1.6 Téléportation quantique

A veut envoyer $|\psi\rangle$ à B

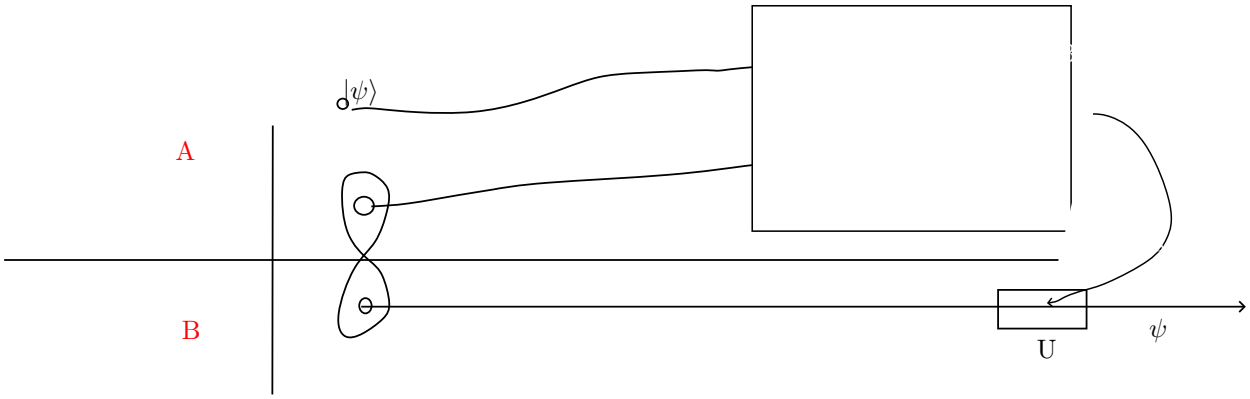


FIGURE 1 – Téléportation quantique 2

$$
\begin{aligned}
|\Psi\rangle \otimes \left|\Phi^+\right\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2}}\left[\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle\right] \\
&= \frac{1}{2}\left[\alpha\left(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle\right)|0\rangle + \alpha\left(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle\right)|1\rangle + \beta\left(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle\right)|0\rangle + \beta\left(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle\right)|2\rangle\right] \\
&= \frac{1}{2}\left[\left|\Phi^-\right\rangle(\alpha\,|0\rangle + \beta\,|1\rangle) + \cdots\right] \\
&= \frac{1}{2}\left[\left|\Phi^+\right\rangle|\Psi\rangle + \left|\Phi^-\right\rangle Z\,|\Psi\rangle + |\Psi\rangle X\,|\Psi\rangle + \left|\Psi^-\right\rangle ZX\,|\Psi\rangle\right]
\end{aligned}
$$

Alice mesure $\{|\psi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ avec 25% chaque.

$$\left|\Psi^+\right\rangle : \mathbb{1} \quad \left|\Psi^-\right\rangle : \text{applique Z} \cdots$$

Aparté notation tensorielle

vecteur `-O-`
Matrice `-[]-`
état à deux qbits : `O==`

$$\Psi = \sum_{ij} c_{ij} |e_i\rangle \otimes |e_j\rangle$$

ket : `O-`
bra : `-O`

Produit tensoriel :
`O-`
$\otimes$
`O-`

Contraction : ($\langle\psi|\phi\rangle$)

`(\psi)--(\phi)`

Produit matrice-vecteur

`(\psi)--[u]-` $= u|\psi\rangle$

Matrice-Matrice

`-[A]-[B]-` $= BA =$ `-[BA]-`

Trace :

```
-----
|   |
L[M]J
```

2 Calcul Quantique

2.1 Calcul classique

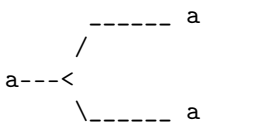
ordinateur classique

$$\rho : \{0,1\}^n \to \{0,1\}^,$$

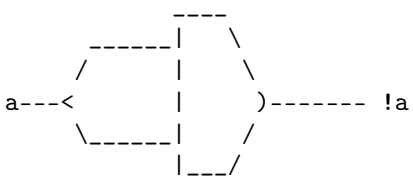
Portes universelles `NAND`

```
    ____
a---|   \
    |    )---- a NAND b
b---|___/
```

COPY:



EX: NOT



COPY est impossible en quantique

Complexité

Difficulté de ρ : Nombre de portes universelle requisent pour le plus petit circuit réalisant ρ

Famille de Problème ou la taille varie

La circuit ne doit pas être adapté à la taille

P : Temps polynomial (facile)

$$|c_n| = n^\alpha$$

u

NP : Temps non-polynomial

NP-difficile : Au moins aussi difficile que le problème le plus dur de NP (Pas forcément dans NP)
NP-comlet : NP difficile **et** dans NP
clairement

$$P \subseteq NP$$

$$\boxed{P =^? NP}$$

2.2 Calcul quantique

Mécanique quantique : Opérateur d'évolution unitaire

$$U^\dagger U = \mathbb{1}$$

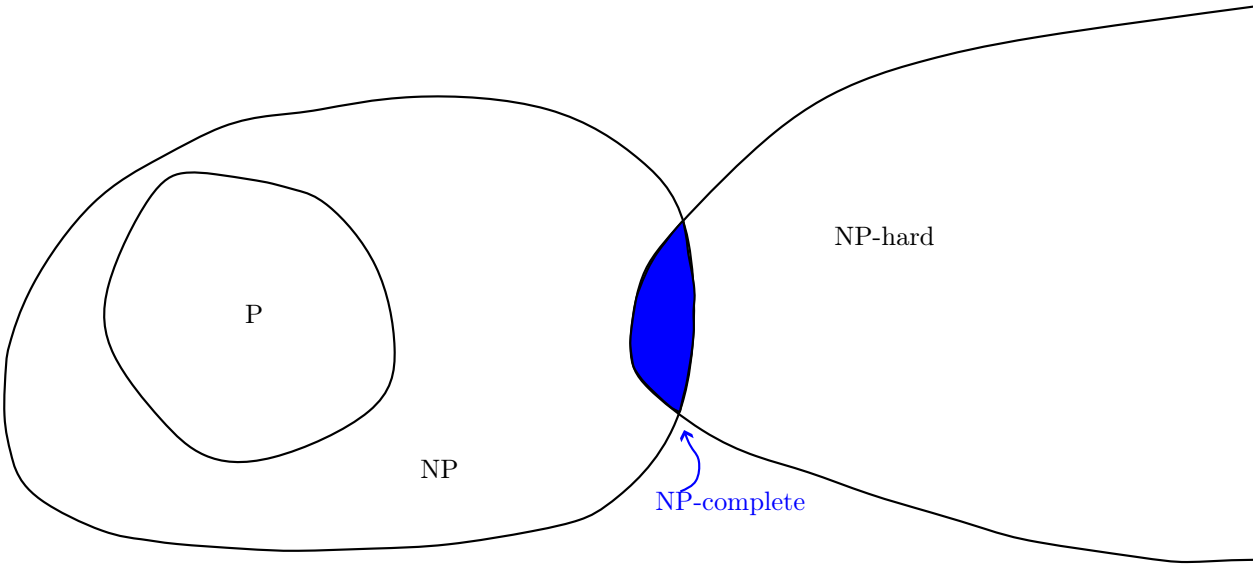


FIGURE 2 – La complexité

La porte `NAND` n'est pas réversible (2bits $\rightarrow$ 1bit)

Il existe des porte réversibles classiqus

Note

ON peut toujours exprimer une fonction

$$\rho : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^m$$

sous la forme

$$g : \mathbb{Z}_2^{n+m} \mapsto \mathbb{Z}_2^{n+m}$$

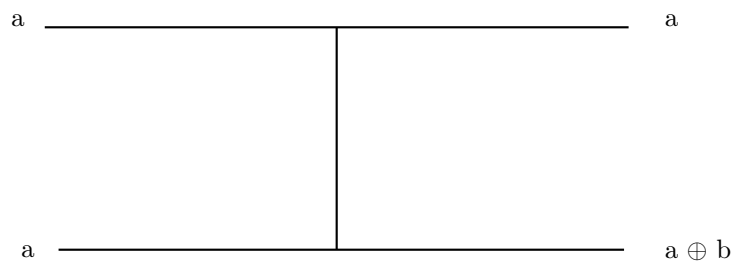
$$g(x, 0) \mapsto g(x, f(x))$$

2.3 Circuits Quantiques

a) état initial ($|0\rangle^{\otimes n}$) : Ce choix est arbitraire. Important de commencer dans un état non-intriqué

b) Transformation unitaire U : On décompose u en un ensemble de portes universelles agissant sur 1-3 qubits. Les U possibles ($U \in SU(2^n)$) forment un groupe continu. On peut générer U à partir d'un circuit fini C La complexité quantique est définie à partir de $|C|$

c) Mesure : Résultat non-détérministe On choisit de mesurer dans la base Z $\{|0\rangle, |1\rangle\}$ On peut mesurer différentes bases



a b	CNOT
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

CNOT

FIGURE 3 – CNOT

en chageant U. On évite de cacher la complexité dans la mesure. On aurait pu choisir de mesurer durant le circuit.

2.4 Complexité quantique

BQP (bounded-error quantum polynomial time) : Esemble des Problèmes faciles pour un ordinateur quantique (Problèmes tel que $|C| \leq n^{\infty}$)

L'ordinateur quantique doit donner la bonne réponse la plupart du temps ($\geq \frac{2}{3}$) (pas deterministe). On moyenne sur un grand nombre de calculs

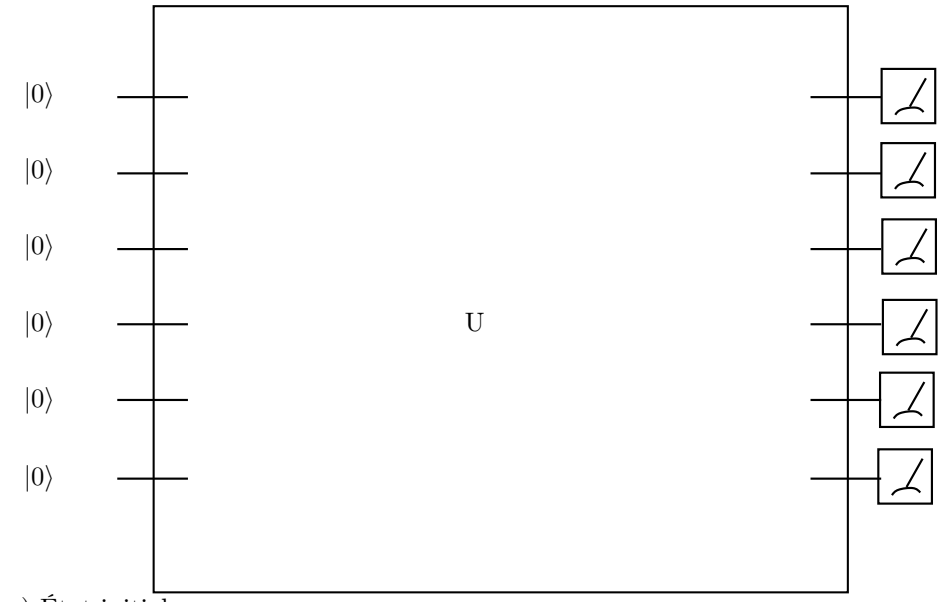


FIGURE 4 – Anatomie d'un circuit quantique

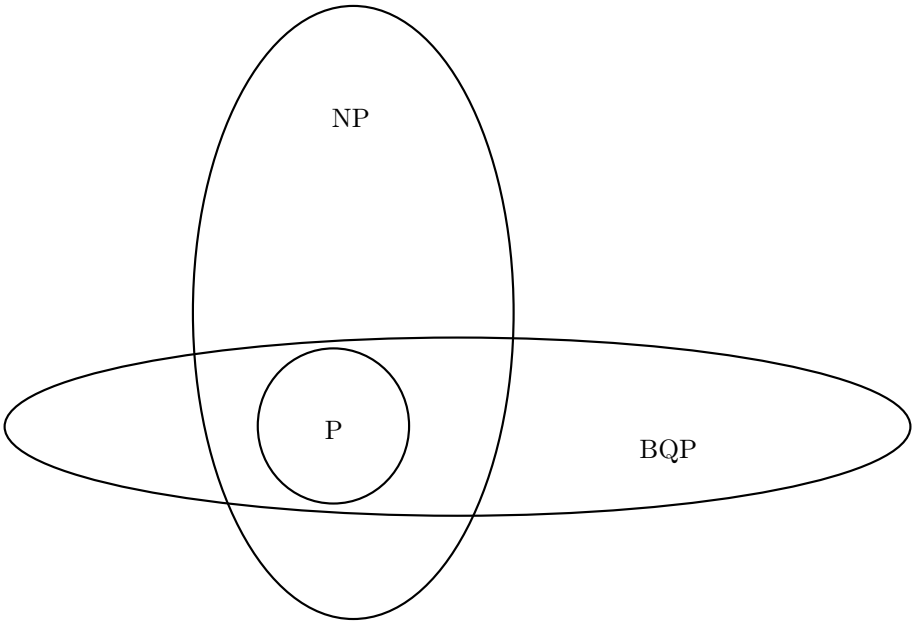


FIGURE 5 – Complexité quantique