Quantum Information and Computation.

$$\text{(A)} \longleftrightarrow \mathcal{H}_A \ (\mathcal{H})$$

Hilbert-space (H.S.) equipped with an inner product.

Dirac Bra-ket notation

$\mathcal{H} \cong \mathbb{C}^n$

$$|a\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \quad a_i, b_i \in \mathbb{C}.$$

$|a\rangle$, $|b\rangle$: kets.

Inner product

let $|u\rangle = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, $|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$.

$$(u, v) \equiv \langle u|v\rangle = \sum_{i=1}^{n} u_i^* v_i.$$

Dirac split the inner product

$$\langle u|v\rangle \rightarrow \langle u| \cdot |v\rangle.$$

bra

$$\langle u| = (u_1^*, \ldots, u_n^*) \Rightarrow \langle u|v\rangle = (u_1^*, \ldots, u_n^*) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Bras are vectors in $\mathcal{H}^*$ ≡ dual to $\mathcal{H}$. In $\mathcal{H}^*$: $\mathcal{H} \rightarrow \mathbb{C}$. elts are linear functionals. $\langle u| \cdot |v\rangle \mapsto \langle u|v\rangle \in \mathbb{C}$.

Prop. of inner products

- Positivity: $\langle v|v\rangle \geq 0$, "$= 0$" iff $|v\rangle = 0$.
- linearity (in 2nd arg): $|v\rangle = c_1|a\rangle + c_2|b\rangle$, $c_1, c_2 \in \mathbb{C}$, then

$$\langle u|v\rangle = c_1\langle u|a\rangle + c_2\langle u|b\rangle.$$

- Antilinear (in 1st arg) $\langle u| = r_1 |u_1\rangle + r_2 |u_2\rangle$,

$$\langle u|v\rangle = r_1^* \langle u_1|v\rangle + r_2^* \langle u_2|v\rangle .$$

- Skew-sym: $\langle u|v\rangle = \langle v|u\rangle^*$.

$|v\rangle \in \mathcal{H}$, $\langle v| \in \mathcal{H}^*$

$$|v\rangle \xleftrightarrow{\text{1-1 map}} \langle v|$$

- $\langle v| = (|v\rangle)^\dagger$. $|v\rangle = (\langle v|)^\dagger$.
- $(c_1|v_1\rangle + c_2|v_2\rangle)^\dagger = c_1^* \langle v_1| + c_2^* \langle v_2|$
- $((|v\rangle)^\dagger)^\dagger = |v\rangle$.

- Mutually orthogonal vecs $(|u\rangle \perp |v\rangle)$.

  $|u\rangle, |v\rangle \in \mathcal{H}$ are orthogonal if $\langle u|v\rangle = 0$.
- The norm of a vector $|v\rangle$

$$\|v\| = \sqrt{\langle v|v\rangle} .$$

<u>A basis in $\mathcal{H}$</u> $(\mathcal{H} \cong \mathbb{C}^n, \ n = \dim \mathcal{H})$

A maximal set of pairwise orth vecs of unit length $\{|e_i\rangle\}_{i=1}^n$ s.t.

$$\langle e_i|e_j\rangle = \delta_{ij} .$$

Any $|v\rangle \in \mathcal{H}$, $|v\rangle = \sum v_i |e_i\rangle$, $v_j = \langle e_j|v\rangle \in \mathbb{C}$.

$\{\langle e_i|\}_{i=1}^n$ is orthonormal basis (onb) of $\mathcal{H}^*$.

$$\langle v| = \sum v_i^* \langle e_i| \quad . \ v_j^* = \langle v|e_j\rangle$$

<u>Computational basis</u> $(\mathcal{H} \cong \mathbb{C}^n)$

$\{|i\rangle\}_{i=0}^{n-1}$ (sometimes $\{|i\rangle\}_{i=1}^n$).

Example $n=2$, $\mathcal{H} \cong \mathbb{C}^2$, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

$\langle 0|0\rangle = 1 = \langle 1|1\rangle$. $\langle 0|1\rangle = 0 = \langle 1|0\rangle$.

Postulates of QM

Postulate I: Any isolated quantum system. which can be prepared in n perfectly distinguishable states, one can associate a H.S. of dimension n s.t. state of the system is given by $|\psi\rangle \in \mathcal{H}$ is of unit length $\langle\psi|\psi\rangle = 1$ (normalised)

$\left(|\psi\rangle \to \text{ray} \{ e^{i\theta} |\psi\rangle \ \forall \theta \in \mathbb{R} \} \right)$.

$\textcircled{A} \leftrightarrow \mathcal{H}$, $\mathcal{H} \cong \mathbb{C}^n$.

State of the quantum sys. given by $|\psi\rangle \in \mathcal{H}$. s.t. $\| \psi \| = 1$, $e^{i\theta}$ global phase is physically irrelavant.

- $\mathcal{H} \cong \mathbb{C}^2$, comp. basis $\{|0\rangle, |1\rangle\}$.

Superposition principle: $\forall |\psi\rangle \in \mathcal{H}$, $|\psi\rangle = a|0\rangle + b|1\rangle$, $a, b \in \mathbb{C}$.

Fundamental unit of q. info: qubit

Any q sys. s.t. $\mathcal{H} \cong \mathbb{C}^2$.

Bit $\begin{cases} 0 \\ 1 \end{cases}$ Qubit $\begin{cases} |0\rangle \\ |1\rangle \end{cases}$.

Physically a qubit:

- electronic spin $|\uparrow\rangle$, $|\downarrow\rangle$
- photon polarisation

In QM, only mutually $\perp$ states are perfectly distinguishable.

In $\mathcal{H} \cong \mathbb{C}^2$.

- Comp. basis $\{|0\rangle, |1\rangle\}$
- Conjugate basis $\{|+\rangle, |-\rangle\}$, $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$.

Note $\mathcal{H} \cong \mathbb{C}^n$, onb $\{|e_i\rangle\}_{i=1}^n$. State $|\psi\rangle \in \mathcal{H}$, $\langle\psi|\psi\rangle = 1$.

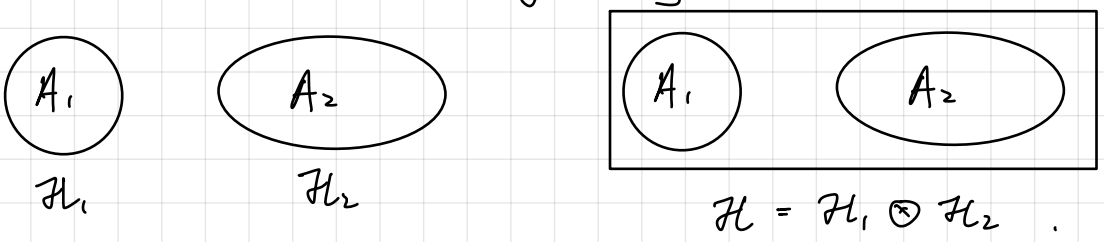
$$|\psi\rangle = \sum_i c_i |e_i\rangle$$

$$1 = \langle\psi|\psi\rangle = \sum_i |c_i|^2$$

$\{|c_i|^2\}$ form a prob. dist.

$c_i = \langle e_i|\psi\rangle$ is the prob. amplitude

Postulate II: States of $A_1 A_2$ given by unit vectors in $\mathcal{H}_1 \otimes \mathcal{H}_2$.



If $\mathcal{H}_1$ onb $\{|a_i\rangle\}_{i=1}^{d_1}$, $\mathcal{H}_2$ onb $\{|b_i\rangle\}_{i=1}^{d_2}$, $d_1 = \dim \mathcal{H}_1$, $d_2 = \dim \mathcal{H}_2$. then $\{|a_i\rangle \otimes |b_j\rangle\}_{\substack{i=1\dots d_1 \\ j=1\dots d_2}}$ onb. of $\mathcal{H}_1 \otimes \mathcal{H}_2$

$\Rightarrow \dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = d_1 d_2$.

Example 2-qubit system $\mathcal{H}_1, \mathcal{H}_2 \cong \mathbb{C}^2$. $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = (\mathbb{C}^2)^{\otimes 2}$

$\{|0\rangle, |1\rangle\}$ onb of $\mathbb{C}^2$, so onb of $\mathcal{H}$:

$$\{|0\rangle\otimes|0\rangle,\ |1\rangle\otimes|0\rangle,\ |0\rangle\otimes|1\rangle,\ |1\rangle\otimes|1\rangle.\}.$$

For $|a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$, $|b\rangle = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$

$$|ab\rangle = |a\rangle|b\rangle = |a\rangle \otimes |b\rangle = \begin{pmatrix} a_1|b\rangle \\ a_2|b\rangle \end{pmatrix}$$

So onb of $(\mathbb{C}^2)^{\otimes 2}$: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Dirac notations for linear operator.

- Linear map $A: \mathcal{H} \longrightarrow \mathcal{H}$. For $|u\rangle = c_1|u_1\rangle + c_2|u_2\rangle$,

$$A|u\rangle = c_1 A|u_1\rangle + c_2 A|u_2\rangle.$$

- Linear operators are endomorphism $A: \mathcal{H} \to \mathcal{H}$.
- Adjoint of A is

$$\langle v|A^\dagger|u\rangle = \langle u|A|v\rangle^* \quad \forall\, |u\rangle, |v\rangle \in \mathcal{H}.$$

- Let $\mathcal{L}(\mathcal{H})$ = set of lin. ops. on $\mathcal{H}$. If $A, B \in \mathcal{L}(\mathcal{H})$, then $|u\rangle \in \mathcal{H}$, $AB|u\rangle = A(B|u\rangle)$.

  $AB|u\rangle = BA|u\rangle$ unless $AB = BA$, ie. $[A,B] = 0$.
- I = identity on $\mathcal{H}$, $I|u\rangle = |u\rangle \quad \forall\, |u\rangle \in \mathcal{H}$.
- A^{-1} : inverse of A. $A^{-1}A = I = AA^{-1}$
- $(AB)^\dagger = B^\dagger A^\dagger$.
- $(\alpha A + \beta B)^\dagger = \alpha^* A^\dagger + \beta^* B^\dagger$.
- $(A^\dagger)^\dagger = A$.

An operator A is

- <u>normal</u> if $AA^\dagger = A^\dagger A$.
- <u>unitary</u> if $AA^\dagger = A^\dagger A = I$
- Hermitian if $A = A^\dagger$.

<u>Outer products</u> $|a\rangle\langle b| \equiv |a \times b|$

If $\mathcal{H} \cong \mathbb{C}^n$, then $|a \times b| \in M_n(\mathbb{C})$, where $M_n(\mathbb{C})$ set of $n \times n$ complex matrix.

$|a\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ $|b\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$, then $|a \times b| = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} (b_1^* \dots b_n^*) \in M_n(\mathbb{C})$.

Outer product is a lin op. (on $\mathcal{H}$ or $\mathcal{H}^*$).

(i) $|u\rangle\langle v|$ on $|x\rangle \in \mathcal{H}$, then

$$|u\rangle\langle v|\,|x\rangle = |u\rangle\langle v|x\rangle = \langle v|x\rangle\,|u\rangle \in \mathcal{H}.$$

(ii) $|u\rangle\langle v|$ on $\langle y| \in \mathcal{H}^*$

$$\langle y|\,|u\rangle\langle v| = \langle y|u\rangle\langle v| \in \mathcal{H}^*.$$

Products of outer products

$A = |a\rangle\langle b|, \quad B = |c\rangle\langle d|$

- $BA = |c\rangle\langle d|\,|a\rangle\langle b| = |c\rangle\langle d|a\rangle\langle b|$

$$= \langle d|a\rangle\,|c\rangle\langle b| \in M_n(\mathbb{C}).$$

Claim Any $A \in \mathcal{L}(\mathcal{H})$ can be presented as a matrix in $M_n(\mathbb{C})$. (i.e. lin. op. ≡ matrix).

Pf: let $\{|e_i\rangle\}_{i=1}^n$ onb. of $\mathcal{H}$. Let $\forall i = 1, \dots, n$.

$$A|e_i\rangle = |f_i\rangle \in \mathcal{H}.$$

Then $A = \sum_{j=1}^n |f_j\rangle\langle e_j|$, since

$$A|e_i\rangle = \sum_{j=1}^n |f_j\rangle\underbrace{\langle e_i|e_j\rangle}_{\delta_{ij}} = |f_i\rangle$$

□

If $\{|f_i\rangle\}_{i=1}^n$ also onb. of $\mathcal{H}$, then A unitary (preserve inner product).

$$A|e_i\rangle = |f_i\rangle \;;\; A|e_j\rangle = |f_j\rangle$$

$$\delta_{ij} = \langle e_i|e_j\rangle = \langle e_i|A^+A|e_j\rangle \Leftrightarrow A^+A = I.$$

- $|f_i\rangle = |e_i\rangle \Rightarrow \boxed{I = \sum_i |e_i\rangle\langle e_i|}.$

For onb $\{|e_i\rangle\}$

- $\langle e_i|e_j\rangle = \delta_{ij}$ (orthogonality)
- $\sum_{i=1}^{n} \langle e_i|e_i\rangle = I$ (completeness relation)

If $\{|f_i\rangle\}_i$ and $\{|e_i\rangle\}_i$ onb of $\mathcal{H}$, then $\exists$ unitary operator U s.t.

$$|f_i\rangle = U|e_i\rangle$$

$$I = \sum_i |f_i\rangle\langle f_i| = \sum_i U|e_i\rangle\langle e_i|U^\dagger$$
$$= U \sum |e_i\rangle\langle e_i| U^\dagger = UIU^\dagger = UU^\dagger.$$

$\Rightarrow U$ unitary.

If $\{|i\rangle\}_{i=1}^n$ onb. of $\mathcal{H} \cong \mathbb{C}^n$, then any $A \in \mathcal{L}(\mathcal{H})$ can be written as

$$A = \sum_{i,j=1}^{n} A_{ij} |i\rangle\langle j|,$$

where $A_{ij} = \langle i|A|j\rangle$.

Orthogonal projectors

$P \in \mathcal{L}(\mathcal{H})$ s.t. $P^2 = P$, $P^\dagger = P$.

$$P^k|u\rangle = P|u\rangle \quad \forall k \geq 1, |u\rangle \in \mathcal{H}$$

$\forall |u\rangle \in \mathcal{H}$ s.t. $\langle u|u\rangle = 1$,

$$P_u = |u\rangle\langle u|.$$

$$|u\rangle\langle u|^\dagger = |u\rangle\langle u|, \quad P_u^2 = |u\rangle\langle u|u\rangle\langle u| = |u\rangle\langle u| = P_u$$

- $P_u|v\rangle = |u\rangle\langle u|v\rangle = \langle u|v\rangle |u\rangle$

component of $|v\rangle$ along $|u\rangle$.

- $\{|e_i\rangle\}_{i=1}^n$ onb of $\mathcal{H} \cong \mathbb{C}^n$.

$$\sum_{i=1}^{k} |e_i\rangle\langle e_i|$$

projects onto the subspace spanned by $|e_1\rangle, \dots, |e_k\rangle$.

- $\sum_{i=1}^{n} |e_i\rangle\langle e_i|$ projects onto $\mathcal{H}$.

$$\forall |v\rangle \in \mathcal{H}, \quad |v\rangle = I|v\rangle = \sum_{i=1}^{n} |e_i\rangle\langle e_i| |v\rangle$$

$$= \sum_{i=1}^{n} |e_i\rangle \langle e_i|v\rangle$$

$$= \sum_{i=1}^{n} v_i |e_i\rangle \quad \cdot \quad v_i \in \mathbb{C} \text{ is prob. amplitude.}$$

Trace of operator

- $\mathrm{Tr}(|a\rangle\langle b|) = \langle b|a\rangle$.

Note $\mathrm{Tr}(A) = \sum_k \langle e_k|A|e_k\rangle = A_{kk}$

$$\mathrm{Tr}(|a\rangle\langle b|) = \sum_k \langle e_k|a\rangle\langle b|e_k\rangle = \sum_k \langle b|e_k\rangle\langle e_k|a\rangle$$

$$= \langle b| \sum_k |e_k\rangle\langle e_k| |a\rangle$$

$$= \langle b|a\rangle$$

$\mathrm{Tr}(A)$ is indep of choice of onb, since any onb, e.g. $\{|f_j\rangle\}_{j=1}^n$ also satisfies $I = \sum_{j=1}^{n} |f_j\rangle\langle f_j|$

Example $\mathcal{H} \cong \mathbb{C}^2$, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

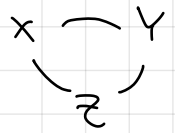
$$|a\rangle = a_1|0\rangle + a_2|1\rangle$$

$$|b\rangle = b_1|0\rangle + b_2|1\rangle$$

Pauli matrices / operators $\in \mathcal{L}(\mathcal{H})$, $\mathcal{H} \cong \mathbb{C}^2$.

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Hermitian and unitary
- Anticommute: $\{X, Y\} = XY + YX = 0$
- traceless
- $XY = iZ$



- $X|0\rangle = |1\rangle$
  $X|1\rangle = |0\rangle$. } X: bit-flip operator
- $Z|0\rangle = |0\rangle$
  $Z|1\rangle = -|1\rangle$ } Z: phase-flip op.
- $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ is an eigenbasis of X:

$$X|+\rangle = |+\rangle \quad , \quad X|-\rangle = -|-\rangle$$

- $Y = -iZX$.
- $X^2 = Y^2 = Z^2 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- $\{I = \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X, Y, Z\}$ is a basis of $M_2(\mathbb{C})$ with the <u>Hilbert-Schmidt inner product.</u>

$A, B \in M_2(\mathbb{C})$, then $\langle A, B \rangle_{HS} = \mathrm{Tr}(A^\dagger B)$

$A, B \in \{I, X, Y, Z\}$. then $\langle A, B \rangle_{HS} = 0$ for $A \neq B$.

$$\langle A, A \rangle_{HS} = 2$$

So $\{I/\sqrt{2}, X/\sqrt{2}, Y/\sqrt{2}, Z/\sqrt{2}\}$ forms orthonormal basis of $M_2(\mathbb{C})$. $\Rightarrow$ any $M \in M_2(\mathbb{C})$ can be written as

$$M = \alpha X + \beta Y + \gamma Z + \delta I.$$

Postulate III (Physical evolution of q states): Any physically admissible evolution of a closed q system is represented by a unitary matrix on $\mathcal{H}$.

- If system is in state $|\psi(t_1)\rangle$ at time t_1 and in $|\psi(t_2)\rangle$ at time t_2, then $\exists$ unitary operator $U(t_1, t_2)$ $(t_2 > t_1)$

$$|\psi(t_2)\rangle = U(t_1, t_2)\,|\psi(t_1)\rangle.$$

Schrödinger eqn (time evolution)

$$\frac{d}{dt}|\psi(t)\rangle = -\frac{i}{\hbar} H\,|\psi(t)\rangle$$

where $H = H^\dagger$, $H \in \mathcal{L}(\mathcal{H})$ Hamiltonian

- If H is time-indep, then

$$|\psi(t)\rangle = U(t)\,|\psi(0)\rangle, \quad U(t) = e^{-iHt/\hbar}.$$

where $e^{-iHt/\hbar} = I - \frac{iHt}{\hbar} + \frac{1}{2}\left(-\frac{it}{\hbar}\right)^2 H^2 + \dots$

- In fact, any unitary matrix can be written as

$$U \equiv U(t) = e^{iAt} \equiv \sum_{n=1}^{\infty} \left(\frac{it}{\hbar}\right)^n \frac{A^n}{n!}$$

for $A = A^\dagger$.

Basic unitaries: quantum logic gates $\Rightarrow$ use to construct more complex unitaries.

Orthogonal subspaces

$\{|e_i\rangle\}_{i=1}^n$ onb, then

(1) $\langle e_i | e_j \rangle = \delta_{ij}$

(2) $\sum_{i=1}^{n} |e_i\rangle\langle e_i| = I$

(1) and (2) can be extended to subspaces of $\mathcal{H}$.

- $E_1, E_2 \subset \mathcal{H}$ mutually orthogonal if $\forall |v_1\rangle \in E_1, |v_2\rangle \in E_2$, $\langle v_1 | v_2 \rangle = 0$.
- $E_1, \dots E_k \subset \mathcal{H}$ form an $\perp$ decomposition of $\mathcal{H}$

$$\mathcal{H} = E_1 \oplus \dots \oplus E_k$$

if any $|v\rangle \in \mathcal{H}$ has a unique decomposition

$$|v\rangle = \sum_{i=1}^{k} |v_i\rangle \quad , \text{where} \quad |v_i\rangle \in E_i .$$

$$1 = \langle v | v \rangle = \sum_j \langle v_j | \sum_i |v_i\rangle$$

$$= \sum_{i,j} \langle v_j | v_i \rangle$$

$\sum_{i=1}^{k} \langle v_i | v_i \rangle = k$ $\Rightarrow$ $\langle v_i | v_i \rangle \neq 1$.

$$|v_i\rangle = \Pi_i |v\rangle$$

↑ orthogonal proj. onto E_1

$$\langle v_i | v_i \rangle = \langle v_i | \Pi_i^\dagger \Pi_i | v_i \rangle = \langle v | \Pi_i | v_i \rangle$$

$$|v\rangle = \sum_{i=1}^{k} |v_i\rangle \quad \text{if} \quad \mathcal{H} = \bigoplus_{i=1}^{k} E_i$$

$$|v_i\rangle = \Pi_i |v\rangle$$

$$\Rightarrow \sum_i \Pi_i = I, \quad \Pi_i \Pi_j = \delta_{ij} \Pi_i \quad \text{(no summation)}$$

orth. rel. for projection $\{\Pi_i\}$

extension of completeness rel. reduces to

$$\sum |e_i \rangle\langle e_i| = I$$

if $\Pi_i = |e_i\rangle\langle e_i|$ rank-1 proj.

Postulate IV (Measurement postulate):

(a) A complete (projective) measurement on a q system with Hilbert space $\mathcal{H}$ is determined by the choice of an onb $\{|e_i\rangle\}_{i=1}^n$. (in fact, every such onb in principle represents a possible mmt).

- Outcome = label of basis vector $|e_i\rangle$
- $\text{Prob}(e_k) = p(k) = |\langle e_k|\psi\rangle|^2$ if initial state of sys is $|\psi\rangle$.

$$|\psi\rangle = \sum_i \langle e_i|\psi\rangle |e_i\rangle$$

If outcome is e_k.

$$|\psi\rangle \longmapsto |\psi'\rangle = |e_k\rangle = \frac{P_k|\psi\rangle}{\sqrt{p(k)}}, \quad P_k = |e_k\rangle\langle e_k|.$$

Example $\mathcal{H} \cong \mathbb{C}^2$, $|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$.

Measure in $\{|0\rangle, |1\rangle\}$

$\text{Prob}(0) = p(0) = |\langle 0|\psi\rangle|^2 = \frac{1}{3}$

$\text{Prob}(1) = p(1) = |\langle 1,\psi\rangle|^2 = \frac{2}{3}$.

If outcome $= 0$,

$$|\psi\rangle \longmapsto |\psi'\rangle = |0\rangle.$$

Example $\mathcal{H} \cong \mathbb{C}^2$, $|\psi\rangle = \sqrt{\frac{2}{7}}|+\rangle + \sqrt{\frac{5}{7}}|-\rangle$, measure in $\{|+\rangle, |-\rangle\}$

Outcomes are $+$, $-$, and $p(+) = \frac{2}{7}$, etc.

Projective Measurement

Measurement is equivalently specified by $\{P_i\}$

$$P_i = |e_i\rangle\langle e_i|$$

if sys is in state $|\psi\rangle$.

$$p(e_k) = p(k) = \text{tr}(P_k|\psi\rangle\langle\psi|)$$

$$= \langle\psi|P_k|\psi\rangle = \langle\psi|e_k\rangle\langle e_k|\psi\rangle = |\langle e_k|\psi\rangle|^2$$

If outcome is e_k,

$$|\psi\rangle \mapsto |\psi'\rangle = \frac{P_k|\psi\rangle}{\sqrt{p(k)}}$$

Example $\mathcal{H} \cong \mathbb{C}^2$, $|\psi\rangle = a|+\rangle + b|-\rangle$, $a, b \in \mathbb{C}$.

Measure in $\{|\pm\rangle\}$.

$$P_+ = |+\rangle\langle+|$$

$$\text{Prob}(+) = p(+) = \text{Tr}(P_+ |\psi\rangle\langle\psi|)$$

$$= \langle\psi|P_+|\psi\rangle = |a|^2$$

If outcome is $+$,

$$|\psi\rangle \mapsto |\psi'\rangle = \frac{P_+|\psi\rangle}{\sqrt{p(+)}} = \frac{a|+\rangle}{|a|} = \frac{|a|e^{i\theta}|+\rangle}{|a|} = |+\rangle.$$

global phase / for some $\theta \in \mathbb{R}$.

Incomplete projective measurement

Let $\mathcal{H} = \bigoplus_{i=1}^{k} E_i$ (1), $\{E_i \subset \mathcal{H}\}$ mutually $\perp$.

Let Π_i orth. proj. on E_i

$$\Pi_i \Pi_j = \delta_{ij} \Pi_i$$

- An incomplete mmt of $|\psi\rangle \in \mathcal{H}$ w.r.t. the decomposition (1).
- mmt outcomes $i \in \{1, \ldots, k\}$.
- $\text{Prob}(i) = p(i) = \langle\psi|\Pi_i|\psi\rangle$.
- If outcome is i, $|\psi\rangle \mapsto |\psi'\rangle = \frac{\Pi_i|\psi\rangle}{\sqrt{p(i)}}$

Note A complete mmt is a special case of an incomplete mmt, where E_i 1-dim subspaces and Π_i rank-1 projections.

An incomplete mmt can be completed via a complete mmt. For $\mathcal{H} \cong \bigoplus_{i=1}^{k} E_i$, $\mathcal{H} \cong \mathbb{C}^n$.

• Choose onb consistent with (*)

$$\{|e_1^{(1)}\rangle, \ldots, |e_{m_1}^{(1)}\rangle, |e_2^{(1)}\rangle, \ldots, |e_{m_2}^{(2)}\rangle, \ldots, |e_1^{(k)}\rangle, \ldots, |e_{m_k}^{(k)}\rangle\}.$$

basis of E_1.

$m_1 = \dim(E_1)$

Denote $\Pi^{(i)} = \sum_{j=1}^{m_i} |e_j^{(i)}\rangle\langle e^{(i)}|$ the orth. proj. on E_i.

• Perform complete mmt on $|\psi\rangle$ in basis $\mathcal{B}$ and recover outcome probs of incomplete mmt by summing relavant probs of complete mmt.

$$\begin{aligned} \text{Prob}(i) &= \langle\psi|\Pi^{(i)}|\psi\rangle \\ &= \langle\psi| \sum_{j=1}^{m_i} |e_j^{(i)}\rangle\langle e_j^{(i)}| \psi\rangle \\ &= \sum_{j=1}^{m_i} |\langle e_j^{(i)}|\psi\rangle|^2. \end{aligned}$$

incomplete mmt $i = 1, \ldots, k$

Example (Parity mmt)

Parity of a 2-bit string $b_1 b_2 \in \{0,1\}^2 = b_1 \oplus b_2$ ← addition mod 2.

$$0 \oplus 0 = 0 = 1 \oplus 1$$

Example (Parity mmt on a state of 2 qubits) $\mathcal{H} \cong (\mathbb{C}^2)^{\otimes 2}$

Incomplete mmt $\mathcal{H} \cong E_0 \oplus E_1$

$E_0 = \text{span}\{|00\rangle, |11\rangle\}$ even par.

$E_1 = \text{span}\{|01\rangle, |10\rangle\}$ odd par.

Let $|\psi\rangle \in \mathcal{H}$ initial state, $|\psi\rangle = \sum_{i,j=0}^{1} a_{ij} |i\rangle|j\rangle$

Possible outcomes of panty mmt are 0, 1

$$\text{Prob}(0) = p(0) = \langle\psi|\Pi_0|\psi\rangle, \quad \Pi_0 = |00\rangle\langle 00| + |11\rangle\langle 11|$$

$$\Rightarrow p_0 = |a_{00}|^2 + |a_{11}|^2$$

Equiv. to doing a complete mmt in basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

$$\text{Prob}(0) = p_{00} + p_{11}$$

$$p_{00} = \text{Prob}(00) = \langle\psi|P_{00}|\psi\rangle = |a_{00}|^2 \quad \text{(complete)}$$

$$p_{11} = \langle\psi|P_{11}|\psi\rangle = |a_{11}|^2$$

Incomp: $\text{Prob}(0) = |a_{00}|^2 + |a_{11}|^2$

- Post measurement states corresponding to even parity outcome

$$|\psi'\rangle = \frac{a_{00}|00\rangle + a_{11}|11\rangle}{\sqrt{p(0)}} = \frac{\Pi_0|\psi\rangle}{\sqrt{p(0)}}.$$

In QM, measure a quantum observable A, and outcome are evals of A.

Spectral decomp. $$A = \sum_{i=1}^{k} a_i \Pi_i$$

- If a_i non-degenerate, then $\Pi_i = |e_i\rangle\langle e_i|$
- If a_i degenerate, Π_i orth. proj. on

$$E_i = \text{span}\{|e_j^{(i)}\rangle,\ j = 1, \dots, m_i\}$$

$\equiv$ incomp. mmt corrsponding to $\mathcal{H} = \bigoplus_{i=1}^{m} E_i$.

with m_i the degeneracy of a_i.

- If a_i non-deg, eval eqn: $A|e_i\rangle = a_i|e_i\rangle$

$$\Pi_i = |e_i\rangle\langle e_i| = P_i.$$

Extended Born Rule

Consider a measurement on only a part of a composite system.

e.g. composite system $S_1 S_2$. $\mathcal{H}_1 \otimes \mathcal{H}_2$.

$\mathcal{B}_1 = \{|e_i\rangle\}_{i=1}^{m}$. $\mathcal{B}_2 = \{|f_j\rangle\}_{j=1}^{n}$ onb of $\mathcal{H}_1 \cong \mathbb{C}^m$. $\mathcal{H}_2 \cong \mathbb{C}^n$.

We want to measure in $\tilde{\mathcal{B}} = \{|e_i\rangle \otimes |e_j\rangle\}_{\substack{i=1,\dots m \\ j=1,\dots,n}}$ onb of $\mathcal{H}_1 \otimes \mathcal{H}_2$.

This amounts to an incomp. mmt.

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = \bigoplus_{i=1}^{m} E_i, \quad E_i = \text{span}\{|e_i\rangle \otimes |\psi\rangle \ \forall\, |\psi\rangle \in \mathcal{H}_2\}$$

Check that $P_i \otimes I = \Pi_i$ orthu. proj. on E_i

Outcomes of mmt $k \in \{1, \ldots, m\}$

$$\text{Prob}(k) = p(k) = \langle\psi| P_k \otimes I |\psi\rangle \qquad [P_k = |e_k\rangle\langle e_k|]$$

Say. $|\psi\rangle = \sum_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} a_{ij} |e_i\rangle|f_j\rangle$., then

$$p(k) = \sum_{i,i',j,j'} a_{ij}^* \langle e_i|\langle f_j| \left(|e_k\rangle\langle e_k| \otimes I\right) a_{i'j'} |e_{i'}\rangle|f_{j'}\rangle.$$

$$= a_{ij}^* a_{i'j'} \langle e_i|e_k\rangle\langle e_k|e_{i'}\rangle\langle f_j|f_{j'}\rangle$$

$$= \sum_{j=1}^{n} |a_{kj}|^2$$

If outcome is k. $\quad |\psi\rangle \longmapsto |\psi'\rangle = \dfrac{(P_k \otimes I)|\psi\rangle}{\sqrt{p(k)}}$.

e.g. Complete mmt in $\{|+\rangle, |-\rangle\}$ characterised by $P_\pm = |\pm\rangle\langle\pm|$

States with guaranteed diff. outcomes lie in mutually $\perp$ subspace of $\mathcal{H}$ $\Rightarrow$ 2 states $|\psi\rangle, |\phi\rangle$ are perfectly distinguishable iff $\langle\psi|\phi\rangle = 0$.

$\therefore$ Perfectly distinguishability of 2 states means that $\exists$ a mmt which gives 2 distinct outcomes w.p. 1 when applied to the 2 states

Entanglement

In QIC, info encoded in states of q systems.

(closed sys): $\mathcal{H}$, $|\psi\rangle \in \mathcal{H}$.

Consider 2 systems A, B ($\mathcal{H}_A$, $\mathcal{H}_B$) (e.g. 2 qubits). Suppose AB is in state

$$|\psi_{AB}\rangle = |\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$$

$|\psi\rangle$ is a <u>product state</u> if it can be written as

$$|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle \quad . \quad |\alpha\rangle \in \mathcal{H}_A, \ |\beta\rangle \in \mathcal{H}_B.$$

if not, then $|\psi\rangle$ is <u>entangled state</u>.

<u>Example</u> $\mathcal{H}_A, \mathcal{H}_B = \mathbb{C}^2$.

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

<u>Claim</u>: This is entangled.

Assume $\exists \ |\alpha\rangle = a|0\rangle + b|1\rangle$, $|\beta\rangle = c|0\rangle + d|1\rangle$ s.t. $|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle$.

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$$

$$= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

$$\Rightarrow ad = 0, \quad bc = 0$$

$$\Rightarrow a = 0 \text{ or } d = 0, \quad b = 0 \text{ or } c = 0. \ \#$$

$$\Rightarrow |\psi\rangle \text{ entangled.}$$

In Sheet, Any $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$.

$|\psi\rangle$ entangled $\Leftrightarrow \alpha\delta - \beta\gamma \neq 0$.

<u>Note</u> $\alpha\delta - \beta\gamma \neq 0$ no longer sufficies if A, B <u>not</u> qubits (Qudit $\mathbb{C}^d$, $\mathbb{C}^n$, $d, n \geq 2$).

Example $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$ ent ?

$= |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + |1\rangle\right) = |0\rangle \otimes |+\rangle$

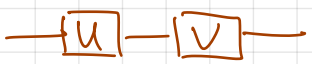
So no.

Entanglement is a valuable resource in QIC.

Quantum logic gates

- Physically it is a device which performs a fixed unitary operation on a selected set of qubits in a fixed period of time
- Mathly, a q. gate = unitary op.
- A quantum circuit : a device consisting of q. gates.

Example U unitary, $\mathcal{H} \cong \mathbb{C}^2$.

- read from left to right.
- line represent a qubit.
- a quantum wire can represent
  - a translation in space (e.g. atoms travelling through a cavity, photons in an optical fibre)
  - a translation in time (e.g. sequence of operations performed on a qubit).
- 

: matrix VU.

Single qubit gates

1. Hadamard gate H

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

In Dirac notation.

$$H = \frac{1}{\sqrt{2}}\left[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right]$$

- $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$
- $H^\dagger = H$, $H^2 = I \Rightarrow H^{-1} = H \Rightarrow H|+\rangle = |0\rangle$, $H|-\rangle = |1\rangle$

H: a special case of a quantum Fourier transform (F_n)

$H = F_2$, where F_n acts on $|x\rangle \in \{0,1\}^n$

$$F_n|x\rangle = \frac{1}{\sqrt{n}} \sum_{y \in \{0,1\}^n} e^{i 2\pi xy/n} |y\rangle.$$

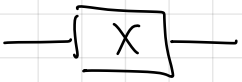
2. X-gate / Not gate (bit flip gate)

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $X|k\rangle = |k \oplus 1\rangle$, $k = 0, 1$

($\oplus$: addition mod 2)

$X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$



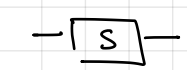
3. Z-gate (phase-flip gate)

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

4. Phase gate

$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$. $P_\theta|0\rangle = |0\rangle$, $P_\theta|1\rangle = e^{i\theta}|1\rangle$.

In particular, $Z = P_\pi$.

- S-gate  $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

- T-gate  $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$.

Rmk Check $HXH^\dagger = HXH = Z$

$HZH = X$

$HYH = -Y$

Unitaries such H which take Pauli ops → Pauli ops under conjugation are called Chifford gates

Question which phase gate is in the Chifford group?

Example $|0\rangle - [H] - [P_\theta] - [H] - |\psi\rangle = ?$

$|0\rangle \xrightarrow{H} |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

$\xrightarrow{P_\theta} \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$

$\xrightarrow{H} \frac{|+\rangle + e^{i\theta}|-\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(1+e^{i\theta})|0\rangle + \frac{1}{\sqrt{2}}(1-e^{i\theta})|1\rangle$

$= e^{i\theta/2}\left(\cos\frac{\theta}{2}|0\rangle + i\sin\frac{\theta}{2}|1\rangle\right)$

So $|0\rangle \longmapsto \cos\frac{\theta}{2}|0\rangle + i\sin\frac{\theta}{2}|1\rangle$.

This Q-circuit is called single-qubit interference circuit.

2-qubit gates

1. CNOT or CX gate (C: controlled)

$$CNOT = \begin{pmatrix} [I] & [0] \\ [0] & [X] \end{pmatrix} = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$$

$CNOT\,|i\rangle|j\rangle = |i\rangle\,|i \oplus j\rangle$, $i, j \in \{0, 1\}$.

$\forall\, |\psi\rangle \in \mathbb{C}^2$

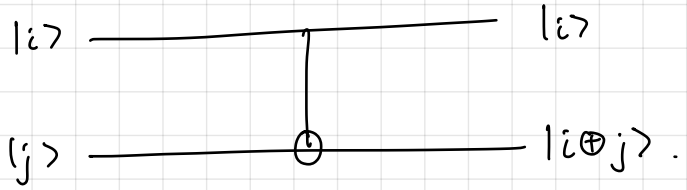
$CNOT\,|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$, $CNOT\,|1\rangle|\psi\rangle = |1\rangle X|\psi\rangle$.

1st qubit: control qubit, 2nd qubit: target qubit.

This can be extended by linearity to arbitrary state of control qubit.

$$CNOT\,|+\rangle|\psi\rangle = CNOT\left(|0\rangle+|1\rangle\right)|\psi\rangle/\sqrt{2}$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle X|\psi\rangle\right)$$



If you change roles of control and target qubits, get a different gate.

$$CNOT_{1,2}\;|0\rangle_1|1\rangle_2 = |0\rangle_1|1\rangle_2$$

$$CNOT_{2,1}\;|0\rangle_1|1\rangle_2 = |1\rangle_1|1\rangle_2$$

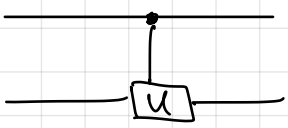
Exercise Check

$$CNOT_{2,1} = (H\otimes H)\,CNOT_{1,2}\,(H\otimes H)$$

Quantum version of discrete FT: $\mathbb{Z}_N = \{0,1,\ldots,N-1\}$, then

$$x,y\in\mathbb{Z}_N.\quad F_N|x\rangle = \frac{1}{\sqrt{N}}\sum_{y\in\mathbb{Z}_N} e^{i2\pi xy/N}|y\rangle.\quad F_2 \equiv H.$$

2. Controlled unitary gate



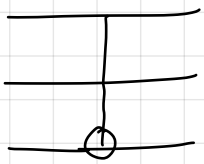
$$CU|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$$

$$CU|1\rangle|\psi\rangle = |1\rangle U|\psi\rangle.$$

e.g. CZ, $U = Z$.

$$CU = \begin{pmatrix} [I] & [0] \\ [0] & [U] \end{pmatrix}$$

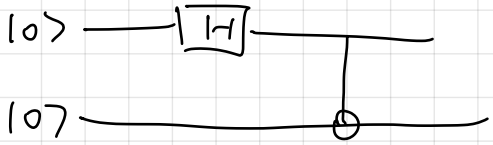
3. Toffole gate



$|\alpha\rangle|\beta\rangle|\psi\rangle \longmapsto |\alpha\rangle|\beta\rangle|\psi\rangle$ if $(\alpha,\beta) \neq (1,1)$

$|1\rangle|1\rangle|\psi\rangle \longmapsto |1\rangle|1\rangle X|\psi\rangle$.

Quantum circuit for entanglement generation



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

$|0\rangle|0\rangle \xrightarrow{H \otimes I} |+\rangle|0\rangle$

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

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

$\xrightarrow{CNOT} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) = |\phi^+\rangle.$

In fact, 

transforms the onb $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ into another onb of $(\mathbb{C}^2)^{\otimes 2}$ of 4 entangled states (Bell basis)

$$C|00\rangle \longmapsto |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$C|01\rangle \longmapsto |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$C|10\rangle \longmapsto |\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$C|11\rangle \longmapsto |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

If reverse circuit : R→L.

Bell basis states ⟶ comp. basis states.

Bell mmt is mmt on 2-qubits in the Bell basis.

Do this, e.g. by 'rotating' Bell basis to comp basis then do mmt in comp. basis.

No cloning theorem

Note CNOT gate can copy a bit value in the first qubit.

$$\text{CNOT}\,|x\rangle|0\rangle = |x\rangle|x\rangle, \quad x \in \{0,1\}.$$

Question: can CNOT also copy superposition states?

$$\text{CNOT}\,|\psi\rangle|0\rangle \longmapsto |\psi\rangle|\psi\rangle. \qquad |\psi\rangle = a|0\rangle + b|1\rangle.$$

No!

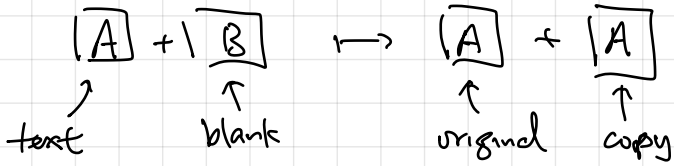
$$\text{CNOT}\,|\psi\rangle|0\rangle = \text{CNOT}\,(a|0\rangle + b|1\rangle)|0\rangle$$

$$= \underbrace{a|00\rangle + b|11\rangle}_{\text{entangled state}}.$$

CNOT: superposition in the control qubit $\longmapsto$ entangled state of both qubits.

No cloning thm:

- classical setting: cloning allowed



- In quantum setting, ∄ a universal quantum cloner / copier.

Quantum cloning involves 3 q systems:

- A: q info to be copied encoded in A. $\mathcal{H}_A$
- B: $\mathcal{H}_B \cong \mathcal{H}_A$ initially in a fixed state $|\psi_0\rangle$ (or $|0\rangle$) of $\mathcal{H}_B$.
- M: cloning machine, initially in say $|M_0\rangle$ (ready state)

Let S be any set of states of a q sys A. that contains at least 1 pair of non-⊥ states, then ∄ any unitary cloning process that achieves cloning for all states in S.

Pf: Assume $\exists$ universal q. cloner. Suppose $|\psi\rangle, |\phi\rangle$ s.t. $\langle\psi|\phi\rangle \neq 0$, $\langle\psi|\phi\rangle \neq 1$ distinct.

Q cloner: $|\psi\rangle|0\rangle|M_0\rangle \longmapsto |\psi\rangle|\psi\rangle|M_\psi\rangle$ (1)

$|\phi\rangle|0\rangle|M_0\rangle \longmapsto |\phi\rangle|\phi\rangle|M_\phi\rangle$ (2)

Since operator unitary, inner prod preserved.

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2 \langle M_\psi|M_\phi\rangle. \quad (3)$$

Let $x = \langle\psi|\phi\rangle$. $x \neq 0$, $x \neq 1$.

(3) $\Rightarrow$ $x = x^2 |\langle M_\psi|M_\phi\rangle|$

$\Rightarrow$ $1 = x\,|\langle M_\psi|M_\phi\rangle| < \langle M_\psi|M_\phi\rangle$.

$\Rightarrow$ $\langle M_\psi|M_\phi\rangle > 1$ $\#$

So states of q systems cannot be cloned. $\square$

Hilbert proposed superluminal communication (he assumed q. cloning was possible).

If q cloning possible $\Rightarrow$ superluminal communication (unphysical).

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

Alice — Bob

$$|\phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right).$$

Claim $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$.

Exercise $\forall M \in M_2(\mathbb{C})$. ricochet condition.

$$(I \otimes M)|\phi^+\rangle = (M^T \otimes I)|\phi^+\rangle$$

$$M = \sum_{i,j=0}^{1} M_{ij}\,|i\rangle\langle j|$$

Pf: $\frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) = \frac{1}{\sqrt{2}}(H \otimes H)(|00\rangle + |11\rangle)$

$= (H \otimes I)(I \otimes H)|\phi^+\rangle = (HH^T \otimes I)|\phi^+\rangle = |\phi^+\rangle$. $\square$

Alice's message	Her action (mmt)	Outcomes and Probs	Final state AB	Final state of B
Yes	in basis $\mathcal{B}_0 = \{\|0\rangle, \|1\rangle\}$	0 w.p. $\frac{1}{2} = p_0$ 1 w.p. $\frac{1}{2} = p_1$	$\|0\rangle\|0\rangle$ $\|1\rangle\|1\rangle$	$\|0\rangle$ $\|1\rangle$
No	in $\mathcal{B}_1 = \{\|+\rangle, \|-\rangle\}$	+ w.p. $\frac{1}{2}$ − w.p. $\frac{1}{2}$	$\|+\rangle\|+\rangle$ $\|-\rangle\|-\rangle$	$\|+\rangle$ $\|-\rangle$

Extended Born rule

$P_0 = |0\rangle\langle 0|, \quad P_1 = |1\rangle\langle 1| \qquad P_\pm = |\pm\rangle\langle\pm|$

$p_0 = \langle \phi^+ | P_0 \otimes I | \phi^+ \rangle$

If '0' : $|\phi^+\rangle \longmapsto (P_0 \otimes I)|\phi^-\rangle / \sqrt{p_0}$

If 'Yes', then B $\begin{cases} |0\rangle \\ |1\rangle \end{cases}$ w.p. $\frac{1}{2}$ } (i)

'No', then B $\begin{cases} |+\rangle \\ |-\rangle \end{cases}$ w.p. $\frac{1}{2}$. } (ii)

Alice's mmt $\Rightarrow$ preparation of B in (i), (ii)

Claim These 2 preparation of state of B are completely indistinguishable to Bob

(a) by any local mmt on B

(b) from the case in which Alice does no mmt.

Pf : Suppose Bob does mmt corresponding to Π_i. (proj. op.). Suppose B is in state $|\psi\rangle$ after Alice's mmt

$$\text{Prob}(\text{outcome} = i) = \langle\psi|\Pi_i|\psi\rangle.$$

$$\text{Pr}_{\text{yes}}(i) = \text{Prob}(\text{Alice} = \text{yes} \Rightarrow \text{Bob} = i)$$

$$= \tfrac{1}{2}\langle 0|\Pi_i|0\rangle + \tfrac{1}{2}\langle 1|\Pi_i|1\rangle$$

$$= \frac{1}{2}\,\mathrm{Tr}(\Pi_i |0\rangle\langle 0|) + \frac{1}{2}\,\mathrm{Tr}(\Pi_i |1\rangle\langle 1|)$$

$$= \frac{1}{2}\,\mathrm{Tr}\left(\Pi_i \left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)\right)$$

$$= \frac{1}{2}\,\mathrm{Tr}(\Pi_i)$$

$$\Pr_{no}(i) = \frac{1}{2}\langle +|\Pi_i|+\rangle + \frac{1}{2}\langle -|\Pi_i|-\rangle = \frac{1}{2}\mathrm{Tr}(\Pi_i).$$

If Alice does no mmt,

$$\Pr(i) = \langle \phi^+| I \otimes \Pi_i |\phi^+\rangle = \frac{1}{2}\mathrm{tr}(\Pi_i).$$

($\Pr(i)$: ↑ Bob's mmt)

□

Herbert: let's clone B.

Alice does mmt on 12pm. Bob: just after 12pm, he clones qubit B. say 10^6 times, and he does mmt on each copy of B in $\mathcal{B}_0 = \{|0\rangle, |1\rangle\}$. ⇒ outcome $b = b_1 b_2 \ldots b_n \in \{0,1\}^n$, $n = 10^6$.

Claim If Alice's message is "Yes", then $b = \begin{cases} 0\ldots0 \\ 1\ldots1 \end{cases}$. Bob has after cloning $\begin{cases} |0\rangle\ldots|0\rangle \\ |1\rangle\ldots|1\rangle \end{cases}$ w.p. 1/2.

If message was "No", bob has $\begin{cases} |+\rangle\ldots|+\rangle \\ |-\rangle\ldots|-\rangle \end{cases}$ w.p. 1/2.

b is now a uniformly random bit string

"$b_1 \ldots b_n$", $b_i = 0, 1$ w.p. 1/2.

Such a string can be distinguished from $\begin{cases} 0\ldots0 \\ 1\ldots1 \end{cases}$ except w.p. $2/2^{10^6}$. Bob could clone more and more, and mmt on each copy ⇒ prob. of error → 0 ⇒ superluminal communication.

Fact A special case of the No Signalling Principle / Thm.

Alice — $|\phi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ — Bob

$\mathcal{H}_A, \mathcal{H}_B \cong \mathbb{C}^2$.

Alice cannot convey any info to Bob just by doing local mmt on A.

i.e. no local action on A alone by Alice can change the outcome prob. dist. of any mmt by Bob on B.

Pf (basic case): Bob does a complete mmt on B in basis $\{|b\rangle\}_{b=1}^{d_B}$, $d_B = \dim \mathcal{H}_B$, onb of $\mathcal{H}_B$. Let $\{|a\rangle\}_{a=1}^{d_A}$, $d_A = \dim \mathcal{H}_A$, onb of $\mathcal{H}_A$.

Case I: only Bob do mmt

$$|\phi_{AB}\rangle = \sum_{a,b} c_{ab} |a\rangle|b\rangle. \quad \in \mathcal{H}_A \otimes \mathcal{H}_B.$$

$$\text{Prob}(b) = p(b) = \langle \phi_{AB} | I_A \otimes P_b | \phi_{AB} \rangle$$

$$= \sum_a |c_{ab}|^2. \qquad (*)$$

If outcome is b,

$$|\phi_{AB}\rangle \longmapsto \frac{(I_A \otimes P_b)|\phi_{AB}\rangle}{\sqrt{p(b)}}.$$

Case II: when Alice does a mmt prior to Bob's mmt.

Suppose Alice does mmt on A in $\{|a\rangle\}$.

- $\text{Prob}(a) = p(a) = \sum_b |c_{ab}|^2$
- If outcome is a,

$$|\phi_{AB}\rangle \longmapsto (P_a \otimes I_B)|\phi_{AB}\rangle / \sqrt{p(a)} \equiv |\phi''_{AB}\rangle.$$

Now Bob mmt on B in $\{|a\rangle\}$.

$$p(b|a) = \langle \phi''_{AB} | I_A \otimes P_b | \phi''_{AB} \rangle.$$

$$= \frac{1}{p(a)} \langle \phi_{AB} | (P_a \otimes I_B)(I_A \otimes P_b)(P_a \otimes I_B) | \phi_{AB} \rangle$$

$$= \frac{1}{p(a)} \langle \phi_{AB} | P_a \otimes P_b | \phi_{AB} \rangle$$

$$\Rightarrow p(a,b) = \langle \phi_{AB} | P_a \otimes P_b | \phi_{AB} \rangle = |c_{ab}|^2$$

$$p(b) = \sum_a p(a,b) = \sum_a |c_{ab}|^2 = (*) \qquad \square$$

Note: The same holds if Alice and B do incomplete mmt.

Distinguishing non-orthogonal states

You are given a q. sys in unknown state $|\psi\rangle$, You are told.

$$|\psi\rangle \begin{cases} |\alpha_0\rangle \\ |\alpha_1\rangle \end{cases} \quad \text{w.p. } 1/2$$

where $|\alpha_0\rangle, |\alpha_1\rangle$ distinct, non-$\perp$. ($\langle\alpha_0|\alpha_1\rangle \neq 0, 1$)

Aim: Determine whether $|\psi\rangle \begin{cases} |\alpha_0\rangle \\ |\alpha_1\rangle \end{cases}$. What is best you can do?

E.g. do nothing: random guess.

Prob. of success = $p_{succ.} = 1/2$.

Claim Can do better by doing a mmt on the sys.

Do mmt $\{\Pi_0, \Pi_1\}$ (infer $|\alpha_0\rangle, |\alpha_1\rangle$ proj. ops. $\Pi_0 + \Pi_1 = I$.

Define average prob. of success

$$p_{succ}(\Pi_0) = \frac{1}{2}\,\text{Prob}(\text{outcome} = 0 \mid |\psi\rangle = |\alpha_0\rangle) + \frac{1}{2}\,\text{Prob}(\text{outcome} = 1 \mid |\psi\rangle = |\alpha_1\rangle)$$

$$= \frac{1}{2} + \frac{1}{2}\,\text{Tr}\left[\Pi_0 \underbrace{(|\alpha_0\rangle\langle\alpha_0| - |\alpha_1\rangle\langle\alpha_1|)}_{=\Delta}\right]$$

$$= \frac{1}{2} + \frac{1}{2}\,\text{Tr}(\Pi_0 \Delta).$$

Consider $\Delta := |\alpha_0\rangle\langle\alpha_0| - |\alpha_1\rangle\langle\alpha_1|$. Properties:

- $\Delta^\dagger = \Delta \Rightarrow$ evals $\in \mathbb{R}$, evecs onb.
- $\forall |\beta\rangle \in \mathcal{H}$ s.t. $\langle\beta|\alpha_0\rangle = 0 = \langle\beta|\alpha_1\rangle$, $\Delta|\beta\rangle = 0$.
  $\Rightarrow \Delta$ acts non-trivially only on states in $V = \text{span}\{|\alpha_0\rangle, |\alpha_1\rangle\}$.
- $\text{Tr}(\Delta) = 0 \Rightarrow$ evals are, say, $+s, -s$. Let corr evec $|p\rangle, |m\rangle$. and

$$P_s = |p\rangle\langle p|, \quad P_{-s} = |m\rangle\langle m|$$

Spectral decomposition

$$\Delta = \delta P_\delta - \delta P_{-\delta} = \delta(|p\rangle\langle p| - |m\rangle\langle m|)$$

In the basis $\{|p\rangle, |m\rangle\}$ of V_1

$$\Delta = \begin{pmatrix} \delta & 0 \\ 0 & -\delta \end{pmatrix}$$

Determine δ in terms of $|\alpha_0\rangle, |\alpha_1\rangle$:

Let $|\alpha_0^\perp\rangle \in V$ is $\langle\alpha_0^\perp|\alpha_0\rangle = 0 \Rightarrow \{|\alpha_0\rangle, |\alpha_0^\perp\rangle\}$ onb of V.

$$\Rightarrow |\alpha_1\rangle = c_0|\alpha_0\rangle + c_1|\alpha_0^\perp\rangle.$$

$V \simeq \mathbb{C}^2$, so WLOG use

$$|\alpha_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle, \quad |\alpha_0^\perp\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle, \quad |\alpha_1\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

$$\Delta = \begin{pmatrix} |c_1|^2 & -c_0 c_1^* \\ -c_0^* c_1 & -|c_1|^2 \end{pmatrix}$$

Find evals of $\Delta \Rightarrow \lambda = \pm|c_1| \Rightarrow \delta = |c_1|, \ -\delta = -|c_1|$

Let $|\alpha_0\rangle, |\alpha_1\rangle$ be s.t. $0 < |\langle\alpha_0|\alpha_1\rangle| < 1$,

$$|\langle\alpha_0|\alpha_1\rangle| = \cos\theta, \quad 0 < \theta < \pi/2.$$

Then $|c_0| = \cos\theta, \quad |c_1| = \sqrt{1-\cos^2\theta} = |\sin\theta|$

$$\Rightarrow |c_1|^2 = \sin^2\theta, \quad \delta = |c_1| = \sin\theta.$$

Then

$$\begin{aligned} P_{\text{succ}}(\Pi_0) &= \tfrac{1}{2} + \tfrac{1}{2}\operatorname{Tr}(\Pi_0 \Delta) \\ &= \tfrac{1}{2} + \tfrac{1}{2}\operatorname{Tr}\left[\Pi_0(\delta|p\rangle\langle p| - \delta|m\rangle\langle m|)\right] \\ &= \tfrac{1}{2} + \tfrac{\sin\theta}{2}\left[\langle p|\Pi_0|p\rangle - \langle m|\Pi_0|m\rangle\right] \end{aligned}$$

Projective mmt Π_0, Π_1 are orth. proj. ops.

Claim: $\langle m|\Pi_0|m\rangle \geq 0$

Pf: $\langle m|\Pi_0|m\rangle = \langle m|\Pi_0^2|m\rangle$

$$= \langle m|\Pi_0^\dagger \Pi_0|m\rangle = \|\Pi_0|m\rangle\|^2 \geq 0.$$

□

$\langle p|\Pi_0|p\rangle \le \langle p|p\rangle = 1$

$$\Rightarrow P_{succ}(\Pi_0) \le \frac{1}{2} + \frac{\sin\theta}{2}\langle p|\Pi_0|p\rangle \le \frac{1}{2} + \frac{\sin\theta}{2}.$$

Can you find $\{\Pi_0, \Pi_1\}$ s.t. equality holds? If $\Pi_0 = |p\rangle\langle p|$, then

$$p^*_{succ} = \max_{\Pi_0} P_{succ}(\Pi_0) \le \frac{1}{2} + \frac{1}{2}\sin\theta, \qquad |\langle\alpha_0|\alpha_1\rangle| = \cos\theta$$

and p^*_{succ} is achieved.

Thm (Helstrom - Holevo thm) Given any one of 2 equally likely (distinct and non $\perp$) states $|\alpha_0\rangle, |\alpha_1\rangle$ with $|\langle\alpha_0|\alpha_1\rangle| = \cos\theta$, for some $0 < \theta < \pi/2$, the prob. P_{succ} of correctly identifying the state by any q. mmt satisfies

$$P_{succ} \le \frac{1}{2} + \frac{\sin\theta}{2}.$$

and this bound is tight.

Entanglement and its applications

- The Bell basis – onb of $\mathbb{C}^2 \otimes \mathbb{C}^2$, consists of 4 maximally entangled states.

$$\{|\phi^+_{AB}\rangle, |\phi^-_{AB}\rangle, |\psi^+_{AB}\rangle, |\psi^-_{AB}\rangle\}$$

$$|\phi^\pm_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad |\psi^\pm_{AB}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

(aka EPR states)

- If we do a local mmt on A (or on B)

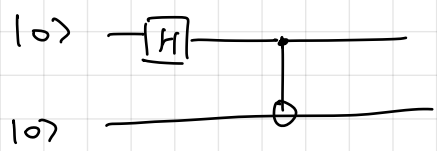
$$\text{Prob}(0) = \frac{1}{2} = \text{Prob}(1).$$

$\Rightarrow$ even though we know the state of AB completely, we know nothing about A (or B) individually.

$$|\Omega_{AB}\rangle = \text{pure state}. \qquad \Omega = \phi^\pm, \psi^\pm.$$

This is quantum phenomenon.

• The 4 Bell states can be characterised by 2 bits.



$\} |\phi^+\rangle$

$00 \mapsto |\phi^+\rangle$
$01 \mapsto |\psi^+\rangle$
$10 \mapsto |\phi^-\rangle$
$11 \mapsto |\psi^-\rangle$.

phase bit → 1 ← parity bit

Parity bit: are spins || or anti-|| ?

$|0\rangle \equiv |\uparrow\rangle, \quad |1\rangle \equiv |\downarrow\rangle$

Parity bit = $\begin{cases} 0 \\ 1 \end{cases}$ if constituent states in superposition have even / odd parity

Phase bit = $\begin{cases} 0 \\ 1 \end{cases}$ if superposition (+) / (−)

If A, B in same location, and do joint mmt on them, then complete mmt in basis $\{|\phi^\pm\rangle, |\psi^\pm\rangle\}$.

Proj. ops:

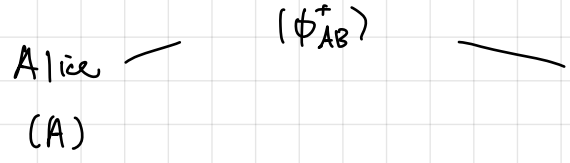
$P_{00} = |\phi^+\rangle\langle\phi^+|$
$P_{01} = |\psi^+\rangle\langle\psi^+|$
$P_{10} = |\phi^-\rangle\langle\phi^-|$
$P_{11} = |\psi^-\rangle\langle\psi^-|$

outcomes: 00, 01, 10, 11

Superdense coding

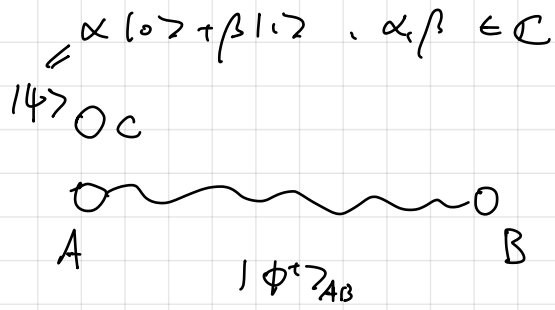
Aim: Alice wants to send 2 bits to Bob, but no way for classical communication (CC).

She can achieve aim if they share a Bell state to start with.



Alice's message	Act on A by a unitary op	Final state of AB	Bob's action
00	I	$\|\phi^+\rangle$	
10	Z	$\|\phi^-\rangle$	Bell mmt.
01	X	$\|\psi^+\rangle$	
11	XZ	$\|\psi^-\rangle$.	

Quantum Teleportation



Alice Bob

Aim: send $|\psi\rangle$ to Bob., but she cannot send C physically to Bob. # any q. channel between them. Only CC is allowed. ↳ classical communication

Protocol: Q teleportation

Initial state : CAB. CA (Alice). B (Bob).

$$|\psi\rangle_C \otimes |\phi^+\rangle_{AB} = (\alpha|0\rangle+\beta|1\rangle)_C \otimes \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)(\alpha|0\rangle+\beta|1\rangle) \leftarrow |\phi^+\rangle_{CA}|\psi\rangle_B$$

$$+\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)(\alpha|0\rangle+\beta|1\rangle) \leftarrow |\phi^-\rangle_{CA}(Z|\psi\rangle_B)$$

$$+\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)(\alpha|0\rangle+\beta|1\rangle) \leftarrow |\psi^+\rangle_{CA}(X|\psi\rangle_B)$$

$$+\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)(\alpha|0\rangle+\beta|1\rangle) \leftarrow |\psi^-\rangle_{CA}(XZ|\psi\rangle_B)$$

- Alice does a Bell mmt $\longrightarrow$ ij, $i,j \in \{0,1\}$
- CC: she sends ij to Bob.

Q: If $i=0, j=1$. What is post-mmt state of CAB?

$$|\psi^+\rangle_{CA} \otimes (X|\psi\rangle)_B$$

So Bob's state is $(X|\psi\rangle)_B$. He acts on this with

$$X(X|\psi\rangle)_B = X^2|\psi\rangle = |\psi\rangle.$$

If outcome ij, Bob needs to act on his final state with Z^iX^j because his final state is $X^jZ^i|\psi\rangle$ before his action. and

$$Z^iX^jX^jZ^i|\psi\rangle = |\psi\rangle.$$

Exercise Check diff. values of i,j.

Bob ends up with a copy of $|\psi\rangle$. Does this violate no-cloning thm? No! C is no longer in state $|\psi\rangle$.

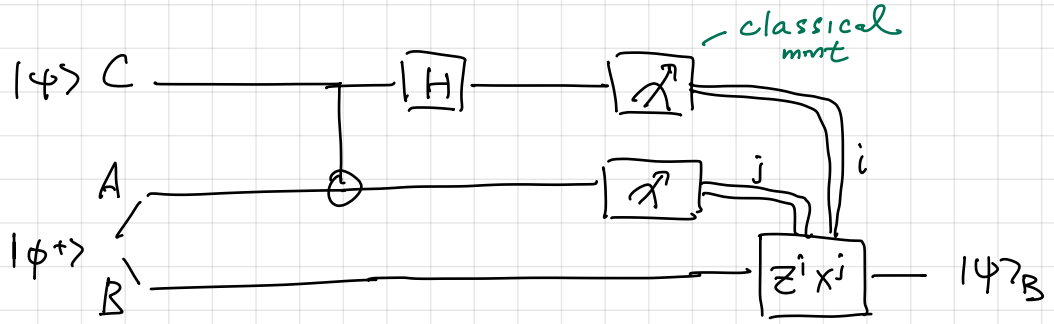
State transfer is unaffected by any physical process in the intervening space.

Example of no-signalling:

- Preparation 1 of B: part of a Bell state $|\psi^+_{AB}\rangle$.
- Prep 2: B's state after Alice's mmt.

$$|\psi\rangle, Z|\psi\rangle, X|\psi\rangle, XZ|\psi\rangle.$$

Bob cannot distinguish before prep. 1, 2 unless he knows Alice's outcome.



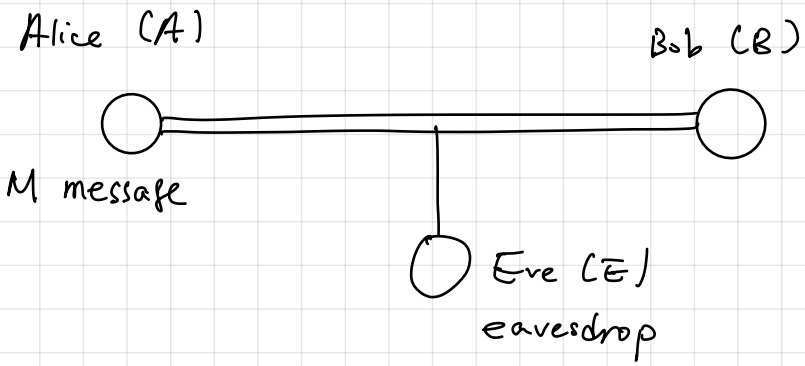
Quantum Cryptography

Disadvantage of encoding info in q. states

- Cannot be reliably identified
- Read / infer message, do a mmt
  - partial info (probabilistic)
  - state damaged

⇒ Advantage for q. cryptography.

One task for q. crypto: secure / private communication



Assume

(1) The channel is authenticated.

B can verify that msg. comes from A. E cannot modify the msg.

∃ a perfectly secure cryptosystem to do this.

One-time pad:

- A, B share a private (E does not know) key K (a sequence of random bits)
- K is created prior to this use

- K input of the msg. (M)
- $|K| = |M|$ (no. of bits), e.g. $K, M \in \{0,1\}^n$.

Steps of one-time pad:

1. A compute $C = M \oplus K$ encrypted msg.
2. Send C to Bob through the channel.
3. Bob does $C \oplus K = M \oplus K \oplus K = M$.

$n = 4$

$M = 0\ 1\ 1\ 0$

$K = 1\ 0\ 1\ 0$

$C = 1\ 1\ 0\ 0$

E knows C, but cannot infer M from it.

$$\text{Prob}(\text{any } K) = \frac{1}{2^n}.$$

(choice of key)

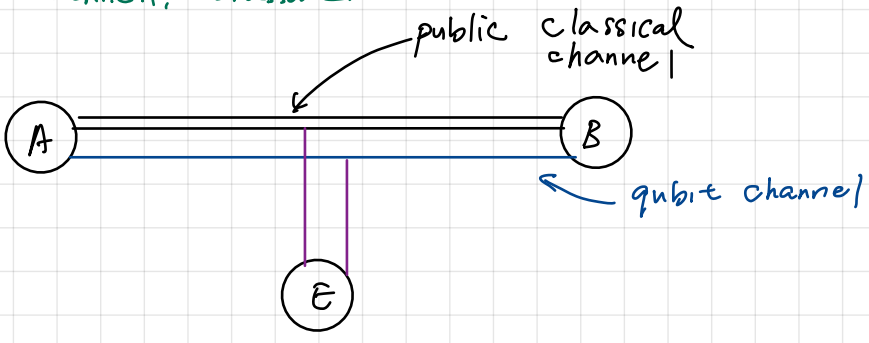
One-time pad is secure but inefficient. This is where QIC helps.

Quantum Key Distribution (QKD)

It allows Alice, Bob generate is secret key (which they can use for the one-time pad) without having to meet or to trust an intermediary.

Note QKD is not used to encode the msg itself, but to generate the key.

Protocols: BB84 (Bennett, Brassard), B91, E91, ...



Steps of BB84:

1. Alice generates 2 m-bit strings uniformly at random.

$$\underline{x} = x_1 x_2 \dots x_m \in \{0,1\}^m$$

$$y = y_1 y_2 \dots y_m \in \{0,1\}^m$$

and prepares m qubits in state

$$|\psi_{\underline{x}\underline{y}}\rangle = |\psi_{x_1 y_1}\rangle \dots |\psi_{x_m y_m}\rangle$$

with $|\psi_{00}\rangle = |0\rangle$, $|\psi_{11}\rangle = |1\rangle$, $|\psi_{01}\rangle = |+\rangle$, $|\psi_{10}\rangle = |-\rangle$.

If $y_i = 0$, then she encodes x_i in $\mathcal{B}_0 = \{|0\rangle, |1\rangle\}$

$y_i = 1$ $\mathcal{B}_1 = \{|+\rangle, |-\rangle\}$

then she sends $|\psi_{x_i y_i}\rangle$, $i = 1, \dots, m$ to Bob through m uses of qubit channel.

Bob receives m qubits. But they need not be in state $|\psi_{\underline{x}\underline{y}}\rangle$ due to
- Eve's tempering (mmt)
- Noise in channel ($|0\rangle \to |1\rangle$ bit flip)

} (*)

Case 1: Assume no (*).

2. Bob generates an m-bit string uniformly at random.

$$y' = y_1' \dots y_m' \in \{0,1\}^m$$

If $y_i' = 0$, then he measures i-th qubit in $\mathcal{B}_0 = \{|0\rangle, |1\rangle\}$.

$y_i' = 1$ $\mathcal{B}_1 = \{|+\rangle, |-\rangle\}$.

Let $\underline{x}' = x_1' \dots x_m' \in \{0,1\}^m$ ← outcomes of the m mmt

Equivalently, $H|\psi_{x_i y_i}\rangle \in \mathcal{B}_0$. then do mmt in $\mathcal{B}_0$.

Claim If $y_i' = y_i$, then $x_i' = x_i$.

Pf: Suppose $y_i' = y_i = 0$, then $|\psi_{x_i y_i}\rangle = |\psi_{x_i 0}\rangle \in \mathcal{B}_0 = \{|0\rangle, |1\rangle\}$.

Since $y_i' = 0$, mmt by Bob in $\mathcal{B}_0$ $\Rightarrow$ w.p. 1 he gets right outcome,

i.e. $x_i' = x_i$.

If $y_i' = y_i = 1$, $|\psi_{x_i 1}\rangle \in \mathcal{B}_1$. Bob: $H|\psi_{x_i 1}\rangle \in \mathcal{B}_0$ and mmt in $\mathcal{B}_0$

$\Rightarrow$ determines x_i' unambiguously, i.e. $x_i' = x_i$. □

3. Alice and Bob compare over the public classical channel y and y'. They discard all x_i, x_i' for which $y_i \neq y_i'$. They do not reveal the other x_i, x_i's. $\Rightarrow$ left with shorter strings $\tilde{x}, \tilde{x}'$

If we are in Case 1, then $\tilde{x} = \tilde{x}' \equiv$ shared secret key.

Example $n = 8$

Generates $x = 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0$

$y = 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1$

Prepare $|\psi_{xy}\rangle = |\psi_{x_1 y_1}\rangle \ldots |\psi_{x_8 y_8}\rangle$

Sends 8 qubits to Bob.

Bob generates $y' = 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0$

$x_1 = 0$, $y_1 = 1$ $\Rightarrow$ $|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$\begin{cases} y_1' = 0 \Rightarrow \text{mmt in } \mathcal{B}_0, \text{ outcome } 0,1 \text{ w.p. } \frac{1}{2} \text{ each.} \end{cases}$

Say $x_1' = 1$

$x_2 = 1$, $y_2 = 1$ $\Rightarrow$ $|\psi_{11}\rangle = |-\rangle$, $y_2' = 1$, $x_2' = 1$ w.p. 1

Suppose we get $x = \not{0}\ 1\ \not{1}\ 0\ \not{0}\ \not{0}\ \not{0}$

$y = 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1$

$y' = 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0$

$\Rightarrow \tilde{x} = \tilde{x}' = 1\ 1\ 0$

$x' = \not{1}\ \not{0}\ 1\ 0\ \not{0}\ \not{0}\ \not{1}$

Claim On average, the shared key $\sim \left[\frac{m}{2}\right]$ bits long.

Pf: $\mathbb{P}(y_i' = y_i) = \frac{1}{2} = \mathbb{P}(y_i' \neq y_i)$

$\Rightarrow \mathbb{P}(\text{discard } x_i, x_i') = \mathbb{P}(y_i \neq y_i') = \frac{1}{2}$ □

Case 2: (*) can happen ($\tilde{x}' \neq \tilde{x}$ in general)

4. Information Reconciliation (IR)

5. Privacy Amplification (PA)

$\Rightarrow$ Shared key where Eve has no info.

4. IR

For $\tilde{x} \neq \tilde{x}'$ in general,

- Alice, Bob want to find the Biterror rate (BER) of $\tilde{x}$, $\tilde{x}'$.

$$\text{BER} = \text{proportion of bits in } \tilde{x}' \text{ which do not match with corr. bits in } \tilde{x}.$$

- To do this, they publicly compare a sample of bits from their strings.

(A) — ✗ — ✗ ✗ — $\tilde{x}$

(B) — ✗ — ✗ ✗ — $\tilde{x}'$

- they determine BER in this sample.
- They discard <u>all</u> the bits x_i, x_i' in the samples.
- left with $\tilde{\tilde{x}}$, $\tilde{\tilde{x}}'$ shorter strings
- They <u>assume</u> that $\tilde{\tilde{x}}$, $\tilde{\tilde{x}}'$ have same BER as in the considered sample.
- They correct these <u>errors</u> (even though they do not know their locations) via IR $\rightsquigarrow$ sacrafice some of it $\rightarrow$ end up of 2 strings which match $x^* = \tilde{x}^*$

$\Rightarrow$ this leaks info to Eve.

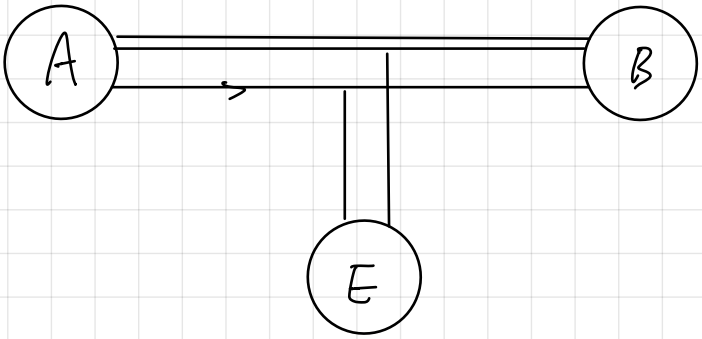
5. PA

From the estimated BER, they infer how info Eve has about final string.

Remarks: • BER depends on info Eve gets. More info ⇒ more disturbance (due to mmt) ⇒ higher BER.

- Key point: Alice using MUBs for encoding.
- Noise (in q. channel) also contributes to BER.
- But Alice, Bob can assume that all errors arose from Eve's tempering

BER ≥ proportion of bits about which Eve holds info.

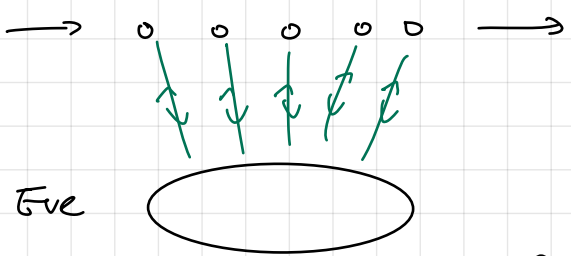


Eve's action:

1. Intercept + resend attack.:

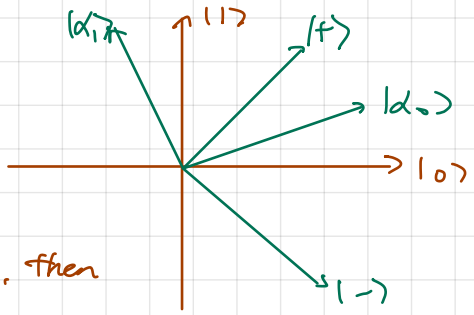
She intercepts the qubits one-by-one and does mmt and records (sends the post mmt states)

2.



Then mmt on ancilla → info about multiple qubits.

Example mmt of each qubit in the Breidbart basis $\{|\alpha_0\rangle, |\alpha_1\rangle\} \in \mathbb{C}^2$.



$$|\alpha_0\rangle = \cos\tfrac{\pi}{8}\,|0\rangle + \sin\tfrac{\pi}{8}\,|1\rangle$$

$$|\alpha_1\rangle = -\sin\tfrac{\pi}{8}\,|0\rangle + \cos\tfrac{\pi}{8}\,|1\rangle.$$

If a qubit sent by Alice is in $|0\rangle$ or $|+\rangle$, then

Eve's mmt outcome $\begin{cases} 0 & (\text{corrs. } |\alpha_0\rangle) \\ 1 & (\text{corrs } |\alpha_1\rangle) \end{cases}$

$$\text{Prob}(0) = \cos^2\tfrac{\pi}{8}, \qquad \text{Prob}(1) = \sin^2\left(\tfrac{\pi}{8}\right).$$

For each of the 4 encoding state $\begin{cases} |0\rangle, |+\rangle, & y_i = 0 \\ |1\rangle, |-\rangle, & y_i = 1 \end{cases}$

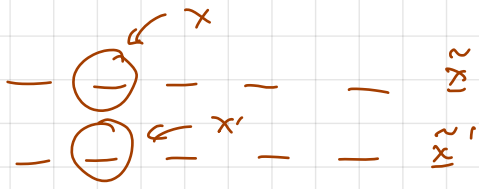
What is $\mathbb{P}rob\,(x' \neq x)$, $x \in \tilde{x}$, $x' \in \tilde{x}'$?

If A sent $|0\rangle$, we know B do mmt in $\mathcal{B}_0 = \{|0\rangle, |1\rangle\}$,

($\tilde{x}, \tilde{x}'$ consists of bits i for which $y_i' = y_i$) x, and $\tilde{x}$ are strings for which <u>mmt basis</u> of B = <u>encoding basis</u> of A.

For $x \in \tilde{x}$, $x' \in \tilde{x}'$, find prob. of error in B's inference.

Say $x = 0$, $x' = 1$



$$\mathbb{P}(X=0, x'=1) = \mathbb{P}(x'=1 \mid \text{A sent } |0\rangle)$$

$$= \mathbb{P}[x'=1 \mid \text{E sent } |\alpha_0\rangle) \cdot \mathbb{P}(\text{E gets } 0 \mid \text{A sent } |0\rangle)$$

$$+ \mathbb{P}(x'=1 \mid \text{E sent } |\alpha_1\rangle)\, \mathbb{P}(\text{E gets } 1 \mid \text{A sent } |1\rangle)$$

$$= |\langle 1|\alpha_0\rangle|^2\, |\langle 0|\alpha_0\rangle|^2 + |\langle 1|\alpha_1\rangle|^2\, |\langle \alpha_1|0\rangle|^2$$

$$= 2\sin^2\tfrac{\pi}{8}\cos^2\tfrac{\pi}{8} = \tfrac{1}{4}.$$

Similarly, $\mathbb{P}(X=0, x'=1) = 1/4$ when A sends $|+\rangle$.

$\mathbb{P}[X=1, x'=0) = 1/4$ when A sends $|1\rangle$ or $|-\rangle$.

$\Rightarrow \mathbb{P}[x' \neq x) = \frac{1}{4} \cdot (4 \cdot \frac{1}{4}) = \frac{1}{4}$.

$\Rightarrow$ Eve's action leads to BER $= 1/4$.

Now A and B estimated BER.

*Simple example of IR

In step 4, suppose A, B have $\tilde{x}, \tilde{x}'$ (7 bits). Estimated BER $= \frac{1}{7}$.

Write $\tilde{x} = \underline{a} = a_1 \dots a_7$, $\tilde{x}' = \underline{b} = b_1 \dots b_7$.

- Using classical channel they decide to act on $\underline{a}, \underline{b}$ by H (check matrix of the Hamming code $[7,4]$), where H is 3×7 matrix of 1's and 0's.

- A compute the syndrome

$$\underline{s}^A = H\underline{a}^T = H\begin{pmatrix} a_1 \\ \vdots \\ a_7 \end{pmatrix} = \begin{pmatrix} s_1^A \\ \vdots \\ s_3^A \end{pmatrix}, \quad s_i^A \in \{0,1\}.$$

She sends $s_i^A \xrightarrow[i=1,2,3]{} B$ via classical channel.

- B computes $\underline{s}^B = H\underline{b}^T = \begin{pmatrix} s_1^B \\ \vdots \\ s_3^B \end{pmatrix}$

$$\underline{s} = \underline{s}^B - \underline{s}^A = H(b-a)^T = H\underline{e}^T. \qquad (1)$$

where $w(\underline{e}) = 1$, Hamming weight of $\underline{e}$ = # 1's in it.

Fact: $\exists!$ bit string $\underline{v} \in \{0,1\}^7$ with $w(\underline{v}) \le 1$ s.t. $H\underline{v}^T = \underline{s}$ (2)

(1), (2) $\Rightarrow \underline{v} = \underline{e}$.

- B replaces $\underline{b}$ by $\underline{b} - \underline{e}$. Possible because B knows $\underline{s}$ and H. and $\underline{b} - \underline{e} = \underline{a}$, the shared key.

Simple example of PA

Suppose A, B end up with $\underline{a} = a_1 a_2 a_3 = \underline{b}$

Suppose E knows at most 1 bit.

let $\underline{c} = (a_1 \oplus a_3,\ a_2 \oplus a_3) \in \{0,1\}^2$

Claim E knows nothing about $\underline{c}$.

Possible values of $\underline{a}$: 000, 001, 010, 011, 100, ... $\} \underline{x} = \underline{x}^* = \underline{c}$

Corr. values of $\underline{c}$: 00, 11, 01, 10, ...

Suppose E knows $a_1 = 0$. This restricts E to these four choices but this yields no info.

$\Rightarrow \underline{c}$ private shared key.

Basic notions of classical computation and computational complexity

- Computational task:
  - input $\equiv$ bit string
  - input size $\equiv$ # bits

Example Given a n-bit string b $\forall n \in \mathbb{N}$, is b prime?

- Output $\equiv$ another bit string
- If output is $\begin{cases} 0 \\ 1 \end{cases}$, the task is a decision problem.
- $B = B_1 = \{0,1\}$ binary alphabet

  $B_n = \{0,1\}^n$

  $B^* = \bigcup_{n=1}^{\infty} B_n$
- Language L is $L \subset B^*$
- A decision problem corr. to the recognition of a language. of those binary string when used as input $\rightarrow$ yes / accept / 0 as answer.

Example (Primality testing)

$L \equiv$ subset of all bit strings that represents numbers in binary

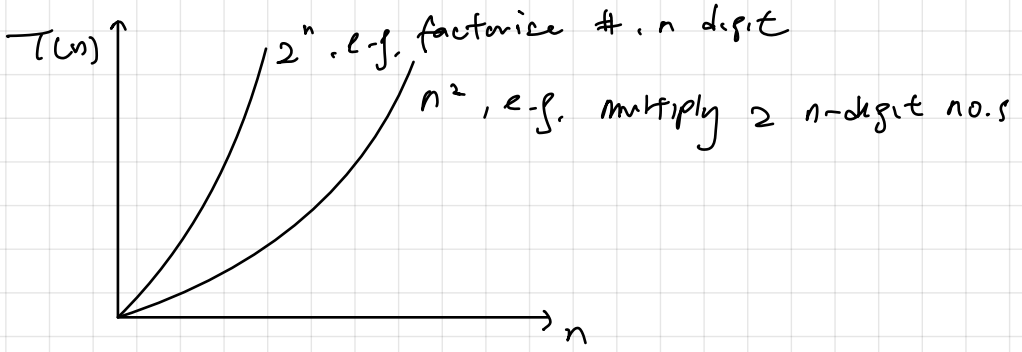
More generally, output is of length $n > 1$..

e.g. FACTOR (x), output y

To solve a problem, we use an algo : precise set of instructions

Efficiency of an algo :

- An algo is efficient if # of elementary steps (runtime $T(n)$) needed to execute it scales no faster than polynomially in n (input size).



Model of classical computation

- Turing machine
- Cellular automata
- Circuit model (gate array)

Circuit model

- Input string $x = b_1 \dots b_n \in \{0,1\}^n$. is extended to $b_1 \dots b_n \underbrace{0 \dots 0}_{\text{extra workspace}}$
- Computational step : application of designated Boolean gates $f : B_n \to B_n$ $\longrightarrow$ updated string

Rmk These fixed operations/gates should not become more complicated as n increase.

- Universal set of gates {AND, NOT, OR} : any Boolean f^n (gate) can be constructed from these.
- Output : Value of some designated bits after the final step.
- Circuit : For each input size n, you have a circuit $C_n \equiv$ a prescribed seq. of computational steps

Rmk C_n only depend on n and not on the particular input

$C_n \equiv$ also. $\equiv$ computer program.

Randomised Classical computation

Input string extended to

$$b_1 \dots b_n \; r_1 \dots r_k \; 0 \dots 0$$

input — random bits (chosen uniformly at random)

- If computation is repeated with same $b_1 \dots b_n$, then $r_1 \dots r_k$ generally different $\Rightarrow$ get diff. output.

$$\text{Prob(any particular output)} \sim \frac{a}{2^k}$$

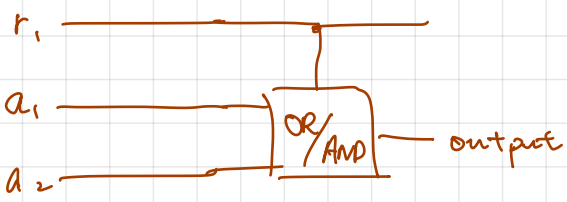
a — no. of strings $r_1 \dots r_k$ giving the output

Require

$$\text{Prob(output correct)} > 1 - \delta$$

for some chosen δ.

Example



Time-complexity of algo.

In a circuit model,

$T(n)$ = total # of gates used in algo.

Q: Is $T(n) < cn^k$ $\forall n$ large enough for some $c>0$? Does $T(n)$ grow faster than polynomial in n?

If faster, called exponential, e.g. 2^n, $2^{\sqrt{n}}$, $n^{\log n}$.

If satisfy, then it is called poly(n) / poly-time algo.

Digression (Notation)

- For a +ve fn $T(n)$, we write $T(n) = O(n)$ if $\exists n_0, c > 0$ s.t. $T(n) \leq cf(n)$ $\forall n \geq n_0$. ("T grows no faster than f")
- $T(n) = O(\text{poly}(n))$ if $T(n) = O(n^k)$ for some $k > 0$.

Time-complexity classes

P (poly-time): class of languages where membership can be decided (w.p.1) by an poly(n) algo. (Class of problems which can be solved on a classical computer with a deterministic algo. in poly time)

BPP (bounded error probabilistic, poly-time): Class of problems solvable in poly time via a randomised algo w.p. $\geq 2/3$.

- Threshold $2/3$ can be increased to $1-\varepsilon$ $\forall$ $0 < \varepsilon < 1/2$

If $\exists$ poly time algo that succeeds w.p. $(\frac{1}{2}+\delta)$ for any chosen $\delta > 0$, then $\exists$ a poly-time algo that succeeds w.p. $(1-\varepsilon)$ $\forall 0 < \varepsilon < 1/2$.

Suppose repeat the algo, say K times, which gives correct answer w.p. $(\frac{1}{2}+\delta)$. Reasonable strategy: take majority vote.

Chernoff bound tells you how well this strategy works.

Thm (Chernoff bound) Let $X_1 \dots X_n$ discrete iid r.v. takes value 1 w.p. $(\frac{1}{2}+\delta)$, 0 w.p. $(\frac{1}{2}-\delta)$, i.e. $X_i \sim \text{Bern}(\frac{1}{2}+\delta)$, then

$$\mathbb{P}\left(\sum_{i=1}^{n} X_i \leq n/2\right) \leq e^{-2\delta^2 n}.$$

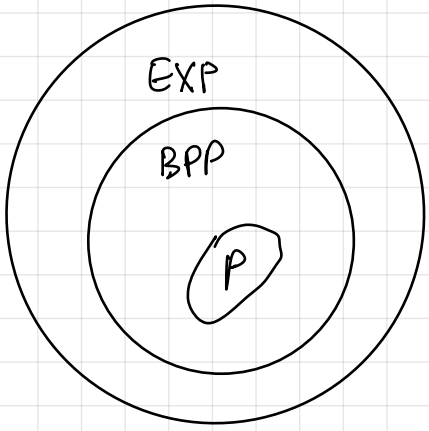
- Interpret value 1 correct result of a decision problem
  0 wrong
- Value of $\sum X_i$ = # correct answers in n trials.

Do K trials.

$$\begin{aligned}
&\mathbb{P}(\text{majority vote gives correct answer}) \\
&= \mathbb{P}\left(\sum_{i=1}^{K} X_i > K/2\right) \\
&\geq 1 - e^{-2\delta^2 K}
\end{aligned}$$

$\Rightarrow$ Prob. of making an error by taking majority vote decreases exponentially in K.

- In BPP, we choose $\frac{1}{2}+\delta = \frac{2}{3}$.
- Choose K a few hundred, then Prob(error) $\sim 10^{-20}$.

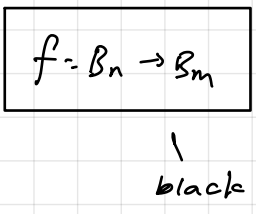


e.g. FACTOR(N, M)
Given integers N, M (in binary digit), $M < N$, decide if N has a non-trivial factor $< M$.

Best known algo: $T(n) = \exp O(n^{1/3}(\log n)^{2/3})$

Black box / Oracle promise problems

Instead of input bit string of length n, we are given $f : B_n \to B_m$.



We can query the oracle by giving it inputs and processing the outputs.

Start: f unknown. you are given a promise about it.

Task: determine / find some desired property of f by querying the oracle the least # of times.

Consider oracle as another gate.

Query complexity: no. of times of the oracle is used (as a f^n of its size)

Examples of Black box promise problem

1. Balanced v.s. constant problem

Input: BB for $f : B_n \to B$ (output: 1 bit)

Promise: f is either const. ($f(x) = 0 \ \forall x$ or $f(x) = 1 \ \forall x$, $x \in B_n$) or balanced ($f(x) = 0/1$ for exactly half the no. of strings, i.e. 2^{n-1} 0's and 1's).

Problem Find if f const. or bal., with some desired prob. (e.g. 0.99)

2. Search

Input : $f : B_n \to B$

Promise : $\exists$ unique $x \in B_n$ s.t. $f(x) = 1$ ($= 0$ o/w)

Problem : Find this special x.

3. Periodicity

Input : $f : \mathbb{Z}_n \to \mathbb{Z}_n$. $\mathbb{Z}_n = \{0, \ldots, n-1\}$

Promise : f periodic with period r . i.e. $f(x+r) = f(x)$ $\forall x$ (addition mod n)

Problem : find r.

Circuit model of quantum computation

	Classical	Quantum
Input	$b_1 \ldots b_n 0 \ldots 0$	$\lvert b_1\rangle \ldots \lvert b_n\rangle \lvert 0\rangle \ldots \lvert 0\rangle$, $b_i \in \{0,1\}$, $\lvert b_i\rangle \in \mathbb{C}^2$

[e.g. $H\lvert 0\rangle = \lvert + \rangle$. mmt in $\{0,1\} \Rightarrow$ outcomes 0, 1 w.p. $1/2$.]

Computational step : application of a q. gate to a prescribed choice of qubits. These gates make up a q. circuit. (C_n).

Output : The result of doing a mmt. on some specified sets of qubits. Mmt is done right at the end.

Quantum computation is defined by

$(C_1, C_2, \ldots, C_n, \ldots)$ family of circuits

Important fact: Q gates reversible, but not for classical one in general.,

e.g. x AND $y = 0$, $xy \in \{01, 10, 00\}$.

$$\text{NOT}(b) \begin{cases} = 0 & \Leftrightarrow b = 1 \\ = 1 & \Leftrightarrow b = 0 \end{cases}$$

Poly-time quantum computations and BQP

BQP (bounded-error quantum poly-time) : class of problems that can be solved in poly-time with some fixed accuracy on a q. computer.

For each input size n, we have a circuit C_n,

$$|C_n| = \text{no. of gates in } C_n = O(\text{poly}(n)).$$

w.p. $\geq 2/3$.

Claim BPP $\subseteq$ BQP.

Reason : Any poly(n) classical circuit can be replaced by an eqv. classical circuit with reversible gates. and this is also a q. circuit albeit consisting of gates which preserve the comp. basis as a set.

Q: Is BQP $\supset$ BPP ? This is open question.

Evidence : FACTOR$(N, N) \in$ BQP . not known if is in BPP.

Black-box promise problems (in q. comp^n)

Cl: $(f : \mathbb{B}_m \to \mathbb{B}_n)$

Quantum analogue : unitary op. U_f which the q. analogue of a reversible version of f. $(\tilde{f})$.

Note Any $f : B_m \to B_n$ can be expressed equ-ly in a reversible form.

$$\tilde{f} : B_{m+n} \to B_{m+n}.$$

For $b \in B_m$, $c \in B_n$,

$$\tilde{f}(b,c) := (b, c \oplus f(b))$$

($\oplus$: + mod 2)

If we can compute f, do $\oplus$ then can we can evaluate $\tilde{f}$.

Conversely, set $c = 0 \ldots 0$ and read out last n bits of $\tilde{f}$, then

$$\tilde{f}(b,c) = (b, f(b))$$

$\tilde{f}$ reversible:

$$\tilde{f}(\tilde{f}(b,c)) = \tilde{f}(b, c \oplus f(b))$$
$$= (b, c \oplus f(b) \oplus f(b)) = (b,c).$$

$\Rightarrow$ Any classical algo using oracle f can equally well be done using an oracle for $\tilde{f}$.

Quantum oracle for $f : B_m \to B_n$ ($\tilde{f} : B_{m+n} \to B_{m+n}$)

$$U_f |x\rangle|y\rangle = |x\rangle |y \oplus f(x)\rangle.$$

($|x\rangle$: m qubit, $|y\rangle$: n qubit)

mimics action of $\tilde{f}$.

$|x\rangle, |y\rangle$: comp basis states, $x \in \{0,1\}^m$, $y \in \{0,1\}^n$

For $|\psi\rangle \in (\mathbb{C}^2)^{\otimes(m+n)}$ has onb $\{|x\rangle \otimes |y\rangle\}_{x \in B_m, y \in B_n}$

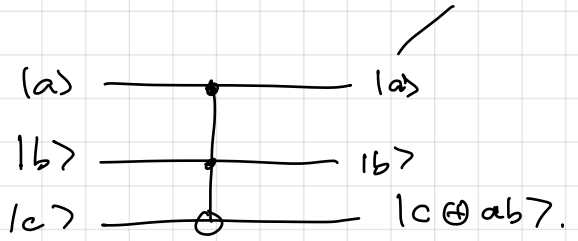
$$|\psi\rangle = \sum_{\substack{x \in B_m \\ y \in B_n}} c_{xy} |x\rangle|y\rangle$$

$$\Rightarrow U|\psi\rangle = \sum c_{xy} U_f |x\rangle|y\rangle$$
$$= \sum c_{xy} |x\rangle |y \oplus f(x)\rangle.$$

We call $|x\rangle$: input register, $|y\rangle$: output register.

In classical, any problem in $P \Leftrightarrow \exists$ poly-time algo using gates $\{AND, NOT\}$, with $X \cup Y = (X^c \cap Y^c)^c$.

In quantum, q version of $\{AND, NOT\} \rightarrow \{Toffoli, X\}$.



It is important to have $|x\rangle$ at the output, since classically, no bits are lost.

Note $\tilde{f}$ is permutation of $(m+n)$-bit string, so U_f corresponds to a classical computation will be a perm. matrix, and randomness in BPP generated by superpositions and mmts

Computation via q. parallelism

U_f can act on a superposition of input registers

$$|\psi_m\rangle = \frac{1}{\sqrt{2^m}} \sum_{x \in B_m} |x\rangle$$ (equal superposition state).

↓ input register

$$U_f |\psi_m\rangle |y\rangle = \frac{1}{\sqrt{2^m}} U_f \sum_{x \in B_m} |x\rangle|y\rangle$$

$$= \frac{1}{\sqrt{2^m}} \sum_{x \in B_m} U_f |x\rangle|y\rangle$$

$$= \frac{1}{\sqrt{2^m}} \sum_{x \in B_m} |x\rangle |y \oplus f(x)\rangle \equiv |\psi_f\rangle.$$

$|\psi_f\rangle$ generated by a single use of U_f depends on $f(x)$ $\forall x \in B_m$. This is computation in q. parallelism.

By further q. processing of $|\psi_f\rangle$ (acting of other gates on it & mmt) can get global info about f with just 1 use of U_f.

Contrast this with classical case: 1 use of f gives output corrs to 1 input.

Q: How do you create $|\psi_m\rangle$?

$$H^{\otimes m}|0\rangle^{\otimes m} = (H|0\rangle)^{\otimes m}$$
$$= |+\rangle^{\otimes m}$$
$$= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \ldots \quad (m \text{ times})$$
$$= \frac{1}{\sqrt{2^m}} \sum_{x \in \mathbb{B}_m} |x\rangle$$

Rmk Created a superposition of 2^m terms with only a linear no. of application of H $(H^{\otimes m})$.

Approximately universal set of q. gates

C1 case: {AND, NOT} universal set

Q case: q. gates are unitary operators.

$U = e^{i\theta A}$, A self-adjoint, $\theta \in \mathbb{R}$.

U parameterised by a cts param. θ. $\Rightarrow$ no finite set of q. gates can generate all other q. gates exactly, even with very large circuits.

But $\exists$ approximately universal sets of q. gates

• The notion of closeness of 2 unitary ops. U, V:

We say $\|U - V\| \leq \varepsilon$, $\varepsilon \in [0,1]$ if

operator norm

$$\max_{\substack{|\psi\rangle \\ \langle\psi|\psi\rangle = 1}} \|U|\psi\rangle - V|\psi\rangle\| \leq \varepsilon.$$

A set of q. gates ($\mathcal{G}$) (acting on qubits) is approximately universal if $\forall$ unitary W acting on any no. of qubits, and $\forall \varepsilon \in [0,1]$, $\exists$ a circuit C composed of gates from $\mathcal{G}$, whose overall unitary action satisfies

$$\|W - C\| \leq \varepsilon.$$

• Generally $|C| = O(\exp(n))$, n = # qubits on which W acts,
(but for QFT. $|C| = O(\text{poly}(n))$.)

Solovay - Kitaev Thm

Roughly, if $\mathcal{G}$ is an approx. uni. set of q. gates, let

$$\|W - \underbrace{g_{i_1} g_{i_2} \cdots g_{i_k}}_{C}\| \leq \varepsilon, \quad g_{i_j} \in \mathcal{G}.$$

with $|C| = k$, then $k \sim (\log 1/\varepsilon)^c$, $c \approx 2$ const.

Suppose $\varepsilon \approx 2^{-12}$, then $k \sim 12$ gates.

The Deutsch - Jozsa (DJ) algo.

• Example of algo showing exponential speed up over cl. one.

Problem Bal. vs. cnst

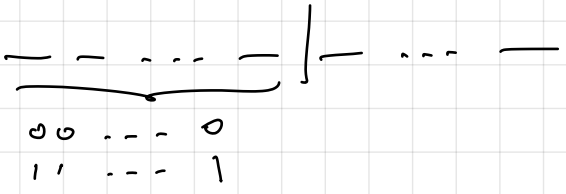
Input Oracle for $f: B_n \to B$

Promise f cnst or bal.

Task: find if f bal. or const.

Classically, one needs $(2^{n-1}+1)$ queries in the worst case scenarios.

- Inspect outputs corr. to first 2^{n-1} inputs
- If o/p same for all 2^{n-1} i/p, check next o/p. $\Rightarrow$ $(2^{n-1}+1)$-th o/p
  If same $\Rightarrow$ const.
  else $\Rightarrow$ bal.



$\Rightarrow$ In worst case scenarios (WCS), checking $2^{n-1}+1$ suffices.

Necessity (Proof) of $2^{n-1}+1$ queries.

Adversary (A) is in control of f (oracle)

- Suppose we have a deterministic cl. algo that solves the problem by making $K \leq 2^{n-1}$ queries
- When the algo is applied, A hasn't yet chosen f.
- A simply output 0's to all queries.
- At the end of K queries, f" f has been fixed on K inputs.

But if $K \leq 2^{n-1}$, then A still has the freedom to choose the next output so as to contradict the outcome of the algo

$\Rightarrow 2^{n-1}+1$ queries are necessary in WCS.

In Quantum, DJ also has query complexity = 1.

Q. oracle $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, $x \in B_n$, $y \in B$

$(n+1)$ qubit states

(i) Initialise all qubits in state $|0\rangle$.

$$|x\rangle|y\rangle = |0\rangle^{\otimes n}|0\rangle.$$

(ii) $\left(H^{\otimes n} \otimes HX\right)\left(|0\rangle^{\otimes n}|0\rangle\right) = |+\rangle^{\otimes n} \otimes |-\rangle.$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |x\rangle \otimes |-\rangle. \equiv |A\rangle \qquad (1).$$

(iii) $U_f|A\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} U_f|x\rangle|-\rangle$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} \left[U_f|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right]$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in B_n} \underbrace{\left(|x\rangle|f(x)\rangle - |x\rangle|f(x)^c\rangle \right)}_{|x\rangle\left(|f(x)\rangle - |f(x)^c\rangle\right)},$$

where $f(x)^c = f(x) \oplus 1$.

$$[\quad] = \underbrace{U_f|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{= (-1)^{f(x)}|x\rangle|-\rangle.} = \begin{cases} |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |x\rangle|-\rangle & \text{if } f(x) = 0 \\ -|x\rangle|-\rangle & \text{if } f(x) = 1 \end{cases}$$

$$\Rightarrow U_f|A\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x \in B_n} (-1)^{f(x)}|x\rangle \right)|-\rangle \qquad (2)$$

Note: First n qubits uncorrelated with last qubit

(iv) Discard last qubit. Left with n-qubit state

$$|f\rangle := \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} (-1)^{f(x)}|x\rangle \qquad (3)$$

Q: what does $|f\rangle$ look like if (a) f const, (b) f bal.?

(a) If f const., $|f\rangle = \pm \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |x\rangle$. ($\because f(x)$ same sign $\forall x \in B_n$)

$$= \pm H^{\otimes n} |0\rangle^{\otimes n} \quad (4)$$

If we apply $H^{\otimes n}$ on $|f\rangle$.

$$H^{\otimes n} |f\rangle = \pm |0\rangle^{\otimes n} \quad (\because H^2 = I) \quad (5)$$

(b) If f bal. $|f\rangle$ has equal no. of $+$, $-$ signs at unknown locations.

Q: How do you detect such a state?

A: Let

$$|\varphi_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x' \in B_n} |x'\rangle \quad (6)$$

Take inner product of $|\varphi_n\rangle$ and $|f\rangle$

$$\langle \varphi_n | f \rangle = \frac{1}{2^n} \sum_{x, x' \in B_n} (-1)^{f(x)} \underbrace{\langle x' | x \rangle}_{= \delta_{xx'}}$$

$$= \frac{1}{2^n} \sum_{x} (-1)^{f(x)} = 0$$

$\Rightarrow$ If f balanced, then $|f\rangle \perp |\varphi_n\rangle$

Write $H_n = H^{\otimes n}$. $|f\rangle$ n-qubit state

- $H_n |f\rangle \perp H_n |\varphi_n\rangle \Rightarrow H_n |f\rangle \perp |0\rangle^{\otimes n}$.

$$\Rightarrow H_n |f\rangle = \sum_{x \in B_n} C_x |x\rangle, \quad (7)$$

with $C_{00\ldots0} = 0$, i.e. $x \neq 00\ldots0$. : if f bal.

(v) Apply H_n on $|f\rangle$.

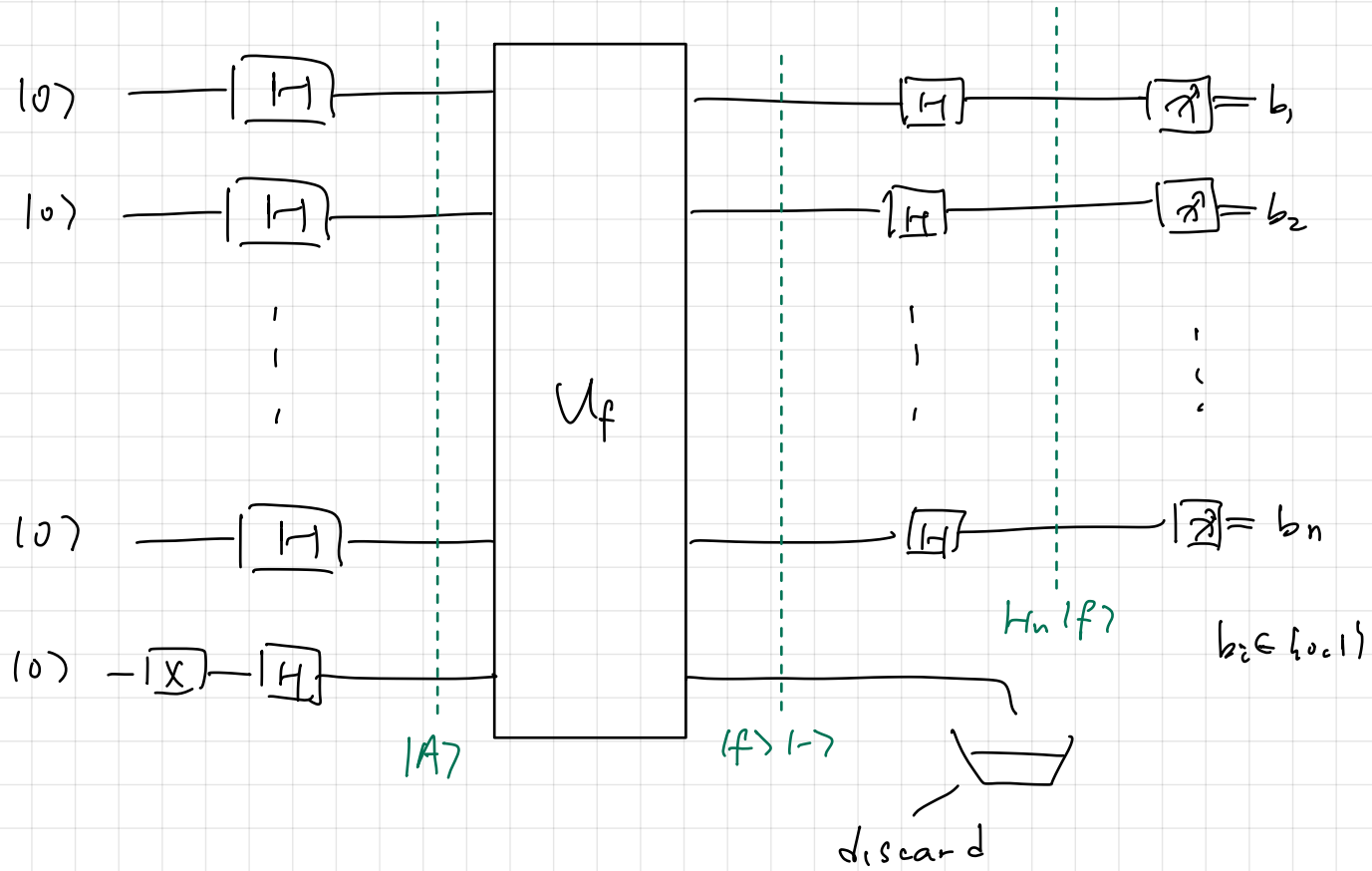
(vi) msmt on these n qubits in comp. basis

- If $|f\rangle$ const. outcome $00\ldots0 \Rightarrow f$ const. w.p.1
- " bal, msmt outcome not all zeros $\Rightarrow f$ bal. w.p.1.

# of query = 1. 1 use of U_f.

+ $(3n+2)$ operations :

- $(n+1)$ H's and 1 X
- n H's on $|f\rangle$
- n single qubit mmt.



Q : What if classically one allow bounded error ?

In Q case, DJ work in 1 query. but, there is a classical bounded error also. that solves the problem with only a const. no. of queries (depend only with ε, not on n)

$$O(\log 1/\varepsilon) \quad \forall n$$

⇒ Exponential speed-up of q. over classical is lost.

Randomised classical algo.

- Choose k bits $x_1 \dots x_k$ uniformly at random.
- Evaluate $f(x_1), f(x_2) \dots f(x_k)$.

(a) If get $f(x_i) = 0 \ \forall i = 1, \dots, k$ or $f(x_i) = 1 \ \forall i = 1, \dots, k$.
infer that f const.

(b) else, f bal.

In case (b), no error.

In case (a), could be an error.

$$p_e = \mathbb{P}(\text{infer } f \text{ const} \mid f \text{ bal}) = \frac{1}{2^{k-1}}$$

Then $p_e < \varepsilon$ if $\frac{1}{2^{k-1}} < \varepsilon \Rightarrow k > \log \frac{1}{\varepsilon} + 1$

$\rightarrow k = O(\log \frac{1}{\varepsilon})$ suffices to guarantee $p_e < \varepsilon \ \forall n$.

Is there a BB promise problem where you do get a q. advantage even when over bounded error classical algo.?

Simon's Problem / Algo

Input oracle $f : B_n \rightarrow B_n$

Promise $f \begin{cases} 1\text{-}1 \ f^n & (f(x) = f(y) \Leftrightarrow x = y) \\ 2\text{-}1 \ f^n & (\exists x \neq x' \text{ s.t. } f(x) = f(x') = f(y)) \end{cases}$

Equivalently, $f(x) = f(y) \Leftrightarrow y = x \oplus \xi \Leftrightarrow x \oplus y = \xi$.

$$\xi = 00\dots0 \Rightarrow 1\text{-}1$$

$$\xi \neq 0\dots0 \Rightarrow 2\text{-}1$$

Problem Determine whether f is $1\text{-}1$ ($\xi = 00\dots0$) or $2\text{-}1$.
and in $2\text{-}1$ case, find ξ.

Note $f(x \oplus \xi) = f(x)$, $f(x \oplus \xi \oplus \xi) = f(x)$ $\Rightarrow f$ has period ξ.

Query complexity: Q: $O(n)$, C: $O(\exp(n))$.

Example of f s.t. $\forall x, y \in B_n$, $\exists!$ $\xi \neq 0\ldots0$ for which $f(x) = f(y)$.

$n=3$ $x = 000, 001, 010, 011, 100, 101, 110, 111$

$f(x) = 101, 010, 000, 110, 000, 110, 101, 010$

$x \oplus y = 000 \oplus 110 = 110$

$x \oplus y = 010 \oplus 100 = 110$ $\Rightarrow \xi = 110$.

Q: Why hard classically?

Need to find 2 diff input x, y s.t. $f(x) = f(y)$, but no structure of f is known.

Suppose make $2^{n/4}$ queries, $X_1 \ldots X_{2^{n/4}}$, $X_i \in B_n$

The # of pairs of queries is

$$\binom{2^{n/4}}{2} < (2^{n/4})^2 \qquad \left(\because \binom{k}{2} = \frac{k(k-1)}{2} < k^2\right)$$

Total no. of pairs of values of $f(x)$ is 2^{n-1} ($\because$ all $f(x)$ values appear in pairs).

$$\text{Prob}(\text{pick a pair of input } (x,y) \text{ s.t. } f(x) = f(y)) = \frac{1}{2^{n-1}}$$

$\Rightarrow$ Total prob. of successfully detecting $\xi \neq 0$ (ie. f is 2-1)

$$< (2^{n/4})^2 \cdot \frac{1}{2^{n-1}} = 2 \cdot 2^{-n/2}$$

Even as many as $2^{n/4}$ queries cannot help you detect that $\xi \neq 0$ with better than exponentially small prob.

$\Rightarrow$ It cannot form the basis of any bounded error algo.

The Quantum Fourier Transform

- Generalisation of Hadamard op. (H) $H|0\rangle = |+\rangle$ etc.

Def^n. Let $\mathcal{H}_N$ be N-dim Hilbert space.

- $\mathcal{B}_N = \{|0\rangle, |1\rangle, \ldots, |N\rangle\}$. i.e. elts labelled by elt of $\mathbb{Z}_N$.

Def^n $QFT_N \equiv$ QFT modulo N. $\equiv$ QFT.

- Unitary op. acts on $\mathcal{H}_N$: $\forall |x\rangle \in \mathcal{B}_N$.

$$QFT_N |x\rangle = \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}_N} e^{i2\pi xy/N} |y\rangle. \quad (1)$$

$$= \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}_N} \omega^{xy} |y\rangle, \quad (2)$$

with $\omega = e^{2\pi i/N}$.

If $N=2$, $\mathcal{H}_N \cong \mathbb{C}^2$, onb $\{|0\rangle, |1\rangle\}$,

$|x\rangle = |0\rangle \Rightarrow QFT|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle.$

$|x\rangle = |1\rangle \Rightarrow QFT|1\rangle = |-\rangle.$

So

$$\boxed{QFT_2 = H}$$

$QFT \in M_N(\mathbb{C})$.

$j,k \in \{0, \ldots, N-1\}$

$$(QFT)_{jk} = \langle j | QFT | k \rangle$$

$$= \frac{1}{\sqrt{N}} \langle j | \sum_{m \in \mathbb{Z}_N} e^{2\pi i km/N} |m\rangle$$

$$= \frac{1}{\sqrt{N}} e^{2\pi i kj/N} = \frac{1}{\sqrt{N}} \omega^{jk}$$

$$\Rightarrow \quad \boxed{(QFT)_{jk} = \frac{1}{\sqrt{N}} \omega^{jk}} \quad (3)$$

Elt of j-th row, $\forall j \in \{0, \ldots, N-1\}$.

$$\frac{1}{\sqrt{N}}, \frac{\omega^j}{\sqrt{N}}, \ldots, \frac{(\omega^j)^{N-1}}{\sqrt{N}},$$

Denote

$$S_j = \sum_{k \in \mathbb{Z}_N} (\omega^j)^k \tag{4}$$

Recall

$$S = \sum_{k=0}^{N-1} \alpha^k = \begin{cases} N & \alpha = 1 \\ \frac{1-\alpha^N}{1-\alpha} & \alpha \neq 1 \end{cases} \tag{5}$$

Set $\alpha = \omega^j = e^{2\pi i j/N}$. (6)

$$\Rightarrow S_j = \begin{cases} N & \omega^j = 1 \\ \frac{1-(\omega^j)^N}{1-\omega^j} & \omega^j \neq 1 \end{cases}$$

$\omega^j = 1 \Leftrightarrow j = 0$, $\because \omega^j = 1 \Leftrightarrow j \equiv 0 \mod N$, but $j \in \{0, \dots, N-1\} \Rightarrow j = 0$.

$$\Rightarrow S_j = \begin{cases} N & j = 0 \\ 0 & j \neq 0 \end{cases} \tag{7}$$

If $j \neq 0$, $S_j = \frac{1-(\omega^j)^N}{1-\omega^j} = 0$.

Using (7) can prove QFT <u>unitary</u>

$$QFT^\dagger \, QFT = I = QFT \cdot QFT^\dagger. \tag{8}$$

<u>Periodicity Determination</u>

<u>Problem</u>: Given input blackbox for a fn $f: \mathbb{Z}_N \to \mathbb{Z}_M$.

<u>Promise</u>: f periodic with period r, ie. r is smallest in $\mathbb{Z}_N$ s.t. $f(x+r) = f(x)$. And assume f 1-1 within each period, ie. $\forall x_1 \neq x_2$, $x_1, x_2 \in \{0, 1, \dots, r-1\}$, $f(x_1) \neq f(x_2)$.

<u>Task</u>: Find a method of determining r with some desired accuracy indpt. of N.

$$O(2^{\log N^{1/2}}) = O(\exp(\log N))$$

In cl., can show $O(N^{1/2})$ queries nec. and suff. (n.a.s.c.)

$\Rightarrow$ Not bounded by poly$(\log(N))$.

In q. case, $O(\log\log n)$ queries suffices, and poly$(\log N)$ further processing steps. $\Rightarrow$ Q algo is exponentially faster than cl. one.

Q. algo for periodicity determination

- Construct $|\psi_N\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle \in \mathcal{H}_N$ (uniform superposition state)
- Consider a state

$$|\psi_N\rangle |0\rangle \in \mathcal{H}_N \otimes \mathcal{H}_N.$$

- $U_f |\psi_N\rangle |0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} U_f |x\rangle |0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle |f(x)\rangle$

Since r period of f, $r | N$. $A = N/r$ is the # periods.

- Do msmt on 2nd register in basis $\mathcal{B}_N$ $\{|0\rangle, \ldots, |N-1\rangle\}$.
- Let outcome be $y = f(x_0)$. $x_0 \in \{0, 1, 2, \ldots, r-1\}$ is the lowest value of x s.t. $f(x) = y$

$y = f(x_0)$

If has period r, $y = f(x_0) = f(x_0+r) = \ldots = f(x_0 + (A-1)r)$

Stop at $x_0 + (A+1)r$, since $x_0 + Ar = x_0 + N = x_0$.

- Prob of outcome $y = f(x_0)$: $p(y)$

Terms contributing to this outcome is

$$\frac{1}{\sqrt{N}} \left(\sum_{j=0}^{A-1} |x_0 + jr\rangle \right) |y\rangle.$$

By extended Born rule,

$$p(y) = \left\| \frac{1}{\sqrt{N}} \sum_{j=0}^{A-1} |x_0 + jr\rangle \right\|^2$$

$$= \frac{1}{N} \sum_{j,j'} \underbrace{\langle x_0 + j'r | x_0 + jr \rangle}_{\delta_{jj'}}$$

$$= \frac{1}{N} \sum_{j=0}^{A-1} 1$$

$$= \frac{A}{N} = \frac{1}{r}.$$

So $P(y = f(x_0)) = 1/r \quad \forall x_0 \in \{0, 1, \ldots, r-1\}$.

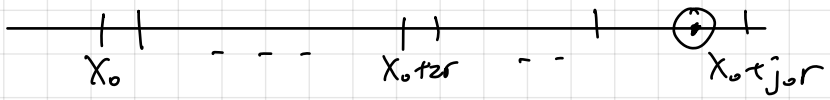
- Post mmt state of 1st register

$$|\text{per}\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{A-1} |x_0 + jr\rangle / \sqrt{p(y)}$$

$$\Rightarrow \boxed{|\text{per}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle.}$$

- Mmt on 1st register in basis B_N. Say outcome is $(x_0 + j_0 r)$ for some $j_0 \in \{0, 1, \ldots, A-1\}$. w.p. $1/A$.

Thus we have a random period j_0 th period and a random # in that period



This gives no info about r.

(outcomes of mmt) labels of kets

Resolution of the problem

- Instead of measuring $|per\rangle$, act on it using QFT ($= QFT_N$):

$\forall |x\rangle \in \mathcal{B}_N$,

$$QFT\,|x\rangle = \sum_{y \in \mathbb{Z}_N} \omega^{xy} |y\rangle. \quad , \quad \omega = e^{2\pi i/N}.$$

$$QFT\,|per\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} QFT\,|x_0 + jr\rangle.$$

$$= \frac{1}{\sqrt{NA}} \sum_{j=0}^{A-1} \sum_{y=0}^{N-1} \omega^{(x_0+jr)y} |y\rangle.$$

$$= \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} \omega^{x_0 y} \underbrace{\left(\sum_{j=0}^{A-1} (\omega^{ry})^j \right)}_{S} |y\rangle$$

$$S = \sum_{j=0}^{A-1} \omega^{jry} = \begin{cases} A & \alpha = \omega^{ry} = 1 \\ \frac{1-\alpha^A}{1-\alpha} & \alpha \neq 1. \end{cases}$$

Note $\alpha = \omega^{ry} = e^{2\pi i y/A}$, and $\alpha = 1$ if $y = kA$, $k = 0, 1, \ldots, r-1$.

If $\alpha \neq 1$, then $y \neq kA$ for some $k \in \{0, 1, \ldots, r-1\}$.

$$\alpha^A = e^{2\pi i y} = 1 \quad \Rightarrow \quad \frac{1-\alpha^A}{1-\alpha} = 0$$

So

$$S = \sum_{j=0}^{A-1} \omega^{jry} = \begin{cases} A & y = kA, \ 0 \leq k \leq r-1 \\ 0 & o/w. \end{cases}$$

Then

$$\boxed{QFT\,|per\rangle = \frac{1}{\sqrt{NA}} \sum_{k=0}^{r-1} \omega^{x_0 kA} A\, |kA\rangle.}$$

Rewriting.

$$QFT\,|per\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega^{x_0 kA} |kA\rangle$$

$$= |\Phi\rangle.$$

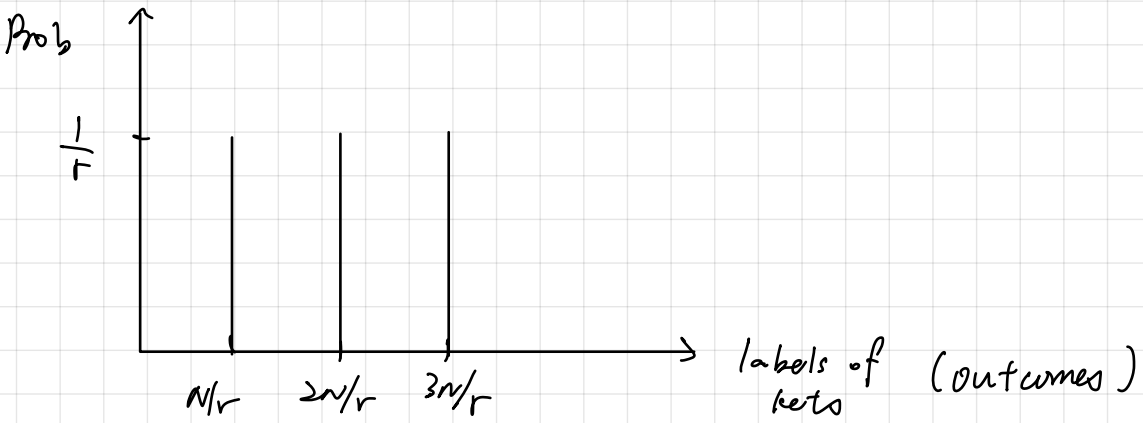
$$\equiv \frac{1}{\sqrt{r}} \sum \omega^{x_0 kN/r} |kN/r\rangle$$

Now, do mmt of state in B_N. Outcome is

$$c \equiv k_0 A = k_0 N/r$$

for some $k_0 \in \{0, \ldots, r-1\}$.

$$\text{Prob}\left(c \equiv k_0 A\right) = \frac{1}{r}\left|\omega^{x_0 k N/r}\right|^2 = \frac{1}{r} \quad \text{(no dependence on } x_0\text{)}$$



$$c \equiv \frac{k_0 N}{r} \Rightarrow \frac{k}{r} = \frac{c}{N}$$

unknown ← known

Q: How can we find r from c and N?

Case I: When $\gcd(k_0, r) = 1$.

- Cancel c/N down to lowest term and denominator is r.

Example $k_0 = 3$, $r = 4$, $c = 18$, $N = 24$

$$\frac{c}{N} = \frac{18}{24} = \frac{3}{4}$$

Case II: $\gcd(k_0, r) \neq 1$.

- Cancellation leads to denominator $< r$

Example $k_0 = 3$, $r = 9$, $c = 15$, $N = 45$

$$\frac{c}{N} = \frac{15}{45} = \frac{1}{3} \Rightarrow r' = 3 < r = 9$$

So see $f(0) \overset{?}{=} f(\tilde{r})$, $\tilde{r}$ = denom after cancellation.

If $f(0) = f(\tilde{r})$, $\tilde{r} = r$ ✓, else $\tilde{r} < r$.

k_0 chosen uniformly at random from $\{0, 1, \ldots, r-1\}$

Q: What is prob. that such a uniformly random k_0 is coprime with (unknown) period r?

Thm (Coprimality thm) The no. of integers less than r that are coprime to r grows as $\Omega(r/\log\log r)$ with increasing r.

So if $k_0 < r$ chosen uniformly at random, then

$$\mathbb{P}((k_0, r) = 1) = O\left(\frac{r/\log\log r}{r}\right) = O(\log\log r)$$

(r: total no. of possible k_0 ($k_0 \in \{0, 1, \ldots, r-1\}$))

Note We write $f(n) = \Omega(g(n))$ if $\exists$ const. α and $n_0 \in \mathbb{N}$ s.t. $\forall n \geq n_0$,

$$f(n) \geq \alpha\, g(n)$$

Claim If we repeat the process $O(\log\log r) < O(\log\log N)$ times, we will obtain a coprime k_0 in at least one case with any fixed const. level of prob.

This follows from

Lem If a single trial has prob. of success p. Repeat trial m times indptly, then $\forall$ const. $\varepsilon \in (0, 1)$.

$$p_{succ} := \mathbb{P}(\geq 1 \text{ trial successful}) > 1 - \varepsilon.$$

if $m = \left\lceil -\frac{\log\varepsilon}{p} \right\rceil$, ie. $m = O(1/p)$.

In our case, $p = 1/\log\log r$ and hence $O(\log\log r)$ suffices to get 1 success.

Pf of lem:

$$p_{succ} = 1 - P(\text{all fail})$$
$$= 1 - (1-p)^m \equiv 1 - \varepsilon$$
$$\Rightarrow (1-p)^m = \varepsilon$$
$$\Rightarrow m \log(1-p) = \log \varepsilon$$
$$\Rightarrow m = \frac{-\log \varepsilon}{-\log(1-p)}$$

$(p < -\log(1-p) \ \forall p \in (0,1))$

$$\Rightarrow m = \left\lceil \frac{-\log \varepsilon}{p} \right\rceil \text{ suffices.}$$

Query complexity

- U_f $\quad 1+1+1 = 3$

  U_f $f(0)$ $f(1)$

If we repeat $O(\log \log N)$, we use $O(\log \log N)$ queries.

Q: What about implementing QFT_N?

A: poly $(\log N)$ $(= (\log N)^2)$ computational steps.

- Cancelling c/N to lowest term (finding gcd, Euclid's algo)

All other steps can be implemented in $O(\text{poly}(\log N))$ steps.

Periodicity determination for periodic f"s on $\mathbb{Z}_N$. → extended to arbitrary group G: hidden subgroup problem.

Quantum Algorithm for Search Problems

Many problems can be cast as search problems.

e.g. Factoring N. ≡ search among all integers $< N$ that divides N exactly.

The unstructured Search problem.

Given : A large database of N items

Aim : Locate a particular (good) item.

Assume: Database is unstructured, but given any item, easy to check if it is a good one.

Require: Algo should locate good item w.p. success $1-\varepsilon$ for some fixed $\varepsilon \in (0,1)$ indpt. of N.

Each access to db is a query.

Classical : $O(N)$ queries necc. and suff.

Quantum : $O(\sqrt{N})$

$\Rightarrow$ quadratic speedup. , algo : Grover's algo.

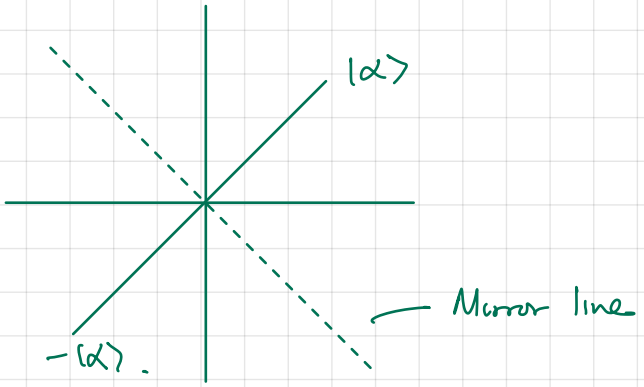
Preliminaries

Let $|v\rangle \in V \equiv \mathcal{H}$, $\langle v|v\rangle = 1$.

Def^n • $\Pi_{|\alpha\rangle} = |\alpha\rangle\langle\alpha|$ rank-1 proj. op.

• $I_{|\alpha\rangle} = I - 2|\alpha\rangle\langle\alpha|$ reflection op.

Note $I_{|\alpha\rangle}|\alpha\rangle = -|\alpha\rangle$.



If $|\psi\rangle$ s.t. $\langle\alpha|\psi\rangle = 0$, $I_{|\alpha\rangle}|\psi\rangle = |\psi\rangle$.

Take any $|\Psi\rangle \in V$,

$$|\Psi\rangle = a|\alpha\rangle + \sum_{i=1}^{\dim S_{|\alpha\rangle}^{\perp}} b_i |\beta_i\rangle,$$

where $S_{|\alpha\rangle}^{\perp} = \text{span}\{|v\rangle \in V \mid \langle v|\alpha\rangle = 0\}$. $\langle\beta_i|\alpha\rangle = 0$, $\langle\beta_i|\beta_j\rangle = \delta_{ij}$.

$$I_{|\alpha\rangle}|\Psi\rangle = -a|\alpha\rangle + \sum b_i|\beta_i\rangle.$$

$I_{|\alpha\rangle}$: flips the sign of amplitude of $|\alpha\rangle$.

Note $\forall$ unitary U.

- $U\Pi_{|\alpha\rangle}U^\dagger = U|\alpha\rangle\langle\alpha|U^\dagger = \Pi_{U|\alpha\rangle}$.
- $UI_{|\alpha\rangle}U^\dagger = I_{U|\alpha\rangle}$.

If $V = \mathbb{C}^2$ or $\mathbb{R}^2$, $|v\rangle \in V$, $|v\rangle = a|\alpha\rangle + b|\alpha^\perp\rangle$.

$$I_{|\alpha\rangle}|v\rangle = -a|\alpha\rangle + b|\alpha^\perp\rangle.$$

$$I_{|\alpha^\perp\rangle}|v\rangle = a|\alpha\rangle - b|\alpha^\perp\rangle. = -I_{|\alpha\rangle}|v\rangle.$$

$\Rightarrow I_{|\alpha^\perp\rangle} = -I_{|\alpha\rangle}$. if V is 2-D.

Grover's algo

- Needs $O(\sqrt{N})$ queries
- Choose $N = 2^n \Rightarrow$ label the items by n-bit str.
- Search problem $\equiv$ black-box problem.
- Replace db. by b.b. for $f: B_n \to B$. $f(x) = \begin{cases} 1 & x = x_0 \\ 0 & \text{o/w} \end{cases}$.

Quantum: U_f : q oracle.

$$U_f|x\rangle|y\rangle.$$

$|x\rangle$: n-qubit state (input reg.)

$|y\rangle$: 1-qubit (output reg.)

In fact, instead of using U_f, use a related operator

$$I_{x_0} \equiv I_{|x_0\rangle}$$

$$I_{x_0}|x\rangle = \begin{cases} -|x\rangle & x = x_0 \\ |x\rangle & x \neq x_0. \end{cases}$$

- If $x_0 = 0 \ldots 0$, $I_{x_0} = I_0 = I_{|0\ldots0\rangle}$.

How can we see I_{x_0} related to U_f ?

($|y\rangle \to |-\rangle$, then $U_f |x\rangle|-\rangle \to$ action of I_{x_0}.)

$$U_f |x\rangle|-\rangle = \frac{1}{\sqrt{2}} U_f \left(|x\rangle|0\rangle - |x\rangle|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}} \left(|x\rangle|f(x)\rangle - |x\rangle|\bar{f}(x)\rangle\right)$$

$$= \begin{cases} -|x_0\rangle|-\rangle. & x = x_0 \\ |x\rangle|-\rangle. & x \neq x_0. \end{cases}$$

$$= I_{x_0}|x\rangle|-\rangle.$$

Want to find $x_0 \in B_n$. with least no. of queries. (of $U_f \equiv I_{x_0}$).

- Start with equal superposition state.

$$|\psi_0\rangle = H_n |0\rangle^{\otimes n}, \quad H_n = H^{\otimes n} \qquad (1)$$

- Consider acting on it by Grover iteration operator

$$\boxed{Q = -H_n I_0 H_n I_{x_0}} \qquad (2)$$

Note

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |x\rangle \qquad (3)$$

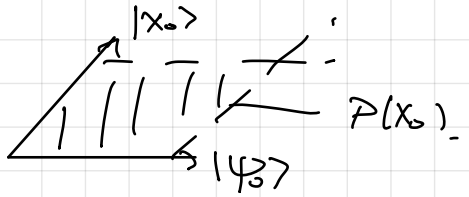
all real.

To analyse action of Q on $|\psi_0\rangle$, use geom. prop. of I_{x_0} (refl) described in terms of <u>real</u> Euclidean geometry.

<u>Facts</u>

(I) In the plane $P(x_0) = \text{span}\{|\psi_0\rangle, |x_0\rangle\}$, Q causes a <u>rot^n</u> through an angle 2α, with

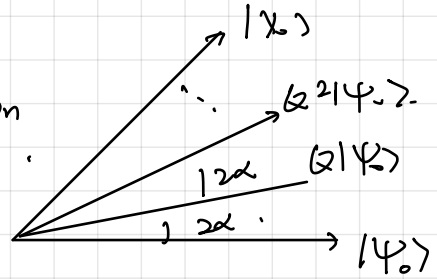
$$\sin\alpha = \frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{N}}.$$



(II) In the plane $\perp$ to $P(x_0)$, Q acts as $-I$.

Q: How do we use these?

A: $|\psi'\rangle$ rotated vector determined by repeated action of Q., $|\psi'\rangle \in (\mathbb{C}^2)^{\otimes n}$.



Note for v. large n, $|\psi_0\rangle$ is almost $\perp$ to $|x_0\rangle$.

$$\langle x_0|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \xrightarrow{n\to\infty} 0.$$

(I) rot^n by 2α, $\sin\alpha = \frac{1}{\sqrt{2^n}} \approx 0 \Rightarrow 2\alpha \approx 2\sin\alpha = \frac{2}{\sqrt{N}}$.

How many iterations of Q needed to move $|\psi_0\rangle$ close to $|x_0\rangle$.

Let β be initial angle $\measuredangle$ $|\psi_0\rangle$ and $|x_0\rangle$.

For v. large N, $\beta \approx \pi/2$.

$$2\alpha \cdot \underbrace{(\#\text{ iter})}_{m} \approx \beta. \quad \Rightarrow m = \frac{\pi}{2}\cdot\frac{1}{2\alpha} \approx \frac{\pi}{4}\sqrt{N}.$$

$\Rightarrow O(\sqrt{N})$ queries suffices (repeated rot^n : $|\psi_0\rangle \to |\psi'\rangle$ close to $|x_0\rangle$ + mmt in comp. basis

For finite N, $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle$.

$$\cos\beta = \langle x_0|\psi_0\rangle = \frac{1}{\sqrt{N}} \Rightarrow \beta = \cos^{-1}(1/\sqrt{N}).$$

Q rotates through 2α.

$$\sin\alpha = \frac{1}{\sqrt{N}} \Rightarrow 2\alpha = 2\sin^{-1}(1/\sqrt{N})$$

$$\Rightarrow m = \frac{\beta}{2\alpha} = \frac{\cos^{-1}(1/\sqrt{N})}{2\sin^{-1}(1/\sqrt{N})} \quad \text{(indpt. of } x_0\text{)}.$$

Example Search one in four.

- $N = 4 \Rightarrow n = 2$.
- rot° 2α, $\alpha = \sin^{-1}\left(\frac{1}{2}\right) \Rightarrow \alpha = \pi/6 \Rightarrow 2\alpha = \pi/3$.
- $|\psi_0\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

$\forall x_0 \in \{00, 01, 10, 11\}$. $\langle x_0|\psi_0\rangle = \cos\beta = 1/2 \Rightarrow \beta = \pi/3$

$$\Rightarrow m = \frac{\beta}{2\alpha} = 1$$

For 1-in-4, just need 1 query to locate good item w.p. 1.

Geometric prop. of Q

Pf of (I):

$$Q = -H_n I_0 H_n I_{x_0}. \quad \text{(a)}$$

$$Q = -I_{|\psi_0\rangle} I_{x_0} \quad \text{(b)}$$

WTS: $H_n I_0 H_n = I_{|\psi_0\rangle}$. (c)

$$\text{LHS} = H_n (I - 2|0\ldots0\rangle\langle 0\ldots0|) H_n$$

$$= I^{\otimes n} - 2(H|0\rangle)^{\otimes n}(\langle 0|H)^{\otimes n}$$

$$= I^{\otimes n} - 2(|+\rangle)^{\otimes n}$$

$$= I^{\otimes n} - 2|\psi_0\rangle\langle\psi_0| = I_{|\psi_0\rangle}.$$

Also, $Q = I_{|\psi_0^\perp\rangle} I_{x_0}$, $|\psi_0^\perp\rangle : \langle\psi_0|\psi_0^\perp\rangle = 0$. (d)

- For any $|v\rangle \in P(x_0)$, $Q|v\rangle \in P(x_0)$, i.e. Q preserves $P(x_0)$.

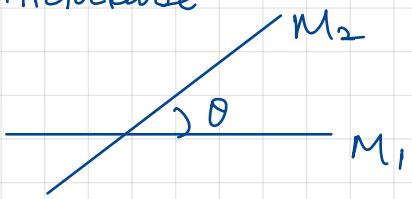
(b): $\forall |v\rangle \in P(x_0)$.

$$I_{x_0}|v\rangle = |v\rangle - 2\langle x_0|v\rangle |x_0\rangle.$$

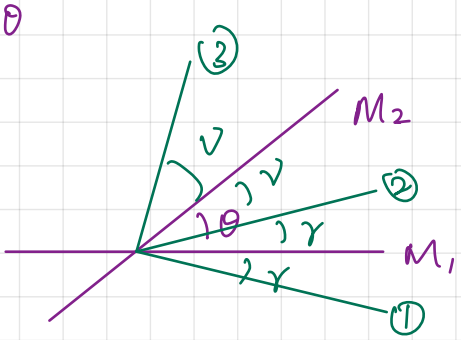
$$I_{|\psi_0\rangle}|v\rangle = |v\rangle - 2\langle \psi_0|v\rangle|\psi_0\rangle.$$

- Causes rotⁿ through angle 2α.

Lem Let M_1, M_2 be 2 mirror lines in $\mathbb{R}^2$, intersecting at 0, Then reflⁿ about M_1, then M_2, is anticlockwise rotⁿ by 2θ.

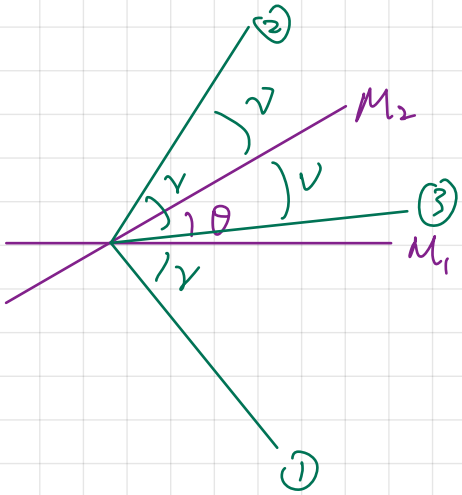


Case 1 $\gamma \leq \theta$



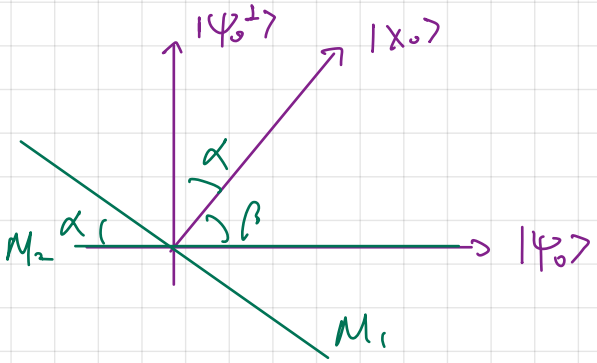
Angle between ①, ③ $= 2\theta$.

Case 2: $\gamma > \theta$.



□

$Q = I_{|\psi_0^\perp\rangle} I_{x_0}$



Q causes rotn of 2α,

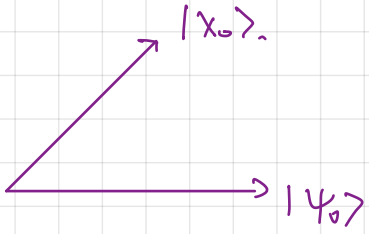
$$\langle x_0|\psi_0\rangle = \cos\beta = \cos\left(\frac{\pi}{2}-\alpha\right) = \sin\alpha$$
$$\| \qquad\qquad \|$$
$$\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}}$$

So Lem $\Rightarrow$ $\sin\alpha = 1/\sqrt{N}$. $\Rightarrow$ (I) □

Pf of (II): Use $Q = -I_{|\psi_0\rangle} I_{x_0}$. If $|v\rangle \in P^{\perp}(x_0)$

$$I_{x_0}|v\rangle = |v\rangle \quad , \quad I_{|\psi_0\rangle}|v\rangle = |v\rangle$$

$\Rightarrow Q|v\rangle = -|v\rangle \Rightarrow Q = -I$

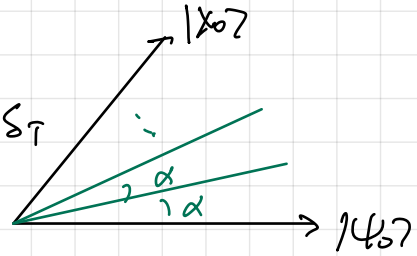


□

No. of iterations needed for large but finite N

Let T = # iter.

Angle between $|x_0\rangle$ and rotated vec $|\psi_0^T\rangle \equiv \delta_T$



$$\delta_T = \beta - 2\alpha T = \left(\frac{\pi}{2}-\alpha\right) - 2\alpha T$$
$$= \frac{\pi}{2} - \alpha(1+2T)$$
$$= \frac{\pi}{2} - (1+2T)\sin^{-1}(1/\sqrt{N}).$$

Do a mmt on $|\psi_0^T\rangle$ in comp. basis in $(\mathbb{C}^2)^{\otimes n}$

$$p(x_0, T) = \text{Prob}(\text{outcome} = x_0 ; T)$$
$$= |\langle x_0|\psi_0^T\rangle|^2.$$
$$= \cos^2\delta_T = \sin^2\left((1+2T)\sin^{-1}(1/\sqrt{N})\right).$$

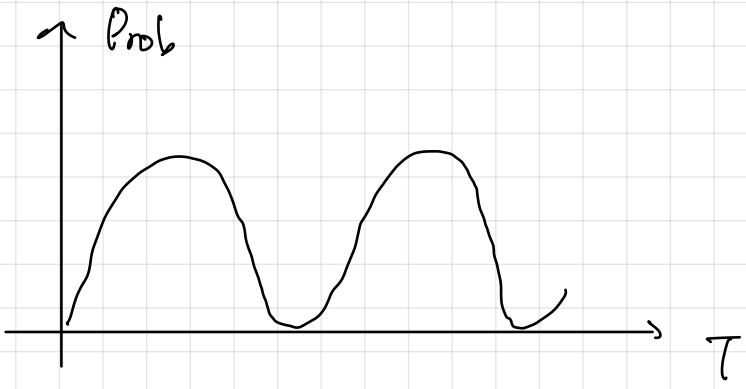
Choose T to be the closet integer for which

$$(1+2T)\sin^{-1}(1/\sqrt{N}) \approx \pi/2 .$$

Use $\sin^{-1}(x) = x + O(x^3)$ for small x.

$$T = \frac{\pi}{4\sin^{-1}(1/\sqrt{N})} - \frac{1}{2} = \frac{\pi}{4}\sqrt{N} - \frac{1}{2} - O\left(\frac{1}{N}\right),$$

i.e. $T = O(\sqrt{N})$.



Exercise Use above to check for 1 in 4, $T=1$ suffices,

$$p(x_0, 1) = 1 .$$

What if there are $r>1$ good items?

- Task: find one/all of them.

$$f: B_n \to B, \qquad f(x) = \begin{cases} 1 & \forall\, i \in \{1,\dots,r\} \\ 0 & \text{o/w.} \end{cases}$$

Analogy to 1-good item case

$$I_{x_0} = I - 2|x_0\rangle\langle x_0| \longrightarrow I_G = I - 2\sum_{i=1}^{r}|x_i\rangle\langle x_i|$$

$$I_G|x\rangle = \begin{cases} -|x\rangle & \text{if } x \in \{1,\dots,r\} \\ |x\rangle & \text{o/w.} \end{cases}$$

$|\psi_b\rangle \perp |\psi_g\rangle$

$$Q = -H^n I_0 H^n I_G, \qquad |\psi_g\rangle = \frac{1}{\sqrt{r}}\sum_{i=1}^{r}|x_i\rangle, \qquad |\psi_b\rangle = \frac{1}{\sqrt{N-r}}\sum_{i=r+1}^{N}|x_i\rangle$$

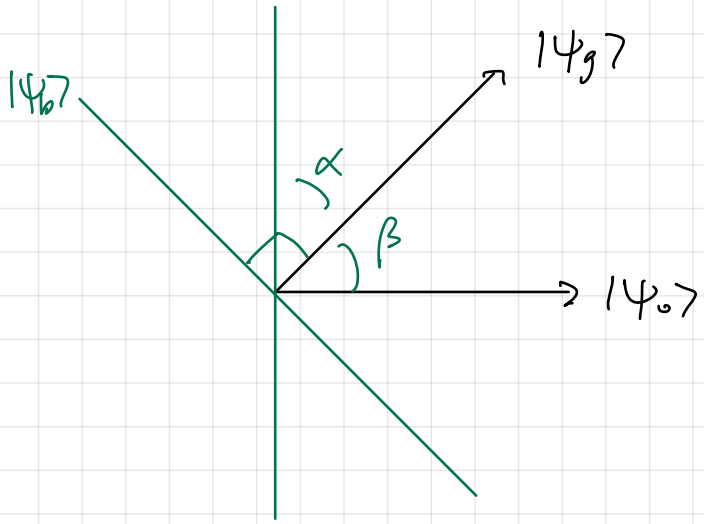
good bad

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B_n} |x\rangle = \frac{\sqrt{r}}{\sqrt{N}} |\psi_g\rangle + \frac{\sqrt{N-r}}{\sqrt{N}} |\psi_b\rangle.$$

$Q = I_{|\psi_0\rangle} I_{|\psi_g\rangle}$.

$\cos\alpha = \langle \psi_0^{\perp} | \psi_g \rangle$.

$\sin\alpha = \langle \psi_0 | \psi_g \rangle = \sqrt{r/N}$.



Shor's factoring Algo.

N: a given pos. int. ($N \in \mathbb{Z}_+$)

Output: (i) a factor, say K, of N, or

(ii) N if N prime

with prob $(1-\varepsilon)$ for a fixed $\varepsilon \in (0,1)$

Claim: Algo runs in $O(n^3)$ time, n: # of binary digit of N.

Cl: Best known algo: runtime $\exp\left(O(n^{1/3}(\log n)^{2/3})\right)$.

Key idea: Convert factoring N to periodicity determination (↖ QFT).
but need some modification.

Factoring as a periodicity determination problem.

Steps ① Choose an integer a ($1 < a < N$) uniformly at random.

② Euclid algo $\Rightarrow$ $b = \gcd(a, N)$

(i) If $b > 1$ $\Rightarrow$ $b \mid N$, output b.

(ii) If $b = 1$ $\Rightarrow$ then $(a, N) = 1$. $\Rightarrow$ number theory.

Thm (Euler's thm). If a, N coprime. $\exists$ least integer r, $1 < r < N$, s.t. $a^r \equiv 1 \mod N$. — (1)

Consider $f: \mathbb{Z} \to \mathbb{Z}_N$ the modulo exponential f^n. (2)

$k \mapsto a^k \mod N$

Fact $f(k_1 + k_2) = f(k_1) f(k_2)$. (3)

(1) $\Rightarrow \exists$ r s.t. $f(r) = 1$ (4)

By (3), (4).

$$f(k+r) = f(k) f(r) = f(k).$$

$\Rightarrow f$ periodic with period r.

Since r is least integer satisfying (1), f must be 1-to-1 within each period.

Suppose we can compute r (using QFT)

Cases

① r even. then $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \mod N$.

ie. N divides the product., but cannot divide $(a^{r/2} - 1)$ by minimality of r. Suppose N does not divide $(a^{r/2} + 1)$, then N partly divides $(a^{r/2} \pm 1)$.

Use Euclid $\Rightarrow$ gcd $(a^{r/2} \pm 1, N) \to$ factors of N.

∴ We find factors if a, N are coprime provided (a) r even (b) $a^{r/2} + 1 \not\equiv 0 \pmod N$

Thm If N odd, $N \neq p^\ell$, p prime, $\ell = \mathbb{Z}_+$, then if a $(1 < a < N)$ chosen unif. at random, and $(a, N) = 1$, then

$$\mathbb{P}(\text{(a) and (b)}) \geq 1/2.$$

$\Rightarrow$ factor w.p. $\geq 1/2$.

- Given a candidate factor, check if in poly(n) time via test division into N.
- Repeating the process k times (e.g. $k = 10$).

$$p_{err}^{(10)} = (1 - p_{succ})^{10} \leq \left(1 - \frac{1}{2}\right)^{10} = 2^{-10} = \varepsilon.$$

- We saw $k = \log 1/\varepsilon$, $p_{succ} \geq 1 - \varepsilon$.

Example $N = 15$, choose $a = 7$., $(a, N) = 1$.

$$f(k) = a^k \bmod N = 7^k \bmod 15$$

Values of f: $1, 7, 4, 13, 1, \ldots$, $\Rightarrow$ $r = 4$ (period) even

- $a^r - 1 = 7^4 - 1 = (7^2 - 1)(7^2 + 1) = 48 \cdot 50$.

$\Rightarrow$ (b) holds.

$$\gcd(48, 15) = 3, \quad \gcd(50, 15) = 5.$$

Summary

(i) N even? Yes $\longrightarrow$ 2

No $\longrightarrow$ go to (ii)

(ii) Is $N = p^\ell$ for some p prime, $\ell \in \mathbb{Z}_+$?

Yes (compute roots of $N^{1/k}$, $k = 2, 3, \ldots, \log N$. Done in poly(n) time. If any result int $\Rightarrow$ factor)

No → go to (iii)

(iii) Choose $1 < a < N$ at random.

Compute $b = \gcd(a, N)$ — $b \neq 1 \rightarrow b$.

$b = 1 \Rightarrow$ coprime → go to (iv)

(iv) Find period r of $f(k) = a^k \bmod N$. (quantum)

- r odd ⇒ return to (iii)
- r even ⇒ compute $(a^{r/2} - 1) \bmod N$. (can do "+" also)
- Compute $t = \gcd(a^{r/2} - 1, N)$

$t > 1 \rightarrow$ output t

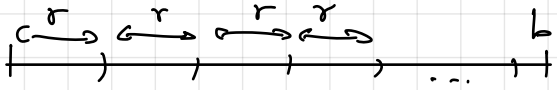
$t = 1 \rightarrow$ failed → (iii).

Computing period r of $f(k)$

Note $f: \mathbb{Z} \to \mathbb{Z}_N$. To use quantum period finding algo, need to restrict domain of f to $\mathbb{Z}_M$ for some suitable $M \in \mathbb{Z}$.

Then restricted f^n is not in general periodic, but

Claim For suff. large M ($= O(N^2)$), there are enough complete periods s.t. the incomplete ones has negligible effect in period-finding algo.



$0 < b < r$.

Choose $M = 2^m$, m is smallest int. s.t. $2^m > N^2$,

$M = Br + b$, B = # complete periods.

Steps for finding r

(i) Construct unif. sup. state

$$|\psi_m\rangle = \frac{1}{\sqrt{2^m}} \sum_{x \in \mathbb{Z}_M} |x\rangle. \qquad (1)$$

(m qubit state)

(ii)

$$U_f |\psi_m\rangle|0\rangle \quad , \quad |0\rangle \in \mathcal{B}_N = \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}.$$

(input reg., output reg.)

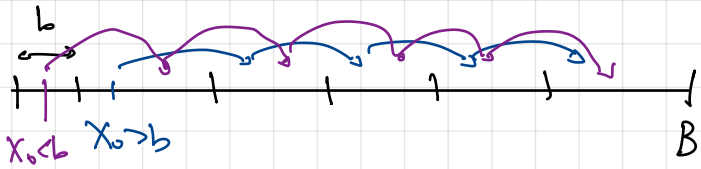
$U_f |x\rangle|0\rangle = |x\rangle|f(x)\rangle$

$$U_f |\psi_m\rangle|0\rangle = \frac{1}{\sqrt{2^m}} \sum_{x \in \mathbb{Z}_M} |x\rangle|f(x)\rangle \qquad (2)$$

(iii) mmt on <u>2nd register</u> in basis $\mathcal{B}_N$. Say outcome $y = f(x_0)$, $0 \le x_0 \le r-1$ uniform at random.

$\because$ r period,

$$f(x_0) = f(x_0 + jr) \quad , \quad j = \begin{cases} 0, 1, 2, \ldots, B-1 & \text{if } x_0 > b \\ 0, 1, 2, \ldots, B & \text{if } x_0 \le b. \end{cases}$$



Write $j = 0, 1, \ldots, A-1$, where $A = \begin{cases} B & x_0 > b \\ B+1 & x_0 \le b. \end{cases}$ (3)

$$\text{Prob}(y = f(x_0)) = \left\| \frac{1}{\sqrt{2^m}} \sum_{j=0}^{A-1} |x_0 + jr\rangle \right\|^2.$$

- Post-mmt state of 1st reg. when outcome is $y = f(x_0)$

$$|\text{per}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle. \qquad (4)$$

$$A = \begin{cases} B+1 = \lfloor 2^m/r \rfloor + 1 & \text{if } x_0 \le b \\ B = \lfloor 2^m/r \rfloor & \text{if } x_0 > b \end{cases} \qquad (5)$$

(iv) Apply QFT_{2^m}

$$QFT_{2^m}|per\rangle = \frac{1}{\sqrt{A}} \cdot \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} \sum_{j=0}^{A-1} \omega^{(x_0+jr)c} |c\rangle$$

$$\omega = e^{2\pi i/2^m}$$

$$\left(QFT_M|x\rangle = \frac{1}{\sqrt{M}} \sum_y \omega^{xy}|y\rangle\right)$$

$$= \sum_{c=0}^{2^m-1} g(c)\,|c\rangle .$$

where

$$g(c) = \frac{1}{\sqrt{A}} \cdot \frac{1}{\sqrt{2^m}} \sum_{j=0}^{A-1} \omega^{x_0 c}\, \omega^{jrc}$$

$$= \frac{\omega^{x_0 c}}{\sqrt{A}\sqrt{2^m}} \sum_{j=0}^{A-1} \alpha^j , \quad \alpha = \omega^{rc} = e^{2\pi i rc/2^m}.$$

Exact periodicity (recall):

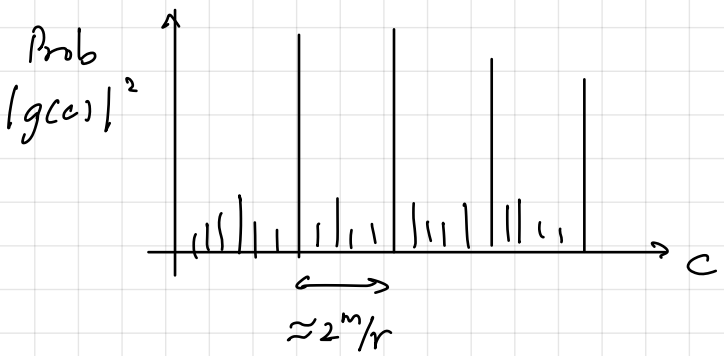
$r \mid 2^m$ exactly, $A = 2^m/r \in \mathbb{Z}$, $S = \begin{cases} A & \alpha = 1 \\ \frac{1-\alpha^A}{1-\alpha} & \alpha \neq 1 \end{cases}$, where

$\alpha^A = e^{2\pi i c} = 1 \Rightarrow S = 0$ if $\alpha \neq 1$.

But now we have <u>inexact periodicity</u>, $2^m = Br + b \Rightarrow$ <u>$S \neq 0$ if $\alpha \neq 1$</u>.

(Non-zero prob. for getting c values even when $\alpha = \omega^{rc} \neq 1$.

<u>Claim</u>: A mmt on $QFT_{2^m}|per\rangle$ yields a value of c which is close to a multiple of $2^m/r$ with high prob.

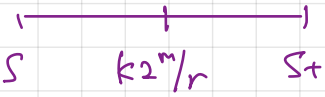


<u>Reason</u>: Consider <u>$k\,2^m/r$</u>, $k = 0, \ldots, r-1$

no longer int.

Fact: Each $k2^m/r$ is within a distance of $1/2$ from a unique nearest int.

Pf: If $k2^m/r = s + \frac{1}{2}$, some $s \in \mathbb{Z}$, (*)



We know $r < N$, $2^m > N^2 \Rightarrow r < 2^m$.

So any factor of 2 in r gets cancelled by 2 in 2^m, and $\nexists$ any remnant 2 in denom, so (*) not possible ⁂

We consider integer values of c (r of them) s.t.

$$|c - k2^m/r| < \tfrac{1}{2}. \qquad (\dagger)$$

We choose $2^m > N^2$ exactly for ($\dagger$) to get a unique integer within $1/2$ of $k2^m/r$ for each $k = 0, \ldots, r-1$. □

Thm If we do msmt on $QFT_{2^m}|per\rangle = \sum_{c=0}^{2^m} g(c)|c\rangle$ in basis $\mathcal{B}_M = \{|0\rangle, \ldots |M-1\rangle\}$, $M = 2^m$ $\forall k = 0, 1, \ldots, r-1$. Let $c = c_k$ be the unique int. s.t. $|c - k2^m/r| < 1/2$, then

$$\mathbb{P}(\text{outcome} = c_k) > \gamma/r,$$

$\gamma \approx 4/\pi^2$

We will be interested in these c_k s.t. k is coprime to r.

By the coprimality thm, prob. of obtaining a good value c

$$\Omega(1/\log\log r) > \Omega(1/\log\log N).$$

⇒ By $O(\log\log N)$ iter, we can obtain a good value of c with high prob.

Where we have arrived: We have a c value s.t.

$$|c - k2^m/r| < 1/2, \quad k, r \text{ coprime.}$$

Task Getting r from such a c value.

$$\left|\frac{c}{2^m} - \frac{k}{r}\right| < \frac{1}{2^{m+1}}$$

Note $r < N$, $2^m > N^2$

$$\Rightarrow 2^{m+1} > 2N^2$$

$$\Rightarrow \left|\frac{c}{2^m} - \frac{k}{r}\right| < \frac{1}{2N^2} \quad \text{with } r < N \quad (**)$$

Note $c/2^m$ is a known fraction.

Claim There is at most one fraction k/r with denominator $r < N$ satisfying $(**)$.

Pf: Suppose k'/r', k''/r'' both satisfy $(**)$. and $k'/r' \neq k''/r''$.

$$\left|\frac{k'}{r'} - \frac{k''}{r''}\right| = \left|\frac{k'r'' - k''r'}{r'r''}\right| \geq \left|\frac{1}{r'r''}\right| > \frac{1}{N^2}.$$

— all integers, and non-zero numerator.

But k'/r', k''/r'' by assumption, is within a distance of $1/2N^2$ of $c/2^m$

$$\Rightarrow \left|\frac{k'}{r'} - \frac{k''}{r''}\right| \leq \frac{1}{N^2} \quad \text{✱}.$$

Hence, there is one unique k/r with $r < N$ satisfying $(**)$. □

Note This uniqueness is reason to choose $2^m > N^2$. It guarantees that k/r is uniquely determined by $c/2^m$.

Example $N = 39$, Suppose $a = 7$

r : period of $f(k) = a^k \bmod N$.

$N^2 = 1521$, $\quad 2^{10} < N^2 < 2^{11} = 2048$. $\Rightarrow$ choose $m = 11$.

Suppose mmt on $QFT_{2^{11}}|per\rangle$ yields $c = 853$. Our theory tells us with high prob.

$$\left| c - \frac{k 2^m}{r} \right| < \frac{1}{2} \quad \text{for } k \in \{0, 1, \ldots, r-1\}.$$

If this is actually the case, then k/r is the unique fraction with denom $r < 39$ $(= N)$ s.t.

$$\left| \frac{c}{2^m} - \frac{k}{r} \right| < \frac{1}{2^{m+1}}$$

What we do to find r : check all $\frac{a}{b}$ $(1 \le a < b < N = 39)$ to see which ones satisfy

$$\left| \frac{c}{2^m} - \frac{a}{b} \right| = \left| \frac{853}{2048} - \frac{a}{b} \right| < \frac{1}{2^{12}}.$$

There are $O(N^2)$ fractions, we find $\frac{a}{b} = \frac{5}{12}$ satisfies this.

This is consistent with $k = 5$, $r = 12$, and $k = 10$, $r = 24$, and $k = 15$, $r = 36$.

But theory guarantees k, r coprime, so $r = 12$.

Check $f(k) = 7^k \bmod 39$. Check $f(r) = 7^{12} \bmod 39 = 1$.

Theory of continued fractions

Any rational s/t (s<t) can be expressed as

$$\frac{s}{t} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_l}}}} \qquad (CF)$$

where $a_1, a_2, \ldots, a_l \in \mathbb{N}$.

To do this, write

$$\frac{s}{t} = \frac{1}{t/s}, \qquad \frac{t}{s} = a_1 + \frac{s_1}{t_1} \quad (a_1 \geq 1) \quad — s_1 < t_1 = s.$$

$$\Rightarrow \frac{s}{t} = \frac{1}{a_1 + \frac{s_1}{t_1}}$$

Repeat for s_1/t_1, $\frac{t_1}{s_1} = a_2 + \frac{s_2}{t_2}$, ...

$$\Rightarrow \frac{s}{t} = \frac{1}{a_1 + \frac{1}{a_2 + \frac{s_2}{t_2}}}$$

Note $s_k < t_k = s_{k-1}$. So we get a seq. of +ve int. a_k, s_k, t_k s.t. $s_k < t_k = s_{k-1}$. $(t_k)_k$ strictly decreasing of non-neg int. $\Rightarrow$ process must terminate after l steps.

Example $\frac{s}{t} = \frac{31}{64}$ $\qquad s/t = [a_1, a_2, \ldots, a_l]$.

$$\frac{31}{64} = \frac{1}{2 + \frac{2}{31}} = \frac{1}{2 + \frac{1}{15 + \frac{1}{2}}} = [2, 15, 2]$$

Note For each $k = 1, 2, \ldots, l$ can truncate CF at k-th level to get a seq. of rational numbers

$$\frac{p_1}{q_1} = [a_1], \quad \frac{p_2}{q_2} = [a_1, a_2], \ldots, \quad \frac{p_k}{q_k} = [a_1, \ldots, a_k]$$

p_k/q_k : the k-th convergent of CF of s/t.

Properties of CFs

Lem Let $a_1, \ldots, a_k$ be +ve numbers (not necc. integers). Set

$p_0 = 0,\ q_0 = 1,\ q_1 = a_1$,

(i) then $[a_1, \ldots, a_k] = p_k/q_k$, where $p_k = a_k p_{k-1} + p_{k-2}$,

$q_k = a_k q_{k-1} + q_{k-2}$, $k \geq 2$

If a_k's integers, then

(ii) $q_k p_{k-1} - p_k q_{k-1} = (-1)^k$ for $k \geq 1$

(iii) $\gcd(p_k, q_k) = 1 \quad \forall\, k \geq 1$

Thm CF s/t $= [a_1, \ldots, a_\ell]$. Let $p_k/q_k = [a_1, \ldots, a_k]$, $k = 1, \ldots, \ell$. If s, t are m-bit length integers (after s/t cancelled to lowest terms), then the length ℓ of CF is $O(m)$. and the CF and the convergence can be calculated in $O(m^3)$ time.

Thm Let $0 < x < 1$, $x \in \mathbb{Q}$ and suppose $p/q \in \mathbb{Q}$ s.t.

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2} \qquad (**)$$

Then p/q is a convergent of CF of x.

Back to our problem: getting r from a good c.

$$\left| \frac{c}{2^m} - \frac{k}{r} \right| < \frac{1}{2^{m+1}} < \frac{1}{2N^2} < \frac{1}{2r^2}$$

$2^m > N^2$ $\qquad$ $r < N$

and $\left| \frac{c}{2^m} - \frac{k}{r} \right| < \frac{1}{2r^2}$ of the form of $(**)$.

We saw $\exists$ unique fraction s.t. $2^m > N^2$, $r < N$ hold.

In the context of (**),

$$x = \frac{c}{2^m}, \quad 0 \le c \le 2^{m-1}, \quad \frac{p}{q} = \frac{k}{r}$$

so $\frac{k}{r}$ is a convergent of CF of $\frac{c}{2^m}$.

Note $c, 2^m$ are $O(m)$ bit integers, $2^m = O(N^2)$. N is n-bit int., so $c, 2^m$ are $O(n)$ bit integers. So all cfts of $c/2^m$ can be computed in $O(n^3)$ time, and $O(n)$ of such cfts.

So compute all cfts of $c/2^m$ and check list of $O(n)$ cfts to find the unique one satisfying (**).

Example $N = 39$, $a = 7$, $N^2 = 1521$., r : period of $f(k) = 7^k \bmod 39$,

$m = 11$.

Suppose $c = 853$, $\frac{c}{2^m} = \frac{853}{2048} = [2, 2, 2, 42, 4]$.

Convergents are $[2] = \frac{1}{2}$, $[2,2] = \frac{2}{5}$, $[2,2,2] = \frac{5}{12}$, ...

Check 5 fractions, we find only $\frac{5}{12}$ satisfies $\left| \frac{c}{2^m} - \frac{k}{r} \right| < \frac{1}{2^{m+1}}$

and has denom $< 39 \Rightarrow r = 12$.