ASHWIN AHUJA

QUANTUM COMPUTING

Quantum Systems made of
1. Superpositions
2. Interference
3. Entanglement

Why? → ① Better to simulate real life.
↳ ② Better for dealing with the laws of physics

Qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$
↳ measurement results in $|0\rangle$ ~~from~~ with prob $|\alpha|^2$ and $|1\rangle$ with prob $|\beta|^2$
↳ After measurement, system is in the measured state

Hadamard Gate H: ~~H|0~~ $H|+\rangle \to |0\rangle$, $H|-\rangle \to |1\rangle$

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
↳ as soon as one qubit is measured, the second collapses.

Hilbert Space: Finite dimension vector space with a defined inner product. Quantum states form a vector space and transformations described by linear operations

$z \in \mathbb{C}$ of form $a + ib$ for $a, b \in \mathbb{R}$. $\mathbb{C}^n$ is vector space of n-tuples of complex numbers $\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$
↳ work as with vectors for ~~vectors~~ addition and scalar multiplication.
↳ For $\underset{n\times m,\ m\times l}{C = A \times B} \Rightarrow C_{ik} = \sum_{j=1}^{m} A_{ij} B_{jk}$ ($i = 1 \ldots n$, $k = 1 \ldots l$) ⇒ Matrix multiplication is associative, distributive and not commutative

Tensor Product

$$\underset{\substack{n\times m \\ n'\times m'}}{A \otimes B} = \begin{bmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \\ a_{1n}B & \cdots & a_{nm}B \end{bmatrix} = \underset{nn' \times mm'}{C}$$

$\Rightarrow (A \otimes B)(\underline{x} \otimes \underline{y}) = (A\underline{x}) \otimes (B\underline{y})$
↳ also associative

Transpose: $z = a + bi$, $z^* = a - bi$

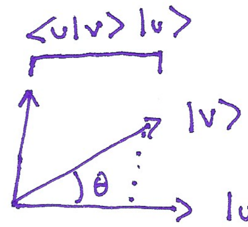
$$A^\dagger = (A^*)^T \qquad (AB)^\dagger = B^\dagger A^\dagger$$

Dirac Notation: → ① Ket is a column vector $|\psi\rangle = \begin{bmatrix} a_1 \\ a_n \end{bmatrix}$
② Bra is conjugate transpose $\langle\psi| = [a_1^* \ \cdots \ a_n^*]$

Inner product:

$|u\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$, $|v\rangle = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$, inner product is: $\langle u|v\rangle = \langle u| \times |v\rangle = \sum_{i=1}^{n} a_i^* b_i$

↳ If $|u\rangle$ and $|v\rangle$ have one non-zero element:
↳ $\langle u|v\rangle = 0 \Rightarrow |u\rangle\ |v\rangle$ are orthogonal
↳ $\langle u|v\rangle = (\langle v|u\rangle)^*$
↳ $\langle u|u\rangle = \sum_{i=1}^{n} |a_i|^2$
↳ $\| |u\rangle \| = \sqrt{\langle u|u\rangle}$
↳ norm of u



Outer Product

If $|u\rangle$ is a unit vector $|u\rangle\langle u|$ is known as a projector that projects an arbitrary vector $|v\rangle$ onto subspace $|u\rangle$

$$(|u\rangle\langle u|)\,|v\rangle = |u\rangle(|u\rangle\langle v|) = (\langle u|v\rangle)|u\rangle$$

② Basis $\mathbb{C}^n$ is minimal collection of vectors: $|v_1\rangle, |v_2\rangle \dots |v_n\rangle$ ($|v_i\rangle \in \mathbb{C}^n$) st every vector $|v\rangle \in \mathbb{C}^n$ can be expressed as linear combination of these vectors.

↳ coefficient $a_i \in \mathbb{C}$

↳ hence $|v_1\rangle, \dots, |v_n\rangle$ (n is dimension) are linearly independent

Orthonormal bases where: $\langle v_i | v_j \rangle = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{else} \end{cases}$

Computational Basis

$|1\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ $|2\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ $|n\rangle = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$

↳ or $|0\rangle$ through $|n-1\rangle$

Any vector can be expressed as a weighted sum of standard basis vectors.

↳ $|v\rangle = a_1|1\rangle + a_2|2\rangle + \dots + a_n|n\rangle$

$$\begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \\ a_{n1} & & a_{nm} \end{bmatrix} = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} |i\rangle\langle j|$$

$A|v\rangle = \lambda|v\rangle$ → eigenvector

L scalar eigenvalue

$\det(A - \lambda I) = 0$

↳ Each square matrix ~~the~~ has at least one eigenvalue

↳ $\det(A)$ = product of eigenvalues

↳ trace (A) = sum of eigenvalues and sum of diagonal element.

A can be represented as: $A = \sum_{i=1}^{n} \lambda_i |v_i\rangle\langle v_i|$

if it is diagonisable.

Matrix is normal if: $A^\dagger A = AA^\dagger$

hermitian if $A = A^\dagger$

unitary if $AA^\dagger = A^\dagger A = I$

↳ all unitary matrices are normal and diagonisable. If U is unitary and $|u'\rangle = U|u\rangle$ and $|v'\rangle = U|v\rangle$

then $\langle u'|v'\rangle = (U|u\rangle)^\dagger (U|v\rangle)$
$= (\langle u|U^\dagger)(U|v\rangle)$
$= \langle u|v\rangle$

Quantum Mechanics Postulates

↳① State Space: associated to any isolated physical system is a complex vector space with an inner product known as the state space of the system. System completely described by state vector (unit vector in system's state space)

↳② Evolution: time evolution of closed quantum system is described by Schrödinger's Equation,

$$H|\psi\rangle = i\hbar \frac{d|\psi\rangle}{dt}$$

Hermitian matrix (Hamiltonian of the closed system)

↳ Planck's Constant

↳ If we discretize time: $|\psi_{t_1}\rangle = U|\psi_{t_0}\rangle$

↳ depends on underlying Hamiltonian

Solution to Schrödinger Equation is: $|\psi_{t_1}\rangle = \exp\left(\frac{1}{\hbar}(iA(t_1 - t_0))\right)|\psi_{t_0}\rangle$

define $U(t_0, t_1) =$ "

↳ this is a $\boxed{\text{unitary}}$ unitary operators are the unique linear map that preserves the norm.

③ Pauli Matrices

$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $X|0\rangle \rightarrow |1\rangle$, $X|1\rangle \rightarrow |0\rangle$

$Y = i\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ $Y|0\rangle \rightarrow i|1\rangle$, $Y|1\rangle \rightarrow -i|0\rangle$

$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $Z|0\rangle \rightarrow |0\rangle$, $Z|1\rangle \rightarrow -|1\rangle$

Hadamard Matrix

$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

$H|0\rangle \rightarrow |+\rangle$ $H|+\rangle \rightarrow |0\rangle$

$H|1\rangle \rightarrow |-\rangle$ $H|-\rangle \rightarrow |1\rangle$

③

↳ ③ <u>Measurement</u>: described by collection of measurement operators $\{M_m\}$

$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$ and state of measurement is:

$$\frac{M_m|\psi\rangle}{\sqrt{(\langle\psi|M_m^\dagger M_m|\psi\rangle)}}$$

↳ Often assume single qubit measurements ~~in~~ the computational basis.

↳ $M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$M_+ = |+\rangle\langle +| = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, $M_- = |-\rangle\langle -| = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$

<u>Global and Relative Phase</u>: $|\psi\rangle = \underbrace{e^{i\theta}}_{\text{global phase}}(\alpha|0\rangle + \beta \underbrace{e^{i\phi}}_{}|1\rangle) = e^{i\theta}|\psi'\rangle$

↳ phase difference between 0 and 1

$U|\psi\rangle = e^{i\theta}U|\psi'\rangle$. For measurement operator P_m,

$\langle\psi|P_m^\dagger P|\psi\rangle = \langle\psi'|e^{-i\theta}P_m^\dagger P e^{i\theta}|\psi'\rangle = \langle\psi'|P_m^\dagger P|\psi'\rangle$

↳ hence typically neglect global phase.

↳ ④ <u>Composition</u>: state space of composite physical system is tensor product of the state spaces of component physical systems.

Joint state of total system = $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$

$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = U_1|\psi_1\rangle \otimes U_2|\psi_2\rangle$ } $|\psi\rangle$ is a seperable state

↳ Single qubit unitary matrices applied to seperable state leads to separable states.

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$|\psi\rangle$ is either: $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$

or: $|\psi_1\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$

~~Can first~~ Given if orthogonal, then can still distinguish which it is using the ~~first~~ transformation first.

$$|\psi\rangle = \begin{bmatrix} \alpha^* & \beta^* \\ \beta & -\alpha \end{bmatrix}|\psi\rangle \qquad \begin{matrix} |\psi_0\rangle \to |0\rangle \\ |\psi_1\rangle \to |1\rangle \end{matrix}$$

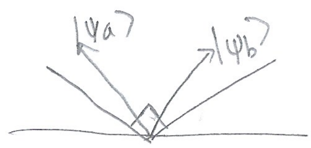
↳ can then perform measurement in computational basis.

↳ equivalent to performing in basis $(|\psi_0\rangle, |\psi_1\rangle)$

<u>Helstrom-Holevo Bound</u> } if ψ_a and ψ_b not orthogonal

If $|\langle\psi_a|\psi_b\rangle| = \cos\theta$, prob of inferring $|\psi\rangle \leq \frac{1}{2}(1 + \sin\theta)$

Can always be achieved by choosing as measurement basis: $|\psi_a\rangle\langle\psi_a| - |\psi_b\rangle\langle\psi_b|$



optimal strategy is to choose basis equally. Can however align basis vectors with state to be distinguished to get measurement we are 100% sure about.

<u>No-Signalling Principle</u>

<u>Setup</u>: Alice and Bell each have one half of bell pair

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

Alice can measure qubit which will collapse Bob's to same state

Trying to find if Bob can infer whether Alice has measured her qubit. Alice measure qubit on some event and signal information to Bob. But all that Bob can do to infer if Alice measured qubit is to measure his own qubit. Are measurement properties altered by Alice performing her measurement.

④ **Proof**: Before Alice measure qubit: $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, so Bob has $\frac{1}{2}$ prob of measuring $|0\rangle$ or $|1\rangle$

↳ After Alice measures, Bob's qubit collapses. (to $|0\rangle$ or $|1\rangle$ with equal prob). Therefore, still measure $|0\rangle$ or $|1\rangle$ with equal probabilities. Therefore no-signalling principle proved.

No-Cloning Principle: Why it matters:
- ① Cannot clone makes quantum error-correction harder
- ② would enable violation of no-cloning principle
- ③ would enable infinite classical information into a single

↳ Setup: Aim to find U qubit and then recovered afterwards

(inner prod) st: $U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$ AND: $U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$

$$\Rightarrow \langle 0|\langle\psi|U^\dagger U|\phi\rangle|0\rangle = (\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle)$$

$$\Rightarrow \langle\psi|\phi\rangle\,\cancel{(\langle 0|0\rangle)} = (\langle\psi|\phi\rangle)^2$$

⇒ Only true if $\psi=\phi$ or orthogonal.

∴ no cloning

↳(1) Map classical bitstring to qubit
↳(2) Communicate qubit
↳(3) Clone infinitely and hence find classical information

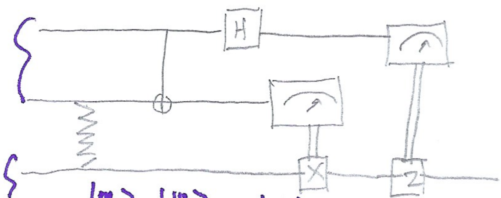
No-Deleting Principle: reverse time of no-cloning yields no-deleting ⇒ no unitary $\tilde{U}$ st can delete one of two copies of quantum state: $\tilde{U}(|\psi\rangle|\psi\rangle) = |\psi\rangle|0\rangle$

Quantum Information Applications

Teleportation: use shared entanglement and two bits of classical information to transfer one qubit.

A

B



$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle+\beta|1\rangle)(|00\rangle+|11\rangle)$$
$$= \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|00\rangle+|11\rangle))$$

$$|\psi_1\rangle = \frac{1}{2}(\alpha|0\rangle(|00\rangle+|11\rangle)+\beta|1\rangle(|10\rangle+|01\rangle))$$

$$|\psi_2\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle))$$

			Qubit 3 before
00	has correction	I	$\alpha|0\rangle+\beta|1\rangle$
01		X	$\alpha|1\rangle+\beta|0\rangle$
10		Z	$\alpha|0\rangle-\beta|1\rangle$
11		ZX	$\alpha|1\rangle-\beta|0\rangle$

after, all are $\alpha|0\rangle+\beta|1\rangle$

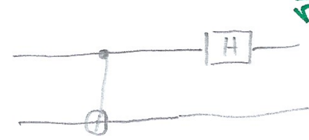
A ~~sends~~ measures two qubits and sends classical information to Bob, who uses correction as above

Super-dense Coding

↳ Alice and Bob share entangled pair.
↳ Alice wants to send two ~~com~~ bits
↳ Apply single qubit unitary to qubit.

Initial State	A's Bitstring	Operation	Final State
$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$	00	I	$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$
"	01	X	$\frac{1}{\sqrt{2}}(|10\rangle+|01\rangle)$
"	10	Z	$\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$
"	11	XZ	$\frac{1}{\sqrt{2}}(|10\rangle-|01\rangle)$

Then apply:



This returns $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Performing measurement means you have bitstring.

Quantum Key Distribution (BB84)

Requires ① authenticated public classical channel and ② Insecure quantum channel

③ Alice has private source of classical bits (random).

④ Alice can produces $|0\rangle, |1\rangle = X|0\rangle, |+\rangle = H|0\rangle, |-\rangle = HX|0\rangle$

⑤ Bob can measure in $(|0\rangle, |1\rangle)$ basis and $(|+\rangle, |-\rangle)$

Process

① For given bitstring, either encode as $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ chosen with equal prob.

② Bob receives qubit and randomly measure in one of the bases.

③ Bob announces over public channel was measured in

④ Alice responds whether this was correct channel

⑤ If same basis, use as part of key, else discard.

⑥ Cannot use intercept, measure, retransmit attack

⑦ Could use intercept, copy, retransmit BUT copy is not possible in quantum world (violates no-cloning)

⑤ Quantum Circuit Model

Can use tensor network to represent operations on single (even entangled) ~~qubits~~ qubits of a state.

$\boxed{S}$ = phase $\oplus$ = CNOT $\boxed{\nearrow}$ → measurement

Quantum circuit is tensor network of n qubits with:
- ① Initialisation $|0\rangle^{\otimes n}$
- ② Quantum gates (unitary operations)
  - ↳ can be represented using a matrix
- ③ Measurements

↳ This meets all required postulates - L5, S8

↳ and does not violate Church-Turing thesis

↳ 2-bit unitaries are universal ⇒ any n-qubit unitary can be decomposed as product of 2-bit unitaries

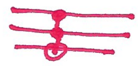
Need for two qubit operations that order is adjacent. Therefore need a swap gate:
$\begin{bmatrix} 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&0&1 \end{bmatrix}$ 

Can approximate (Solovay - Kitaev Theorem) any circuit containing m CNOTs and any single qubit unitaries using finite gate set to accuracy ε in $O(m\log^c(m/\varepsilon))$ where $c\approx 2$ (on classical computer)

Universal Set from H, CNOT and T gate $\to \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$ ~~(TOFFOLI GATE)~~

↳ $S = T^2$, $Z = S^2$, $X = HZH$, $Y = iXZ = SXSZ$

↳ As all gates are unitary, they are reversible

Can use T gate to produce Quantum (reversible) AND gate: 

↳ this is a TOFFOLI GATE

Deutsch-Jozsa Algorithm

(ORACLE is effectively something that recognises a correct answer)

$|x\rangle = |x_1 x_2 \cdots x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$ (function can be constant or balanced)

Aim to find:

Hence implies that $f(x)$ can be efficiently encoded to a specified accuracy. Can show 4 functions for a 1 bit function. Classically requires 2 operations, to tell if function is balanced but can be done with one in quantum system, by passing items in entangled state (hadamard input). Then pass through unitary, then Hadamard again.

Measurement Returns ~~1~~ 0 if constant, 1 if balanced

Quantum Complexity: number of queries to unknown function (oracle / black box)

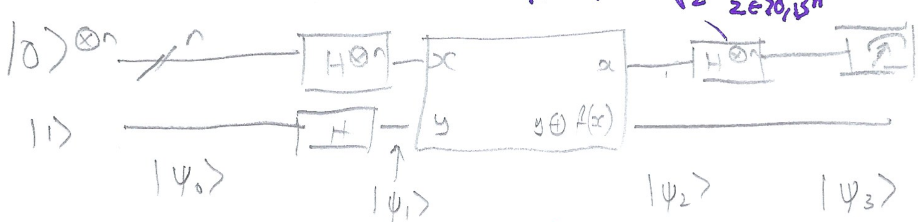
Deutsch-Jozsa extends the above (for 2 qubit input) to any input ~~for~~ size $f: \{0,1\}^n \to \{0,1\}$

↳ Can still be done with a single query rather than classical $2^{n-1}+1$ | ↳ function is either balanced or constant.

$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{xz}|z\rangle$

$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$

$|\psi_1\rangle = \sum_{x\in\{0,1\}^n}\frac{1}{\sqrt{2^{n+1}}}|x\rangle(|0\rangle - |1\rangle)$



$|\psi_2\rangle = \sum_{x\in\{0,1\}^n}\frac{1}{\sqrt{2^{n+1}}}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$ → $|-\rangle$

$|\psi_3\rangle = \left(\sum_{x\in\{0,1\}^n}\sum_{z\in\{0,1\}^n}\frac{1}{2^n}(-1)^{xz+f(x)}|z\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - |1\rangle\right)$

6 Measurement then finds the probability of measuring zero on every qubit
↳ coefficient of when $|z\rangle = |0\rangle^{\otimes n}$

If constant, $\sum_x (-1)^{f(x)}/2^n = \pm 1 \Rightarrow$ get $|0\rangle^{\otimes n}$ with prob 1.

Else: $\sum_x (-1)^{f(x)}/2^n = 0$, never measure $|0\rangle^{\otimes n}$

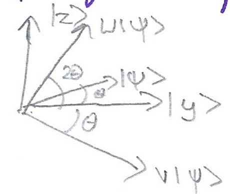
Quantum Search

Grover's Algorithm: consider search oracle V which marks a single element as 1 and all others as 0.
↳ Consider input string x and final qubit $|-\rangle$. Oracle transforms this to $(-1)^{f(x)}|x\rangle|-\rangle$

↳ Apply $H^{\otimes n}$ to search register - hence uniform superposition over all bitstrings of the correct length. Search oracle effectively reflects in the $|y\rangle$ axis. However, need to rotate such that probability of detecting the reflection ~~of 1~~ is increased, reflecting back into positive $|z\rangle$ as well. Hence, reflect about line of original superposition given by

↳ $W = (2|\psi\rangle\langle\psi| - I)$

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



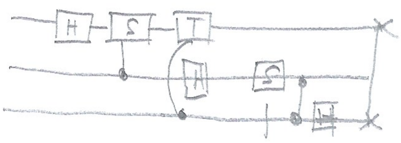
Can implement W using $= -H^{\otimes n} X^{\otimes n} (I_{n-1} \otimes H)\, C_{n-1}X\, (I_{n-1} \otimes H) X^{\otimes n} H^{\otimes n}$

Every iteration (WV) leads to rotation of 2θ → requires $\frac{\pi\sqrt{N}}{4}$ iterations ($O\sqrt{N}$) as opposed to $O(N)$.
↳ can measure correctly with at least prob $(N-1)/N$

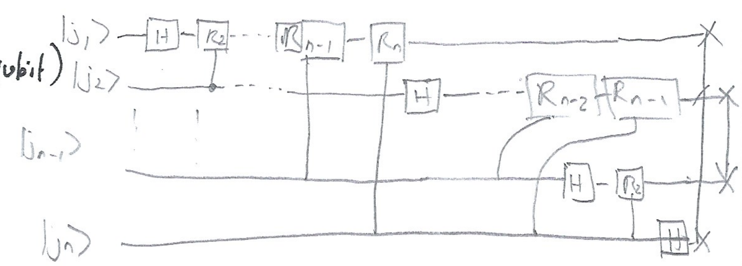
Quantum Fourier Transform

DFT: $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$

QFT Circuit: (3-qubit)



(n-qubit)



This is easily inverted by using inverse of each gate

where R is $\begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$ (single qubit unitary rotation gate)

Hence QFT is (where $N = 2^n$): $\frac{1}{\sqrt{N}}(|0\rangle + e^{\pi i j_n}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{\pi i (j_2 + j_3/2 + \cdots j_n/2^{n-1})}|1\rangle)$

$\otimes (|0\rangle + e^{\pi i (j_1 + j_2/2 + \cdots j_n/2^n)})$

Using binary decimals: $\frac{1}{\sqrt{N}}(|0\rangle + e^{2\pi i (0.j_n)}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i (0.j_2 j_3 \cdots j_n)}|1\rangle)$

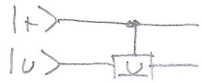
$\otimes (|0\rangle + e^{2\pi i (0.j_1 j_2 \cdots j_n)}|1\rangle)$

$= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} (|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle)$

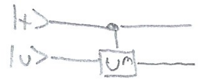
$= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$

⑦ Quantum Phase Estimation

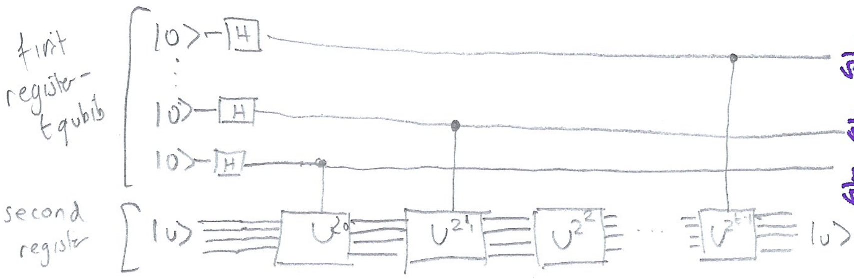
Aim is to estimate phase ϕ of eigenvalue of unitary U to t bits of precision



$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|u\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|u\rangle+|1\rangle e^{2\pi i\phi}|u\rangle)=\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i\phi}|1\rangle)|u\rangle$



$\frac{1}{\sqrt{2}}(|0\rangle+e^{2m\pi i\phi}|1\rangle)|u\rangle$



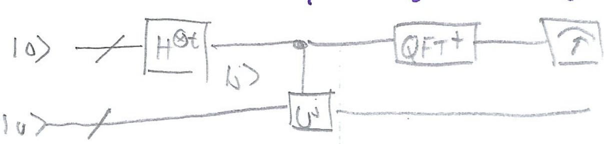
$\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i(2^{t-1}\phi)}|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i(2^1\phi)}|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i(2^0\phi)}|1\rangle)$

$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi i\phi j}|j\rangle|u\rangle$

Now perform inverse QFT on the first register. This gives approximation of eigenvalue phase.



{you have a known U and |u>}

Factoring (in polynomial time)

↳① is N even? If so output 2 and stop

↳② Check if $N = c^l$ for integers $c, l \geq 2$ and compute and return c. Classical algorithm to do this.

↳③ Randomly choose $1 < x < N$ and compute $s = \gcd(x; N)$ using Euclid's division algorithm. If $s \neq 1$, output s and stop

↳④ If $s = 1$, find order r of function $x \bmod N$. If r odd, goto③ pick random number x. If r even, efficient post-processing to extract a factor of N to output.
↳ Least positive integer r st $x^r \equiv 1 \bmod N$ ⇒ can be done efficiently using QPE

QPE using $U|y\rangle = |(xy) \bmod N\rangle$ where y is an integer st $0 \leq y < N$
↳ unitary since it is a permutation matrix (when x and N are co-prime)

$U^{2^j}|y\rangle = |((x^{2^j} \bmod N)y) \bmod N\rangle$
precompute these values
$(O(n^2 t))$ $t \in O(n)$
$\therefore O(n^3)$

Eigenstates are: $|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi i sk/r}|x^k \bmod N\rangle$

phase is s/r. Hence, QPE returns estimate of s/r for unknown s. However, classical algorithm (continued fractions algorithm) that can get r from s/r with high probability but not 1 = P(A)

Equal superposition of all eigenstates is $|1\rangle$ (L10, S13)

Four possibilities for even r:

↳ $x^{r/2} \equiv 1 \bmod N$ → cannot occur

↳ $x^{r/2} \equiv -1 \bmod N$ → algorithm fails] P(B) $P(A)+P(B) < \frac{1}{2}$

↳ $(x^{r/2}-1)(x^{r/2}+1) = N$: $(x^{r/2}-1)$ and $(x^{r/2}+1)$ are factors $< \varepsilon$ for some ε

↳ " $= kN$ $\therefore \gcd((x^{r/2}+1); N)$ or $\gcd((x^{r/2}-1); N)$ is a non-trivial factor → can run Euclid's algorithm therefore succeeds with $O(1)$

Classical Algorithm = exp $(\Theta(n^{1/3}\log^{2/3} n))$

Quantum: $O(n^3)$

Therefore exponential speedup

8

Quantum Chemistry

Quantum Systems = Superposition → Use entanglement to search solution space → interfere to extract the final entangled solution

↳ entangled spaces larger than unentangled counterparts. n-qubit product states longer than classical n-bit binary number and all n-qubit states

Quantum Simulation: To simulate system, need to solve Schrödinger's Equation - exponentiation and first approx is not enough.

Decompose quantum system: $H = \sum_{k=1}^{K} H_k$ ∴ Schrodinger $|\varphi_t\rangle = e^{-i\sum_k H_k t}|\varphi_0\rangle$

Use Trotters formula $\lim_{n\to\infty}\left(e^{iH_1t/n}e^{iH_2t/n}\right)^n = e^{i(H_1+H_2)t}$

∴ algorithm is: ① $|\tilde{\varphi}_0\rangle = |\varphi_0\rangle$

② $|\tilde{\varphi}_{j+1}\rangle \leftarrow U_{\Delta t}|\tilde{\varphi}_j\rangle$ $U_{\Delta t} = e^{iH_1\Delta t}e^{iH_2\Delta t}\dots e^{iH_k\Delta t}$

③ $j{+}{+}$; if $j\Delta t < t$ goto 2

④ Output $|\tilde{\varphi}_j\rangle$

QPE for ground state energy estimation

① Initialise second register in state $|\varphi\rangle = \sum_i a_i |u_i\rangle$

② Perform QPE to evolve U.

③ Final state is $\sum_i a_i |bin(\phi_i)\rangle|u_i\rangle$

↳ binary estimate of the ith eigenvalue.

Quantum Chemistry setup

① System Hamiltonian encoded as qubit Hq

② Find min eigenvalue phase of unitary $U = e^{-iHt}$

③ $|\varphi\rangle = \sum_i a_i|u_i\rangle$ - superposition of eigenvectors of U. these form an orthogonal basis

$|a_0|^2$ prob of collapsing into desired state $|u_0\rangle$. Therefore need to prepare initial state so dominated by $|u_0\rangle$

can be done using Adiabatic State Preparation

QPE requires a fault tolerant Quantum Computer, hence lots of research on hybrid quantum-classical algorithms (since quantum simulation is intractable on classical machines) ⇒ simulate shallow-depth quantum circuits - no unmanageable error. example is the Variational Quantum Eigensolver ⇒ relies on Rayleigh Ritz principle: $\langle \underbrace{\varphi(\theta)}_{\text{quantum state parameterised by }\theta} | H | \varphi(\theta)\rangle \geq \underline{E_0}$

↳ lowest energy eigenvalue.

↳ Hence can find ground-state energy by minimising $\langle\varphi(\theta)|H|\varphi(\theta)\rangle$

Iterates the following: ① Run shallow-depth quantum circuit $U(\theta): |0\rangle \to |\varphi(\theta)\rangle$

② Measure to get $E(\theta)$

③ Perform classical optimisation to update θ

Quantum Complexity

Church-Turing Thesis: Function on natural numbers can be calculated by an effective method iff computable by a Turing machine. ~~Strong~~ Strong Church-Turing thesis says that any algorithmic process can be simulated efficiently Turing machine.

↳ polynomial time overhead

Finite Automata has:

↳① n_s states

↳② alphabet of size n_a

↳③ state transitions: $n_s \times n_s$ matrix for each n_a letter

↳④ start state

↳⑤ Accept state

deterministic finite automata: for each state-letter pair, only one outgoing arrow - only ~~one column~~ one 1 in each column.

nondeterministic finite automata: number of outgoing arrows from each state-letter pair.

⑨ **Probabilistic Automata**: transition matrices contain fractional values st each column sums to one.
↳ Hence, accepted language is set of strings that end up in final state with probability above some threshold.

Quantum Automata: transition matrices are unitary matrices consisting of complex matrices.
↳ binary permutation matrices is where only one 1 in each column and row.

P = class of problems decidable on Turing machine in polynomial time.

Turing Machine: DFA with infinitely long read-write tape. Head over one space on tape. Transition function defines given current state and symbol: → ① Symbol to overwrite on current space on tape
② whether to move head left or right
③ which next state the DFA moves to.
↳ machine halts if in accept state

Nondeterministic Turing Machines: Allow multiple actions, hence branching in possibilities. If height of tree bounded by polynomial, this is NP.

↳ **Probabilistic Turing Machine**: each edge is given a probability. BPP is set of languages L for which $\exists$ probabilistic Turing Machine M running in polynomial time with:

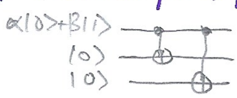
$$P(M \text{ accepts } w) = \begin{cases} > \frac{2}{3} & \text{if } w \in L \\ < \frac{1}{3} & \text{if } w \notin L \end{cases}$$

{conjectured that $P = BPP$}

↳ **Quantum Turing Machine**: complex amplitudes for probabilities. BQP is equivalent to BPP for Quantum Turing Machine. $BPP \subseteq BQP$ (but $BPP \neq BQP$?), $NP \nsubseteq BQP$, $BQP \nsubseteq NP$

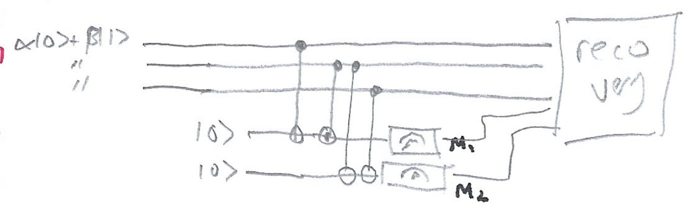
Quantum Error Correction: important for satisfactory performance

Classical Error Correction → ① Majority Voting: $p_e' = 3p_e^2(1-p_e) + p_e^3$ (less than p_e if $p_e < 0.5$)
↳ suppresses error to $O(p_e^2)$



Quantum Error Correction Challenges!
① No Cloning
② Measurement destroys info
③ Quantum errors continuous

3-qubit bit-flip code (Quantum Maj Voting): → ① $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$

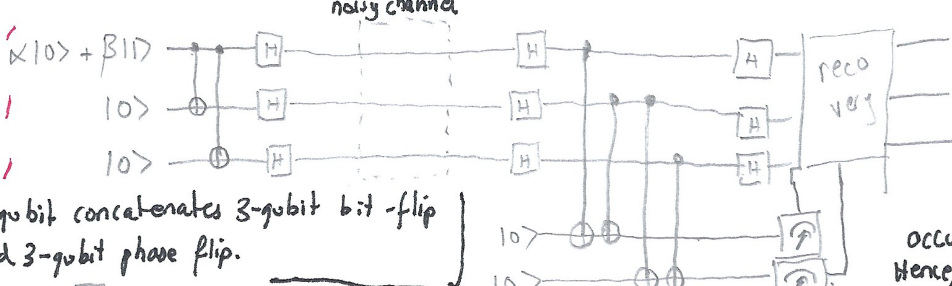


Bit flip	M_1	M_2	Recovery
–	0	0	$I \otimes I \otimes I$
1	0	1	$I \otimes I \otimes X$
2	1	1	$I \otimes X \otimes I$
3	1	0	$X \otimes I \otimes I$

Since just comparative measurement, does not collapse wave function

USES ENTANGLEMENT NOT CLONING

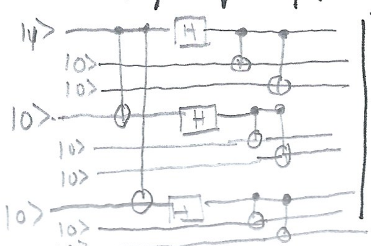
3-qubit phase-flip code



We effectively digitize continuous errors in a quantum system.

performing parity checks for phase flip and bit flip collapses general state into either occurred or not depending on measurement. Hence, correct continuum of errors from just phase flip and bit flip

Shor Code: 9-qubit concatenates 3-qubit bit-flip and 3-qubit phase flip.



$$|0\rangle \rightarrow |0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \rightarrow |1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

Hence, can correct bit and phase flips.

See L13, S16 for connection

(10)

Depolarising Channel

$P_e/3$ bit flip, $p_e/3$ phase flip, $p_e/3$ both. Shor's code suppresses error from p_e to $O(cp_e^2)$ in the depolarising channel. This only works on single errors, but this is often good enough for low noise settings.

Hamming Code: $c = Gd \bmod 2$ where $G = \begin{bmatrix} 1&1&0&1 \\ 1&0&1&1 \\ 1&0&0&0 \\ 0&1&1&1 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix}$, parity check $p = Hc \bmod 2$ $\Rightarrow$ all 0's if valid, else $\rightarrow$ others each indicate single bit error.

$$H = \begin{bmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \end{bmatrix}$$

Calderbank-Steane-Shor Codes (CSS Codes): use classical linear codes to find quantum code.

$\hookrightarrow$ Steane Code constructed from Hamming code:

$$|0_L\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle)$$

$$|1_L\rangle = \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)$$

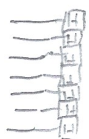
Fault Tolerant Quantum Computing

Setup $\rightarrow$ ① Encoded qubits - using Steane Code to represent each logical qubit

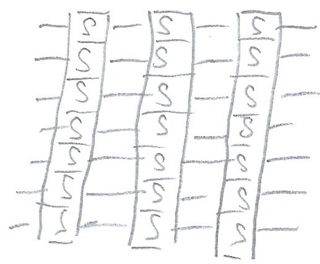
② Use Fault Tolerant Quantum Gates - single error in gate propagates to at most one error in encoded block of qubits

③ Error correction before + after every gate + at random intervals.

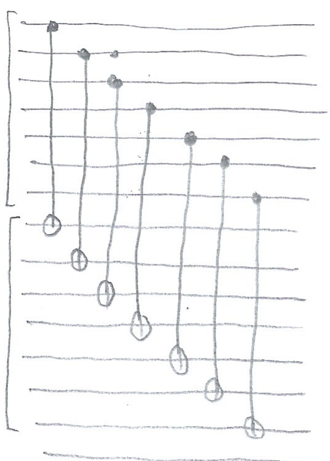
Fault Tolerant Hadamard:



Fault Tolerant S gate



Fault Tolerant CNOT



For full fault tolerant systems, need:

① Fault tolerant state preparation

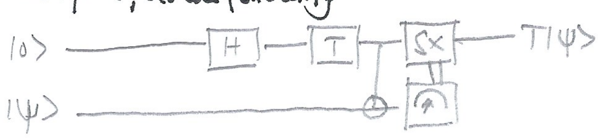
② Fault tolerant gates

③ Fault tolerant error correction

④ Fault tolerant measurement.

But T gate cannot be performed transversally, therefore no universal gate set. But H, S, CNOT generate Clifford Group - can be efficiently simulated on classical machine (Gottesman-Knill Theorem)

Instead for T, do the following:



⑤ Existence of quantum error correcting codes

⑥ Ability to concatenate error correcting codes $\Rightarrow$ concatenate Steane code by encoding single logical qubit with seven qubits which are then encoded using Steane code, etc for some layers k. $\Rightarrow$ Error is $\frac{(cp_e)^{2^k}}{c}$

prob of computation failure $= P_f \leq p(n)\, p'_e$ (gates) $= p(n)\frac{(cp_e)^{2^k}}{c}$ $\therefore$ choose k s.t. $\frac{(cp_e)^{2^k}}{c} \leq \frac{\varepsilon}{p(n)}$ (desired maximum error) $\Leftarrow$ exists iff $p_e < \boxed{p_{th}} = \frac{1}{c}$ (code threshold)

(11)

Extra computation

k level concatenation means d^k ~~operations~~ $p(n)$ operations

$$d^k = \left(\frac{\log(p(n)/(c\varepsilon))}{\log(1/(p_e c))}\right)^{\log_2 d} \in O(\mathrm{poly}(\log(p(n)/\varepsilon))$$

Hence, a quantum circuit containing $p(n)$ gates may be simulated with max prob of error ε in $O(\mathrm{poly}(\log p(n)/\varepsilon)p(n))$ quantum gates whose gates fail with prob $\leq p_e$ (as long as $p_e < p_{th}$)

Since physical qubits used to encode logical qubits may be far from each other, so need to have lots of SWAP gates (on physical qubits) $\Rightarrow$ not fault tolerant) - instead surface codes where qubits laid out on rectangular grid where every other qubit is a parity check ancilla. Therefore can be fault tolerant (L14, S19)

Quantum Adiabatic Theorem: if we have a time varying Hamiltonian ($H(t)$) - initially at H_I at $t=0$ and H_F at $t=t_f$, then if system is initially in ground state of H_I and if time evolution is sufficiently slow, system will remain in ground state at $t=t_f$ $\rightarrow$ where $s(t)$ is the adiabatic evolution path

$$H(t) = s(t)H_I + (1-s(t))H_F$$

Adiabatic quantum computing is polynomially equivalent (in terms of computational complexity) to gate based quantum computing.

Adiabatic State Preparation in Quantum Chemistry

Necessary to prepare state of second register in ground-state of system of interest for QPE and the Variational Eigensolver Algorithm. Use adiabatic state evolution, approximated by discretized evolution on gate based ~~evolution~~ quantum compute, from ground state of easy to prepare Hamiltonian to the ground state of Hamiltonian of interest.

Optimisations
- $\rightarrow$ algebraically solvable optimization
- $\rightarrow$ Find global maximum and minimum
- $\hookrightarrow$ Find local maxima and minima

metaheuristics are used to find good approximate solution - search policy to explore optimisation function, evaluating at different x values.
- $\hookrightarrow$ all based around idea that good solutions are near other good solutions
- $\hookrightarrow$ Heuristic is an exploration vs optimisation tradeoff
- $\hookrightarrow$ generally, explore at the start and exploitation later

Simulated Annealing

Choose initial x:
- $\hookrightarrow$ ① Evaluate $f(x)$
- $\hookrightarrow$ ② At random, choose neighbour x' of x — need defined notion of neighbourhood
- $\hookrightarrow$ ③ Evaluate $f(x')$
- $\hookrightarrow$ ④ If $f(x') < f(x)$ $x \leftarrow x'$
  else randomly decide to leave x as is or to set $x \leftarrow x'$ $\Rightarrow$ choose this based on attempting exploitation initially and exploitation later:
  $$p(\text{Accept}) = \exp\left(-\frac{f(x')-f(x)}{T}\right)$$
  T is temperature which is reduced as the algorithm progresses.
- $\hookrightarrow$ ⑤ Repeat a specified number of times.

Quantum Annealing

Setup: ① Final Hamiltonian H_F, whose ground-state encodes the solution of optimisation problem

② Transverse Hamiltonian H_D that does not commute with H_F

③ ~~Start~~ Evolve system using:

$$H(t) = H_F + \Gamma(t)H_D$$

($\Gamma(t)$ is the transverse field coefficient)

- It has Quantum Tunnelling, therefore height not width of peak limits ability to escape.
  - $\hookrightarrow$ High narrow peaks are no issue

Arbitrary initial state choice is part of metaheuristic.

(12) **D-Wave** (2048 qubit quantum annealer)

D-Wave uses quantum annealing to solve single optimization problem - Ising Model, minimization of f by adjusting x.
↳ natural problem

$$f(x) = \sum_i h_i x_i + \sum_{i<j} J_{ij} x_i x_j$$

fixed adjustable parameters

To solve arbitrary optimization problem
↳ ① Map optimization problem of interest to optimization of some instance of Ising model
↳ ② Map instance of Ising model to ~~optim~~ instance that runs natively on D-Wave

But: ① Not universal quantum computer
② D-Wave focussed on high numbers of qubits, but poor coherence
③ Highly expensive

Particularly useful for machine learning tasks such as running classifier training algorithms directly on D-Wave

Case Studies

Noisy Intermediate-Scale Quantum: much focus is on finding advantageous applications of quantum computing using NISQs eg VQE and Quantum Annealing
↳ Quantum Algorithm Zoo lists a large number (60) of quantum algorithms
L HHL: for solving sparse system of linear equations
L QAOA: Quantum Approximate Optimization Algorithm

Example is construction of recommendation systems - n products and m uses. Originally $O(poly(mn))$. Then quantum algorithms (2016) → $O(poly(\log(mn)))$ ⇒ then classical, in 2018 $O(poly(\log(mn)))$

due to existence of lots of good quantum chemistry algorithms lots of people think we might be going into quantum winter

Quantum Machine Learning → ① Quantum Machine Learning on Classical Data.
↳ Use Quantum ~~machine~~ ~~learn~~ algorithms to enhance classical machine learning. Eg. Annealing, Grover search, etc.

Data comes from either
① output of quantum process - eg quantum sensor
② Processed from classical data
③ QRAM: method of efficiently addressing an arbitrary superposition of classical data bits

↳ ② Classical Machine Learning on Quantum Data
↳ Classical algorithms on quantum data, eg Quantum Topography. (data collapsed into classical data)

↳ ③ Quantum Machine Learning on Quantum Data ⇒ can gain extra information by using quantum techniques.

(classical data → Quantum)
Nd-dimensional vector → $\log(Nd)$ qubits in $O(\log Nd)$

Quantum Software is made of: ① Quantum Algorithms, ② Quantum Compiler design, ③ Software Development Challenge → use classical and quantum components ~~ex~~ effectively - then hand control back to classical computer.

Full-Scale Era - adds fault tolerance. This requires an error overhead of between 100 and 1000. Therefore, 100-1000 physical qubits per logical qubit
↳ this requires a massive scaling up of number of qubits ↗ might consider a design of a quantum transistor - scalable realisation of qubit.

Types of Qubits

① Superconducting qubits - fast gate times - Oxford Quantum Circuits, Google (53 qubits), IBM (53 qubits), Intel (49 qubits), Rigetti (32 qubits)
② Trapped-ion qubits - highest fidelity, can also be networked - hence greater non-planar connectivity than superconducting quantum computers (rectangular grid)
↳ more scalable
University of Sussex and NQIT
③ Silicon Qubits
④ Nitrogen Vacancy Qubits
⑤ optical qubits
⑦ Topological Qubits - intrinsically error resistant (Microsoft)

* Some researches claim that random algorithms are not a good choice. instead quantum software design ...

Measuring Effectiveness of Quantum Computer
① Number of qubits
② Quality / fidelity of qubits
③ Connectivity of qubits

Quantum Volume

$$Q_V = (\min(n, d))^2$$

n: number of qubits
d: depth of random* circuit before expected error

min reflects finding the limiting factor

this has been shown to provide a good benchmark: function of fidelity and depth overhead (connectivity)