Basic algorithms

0. Reminders

1. Oracles & universality

$$U_f |x\rangle \otimes |0\rangle^{\otimes} = |x\rangle |f(x)\rangle$$

oracle if black box that can be queried

if x & $f(x)$ bit string → boolean.

if $U_f' |x\rangle = (-1)^{f(x)} |x\rangle$ → phase oracle.

building any oracle ⇔ building any unitaries
⇔ being universal.

2. Big O notation & complexity

$f(n) \in \mathcal{O}(g(n))$; or $f(n) = \mathcal{O}(g(n))$

$\Leftrightarrow \exists n_0 \in \mathbb{N} ; C \in \mathbb{R}^+$ s.t. $\forall n > n_0 \quad |f(n)| \leqslant C|g(n)|$

i.e. as $n \to +\infty$; $|f(n)|$ monotonically evolve slower than $|g(n)|$

Rq: × this is an "upper bound" than is not strict:

$$1 = \mathcal{O}(n)$$

× small o exists: $f(n) = o(g(n)) \Rightarrow \left|\frac{f(n)}{g(n)}\right| \xrightarrow[n\to+\infty]{} 0$

→ stricter "upper bound"

$$\frac{1}{n^2} = o\left(\frac{1}{n}\right)$$

× « just right » is an equivalent : $f(n) \sim g(n)$

$\Leftrightarrow \frac{f(n)}{g(n)} \xrightarrow[n\to+\infty]{} 1$

⇒ correct asymptote + correct coefficient.

Example : classical sum

		1	3	7	2	4	← n 10-its (input)
+		9	8	6	5	1	← n 10-its (input)
	1	1^1	2^1	3	7	5	← n bits (intermed) ← n+1 10-its (output)

$n_{output} + n_{inter} \leqslant n_{input} = 2n$

⇒ ressource complexity of $2n$ (space) ⇒ $\mathcal{O}(n)$

⇒ time complexity of n (time) ⇒ $\mathcal{O}(n)$

classical addition: $\mathcal{O}(n)$ cx^y (usually refer to time)

Could be gates instead; number of transistors...

Typical cx^y we talk about:

$\mathcal{O}(1)$: i.e. the ressource does not ↗ as cx^y ↗. The best case (then we have to look at the pre-factor)

$\mathcal{O}(\log n)$: « sub-polynomial »

$\mathcal{O}(n)$; $\mathcal{O}(n^2)$ ... : polynomial, the staple of « simple » algorithm

$\mathcal{O}(e^n)$ or $e^{\mathcal{O}(n)}$ or $\mathcal{O}(e^{\mathcal{O}(n)})$: exponential, the staple of « hard » algorithm (P vs NP)

Remember simulating N spin $\frac{1}{2}$:

2^n bits to list out comes (size of matrix) → $\mathcal{O}(2^n)$

but only n qubits → $\mathcal{O}(n)$

$n < 2^n$ ⇒ « quantum advantage [possible?] » (+ substantial gain)

I. Basic algorithms

Effect of Hadamard on bit strings :

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_x |x\rangle$$
all the bit strings

$$H^{\otimes} |s\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_x (-1)^{s.x} |x\rangle$$
a bit string

$$s \cdot x = \sum_j s_j x_j \quad \text{if} \quad s = s_1 s_2 \dots s_n, \quad x = x_1 x_2 \dots x_n$$
e.g. $0 \; 1 \dots 1$

1) Deutsch - Jozsa

Say we have $f(x)$ unknown in details but
- x is bit string $\Rightarrow f(x)$ is bit string
- f is either constant or balance

constant $\Leftrightarrow \forall x \; f(x) = b$ (0 or 1)

balanced $\Leftrightarrow f(x) = \begin{cases} 0 & \text{for half of the possible } x \\ 1 & \text{for the other half} \end{cases}$

Problem: Is f constant or balanced?

Classically: test $2^{\frac{n}{2}}+1$ x at most to conclude
$\Rightarrow \mathcal{O}(e^{\Theta(n)})$ (bad)

Quantum : assuming you have the phase oracle of f.

$$U_f^P H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle$$

* if f cst:

$$\Rightarrow H^{\otimes n} U_f^P H^{\otimes n} |0\rangle^{\otimes n} = \overbrace{(-1)^b}^{\text{irrelevant}} |0\rangle^{\otimes n}$$

$\Rightarrow P(\text{find } 0\dots) = 1$

* if f balanced :

$$\Rightarrow H^{\otimes n} U_f^P H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |\tilde{x}\rangle$$

where $|\tilde{x}\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$

$$P(\text{find } 0\dots) = |\langle 01\dots|^2 = \left|\frac{1}{2^n} \sum_x (-1)^{f(x)}\right|^2 = 0$$
"interference"

$\Rightarrow P(\text{find } 0\dots) = 0$

$\Rightarrow$ In 1 run, you have the answer $\rightarrow \mathcal{O}(1)$ (instead of $\mathcal{O}(2^{\Theta(n)})$)

Of course, we need:
- U_f^P as a black box somehow ($f(x)$ prior)
- n reliable qubits
- if ok w/ proba $\sim \frac{1}{2^k} \Rightarrow$ classically $\mathcal{O}(k)$
  to compare w/ noisy Q.C.

2) Bernstein - Vazirani:

→ seen in practise 2

We have

$f(x) = s \cdot x \mod 2$ s unknown.

Problem: what is s ?

Classicaly: try all $x_i = 0\ldots010\ldots0$
↑ i-th spot

s.t. $f(x_i) = s_i$ ⇒ find s this way

⇒ $\mathcal{O}(n)$ complexity (not bad)

Quantum: assuming $U_f^{\uparrow}$:

$$U_f^{\uparrow} H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle$$

$$= H^{\otimes n} |s\rangle$$

$$\Rightarrow H^{\otimes n} U_f^{\uparrow} H^{\otimes n} |0\rangle^{\otimes n} = |s\rangle$$

$P(\text{measure } s) = 1$ → get it on 1^{st} try

⇒ $\mathcal{O}(1)$ complexity (better than $\mathcal{O}(n)$)

3) Simple quantum communication

* Bell states:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle + |{-}{-}\rangle\right)$$

$$|\phi^-\rangle = \qquad\qquad -$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

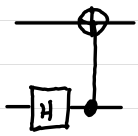
$$|\psi^-\rangle = \qquad\qquad -$$

$$|\phi^-\rangle = Z\otimes I\,|\phi^+\rangle; \quad |\psi^+\rangle = X\otimes I\,|\phi^+\rangle;$$

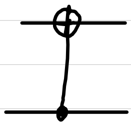
$$|\psi^-\rangle = \underbrace{i}_{\text{irrelevant}}\,Y\otimes I\,|\phi^+\rangle$$

* Communication:

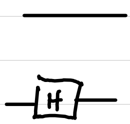
$|00\rangle$		$|\phi^+\rangle$		$|{+}0\rangle$		$|00\rangle$
$|01\rangle$	$\longrightarrow$	$|\psi^+\rangle$	$\longrightarrow$	$|{+}1\rangle$	$\longrightarrow$	$|01\rangle$
$|10\rangle$		$|\phi^-\rangle$		$|{-}0\rangle$		$|10\rangle$
$|11\rangle$		$|\psi^-\rangle$		$|{-}1\rangle$		$|11\rangle$



encryption key (H) + support at Alice's



un-support at Bob's



decryption

4) Superdense coding

Alternative to the above :

1. Charlie send $|\phi^+\rangle$ to Alice & Bob (1 qubit each)
2. Alice apply nothing on her qubit if she wants to send $|00\rangle$

   X — $|01\rangle$

   Y — $|11\rangle$

   Z — $|10\rangle$

   to Bob
3. Alice sends her qubit to Bob
4. Bob din support & decode (CNOT local only)
5. Bob measure and get two classical bit of info

$\Rightarrow$ From 1 entangle qubit paid, get 2 classical bit

5| Teleportation protocal

1. Charlie send $|\phi^+\rangle$ to Alice & Bob
2. Alice wants to send $|\sigma\rangle \alpha|0\rangle + \beta|1\rangle$ to Bob, but either doesn't know what it is (and has a single copy) or doesn't want to say

-. Math says that

$$|\sigma_1\rangle|\phi^+_{23}\rangle = \frac{1}{2}\Big(|\phi^+_{12}\rangle|\sigma_3\rangle + |\phi^-_{12}\rangle X_3|\sigma_3\rangle + |\psi^+_{12}\rangle Z_3|\sigma_3\rangle + |\psi^-_{12}\rangle Y_3|\sigma_3\rangle\Big)$$

n° of qubit

up to a permutation & phase, you check.

3. Alice does 2 correlated measurements on qubit 1 and 2 to project the state on $\{\phi^\pm_{12}, \psi^\pm_{12}\}$
4. Alice tells Bob classically the result of these measurment (2 bits of info).
5. Bob apply nothing, X, Y, or Z to get $|\sigma_3\rangle$

$\Rightarrow$ 2 bit of info + entanglement paid, get 1 qubit of info.

6) Conclusions

- ∃ quantum algorithm that have space &/or time complexity smaller than classical
- Algorithm relies on superposition / interference or entanglement
- Q. communicat° needs direct entanglement pair exchange or entanglement provider. Classical exchange still useful.
- Bright painting darken by tech limitations (reliability + noise)