \rho)$. Define $\eta : x \mapsto x \log x$.

If $|r-s| \leq \frac{1}{2}$, $|\eta(r) - \eta(s)| \leq \eta(|r-s|)$.

$$|S(\rho) - S(\sigma)| = \left|\sum_i (\eta(r_i) - \eta(s_i))\right|$$

$$\leq \sum |\eta(r_i) - \eta(s_i)|$$

$$\leq \sum \eta(|r_i - s_i|)$$

Define $p_i = |r_i - s_i| / \delta$

$$\eta(|r_i - s_i|) = \delta\, \eta\left(\frac{|r_i - s_i|}{\delta}\right) - |r_i - s_i| \log \delta$$

so, $\sum \eta(|r_i - s_i|) = \delta \sum \left(\eta(|r_i - s_i|)/\delta - |r_i - s_i| \log \delta\right)$

$$= \delta \sum \eta(p_i) - \delta \log \delta$$

$$\leq \delta \log d - \delta \log \delta$$

3. If σ and ρ have the same eigenvalues,

$|S(\sigma) - S(\rho)| = 0 \leq 0 = \Delta(\sigma, \rho)$

Otherwise, $\delta > 0$ and so $|S(\sigma) - S(\rho)| \leq \delta \log d - \delta \log \delta$

$$\leq \Delta(\rho, \sigma) \log_2 d - \Delta(\rho, \sigma) \log \Delta(\rho, \sigma)$$

as $\delta \leq \Delta(\rho, \sigma) \leq \frac{1}{2}$.

II Density matrices and von Neuman entropy

1) a. $\rho_{XA} = \begin{pmatrix} p_1 \rho_1 & & \\ & \ddots & \\ & & p_n \rho_n \end{pmatrix}$

b. $tr_X(\rho_{XA}) = tr_X\left(\sum p_x |x\rangle\langle x| \otimes \rho_x\right)$

$$= \sum p_x \, tr_X(|x\rangle\langle x| \otimes \rho_x)$$

$$= \sum p_x \, tr(|x\rangle\langle x|) \rho_x = \sum p_x \rho_x$$

$tr_A(\rho_{XA}) = tr_A\left(\sum p_x |x\rangle\langle x| \otimes \rho_x\right)$

$$= \sum p_x \, tr(\rho_x) |x\rangle\langle x| = \sum p_x |x\rangle\langle x|.$$

c) Let $(\lambda_i^{(x)})$ be the eigenvalues of ρ_x: $\rho_x = U_x^\dagger D_x U_x$

$U_{tot} = \sum |x\rangle\langle x| \otimes U_x$

so $U_{tot} U_{tot}^\dagger = \left(\sum |x\rangle\langle x| \otimes U_x\right)\left(\sum |x\rangle\langle x| \otimes U_x^\dagger\right)$

$$= \sum |x\rangle\langle x| \otimes U_x U_x^\dagger$$

$$= \sum |x\rangle\langle x| \otimes \mathbb{1} = \mathbb{1}$$

$$U_{tot}\,\rho_{XA}\,U_{tot}^{\dagger} = \sum p_x |x\rangle\langle x| \otimes U_x \rho_x U_x^{\dagger}$$
$$= \sum p_x |x\rangle\langle x| \otimes \mathrm{diag}(\lambda_1^{(x)}, \dots, \lambda_n^{(x)})$$

d) $H(\{p_1, \dots, p_n\}) = S\left(\sum p_x |x\rangle\langle x|\right)$.

$$S(\rho_{XA}) = -\sum_{x,i} p_x \lambda_i^{(x)} \log(p_x \lambda_i^{x})$$
$$= -\sum p_x \lambda_i^{(x)} (\log p_x + \log \lambda_i^{(x)})$$
$$= -\sum p_x \left(\sum \lambda_i^{(x)}\right) \log p_x - \sum p_x \sum_i \lambda_i^{(x)} \log \lambda_i^{(x)}$$
$$= H(\{p_1, \dots, p_n\}) + \sum p_x S(\rho_x).$$

2. a) $$\rho = \frac{1}{2}\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{pmatrix}\right)$$
$$= \frac{1}{2}\begin{pmatrix} 1+\cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{pmatrix}$$
$$= \frac{\sin\theta\cos\theta}{2}\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{X} + \frac{1}{2}\begin{pmatrix} 1+\cos^2\theta & 0 \\ 0 & 1-\cos^2\theta \end{pmatrix}$$
$$= \frac{\sin\theta\cos\theta}{2} X + \frac{1}{2} I + \frac{\cos^2\theta}{2} Z \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

b. $tr(\rho) = 1$

$$\det(\rho) = \frac{1}{4}\left((1+\cos^2\theta)\sin^2\theta - \cos^2\sin^2\theta\right) = \sin^2\theta / 4$$

$$\lambda_1, \lambda_2 = \frac{1}{4}\sin^2\theta \pm \frac{1}{2}\sqrt{1-\sin^2\theta} = \frac{1}{4}\sin^2\theta \pm \frac{1}{2}\cos\theta$$

$$\rightsquigarrow \quad Sp(\rho) = \left\{\frac{1 \pm \cos\theta}{2}\right\}.$$

III Entanglement & nonlocality

a) $\rho_W(p) = \frac{p}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right)$

$+ \frac{1-p}{4}\left(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|\right)$

$$\rho_W(p) = \begin{pmatrix} \frac{1+p}{4} & 0 & 0 & p/2 \\ 0 & \frac{1-p}{4} & 0 & 0 \\ 0 & 0 & 1-p/4 & 0 \\ p/2 & 0 & 0 & 1+p/4 \end{pmatrix}$$

b) $x \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ $\quad x = \sum_i x_i^{(A)} \otimes x_i^{(B)}$

$x^{T_B} = \sum_i x_i^{(A)} \otimes \left(x_i^{(B)}\right)^T$

$$\rho_W(p)^{T_B} = \begin{pmatrix} \frac{1+p}{4} & 0 & 0 & 0 \\ 0 & \frac{1-p}{4} & p/2 & 0 \\ 0 & p/2 & 1-p/4 & 0 \\ 0 & 0 & 0 & 1+p/4 \end{pmatrix}$$

c) Let p s.t. $\rho_W(p)^{T_B} \geq 0$

$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ are eigenvectors of $\frac{1+p}{4}$

$\begin{pmatrix} \frac{1-p}{4} & p/2 \\ p/2 & \frac{1-p}{4} \end{pmatrix}$ has eigenvectors $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ w/ eigenvalue $\frac{1+p}{4}$

$\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ w/ eigenvalue $\frac{1-3p}{4}$

d) $(\rho_A \otimes \rho_B)^{T_B} = \underbrace{\rho_A}_{\geq 0} \otimes \underbrace{\rho_B^T}_{\geq 0} \geq 0$

e) if $p \leq 1/3$, $\rho_W(p)^{T_B} \geq 0$ so $\rho_W(p)^{T_B}$ product

and so $\rho_W(p)^{T_B}$ entangled when $p > 1/3$

IV Quantum Channels

If ϕ is a quantum channel then there exists an environment E and $V: A \to BE$ st

$$\phi(\rho) = tr_E(V \rho V^T)$$
$$= tr_E(U \rho \otimes |0\rangle\langle 0|_E \otimes U^\dagger)$$