# Grover, and its killer, noise

## 0. Reminder:

* Universality ⟺ do any unitary operation
  → a basis set is enough, several set available, one chosen by the technology.
* Oracle:

$$U_f\ |x\rangle \otimes |0\rangle^{\otimes n} \longrightarrow \ldots |x\rangle \otimes |\ldots\rangle$$

optional — optional — optional

└ oracle if black box, ie. can query at will, but do not know what it is

* boolean oracle ; phase oracle
* seen Deutsh - Josza ; Bernstein - Vazirani ; simple quantum com ; superdense coding ; teleportation protocol.

→ all use superposition / entanglement as a ressource
it would be a shame if something where to destroy these ressources!

# I] Looking through a list

## 1] Done by a human

- ex : phone book (alphabetical order) when having a name
  - × use dichotomy algorithm
    → complexity $\mathcal{O}(\log_2(N))$ w/ $N = \#$ names
    (better: use an index !)
- when looking up names from phone number (unordered list) → look through them all; on average; only $\frac{N}{2}$ → complexity $\mathcal{O}(N)$

## 2] By a classical computer

Case of boolean search

* If structured :

| | | | |
|---|---|---|---|
| Step 1 | a | AND | (NOT b) |
| Step 2 | a=1 | ; | NOT b = 1 |
| Step 3 | a = 1 | ; | b = 0 |

fast by unraveling structure

* If unstructured : brute force

build look up table of $f(a,b)$

⇒ complexity $\mathcal{O}(2^n)$

## 3) By a Q.C. : Grover

* $|w\rangle = |000.10110\ldots\rangle$ the winning state we want to find (one out of $2^n$ bitstrings) (generalizat° to several possible)

* initial state $|s\rangle$.

requierement : $\langle s|w\rangle \neq 0$

$\to$ impossible to ensure in general w/o knowing $|w\rangle$.

here, we know that $w$ is a bit string, so

$|s\rangle = \frac{1}{\sqrt{2^n}} \sum_b |b\rangle$ works

bitstring

$= |+\rangle^{\otimes n}$

* define $|s'\rangle \equiv \frac{1}{\sqrt{2^n-1}} \sum |b\rangle$ (useful for later)

s.t. $\langle w|s'\rangle = 0$

* define $U_f^\dagger = -|w\rangle\langle w| + \sum_{b\neq w} |b\rangle\langle b|$ $\to$ "easier" to build because it just test input

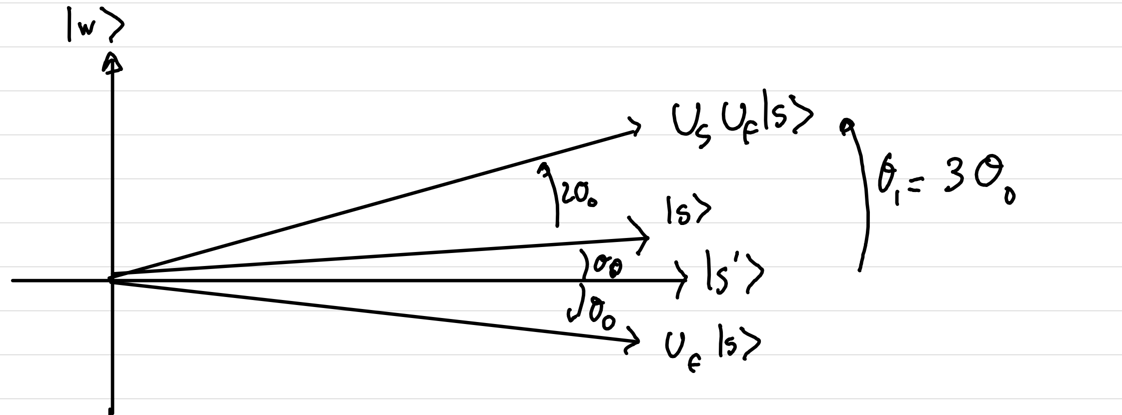
$\to U_s^\dagger = |s\rangle\langle s| - (\mathbb{1} - |s\rangle\langle s|)$

$= 2|s\rangle\langle s| - \mathbb{1}$ $\to$ buildable bc. we know $|s\rangle$

phase oracle in the X space instead of Z space.

Can rewrite $|s\rangle = \cos\theta_0 |s'\rangle + \sin\theta_0 |w\rangle$

$= \sqrt{\frac{N-1}{N}} |s'\rangle + \frac{1}{\sqrt{N}} |w\rangle \to \theta_0 \simeq \frac{1}{\sqrt{N}}$




if we do $(U_s U_f)^t |s\rangle$

$\Rightarrow \theta_t = (2t+1)\theta_0$

We want $\theta_t = \frac{\pi}{2} \Rightarrow t = \left(\frac{\pi\sqrt{N}}{2} - 1\right)\frac{1}{2} = \mathcal{O}(\sqrt{N})$

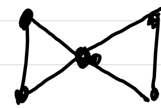
independant of what $|w\rangle$ is.

comparable to $\mathcal{O}(N)$ classicall

$\to$ polynomial improv

# II The killer : noise

## 1] Noise is the frontier

- \# qubits → needs more than available
- connectivity →  (assuming $\overline{U}$ set)
- noise

↗ # qubits ⇒ ↗ noise & sparser connectivity
(the connectivity does not scale)

compensating connectivity w/ more gates ↗ noise
(and quantum volume)
aka overhead

→ noise is the obstacle

## 2) The density matrix (info dump)

### a) Why useful?

Axiom of Q.M : an isolated Q. syst is completely described by a state vector $|\psi\rangle$

$\Rightarrow$ a state vector can only ever evolve into another state vector,

$\Rightarrow$ such an evolut° can only be unitary

$\Rightarrow$ measurement not unitary $\rightarrow$ should not be possible...

$\Rightarrow$ not isolated anymore

$\Rightarrow$ need a more generic descript° to account for the environment $\Rightarrow$ densit matrix

### b) For pure states

density matrix $\Leftrightarrow$ state vector

$$\rho = |\psi\rangle\langle\psi|$$

ex : if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\Rightarrow \rho = |\alpha|^2 |0\rangle\langle 0| + \alpha\beta^* |0\rangle\langle 1| + \alpha^*\beta |1\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$$

the "coherence"

$$= \begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix}$$

in the basis $|\psi\rangle$ ; $|\psi^\perp\rangle$ s.t. $\langle\psi^\perp|\psi\rangle = 0$

$$\Rightarrow \rho = |\psi\rangle\langle\psi| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

if $U : \{|0\rangle ; |1\rangle\} \longmapsto \{|\psi\rangle ; |\psi^\perp\rangle\}$

$$\Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = U \begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix}$$

$\Rightarrow$ pure state i.e. $\exists |\psi\rangle$ s.t. $\rho = |\psi\rangle\langle\psi|$ iff $\exists$ a basis s.t. $\rho = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

corrollary : if state pure & more than 1 non-zero diago elt then some coherence $\neq 0$.

## c) Non-pure states = mixed states

ex : $\rho = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & \frac{2}{3} \end{pmatrix}$

$\Rightarrow \nexists\ \alpha, \beta$ st. that $\rho = |\psi\rangle\langle\psi|$ w/ $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\rho = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|$$

↳ not called a "superposition" because not on the Bloch sphere.
(sometimes put in a radius $< 1$)

* particular :

- $\rho = \begin{pmatrix} e^{-\frac{E_0}{k_B T}} & & & 0 \\ & e^{-\frac{E_1}{k_B T}} & & \\ & & \ddots & \\ 0 & & & e^{-\frac{E_n}{k_B T}} \end{pmatrix}$

  → thermal mix "classically random"

- $\rho = \frac{1}{N} \mathbb{1}$ → classical mix

  → written like this in every basis bc:
  $U \mathbb{1} U^\dagger = U U^\dagger = \mathbb{1}$

$\Rightarrow$ any state has the same proba $\frac{1}{N^2}$ to be measured

→ RNG, no information.

ex: $\rho = \frac{1}{2}\mathbb{1}$ ; $\Rightarrow \langle S^i \rangle = 0 \ \ \forall i$

## d) Properties of $\rho$

Normalization: $Tr(\rho) = 1$

why: diago term are proba of finding the state $\rho$ in the choice of basis:

$$\rho = \begin{pmatrix} p_1 & * & \cdots & * \\ * & p_2 & \ddots & \vdots \\ * & * & p_3 & \\ * & * & * & \ddots \end{pmatrix} \begin{array}{l} |1\rangle \\ |2\rangle \\ |3\rangle \\ \vdots \end{array}$$

$$Tr(\rho) = \underbrace{\sum_i p_i = 1}_{\text{normalizat}^\circ}$$

Hermicity: $\rho = \rho^\dagger$ $\Rightarrow$ cf lot the axiom of QM

$\Rightarrow$ $\rho$ diagonalizable

$\Rightarrow \exists$ basis s.t. $\rho = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$

only when $\exists ! \, i$ s.t. $\lambda_i = 1$ do we have a pure state.

$\frac{1}{2}$-def $\oplus$: $\rho$ is semi definite positive i.e. $\forall |\psi\rangle$; $\langle\psi|\rho|\psi\rangle \geq 0$

why: show it yourself, look at the basis where $\rho$ is diago.

Square: $1 \geq Tr(\rho^2) > 0$

$\uparrow$ equal iff pure state

why $Tr(\rho^2) = \sum_i p_i^2 > 0$

$\uparrow = 1$ iff $\exists ! \, i$ s.t. $p_i = 1$

$\Rightarrow$ the usual condition to check if pure

## 3) Effect of noise

### a) Decoherence

Therefore noise can have 2 effects

$$|0\rangle \xrightarrow{\text{flawed}} (\alpha+\varepsilon)|0\rangle + (\beta-\varepsilon)|1\rangle$$

a bit off, but coherent

$$|0\rangle \xrightarrow{U} \alpha|0\rangle + \beta|1\rangle$$

ideal

$$|0\rangle \xrightarrow{\text{decoherence}} \rho = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* - \varepsilon \\ \alpha^*\beta - \varepsilon & |\beta|^2 \end{pmatrix}$$

loss of its quantum quality, removal of superposit° & entanglem$^t$

### b) Measurement noise

Simpler version: noise on measurement

$|0\rangle$ — $\boxed{\measuredangle}$ — $1$    Sometimes, because of many reasons we cannot control

$\Rightarrow$ Confusion matrix

$$M = \begin{array}{cc} 0 & 1 \\ \left(\begin{array}{cc} P(0|0) & P(1|0) \\ P(0|1) & P(1|1) \end{array}\right) & \begin{array}{l} = 1 \\ = 1 \end{array} \end{array}$$

$\uparrow$ close to 0    $\uparrow$ close to 1

$\Rightarrow$ this is obtainable by experiment

Ex: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\Rightarrow P(0)_{ideal} = |\alpha|^2 \; ; \; P(1)_{ideal} = |\beta|^2$$

$$P(0)_{obs} = |\alpha|^2 P(0|0) + |\beta|^2 P(0|1)$$

$$P(1)_{obs} = |\alpha|^2 P(1|0) + |\beta|^2 P(1|1)$$

$$= P_{ideal}$$

# 4) Simple error mitigation

One example of mitigation:

$$P_{ideal} = M^{-1} P_{obs}$$ ⇒ we mitigated (not corrected the error)

But:
- not perfect (sampling)
- costly as # qubits ↗
- the source of error change in time, so does $M$, largely unpredictable
- $M$ not always invertible, an even when it is, it is costly to do ( $O(n^3)$ ; $O(n^5 (\log n)^2)$.. )
- there exists compromise

# III Conclusion

## 1) Error at a glance

Measurement fidelity $\sim \dfrac{P(0|0) + P(1|1)}{2} \sim 0,99$

i.e. what is the proba to do what it is supposed to do?

Enough : $0,\underbrace{9\ldots9}_{<7>}$

Best in market : $0,\underbrace{9\ldots9}_{<5>}$ $\rightarrow$ comes at a price.

Av NISQ : $0,\underbrace{99}_{<2>}$

Commonly seen : $0,97$

Random : $0,5$

## 2) Why Grover insufficient

classical : $\mathcal{O}(N)$ vs ideal Grover : $\mathcal{O}(\sqrt{N})$

Grover + error mitigation (ex $\mathcal{O}(n^3)$) + accepting some error

$\Rightarrow$ more complex than classical

$\Rightarrow$ the same for many, if not all algo

That is why "quantum advantage" will come from classical very complex (at least $\mathcal{O}(e^{\mathcal{O}(n)})$) and quantum very simple ($\mathcal{O}(n)$ at most)