0. Reminder +

1. Q. C. vocabulary

1 Paradigm of Q. C : circuits made of gate

Gate = unitary operation applyied on 1 to all Qbits

Qbits state : ~~represented by a~~ complex vector of
* dim = $2^{\# \text{qubits}}$
* norm$_2$ = 1 (interpretat° as proba)
* irrelevant global phase (equiv relat°)

→ together form a Hilbert space.

$$\mathcal{H}_{N \text{ qubits}} = \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_1 \cdots = \bigotimes_N \mathcal{H}_1$$

start w/ this.

Other "technological" definition of a qubit for Q.C.
(DiVicenzo ; Loss)

1. scalable φ^{al} syst. w/ well-characterized Qubit
2. ability to initialize the state of the qubits to a simple fiducial state
3. Long relevant Quantum coherence time
4. A "universal" set of quantum gates
5. Qubit-specific measurement capability

For quantum communication

1. Ability to interconvert stationary and flying qubits
2. Ability to faithfully transmit flying qubits between specified locations.

2. Gates

a gate is represented by a unitary complex matrix U ($U(N)$)

- i.e. $UU^{+} = U^{+}U = \mathbb{1}$
- det & vp of module 1; $\Leftrightarrow$ conserve norm$_2$ of vector on which it is applied.
- always diagonalizable;
- interpretable as a matrix of change of basis
- $U_1, U_2 \in U(N) \Rightarrow U_1 U_2 \in U(N)$

  $\Rightarrow$ a circuit is just a carefully prepared change of basis $\Leftrightarrow$ rotation in Hilbert space.
- for $U \in U(N)$, $\exists H$ hermitian ($H^{+} = H$) s.t. $U = e^{iH}$
- applying the change of basis $\{|b_1\rangle\} \to \{|b_2\rangle\}$ w/ $|b_2\rangle = U|b_1\rangle$ on a matrix M is written as: $M' = U M U^{+}$ why? (memo tech :)

$$M'|b_2\rangle = U M \underbrace{U^{+} U}_{\mathbb{1}} |b_1\rangle = U \underbrace{M|b_1\rangle}_{|s_1\rangle}$$

$$= U|s_1\rangle = |s_2\rangle$$ $|s_1\rangle$ in the new basi

- since global phase is irrelevant. often restrictable to $SU(N)$ instead

3. Hermitian matrices

a) Generalities

About Hermitian matrix ($H = H^+$):

- always diagonalizable by unitary change of basis: $H = UDU^+$; $D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$, $\lambda_i \in \mathbb{R}$
- $\forall H$; $e^{iH} \in U(N)$

b) For Qubits only

For qubits ~~space~~ Hilbert space ONLY

1-qubit : $H = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $H = H^+$

$= \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} \Rightarrow$ $a = a^*$, $b = c^*$, $c = b^*$, $d = d^*$

$\Rightarrow$ $H(1) = \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}$; $a, c \in \mathbb{R}$

$b = \alpha - i\beta$, $\alpha, \beta \in \mathbb{R}$

$$= \frac{a+c}{2} \underbrace{\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}}_{I} + \frac{a-c}{2} \underbrace{\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}}_{X} + \alpha \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{Y} + \beta \underbrace{\begin{pmatrix} & -i \\ i & \end{pmatrix}}_{Z}$$

$\Rightarrow$ by construct°: $H(N) = \sum H_1(1) \otimes H_1(1) \otimes H_1(1) \otimes H_1(1) \dots$

$$= \sum_{\{i\}} \alpha_{i_1, i_2, \dots, i_N} P_{i_1} \otimes \dots \otimes P_{i_N}$$

w/ $P_i \in \{1, X, Y, Z\}$

$\Rightarrow$ any U written as $e^{i \sum_{\{i\}} \alpha_{\{i\}} \otimes P_i}$ ← most generic writing

BCH: $\prod_{\{i\}} e^{i \alpha_{\{i\}} P_i}$ in general

But : $\exists \beta_{\{i\}}$ s.t. $\prod_{\{i\}} e^{i \beta_{\{i\}} \otimes P_i} = e^{i \sum_{\{i\}} \alpha_{\{i\}} \otimes P_i}$

$\Rightarrow$ being able to do any of [this] is also been any of the product of [this] means doing any [this] means doing any U

c) Remarks

1. For $e^{i\alpha I + i \sum \alpha_{\{i\}} \otimes P_i}$ (not I) $= e^{i\alpha I} e^{i \sum_i \alpha_i \otimes P_i}$ bc I commutes w/ everything
$\Rightarrow$ we only take traceless H.
$= e^{i\alpha} e^{\dots}$
↑ a global phase → irrelevant
$\Rightarrow$ reason why reducible to $SU(N)$

2. For 1 qbit
$e^{i\theta \vec{n} \cdot \vec{\sigma}} = \cos\theta I + i \sin\theta \, \vec{n} \cdot \vec{\sigma}$
($\vec{n}^2 = 1$)

For n qbit

→ no general Formula

I Universality

1. Classically

n_{input} bits $\to$ 2^{n_i} possible input $x \in$ Input

n_{output} bits $(< n_{input})$ $\to$ 2^{n_o} possible output $y \in$ Out

$$f : x \in \text{Input} \longmapsto y \in \text{Output}$$

What is f ? :

	Input	$\xrightarrow{f}$	Output	
Look up table	x_1		y_1	may be the same.
	x_2		y_2	
	x_3		y_3	
	$\vdots$			

How many f possible? $\underbrace{2^{n_o} \times 2^{n_o} \times \dots \times 2^{n_o}}_{2^{n_i}}$

$$= 2^{n_o 2^{n_i}}$$

$\Rightarrow$ if all f implementable, classically universal

ex : NAND gate

2. Quantum

circuit $\Leftrightarrow$ unitary $\Leftrightarrow$ reversible

- $\Rightarrow$ $n_i = n_o$ (its ok, we can always ignore some)

- every unique input has a unique output (bijectⁿ) i.e. $f(x_1) = f(x_2)$, $x_1 \neq x_2$ not poss

  → not a big deal, just take more qubits ~~than~~ necessary:

$$\begin{tikzcd}
x \arrow[r, "\text{``copy''}"'] \arrow[rrr, bend right, "f"'] & x, x \arrow[r, "\mathrm{id}, f"] \arrow[r, bend right, "\text{``unique'' Q.C.}"'] & x, f(x) \arrow[r, "\text{keep}", "\text{second}"'] & f(x)
\end{tikzcd}$$

Therefore, quantum universality is ability to implement

any $U_f : |x\rangle \otimes |0\rangle^{\otimes n_o} \longmapsto |x\rangle \otimes |f(x)\rangle$

(instead of) $f : x \longrightarrow f(x) = y$

$\Rightarrow$ largely equivalent.

ex: Toffoli $\leftrightarrow$ NAND $\leftrightarrow$ univ.

Simplificatⁿ: implement any $U \in U(N)$ $\Leftrightarrow$ universal

3. Example of base set :

a) Clifford + $R_x(\theta)$

Mention of Clifford gate :

plenty : but «generated» by

- H (Hadamard) (1 qubit)
- S gate $\begin{pmatrix} 1 & \\ & e^{i\frac{\pi}{2}} \end{pmatrix}$ (1 qubit)
- CNOT (2 qubits)

Any product of any of the above is a Clifford

X, Y, Z are Clifford

⇒ cannot do all U still !

↳ e.g. need $R_x(\theta)$

$R_x(\theta) = e^{i\frac{\theta}{2}X}$ + H & S ⇒ any 1 qubit gate

↳ w/ CNOT $e^{i\frac{\theta}{2}X\otimes X}$ + H & S ⇒ any 2 qubit gates

↳ w/ CNOT ...

⇒ able to build any $e^{i\frac{\theta}{2}\otimes P} = U_i$

after applicat° append U_{i+1} ...

⇒ able to buid any $\prod e^{i\frac{\theta_i}{2}\otimes P}$ i.e. any U.

ex: $U = e^{i\left(\frac{\theta}{2}P + \frac{\theta'}{2}P'\right)} \neq e^{i\frac{\theta}{2}P} e^{i\frac{\theta'}{2}P'}$ how ?

then $U \approx \left(e^{i\frac{\theta}{2N}P} e^{i\frac{\theta'}{2N}P'}\right)^N + \delta$ w $N = \text{poly}\left(\frac{1}{\delta}\right)$

(Trotter - Suzuki method not great in general)

b) Clifford + T

or $T = \begin{pmatrix} 1 & \\ & e^{i\frac{\pi}{4}} \end{pmatrix} = \sqrt{S} = \sqrt[4]{Z}$ phase shift $\frac{\pi}{8}$ gate

→ arbitrary approx of any U w/ ∞ precision

c) Toffoli + H

4. Ccl on universality

Being able to build any $U \in U(N)$ (or at least $SU(N)$)

$\Leftrightarrow$ being able to build any state in $\mathcal{H}_N$

$\Leftrightarrow$ " from $|0...0\rangle$

$\Leftrightarrow$ anything that can ever be able to do and hope for by a Q.C (except measur

$\Leftrightarrow$ do any physical evolut^{n} of a (q. mech) physical system

$\Leftrightarrow$ be universal

II What to use a QC for? / Motivation

1a) Simulating quantum system

Spin $\frac{1}{2}$	$\lvert + \rangle$	$\lvert - \rangle$
Photon	$\lvert \circlearrowleft \rangle$	$\lvert \circlearrowright \rangle$
Qubits	$\lvert 0 \rangle$	$\lvert 1 \rangle$

System of n spin $\frac{1}{2}$ $\rightsquigarrow$ 2^n outcome

$\hookrightarrow$ need 2^n bits at least

$\hookrightarrow$ need n qubits at least

$\hookrightarrow$ "advantage"!

These system evolve in time according to Shroedinger's equation $i\partial_t |\psi\rangle = H|\psi\rangle$

H is the Hamiltonian $\rightsquigarrow$ is hermitian

$$|\psi(t)\rangle = e^{iHt} \, |\psi(t=0)\rangle \quad (\text{if } H\cancel{(t)})$$

$$= U \, |\psi(t=0)\rangle$$

$\uparrow$ implementable by a universal Q.C.

2) Notion of oracle (useful in the following week)

$U_A |x\rangle \otimes |0\rangle = |x\rangle \otimes |f(x)\rangle$ input → oracle → output (black box)

a) Boolean : aka classical algo

$$U_f^b \, |x\rangle \otimes |0\rangle^{\otimes n_0} = |x\rangle \otimes |f(x)\rangle$$

x: only 0 & 1 — $f(x)$: only 0 & 1 (if x only 0 & 1)

U_f^b: fixed boolean oracle

s.t.

$$U_f^b \sum_x c_x |x\rangle \otimes |0\rangle^{\otimes n_0} = \sum_x c_x |x\rangle \otimes |f(x)\rangle$$

b) Phase (also only 0 & 1)

$$U_f^p |x\rangle = (-1)^{f(x)} |x\rangle \qquad f(x) \in \{0,1\}$$

U_f^p: fixed phase oracle

c) Why boolean ⇒ phase

$$U_f^b \, |x\rangle \otimes |0\rangle \longrightarrow \begin{cases} |x\rangle \otimes |0\rangle & \text{if } f(x) = 0 \\ |x\rangle \otimes |1\rangle & \text{if } f(x) = 1 \end{cases}$$

therefore

$$U_f^b \, |x\rangle \otimes |-\rangle \longrightarrow \begin{cases} |x\rangle \otimes |-\rangle & \text{if } f(x) = 0 \\ -|x\rangle \otimes |-\rangle & \text{if } f(x) = 1 \end{cases}$$

↓ "forgetting" to write the $|-\rangle$ (not outright) we have

$$U_f^p \, |x\rangle \longrightarrow (-1)^{f(x)} |x\rangle$$

d) Implementing boolean oracle w/ unitaries.

Step 1: in:

$$|x\rangle \otimes |0...\rangle \otimes |0...\rangle \otimes |0...\rangle$$

input register, register 1, register 2, register 3 ...

Step 2: apply to desired unitary

$$U |x\rangle \otimes |0...\rangle \otimes |0...\rangle \otimes |0...\rangle$$
$$= |x\rangle \otimes |f(x)\rangle \otimes |g(x)\rangle \otimes |0...\rangle$$

"answer"

"garbage" qubits entangled w/ answer due to protocol

not touched by construct

Problem: how to get rid of $|g(x)\rangle$?

ideally, we want $\forall x, n \quad |g.(x)\rangle \rightarrow |0...\rangle$ (for example)

$\Rightarrow$ NOT a unitary operat°

$\Rightarrow$ measurements ok, but modify $|f.(x)\rangle$! b.c. entangled $\Rightarrow$ useless

Solution: do a "copy" of the answer

$\rightarrow$ strictly speaking, a copy is only possible if we know perfectly the state we want to copy. I.e. not really a copy, but rather, a second print.

When unknown $\rightarrow$ directly useful copy is impossible but we can do this

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \xrightarrow{CNOT} \alpha|00\rangle + \beta|11\rangle$$

Step 3: apply CNOTs

$$CNOT_s \; |x\rangle \otimes |f.(x)\rangle \otimes |g(x)\rangle \otimes |0...\rangle$$
$$= |x\rangle \otimes |f.(x)\rangle \otimes |g.(x)\rangle \otimes |f.(x)\rangle$$

Step 4: undo the U:

$$U^{+} |x\rangle \otimes |f(x)\rangle \otimes |g(x)\rangle \otimes |f(x)\rangle$$
$$= |x\rangle \otimes |0...0\rangle \otimes |0...0\rangle \otimes |f(x)\rangle$$

$$= U_f^b |x\rangle \otimes [...] \otimes |0...\rangle$$