

# Homework

(Guess : 40/50 points)

## 1 Basic operation and their notation

### Exercise 1.1: Inner/outer products in Dirac notation

$$\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 11 \end{pmatrix}$$

The last one in Dirac notation :

$$\begin{aligned} & (\langle 0| + 2\langle 1|) \times (3|0\rangle + 4|1\rangle) \\ &= 3\langle 0|0\rangle + 4\langle 0|1\rangle + 6\langle 1|0\rangle + 8\langle 1|1\rangle \\ &= 3 + 8 \\ &= 11 \end{aligned}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 4 & 8 \end{pmatrix}$$

The last two in Dirac notation :

$$\begin{aligned} & (3|0\rangle + 4|1\rangle) \times (\langle 0| + 2\langle 1|) \\ &= 3|0\rangle\langle 0| + 6|0\rangle\langle 1| + 4|1\rangle\langle 0| + 8|1\rangle\langle 1| \end{aligned}$$

### Exercise 1.2: Matrix products in Dirac notation

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 23 \\ 34 \end{pmatrix}$$

The last one in Dirac notation :

$$\begin{aligned} & (|0\rangle\langle 0| + 3|0\rangle\langle 1| + 2|1\rangle\langle 0| + 4|1\rangle\langle 1|) \times (5|0\rangle + 6|1\rangle) \\ &= 5|0\rangle\langle 0|0\rangle + 6|0\rangle\langle 0|1\rangle + 15|0\rangle\langle 1|0\rangle + 18|0\rangle\langle 1|1\rangle + \\ & \quad 10|1\rangle\langle 0|0\rangle + 12|1\rangle\langle 0|1\rangle + 20|1\rangle\langle 1|0\rangle + 24|1\rangle\langle 1|1\rangle \\ &= 5\langle 0|0\rangle|0\rangle + 18\langle 1|1\rangle|0\rangle + 10\langle 0|0\rangle|1\rangle + 24\langle 1|1\rangle|1\rangle \\ &= 5|0\rangle + 18|0\rangle + 10|1\rangle + 24|1\rangle \\ &= 23|0\rangle + 24|1\rangle \end{aligned}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The last one in Dirac notation :

$$\begin{aligned} & (1/\sqrt{2}|0\rangle\langle 0| + 1/\sqrt{2}|0\rangle\langle 1| + 1/\sqrt{2}|1\rangle\langle 0| - 1/\sqrt{2}|1\rangle\langle 1|)^2 \\ &= 1/2|0\rangle\langle 0|0\rangle\langle 0| + 1/2|0\rangle\langle 0|0\rangle\langle 1| + 1/2|0\rangle\langle 1|1\rangle\langle 0| - 1/2|0\rangle\langle 1|1\rangle\langle 1| \\ & \quad 1/2|1\rangle\langle 0|0\rangle\langle 1| + 1/2|1\rangle\langle 0|0\rangle\langle 0| - 1/2|1\rangle\langle 1|1\rangle\langle 0| + 1/2|1\rangle\langle 1|1\rangle\langle 1| \\ &= 1/2|0\rangle\langle 0| + 1/2|0\rangle\langle 0| + 1/2|1\rangle\langle 1| + 1/2|1\rangle\langle 1| \\ &= |0\rangle\langle 0| + |1\rangle\langle 1| \end{aligned}$$

**Exercice 1.3: Tensor products in Dirac/Coecke notation**

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

The last two in Dirac notation :

$$(|0\rangle + 2|1\rangle) \otimes (3|0\rangle + 4|1\rangle) = 3|00\rangle + 4|01\rangle + 6|10\rangle + 8|11\rangle$$

$$|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle = |00\rangle + |11\rangle$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

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

In Dirac notation :

$$\begin{aligned} & (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |1\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \\ &= |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3| \end{aligned}$$

$$\begin{aligned} & (|0\rangle\langle 0|) \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |1\rangle\langle 1| \\ &= |0\rangle\langle 0| + |1\rangle\langle 1| \end{aligned}$$

$$\begin{aligned} & 1/\sqrt{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \otimes 1/\sqrt{2}(|0\rangle\langle 0| + |1\rangle\langle 0| + |1\rangle\langle 0| - |1\rangle\langle 1|) \\ &= 1/2(|0\rangle\langle 0| + |0\rangle\langle 1| + |0\rangle\langle 2| + |0\rangle\langle 3| + \\ & \quad |1\rangle\langle 0| - |1\rangle\langle 1| + |1\rangle\langle 2| - |1\rangle\langle 3| + \\ & \quad |2\rangle\langle 0| + |2\rangle\langle 1| - |2\rangle\langle 2| - |2\rangle\langle 3| + \\ & \quad |3\rangle\langle 0| - |3\rangle\langle 1| - |3\rangle\langle 2| + |3\rangle\langle 3|) \end{aligned}$$

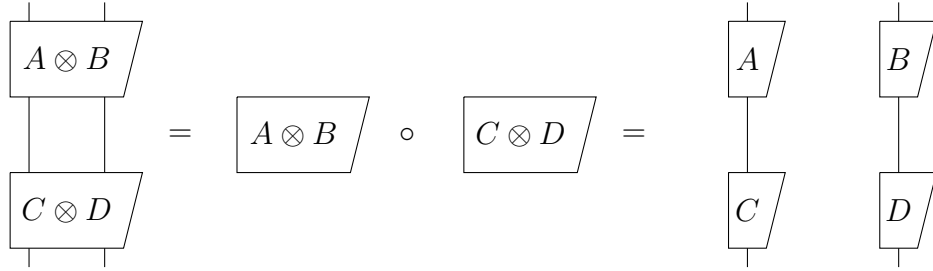
We want to prove  $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

- Dirac's notation :

We have  $A = \sum_{i,j} a_{i,j} |i\rangle \langle j|$  and  $D = \sum_{k,l} d_{k,l} |k\rangle \langle l|$

$$\begin{aligned}
 (A \otimes B)(C \otimes D) &= ((\sum_{i,j} a_{i,j} |i\rangle \langle j|) \otimes B)(C \otimes (\sum_{k,l} d_{k,l} |k\rangle \langle l|)) \\
 &= (\sum_{i,j} a_{i,j} |i\rangle \langle j|)C \otimes B(\sum_{k,l} d_{k,l} |k\rangle \langle l|) && \text{bilinearity of } \otimes \\
 &= (AC) \otimes (BD)
 \end{aligned}$$

- Coecke's notation :



#### Exercice 1.4: Dagger in Dirac/Coecke notation

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}^\dagger = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \quad \begin{pmatrix} 1 & 3i \\ 2 & 4i \end{pmatrix}^\dagger = \begin{pmatrix} 1 & 2 \\ -3i & -4i \end{pmatrix}$$

In Dirac notation:

$$\begin{aligned}
 &1/\sqrt{2}(|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| - |1\rangle \langle 1|)^\dagger \\
 &= 1/\sqrt{2}(|0\rangle \langle 0| + |1\rangle \langle 0| + |0\rangle \langle 1| - |1\rangle \langle 1|)
 \end{aligned}$$

$$\begin{aligned}
 &(|0\rangle \langle 0| + 3i |0\rangle \langle 1| + 2 |1\rangle \langle 0| + 4i |1\rangle \langle 1|)^\dagger \\
 &= (|0\rangle \langle 0| - 3i |1\rangle \langle 0| + 2 |0\rangle \langle 1| - 4i |1\rangle \langle 1|)
 \end{aligned}$$

#### Exercice 1.5: Gates in Dirac notations

$$H = 1/\sqrt{2}(|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| - |1\rangle \langle 1|)$$

$$CNot = |0\rangle \langle 0| + |1\rangle \langle 1| + |3\rangle \langle 2| + |2\rangle \langle 3|$$

$$T = |0\rangle \langle 0| + e^{\frac{i\pi}{4}} |1\rangle \langle 1|$$

Proof that are unitary matrix :

- $H : H^\dagger H = Id_1$  already do in Exercie-1.2
- $CNot$ :

$$\begin{aligned}
 CNot^\dagger CNot &= (|0\rangle \langle 0| + |1\rangle \langle 1| + |3\rangle \langle 2| + |2\rangle \langle 3|)(|0\rangle \langle 0| + |1\rangle \langle 1| + |2\rangle \langle 3| + |3\rangle \langle 2|) \\
 &= (|0\rangle \langle 0| + |1\rangle \langle 1| + |2\rangle \langle 2| + |3\rangle \langle 3|) \\
 &= Id_4
 \end{aligned}$$

- $T$ :

$$\begin{aligned}
& (|0\rangle\langle 0| + e^{\frac{i\pi}{4}}|1\rangle\langle 1|)(|0\rangle\langle 0| + e^{-\frac{i\pi}{4}}|1\rangle\langle 1|) \\
&= |0\rangle\langle 0|0\rangle\langle 0| + e^{\frac{i\pi}{4}}|0\rangle\langle 0|1\rangle\langle 1| + e^{\frac{i\pi}{4}}(|1\rangle\langle 1|0\rangle\langle 0|) + e^{\frac{i\pi}{2}}(|1\rangle\langle 1|1\rangle\langle 1|) \\
&= |0\rangle\langle 0| + |1\rangle\langle 1|
\end{aligned}$$

### Exercise 1.6: Pauli matrices in Dirac/Coecke notation

- For all  $i, k \in [0, 3]$  we want to show  $\sigma_i \sigma_j = \delta_{ij} I + i \sum_k \epsilon_{ijk} \sigma_k$ 
  - If  $i = j$  then  $\sigma_i \sigma_j = I$  and for all  $k$  we have  $\epsilon_{ijk} = 0$ .  
So we have  $\delta_{ij} I = I = \sigma_i \sigma_j$
  - If  $j = i + 1$
- For all  $i, k \in [0, 3]$  we want to show  $[\sigma_i, \sigma_j] = 2i \sum_k \epsilon_{ijk}$

$$\begin{aligned}
[\sigma_i, \sigma_j] &= \sigma_i \sigma_j - \sigma_j \sigma_i \\
&= (\delta_{ij} I + i \sum_k \epsilon_{ijk} \sigma_k) - (\delta_{ji} I + i \sum_k \epsilon_{jik} \sigma_k) \\
&= i \sum_k \epsilon_{ijk} \sigma_k - i \sum_k \epsilon_{jik} \sigma_k \\
&= i \sum_k \epsilon_{ijk} \sigma_k + i \sum_k \epsilon_{ijk} \sigma_k \\
&= 2i \sum_k \epsilon_{ijk} \sigma_k
\end{aligned}$$

- For all  $i, k \in [0, 3]$  with  $i \neq j$  we want to show  $\{\sigma_i, \sigma_j\} = 0$

$$\begin{aligned}
\{\sigma_i, \sigma_j\} &= \sigma_i \sigma_j + \sigma_j \sigma_i \\
&= \delta_{ij} I + i \sum_k \epsilon_{ijk} \sigma_k + \delta_{ji} I - i \sum_k \epsilon_{jik} \sigma_k & \epsilon_{jik} = -\epsilon_{ijk} \\
&= 2\delta_{ij} I \\
&= 0 & i \neq j
\end{aligned}$$

## 2 Postulates on pure states

### Exercise 2.1: Evolutions

Let  $|\psi\rangle = |0\rangle \otimes |0\rangle$  the initial state of two qubits. We want to compute  $CNot(H \otimes I) |\psi\rangle$ .

$$\begin{aligned}
CNot(H \otimes I)(|0\rangle \otimes |0\rangle) &= CNot((|0\rangle + |1\rangle)/\sqrt{2} \otimes |0\rangle) \\
&= \frac{1}{\sqrt{2}} CNot(|00\rangle + |10\rangle) \\
&= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) := |\psi'\rangle
\end{aligned}$$

$$\begin{aligned}
(H \otimes I)CNot|\psi'\rangle &= (H \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\
&= |00\rangle
\end{aligned}
\qquad H^2|\psi\rangle = |\psi\rangle$$

We have  $I := H^2$

1.  $T^4H|0\rangle$
2.  $HT^4H|0\rangle$
3.  $CNot(H \otimes HT^4H)(|0\rangle \otimes |0\rangle)$
4.  $(I \otimes CNot)(CNot \otimes I)(H \otimes I \otimes I)(|0\rangle \otimes |0\rangle \otimes |0\rangle)$
5.  $(H \otimes H)(|0\rangle \otimes |0\rangle)$

### Exercise 2.2: Measuring in another basis

- orthogonal :

$$\begin{aligned}
\langle +|- \rangle &= \left(\frac{1}{\sqrt{2}}\right)^2 + \frac{1}{\sqrt{2}} \times \frac{-1}{\sqrt{2}} \\
&= \left(\frac{1}{\sqrt{2}}\right)^2 - \left(\frac{1}{\sqrt{2}}\right)^2 \\
&= 0
\end{aligned}$$

- norm one :

$$\begin{aligned}
\langle ++ \rangle &= \left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 & \langle -- \rangle &= \left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{-1}{\sqrt{2}}\right)^2 \\
&= \frac{1}{2} + \frac{1}{2} & &= \frac{1}{2} + \frac{1}{2} \\
&= 1 & &= 1
\end{aligned}$$

- generate  $\mathbb{C}^2$

Let  $c = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$  we want to find  $x$  and  $y$  such that  $x|+\rangle + y|-\rangle = c$ .

$$\begin{aligned}
x|+\rangle + y|-\rangle &= \frac{x}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{y}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \left(\frac{x+y}{\sqrt{2}}\right)|0\rangle + \left(\frac{x-y}{\sqrt{2}}\right)|1\rangle
\end{aligned}$$

So we have this system :

$$\begin{aligned}
 \begin{cases} (x+y)/\sqrt{2} &= \alpha \\ (x-y)/\sqrt{2} &= \beta \end{cases} &\Rightarrow \begin{cases} x+y &= \sqrt{2}\alpha \\ x-y &= \sqrt{2}\beta \end{cases} \\
 &\Rightarrow \begin{cases} 2x &= \sqrt{2}(\alpha + \beta) \\ x-y &= \sqrt{2}\beta \end{cases} \\
 &\Rightarrow \begin{cases} x &= \frac{\sqrt{2}}{2}(\alpha + \beta) \\ -x+y &= -\sqrt{2}\beta \end{cases} \\
 &\Rightarrow \begin{cases} x &= \frac{\sqrt{2}}{2}(\alpha + \beta) \\ y &= \frac{\sqrt{2}}{2}(\alpha - \beta) \end{cases}
 \end{aligned}$$

$B = \{|0\rangle, |1\rangle\}$  is another o.n.b of  $\mathbb{C}^2$

We need to show that  $\sum_{M \in \mathcal{M}_{\pm}} M^{\dagger} M = 1$

$$\begin{aligned}
 \sum_{M \in \mathcal{M}_{\pm}} &= (|+\rangle \langle +|)^{\dagger} (|+\rangle \langle +|) + (|-\rangle \langle -|)^{\dagger} (|-\rangle \langle -|) \\
 &= (|+\rangle \langle +| + |-\rangle \langle -|) (|+\rangle \langle +| + |-\rangle \langle -|) \\
 &= (|+\rangle \langle +| + |-\rangle \langle -|) \\
 &= \frac{1}{2}(|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) + \frac{1}{2}(|0\rangle \langle 0| - |0\rangle \langle 1| - |1\rangle \langle 0| + |1\rangle \langle 1|) \\
 &= |0\rangle \langle 0| + |1\rangle \langle 1| \\
 &= 1
 \end{aligned}$$

So  $\mathcal{M}_{\pm}$  is a valid measurement.

We have  $|\psi\rangle = \frac{1}{3}|0\rangle + \frac{\sqrt{8}}{3}|1\rangle$

- For  $|+\rangle \langle +|$

$$\begin{aligned}
 p(|+\rangle \langle +|) &= \langle \psi | (|+\rangle \langle +|)^{\dagger} |+\rangle \langle +| \psi \rangle \\
 &= \langle \psi | |+\rangle \langle +| \psi \rangle \\
 &= \langle \psi | \frac{1}{2}(|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) \psi \rangle \\
 &= \frac{1}{2}(\frac{1}{3}\langle 0| + \frac{\sqrt{8}}{3}\langle 1|)(|0\rangle \langle 0| + |0\rangle \langle 1| + |1\rangle \langle 0| + |1\rangle \langle 1|) \psi \rangle \\
 &= \frac{1 + \sqrt{8}}{6}(\langle 0| + \langle 1|)\frac{1}{2}(\frac{1}{3}|0\rangle + \frac{\sqrt{8}}{3}|1\rangle) \\
 &= \frac{9 + 2\sqrt{8}}{18} = \frac{1}{2} + \frac{\sqrt{8}}{9}
 \end{aligned}$$

- For  $|-\rangle \langle -|$

$$\begin{aligned}
p(|-\rangle \langle -|) &= \langle \psi | (|-\rangle \langle -|)^\dagger |-\rangle \langle -| | \psi \rangle \\
&= \langle \psi | |-\rangle \langle -| | \psi \rangle \\
&= \langle \psi | \frac{1}{2}(|0\rangle \langle 0| - |0\rangle \langle 1| - |1\rangle \langle 0| + |1\rangle \langle 1|) | \psi \rangle \\
&= \frac{1}{2} \left( \frac{1}{3} \langle 0| + \frac{\sqrt{8}}{3} \langle 1| \right) (|0\rangle \langle 0| - |0\rangle \langle 1| - |1\rangle \langle 0| + |1\rangle \langle 1|) | \psi \rangle \\
&= \frac{1}{2} \left( \frac{1-\sqrt{8}}{3} \langle 0| + \frac{\sqrt{8}-1}{3} \langle 1| \right) \left( \frac{1}{3} |0\rangle + \frac{\sqrt{8}}{3} |1\rangle \right) \\
&= \frac{1}{2} \left( \frac{1-\sqrt{8}}{9} + \frac{8-\sqrt{8}}{9} \right) \\
&= \frac{1}{2} \left( \frac{9-2\sqrt{8}}{9} \right) = \frac{1}{2} - \frac{\sqrt{8}}{9}
\end{aligned}$$

The post measure states are :

$$|\psi_+\rangle = \frac{1}{\sqrt{\frac{1}{2} + \frac{\sqrt{8}}{9}}} \begin{pmatrix} \frac{1+\sqrt{8}}{6} \\ \frac{1+\sqrt{8}}{6} \end{pmatrix}$$

$$|\psi_-\rangle = \frac{1}{\sqrt{\frac{1}{2} - \frac{\sqrt{8}}{9}}} \begin{pmatrix} \frac{1-\sqrt{8}}{6} \\ \frac{\sqrt{8}-1}{6} \end{pmatrix}$$

### Exercise 2.3: Measuring to distinguish

We defined:

$$M_0 = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix} \quad M_+ = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad M_f = \begin{pmatrix} \frac{-1-i}{2} & i \\ \frac{1-i}{2} & i \end{pmatrix}$$

$$\langle 0 | M_0^\dagger M_0 | 0 \rangle = 1$$

$$\langle + | M_0^\dagger M_0 | + \rangle = 0$$

$$\langle 0 | M_+^\dagger M_+ | 0 \rangle = 0$$

$$\begin{aligned}
\langle + | M_+^\dagger M_+ | + \rangle &= \langle + | M_+ | + \rangle \\
&= \frac{2}{\sqrt{2}} \langle 1 | + \rangle \\
&= \frac{2}{\sqrt{2}} \times \frac{1}{\sqrt{2}} = 1
\end{aligned}$$

The measure  $\mathcal{M}$  is valid :

$$M_0^\dagger M_0 = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \quad M_+^\dagger M_+ = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} \quad M_f^\dagger M_f = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$$

$$M_0^\dagger M_0 + M_+^\dagger M_+ + M_f^\dagger M_f = I_2$$

**Exercise 2.4: Measuring the phase**

The probability to get a result  $x$  when we measure  $e^{i\theta} |0\rangle$  is :

$$\begin{aligned} p(x) &= e^{-i\theta} M_x^\dagger M_x e^{i\theta} |0\rangle \\ &= e^{-i\theta} \times e^{i\theta} (\bar{\alpha} \langle 0| + \bar{\beta} \langle 1|)(\alpha |0\rangle + \beta |1\rangle) \\ &= \langle \alpha | \alpha \rangle + \langle \beta | \beta \rangle \end{aligned}$$

The result does not depend on  $\theta$ . So, we don't have a measure who can distinguish  $|0\rangle$  from  $e^{i\theta}$ . We have the measurement  $M_+$  who can sometimes tell the difference between  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and  $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta} |1\rangle)$

$$\begin{aligned} p(|+\rangle) &= \langle \psi | M_+^\dagger M_+ | \psi \rangle \\ &= \frac{1}{2} + \frac{1}{4}e^{i\theta} + \frac{1}{4}e^{i\theta} \end{aligned}$$

The result depends on  $\theta$  :)

**Exercise 2.5: Measuring a subsystem**

$\mathcal{M}$  is a valid measurement description :

$$\begin{aligned} \sum_m M_m^\dagger M_m &= (|0\rangle \langle 0| \otimes I)^2 + (|1\rangle \langle 1| \otimes I)^2 \\ &= |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes I \\ &= I \otimes I \\ &= 1 \end{aligned}$$

We will apply the measurement operator:

$$\begin{aligned} p(0) &= \langle \beta_0 | M_0^\dagger M_0 | \beta_0 \rangle = \frac{1}{\sqrt{2}} \langle 00 | \frac{1}{\sqrt{2}} | 00 \rangle = \frac{1}{2} \\ p(1) &= \langle \beta_0 | M_1^\dagger M_1 | \beta_0 \rangle = \frac{1}{\sqrt{2}} \langle 11 | \frac{1}{\sqrt{2}} | 11 \rangle = \frac{1}{2} \end{aligned}$$

Finally, the post-measurement state are :

$$\begin{aligned} |\psi_0\rangle &= \frac{M_0 \beta_0}{\frac{1}{\sqrt{2}}} = |00\rangle \\ |\psi_1\rangle &= \frac{M_1 \beta_0}{\frac{1}{\sqrt{2}}} = |11\rangle \end{aligned}$$

### 3 Some mathematics

**Exercise 3.1: Spectral theorems complements**

Let  $D$  and  $D'$  two diagonal matrices and  $U$  a unitary matrix.



- Let  $A = UDU^\dagger$  and  $B = UD'U^\dagger$

$$\begin{aligned}
 AB &= UDU^\dagger UD'U^\dagger \\
 &= UDD'U^\dagger & U \text{ is a unitary matrix} \\
 &= UD'DU^\dagger & D \text{ and } D' \text{ are diagonal} \\
 &= UD'U^\dagger UDU^\dagger \\
 &= BA
 \end{aligned}$$

- Let  $M = UDU^\dagger$

$$\begin{aligned}
 MM^\dagger &= UDU^\dagger (UDU^\dagger)^\dagger \\
 &= UDU^\dagger (U^\dagger)^\dagger D^\dagger U^\dagger \\
 &= UDU^\dagger UD^\dagger U^\dagger \\
 &= UDD^\dagger U^\dagger \\
 &= UD^\dagger DU^\dagger \\
 &= UD^\dagger U^\dagger UDU^\dagger \\
 &= (UDU^\dagger)^\dagger UDU^\dagger \\
 &= M^\dagger M
 \end{aligned}$$

- Let  $E = UDU^\dagger$  with having only non-negative value.

Let  $|\psi\rangle \in \mathcal{M}_{n,1}(\mathbb{C})$ ,  $d_i$  such that  $E_{i,i} = d_i$

$$\begin{aligned}
 \langle \psi | E | \psi \rangle &= \langle \psi | UDU^\dagger | \psi \rangle \\
 &= (U^\dagger | \psi \rangle)^\dagger D (U^\dagger | \psi \rangle) \\
 &= \sum_{i=1}^n d_i (U_i | \psi \rangle)^2 \\
 &\geq 0
 \end{aligned}$$

- Let  $V = UDU^\dagger$  with  $D$  having only modulus one values.

$$\begin{aligned}
 VV^\dagger &= UDU^\dagger (UDU^\dagger)^\dagger \\
 &= UDU^\dagger UD^\dagger U^\dagger \\
 &= UDD^\dagger U^\dagger \\
 &= UU^\dagger & D \text{ has only modulus one values} \\
 &= I
 \end{aligned}$$

So  $V$  is a unitary matrix.

- Let  $E$  a non-negative matrix.  $E$  is spectrally decomposable with non-negative eigenvalues. We can take  $M := \sqrt{E}$  which is defined by its spectral decomposition being with the square roots of the eigenvalues of  $E$ .  $M$  is hermitian and  $E = MM$ , so  $E^\dagger = (MM)^\dagger = M^\dagger M^\dagger = MM = E$ .
- The follow matrix is not normal :

$$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$MM^\dagger = \begin{pmatrix} 5 & 11 \\ 11 & 25 \end{pmatrix} \neq \begin{pmatrix} 10 & 14 \\ 14 & 20 \end{pmatrix} = M^\dagger M$$

### Exercice 3.2: Isometry versus unitary versus involution

- Let  $M$  a unitary and hermitian matrix.

$$\begin{aligned} MM &= MM^\dagger & M \text{ is hermitian} \\ &= I & M \text{ is unitary} \end{aligned}$$

- Matrix  $2 \times 2$  unitary that is not an involution :

$$M = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

The inverse of  $M$  is :

$$M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$$

We have  $M \neq M^{-1}$  so  $M$  is not an involution.

- Matrix  $m \times n$  isometry that is not a unitary:

$$M = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$M^\dagger M = \begin{pmatrix} 1 \end{pmatrix} = I_1 \quad MM^\dagger = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq I_2$$

- Let  $M$  an  $n \times n$  isometry matrix ( $M^\dagger M = I_n$ )

$$\begin{aligned} MM^\dagger &= \sum_{i,j} M_{i,j} |i\rangle \langle j| \sum_{i,j} M_{j,i} |i\rangle \langle j| \\ &= \sum_{i,j} M_{i,j} M_{j,i} |i\rangle \langle i| \\ &= \sum_{i,j} M_{j,i} M_{i,j} |i\rangle \langle j| \\ &= \sum_{i,j} M_{j,i} |i\rangle \langle j| \sum_{i,j} M_{i,j} |i\rangle \langle j| \\ &= M^\dagger M \\ &= I_n \end{aligned}$$

## 4 On the nature of quantum information

### Exercice 4.1: Hadamard

- $a = 0$

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^0|1\rangle) \end{aligned}$$

- $a = 1$

$$\begin{aligned} H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^1|1\rangle) \end{aligned}$$

#### Exercise 4.2: Who controls whom?

We define :

$$NotC = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$NotC|00\rangle = |00\rangle$$

$$NotC|01\rangle = |11\rangle$$

$$NotC|10\rangle = |10\rangle$$

$$NotC|11\rangle = |01\rangle$$

We want to proof  $(H \otimes H)CNot(H \otimes H) = NotC$  :

$$\begin{aligned} (H \otimes H)(|x\rangle \otimes |y\rangle) &= (H|x\rangle \otimes H|y\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + (-1)^y|1\rangle) \\ &= \frac{1}{2}(|00\rangle + (-1)^x|10\rangle + (-1)^y|01\rangle + (-1)^{x+y}|11\rangle) \end{aligned}$$

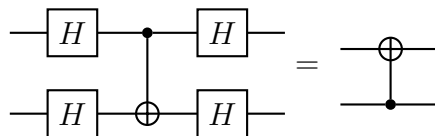
We apply the operator  $CNot$ :

$$\begin{aligned} &CNot\left(\frac{1}{2}(|00\rangle + (-1)^x|10\rangle + (-1)^y|01\rangle + (-1)^{x+y}|11\rangle)\right) \\ &= \frac{1}{2}(|00\rangle + (-1)^x|11\rangle + (-1)^y|01\rangle + (-1)^{x+y}|10\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x+y}|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + (-1)^y|1\rangle)\right) \\ &= H|x \oplus y\rangle \otimes H|y\rangle \end{aligned} \quad (-1)^{x+y} = (-1)^{x \oplus y} \quad (x \oplus y \in \{0, 1\})$$

Finlay we apply  $(H \otimes H)$ :

$$\begin{aligned} (H \otimes H)(H|x \oplus y\rangle \otimes H|y\rangle) &= HH|x \oplus y\rangle \otimes HH|y\rangle \\ &= |x \oplus y\rangle \otimes |y\rangle \\ &= NotC(|x\rangle \otimes |y\rangle) \end{aligned}$$

In quantum circuit :



## 5 Protocols

### Exercise 5.1: Canonical basis versus diagonal basis

- If Bob measures the result in the same basis then he can retrieve the information sent
- If Bob measures in an other basis then he learns nothing about the message.
- If Eve intercepts and measures it in the same basis then Bob can have some information on the message if he read the message in the same basis.
- But if Eve intercepts and measures it in an other basis and Bob read the message in the original basis then he learns nothing about the message.

### Exercise 5.2: BB84

1. Alice will start by producing a random string of bits, encode each of them either into the canonical or the diagonal basis, and send that to Bob.
2. Bob will measure them either using the canonical basis or the diagonal basis, at random.
3. Bob will broadcast which bases he used
4. Alice will know when Bob used the same base. When Bob has used the right base, Bob's information is correct, otherwise it is wrong (previous exercise).
5. Eve does not know the bases like Bob And she has very little chance of having the right basic sequence ( $\frac{1}{2^n}$ ). But she's going to disrupt Bob's measurements.
- 6.

They can use common measurements bases to create an encryption key. For example, a basic measurements base sequence can become a binary code with 0 when we have the base  $\mathcal{M}$  and 1 if we have the base  $\mathcal{M}'$ . With this generate key we can communicate with an existing encryption protocol.

### Exercise 5.3: Quantum random access code

We have 4 cases (The calculations are not too detailed to make them easier to read):

- $x = y = 0$

$$p(|+\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

$$p(|-i\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

- $x = 0$  and  $y = 1$

$$p(|+\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

$$p(|i\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

- $x = 1$  and  $y = 0$

$$p(|-\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

$$p(|-i\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

- $x = y = 1$

$$p(|-\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

$$p(|-i\rangle) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

If Bob wants to find  $x$  he needs to use  $\mathcal{M}_x$ . If Bob wants to find  $y$  he needs to use  $\mathcal{M}_{xi}$ .  
With this method the probability to success is :

$$\begin{aligned}\mathbb{P}(win) &= \frac{1}{4}(p(+)_{x=1} + p(-)_{x=0} + p(+i)_{y=0} + p(-i)_{y=1}) \\ &= \frac{1}{4} \times 4\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \\ &= \frac{1}{2} + \frac{1}{2\sqrt{2}} \\ &> \frac{3}{4}\end{aligned}$$

#### Exercise 5.4: The Bell basis

$$|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\beta_1\rangle = (X \otimes I) |\beta_0\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

$$|\beta_2\rangle = (Y \otimes I) |\beta_0\rangle = \frac{i}{\sqrt{2}}(|10\rangle - |01\rangle)$$

$$|\beta_3\rangle = (Z \otimes I) |\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

These four states are orthogonal and orthonormal,  
orthogonal:

$$\langle\beta_0|\beta_1\rangle = \frac{1}{2} \times 0 = 0$$

$$\langle\beta_0|\beta_2\rangle = \frac{i}{2} \times 0 = 0$$

$$\langle\beta_0|\beta_3\rangle = \frac{1}{2} - \frac{1}{2} = 0$$

$$\langle\beta_1|\beta_2\rangle = \frac{i}{2} - \frac{i}{2} = 0$$

$$\langle\beta_1|\beta_3\rangle = \frac{1}{2} \times 0 = 0$$

$$\langle\beta_2|\beta_3\rangle = \frac{i}{2} \times 0 = 0$$

orthonormal:

$$\langle\beta_0|\beta_0\rangle = \frac{1}{2} + \frac{1}{2} = 1$$

$$\langle\beta_1|\beta_1\rangle = \frac{1}{2} + \frac{1}{2} = 1$$

$$\langle\beta_2|\beta_2\rangle = \frac{1}{2} + \frac{1}{2} = 1$$

$$\langle\beta_3|\beta_3\rangle = \frac{1}{2} + \frac{1}{2} = 1$$

So, this states are an orthonormal basis.  
It is also a valid measurement :

$$\begin{aligned}\sum_i \mathcal{M}_i &= |\beta_0\rangle \langle\beta_0| + |\beta_1\rangle \langle\beta_1| + |\beta_2\rangle \langle\beta_2| + |\beta_3\rangle \langle\beta_3| \\ &= I_4\end{aligned}$$

#### Exercise 5.5: Superdense coding

At the beginning, Alice and Bob share an entangled state  $|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  Alice can change  $|\beta_0\rangle$  in  $|\beta_k\rangle$  with this operation :

- $|\beta_0\rangle$  : do nothing
- $|\beta_1\rangle$  : apply the matrix  $X$

$$\begin{aligned} X |\beta_0\rangle &= (X \otimes I) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ &= |\beta_1\rangle \end{aligned}$$

- $|\beta_2\rangle$  : apply the matrix  $Y$

$$\begin{aligned} Y |\beta_0\rangle &= (Y \otimes I) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{i}{\sqrt{2}}(|10\rangle - |01\rangle) \\ &= |\beta_2\rangle \end{aligned}$$

- $|\beta_3\rangle$  : apply the matrix  $Z$

$$\begin{aligned} Z |\beta_0\rangle &= (Z \otimes I) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ &= |\beta_3\rangle \end{aligned}$$

So Alice can encode the four possible pairs of bits (00, 01, 10 and 11) with the 4 Bell states. We have shown that Alice can modify  $|\beta_0\rangle$  on her own, so with qubit she can change the communication state to one of the 4 states. Bob can measure the result and retrieve the information from Alice.

### Exercise 5.6: Discussion: classical description of a single qubit

A qubit is coded with this formula :  $\alpha |0\rangle + \beta |1\rangle$ . We just need to send 2 complexes numbers. So if a number is encoded with  $n$  bits we send  $4n$  bits.

### Exercise 5.7: Teleportation

$$\begin{aligned} \frac{1}{2} \sum_i |\beta_i\rangle \otimes \sigma_i |\psi\rangle &= \frac{1}{2\sqrt{2}} ((|00\rangle + |11\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle) + \\ &\quad (|10\rangle + |01\rangle) \otimes (\alpha |1\rangle + \beta |0\rangle) + \\ &\quad (i |10\rangle - i |01\rangle) \otimes (i\alpha |1\rangle - i\beta |0\rangle) + \\ &\quad (|00\rangle - |11\rangle) \otimes (\alpha |0\rangle - \beta |1\rangle)) \\ &= \frac{1}{\sqrt{2}} (\alpha |000\rangle + \beta |100\rangle + \alpha |011\rangle + \beta |111\rangle) \\ &= \frac{1}{2\sqrt{2}} (2\alpha(|000\rangle + |011\rangle) + 2\beta(|100\rangle + |111\rangle)) \\ &= \frac{1}{\sqrt{2}} (\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)) \\ &= \frac{1}{\sqrt{2}} ((\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle \otimes |0\rangle + (\alpha |0\rangle + \beta |1\rangle) \otimes |1\rangle \otimes |1\rangle) \\ &= \frac{1}{\sqrt{2}} (|\psi\rangle \otimes |0\rangle \otimes |0\rangle + |\psi\rangle \otimes |1\rangle \otimes |1\rangle) \end{aligned}$$

**Exercice 5.8: The swap test**

Before the measurement we have this state :

$$\begin{aligned}
|\kappa\rangle &= (H \otimes I \otimes I) CSwap(H \otimes I \otimes I) |0\rangle \otimes |\phi\rangle \otimes |\psi\rangle \\
&= (H \otimes I \otimes I) CSwap\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes |\phi\rangle \otimes |\psi\rangle \\
&= (H \otimes I \otimes I) CSwap \frac{1}{\sqrt{2}}(|0\phi\psi\rangle + |1\phi\psi\rangle) \\
&= (H \otimes I \otimes I) \frac{1}{\sqrt{2}}(|0\phi\psi\rangle + |1\psi\phi\rangle) \\
&= \frac{1}{2}(|0\rangle \otimes (|\phi\psi\rangle + |\psi\phi\rangle) - |1\rangle \otimes (|\phi\psi\rangle + |\psi\phi\rangle)) \\
&= \frac{1}{2}(|0\phi\psi\rangle + |0\psi\phi\rangle + |1\phi\psi\rangle - |1\psi\phi\rangle)
\end{aligned}$$

We apply the measures :

$$\begin{aligned}
p(0) &= \langle \kappa | 0 \rangle \langle 0 | \kappa \rangle \\
&= \frac{1}{2}(\langle \phi\psi | + |\psi\phi\rangle) \times \frac{1}{2}(\langle \phi\psi | + |\psi\phi\rangle) \\
&= \frac{1}{4}(2 + \langle \phi\psi | \psi\phi \rangle + \langle \psi\phi | \phi\psi \rangle) \\
&= \frac{1}{4}(2 + 2 \langle \phi\psi | \psi\phi \rangle) \\
&= \frac{1}{2} + \frac{\langle \psi\phi | \psi\phi \rangle}{2} \\
&= \frac{1}{2} + \frac{1}{2} |\langle \psi | \phi \rangle|^2
\end{aligned}$$

we have  $p(1) = 1 - p(0)$  so  $p(1) = \frac{1}{2} - \frac{1}{2} |\langle \psi | \phi \rangle|^2$

**Exercice 5.9: Quantum fingerprinting**

TODO

## 6 Quantum error correction

**Exercice 6.1: Proof of the 3 qubit code against bit flip errors**

Let  $P = |000\rangle \langle 000| + |111\rangle \langle 111|$

We define the corresponding CPTP map  $\mathcal{E}$  (course not definition):

$$\mathcal{E}(\rho) = p^3 \rho + p^2(1-p)[X_1 \rho X_1 + X_2 \rho X_2 + X_3 \rho X_3]$$

$p$  is the probability that a qubit will flip and  $X_i$  represent  $i^{th}$  qubit flip.

We decompose  $\mathcal{E}$ :

$$E = \{\sqrt{(1-p)^2} X_1, \sqrt{(1-p)^2} X_2, \sqrt{(1-p)^2} X_3, \sqrt{(1-p)^2} I\}$$

Now we will check the quantum error-correction conditions:

$$\begin{aligned}
PE_i^\dagger E_j P &= 0 & i \neq j \\
PE_i^\dagger E_i P &= (1-p)^2 p & i \in \{0, 1, 2\} \\
PE_3^\dagger E_3 P &= (1-p)^3
\end{aligned}$$

This equation define the matrix

$$\begin{pmatrix}
(1-p)^2 p & 0 & 0 & 0 \\
0 & (1-p)^2 p & 0 & 0 \\
0 & 0 & (1-p)^2 p & 0 \\
0 & 0 & 0 & (1-p)^3
\end{pmatrix}$$

This matrix is clearly Hermitian, so the code corrector  $P$  can correct the noisy channel  $\mathcal{E}$

## 7 Bell

### Exercise 7.1: Probability of winning the CHSH game

We have 4 case :

- $s = r = 0$

$$\begin{aligned}
\mathcal{P}(\text{win}) &= \mathcal{P}(a = b = 0) + \mathcal{P}(a = b = 1) \\
&= |((\cos(0) \langle 0| + \sin(0) \langle 1|) \otimes ((\cos(\frac{\pi}{8}) \langle 0|) + \sin(\frac{\pi}{8}) \langle 1|)) |\beta_0\rangle|^2 + \\
&\quad |((\sin(0) \langle 0| - \cos(0) \langle 1|) \otimes ((\sin(\frac{\pi}{8}) \langle 0|) - \cos(\frac{\pi}{8}) \langle 1|)) |\beta_0\rangle|^2 \\
&= |(\cos(\frac{\pi}{8}) \langle 00| + \sin(\frac{\pi}{8}) \langle 01|) |\beta_0\rangle|^2 + |(-\sin(\frac{\pi}{8}) \langle 10| + \cos(\frac{\pi}{8}) \langle 11|) |\beta_0\rangle|^2 \\
&= |\frac{1}{\sqrt{2}} \cos(\frac{\pi}{8})|^2 + |\frac{1}{\sqrt{2}} \cos(\frac{\pi}{8})|^2 \\
&= \frac{1}{2} \cos^2(\frac{\pi}{8}) + \frac{1}{2} \cos^2(\frac{\pi}{8}) \\
&= \cos^2(\frac{\pi}{8})
\end{aligned}$$

- the following calculations are similar and we obtain  $\cos^2(\frac{\pi}{8})$

There are 4 different ways to draw  $s$  and  $r$  :

$$\mathcal{P}(\text{win}) = 4 \times \frac{1}{4} \times \cos^2(\frac{\pi}{8}) = \cos^2(\frac{\pi}{8})$$