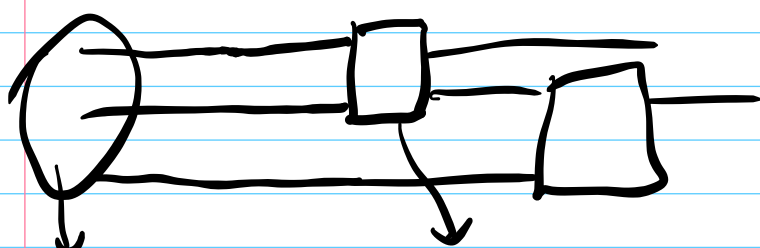
07/26 IPAM - Intro to QC

1. Basics
   - qubit, measurement, q circuit ...
2. Quantum algorithms
   - Simon, factoring (Shor/Kitaev)
   - Grover
3. Quantum information
   - density, POVM, distance

Two systems

- state vectors. unitary.
- density matrices. channels.

0. Circuit model



Quantum bits Quantum op's

1. Quantum formalism

a Qubit

- Register X
- state of X : $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ $\alpha, \beta \in \mathbb{C}$ $|\alpha|^2 + |\beta|^2 = 1$ $\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$ $p_0 + p_1 = 1$ $p_0, p_1 \geq 0$

probabilities → amplitudes

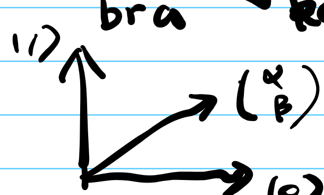
1-Norm → 2-norm

- Dirac Notation $\langle \; | \; \rangle$

bra ket

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\langle 0| = (1 \;\; 0)$

$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\langle 1| = (0 \;\; 1)$



$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + |1\rangle$ "superposition"

$|\phi\rangle$

1

$|+\rangle \quad |-\rangle$

$$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \quad \text{vs} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Classical coin

- inner product: $\langle 0|0\rangle = 1 \quad \langle 0|1\rangle = 0$

b. Unitary op's

unitary $U \Leftrightarrow U^{\dagger}U = \mathbb{1}$.

$U^{\dagger} = \overline{U^{T}} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\dagger} = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$

$\overline{x+yi} = x - yi$

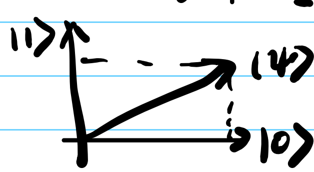
- Examples.
  - $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad |b\rangle - \boxed{I} - |b\rangle$
  - $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad |b\rangle - \boxed{X} - |1-b\rangle$ NOT gate, bit flip
  - $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ$ $\quad |0\rangle - \boxed{Y} - i|1\rangle$, $\ |1\rangle - \boxed{Y} - -i|0\rangle$
  - $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad |0\rangle - \boxed{Z} - |0\rangle$, $\ |1\rangle - \boxed{Z} - -|1\rangle$ phase flip $e^{i\theta}$

$\hookrightarrow$ Pauli op's. $\quad X^2 = Y^2 = Z^2 = \mathbb{1}$

c. measurement

- observe a qubit.

State	see	w.p.	post. state
$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$	"0"	$|\alpha|^2$	$|0\rangle$
	"1"	$|\beta|^2$	$|1\rangle$



d. multi-qubit systems.

- 2 qubits

  X Y

  $|\psi\rangle \otimes |\phi\rangle$

$|00\rangle := |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}$

$$= \begin{pmatrix}1\cdot\begin{pmatrix}1\\0\end{pmatrix}\\ 0\cdot\begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$

$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$

$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

- ABR. 2-qubit state

  $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$

  $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \qquad \cong \mathbb{C}^4$

- n-qubit

  $\{ |0\rangle^{\otimes n}, |0\rangle^{\otimes n-1}|1\rangle \; \dots \; |1\rangle^{\otimes n} \}$

  $|0^n\rangle \quad |0^{n-1}1\rangle \qquad |1^n\rangle$

  $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} \qquad \begin{pmatrix}0\\\vdots\\1\end{pmatrix}$

  (computational)

  Standard basis in $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$

- n-qubit op's

  - unitary $\quad (U)_{2^n \times 2^n} \quad U^\dagger U = \mathbb{1}.$

  - meas. $\begin{pmatrix}\vdots\\\alpha_x\\\vdots\end{pmatrix} \xrightarrow{\text{meas.}}$ see "x" w.p $p_x = |\alpha_x|^2$, p.m. state $|x\rangle$.

3

e. Examples

· Entanglement.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \neq \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

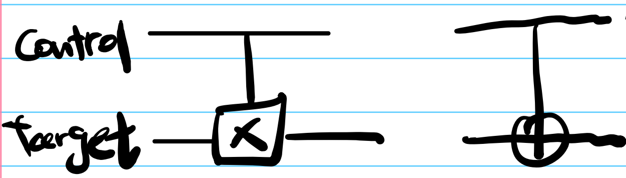
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

(EPR pair)

$$\boxed{\begin{aligned} |\phi^\pm\rangle &= |00\rangle \pm |11\rangle \\ |\psi^\pm\rangle &= |01\rangle \pm |10\rangle \end{aligned}}$$

Bell states

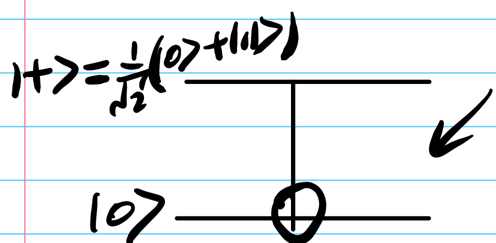
· Controlled NOT (CNOT)



✓ Flip the target

iff. control = 1

in	out
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$



?

$$(|0\rangle + |1\rangle) \otimes |0\rangle$$

$$\xmapsto{CNOT} CNOT|00\rangle + CNOT|10\rangle$$

$$= \boxed{|00\rangle + |11\rangle}$$

3. Some QIP tasks

a. Distinguishing state

- Given: $|+\rangle = |0\rangle + |1\rangle$ $\quad \rightarrow \boxed{H} \rightarrow$ $|0\rangle$ / $|1\rangle$

  OR $|-\rangle = |0\rangle - |1\rangle$
- Can you tell?

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad |0\rangle, |1\rangle \; — \boxed{H} — \; |+\rangle, |-\rangle$$

Hadarmard gate

$$|0\rangle \xrightarrow{H} \begin{matrix} |0\rangle \\ + \\ |1\rangle \end{matrix} \xrightarrow{H} \begin{matrix} |0\rangle + |1\rangle \\ |0\rangle - |1\rangle \end{matrix} \rightarrow |0\rangle$$

constructive interference.

- $|0\rangle$ vs. $|+\rangle$?

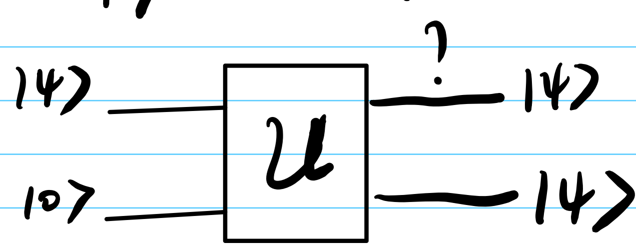
$\langle + | - \rangle = 0$ "orth"

$\langle 0 | + \rangle \neq 0$

Claim non-orth states can not be distinguished perfectly.

b. No-cloning theorem.

- copy a Quantum State



U

$$|0\rangle|0\rangle \mapsto |0\rangle|0\rangle$$
$$|1\rangle|0\rangle \mapsto |1\rangle|1\rangle$$
$$|+\rangle|0\rangle \overset{\text{WANT}}{\longmapsto} |+\rangle|+\rangle$$
$$\rightarrow U(|0\rangle|0\rangle) + U(|1\rangle|0\rangle)$$
$$= |0\rangle|0\rangle + |1\rangle|1\rangle$$
$$\neq |+\rangle|+\rangle$$

$$|\psi\rangle|0\rangle \longmapsto |\psi\rangle|\psi\rangle$$
$$|\phi\rangle|0\rangle \longmapsto |\phi\rangle|\phi\rangle$$
$$\langle\psi|\phi\rangle = \langle\psi|\langle\psi| \, |\phi\rangle|\phi\rangle$$
$$= \langle\psi|\phi\rangle\langle\psi|\phi\rangle$$
$$\Leftrightarrow \langle\psi|\phi\rangle = 0$$

c. Teleportation : send qubit via classical bits

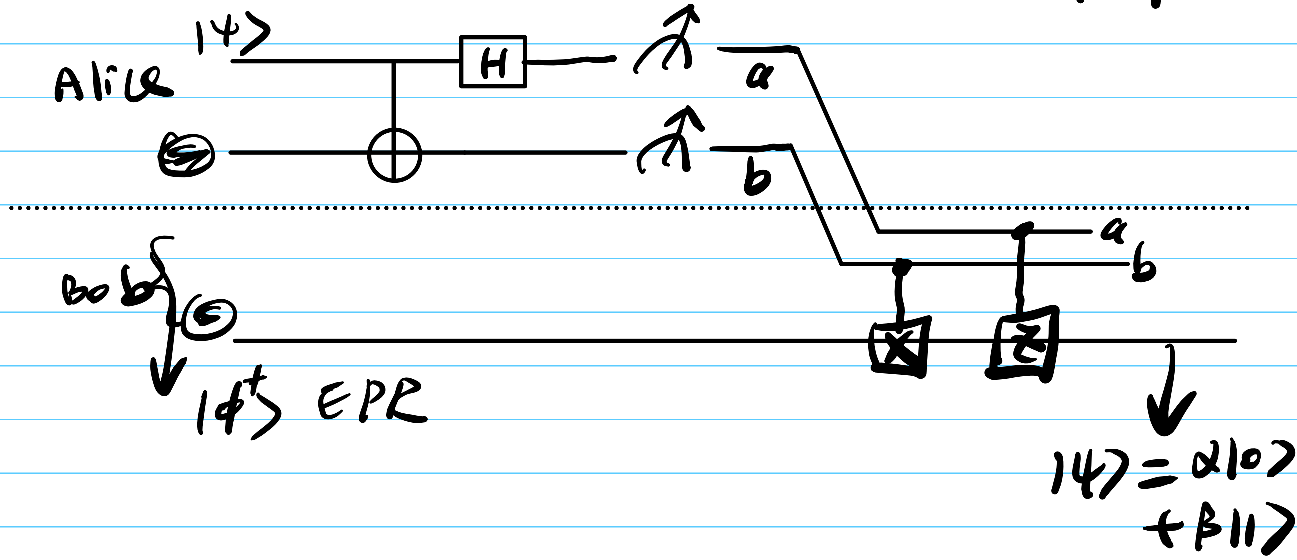
- send amplitude

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

$\alpha = 0.13 \ldots$

(EPR)

- $\forall |\psi\rangle$: 2-classical bits + 1-ebit prepare



4. Universal gate set.

- one-qubit: $\{H, T\}$ $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
- universal: $\{H, T, CNOT\}$
- Clifford op's: $\langle H, CNOT, S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \rangle$

1. Black-black function & query model.

a. Classical B.B.

- **Given**: function f

$$x \longrightarrow \boxed{f} \longrightarrow f(x)$$

- **Goal**: learn sth about f.

b. Quantum B.B. function

- $|x\rangle \longrightarrow \boxed{f} \longrightarrow |f(x)\rangle$

- $$\begin{array}{l} |x\rangle \\ |y\rangle \end{array} \boxed{U_f} \begin{array}{l} |x\rangle \\ |y \oplus f(x)\rangle \end{array}$$

- Complexity meas.: # queries

2. Basic Q Algs

a. Deutsch problem & Alg.

- **Given**: $f: \{0,1\} \to \{0,1\}$

4 possibilities

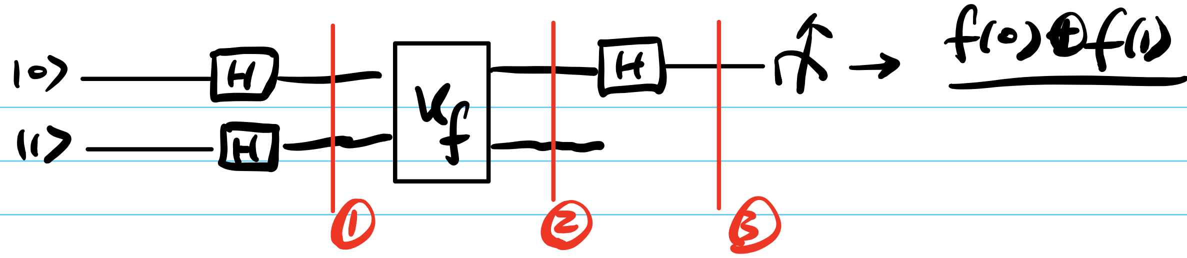
	f_0	f_1	f_2	f_3
0	0	1	1	0
1	0	1	0	1

$\underbrace{f_0 \quad f_1}_{\text{contant}} \qquad \underbrace{f_2 \quad f_3}_{\text{balanzed.}}$

- **Goal**: f constant ? balanced.

- classical: 2 queries

$\boxed{\text{Claim: 1 quantum query suffices.}}$



$$|0\rangle|1\rangle$$

$$① \overset{H\otimes H}{\longmapsto} |+\rangle|-\rangle$$

$$= |0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)$$

$$② \overset{U_f}{\longmapsto} |0\rangle(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle) + |1\rangle(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle)$$

$$= |0\rangle \otimes (-1)^{f(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes (-1)^{f(1)}(|0\rangle - |1\rangle)$$

$$\boxed{|0\oplus z\rangle - |1\oplus z\rangle = (-1)^{z}(|0\rangle - |1\rangle)}$$

$$= \left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)(|0\rangle - |1\rangle)$$

$$\boxed{|b\rangle|-\rangle \overset{U_f}{\longmapsto} (-1)^{f(b)}|b\rangle|-\rangle}$$

$$\overset{H\otimes 1}{\longmapsto} |\underline{f(0)\oplus f(1)}\rangle \otimes |-\rangle$$

$$\overset{\text{measure}}{\longmapsto}$$

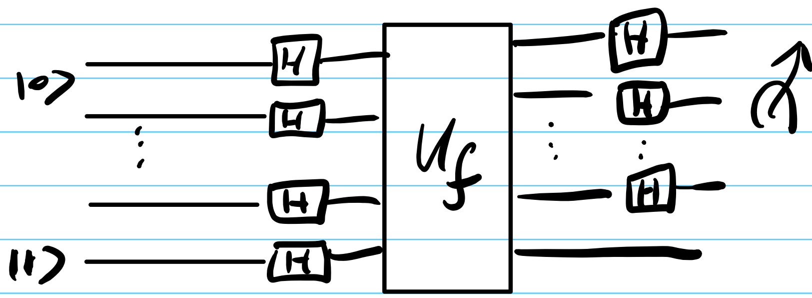
b. Deutsch-Josza Alg.

Given: $f: \{0,1\}^n \to \{0,1\}$

Promise: f is contant

OR balanced

Goal: decide which case



$\to y = 0^n$

iff f constant

Classical	R	Quantum
$2^n/2 + 1$	$\Omega(n)$ w/err	1 no err

c. Simon's Alg.

- Given: $f: \{0,1\}^n \to \{0,1\}^n$

Promise: $\exists s \neq 0^n$ s.t. $x \neq y$

$f(x) = f(y)$ iff. $x \oplus s = y$

0	s	$\xrightarrow{f} f(0)$
1	$1 \oplus s$	$f(1)$
⋮	⋮	⋮

- Goal: find s

$x \oplus y = s$

- Classical: - Det. $2^{n-1} + 1$
  - Rand: collision $x \neq y, f(x) = f(y)$

Birthday bound $\sqrt{2^n}$

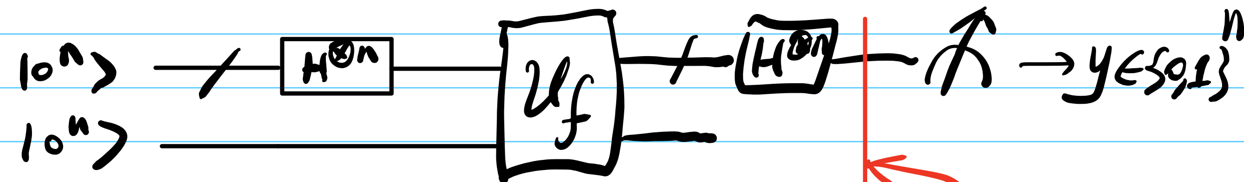
· Quantum : $O(n)$

Simon's Alg.

1. Run Simon's q. sampling subroutine k-time
$\{y_1, \cdots, y_k\}$

2. Classical post-processing
solve linear. equ's find s.

$k = O(n)$ suffice.



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

$$x \cdot y = x_1 \cdot y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n$$

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

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y} (-1)^{x \cdot y} |y\rangle |f(x)\rangle$$

$\xrightarrow[\text{Top n qubits}]{\text{meas.}}$ outcome y w/. prob.

$$p_y := \left\| \frac{1}{2^n} \sum_x (-1)^{x \cdot y} |f(x)\rangle \right\|^2$$

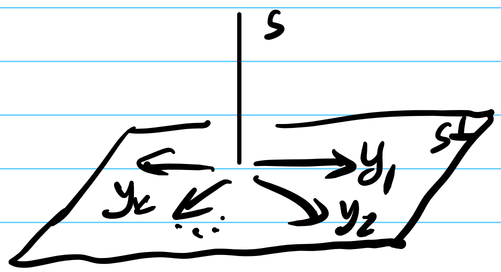
$$= \left\| \frac{1}{2^n} \sum_{z \in \mathrm{range}(f)} \alpha_z |z\rangle \right\|^2$$

$$\alpha_z = (-1)^{x_z \cdot y} + (-1)^{(x_z \oplus s)\cdot y}$$

$$= (-1)^{x_z \cdot y}\left(1 + (-1)^{s\cdot y}\right)$$

$$= \begin{cases} 0 & y\cdot s = 1 \\ \neq 0 & y \cdot s = 0 \end{cases}$$

$$p_y := \begin{cases} 0 & \text{if } y\cdot s = 1 \\ \frac{1}{2^{n-1}} & \text{if } y \cdot s = 0 \end{cases}$$



- $s^\perp = \{y : y\cdot s = 0\}$
- Q sampling subroutine
  unif. sample $\leftarrow s^\perp$
- Reconstruct $s^\perp \to s$

D	R	Q
$2^{n-1}+1$	$\sqrt{2^n}$	$O(n)$

3. Quantum Fourier Transform.

Standard basis $\qquad\qquad\qquad\qquad$ Fourier basis

$$\{|j\rangle\} \xrightarrow{F_M} \left\{ |\phi_j\rangle = \frac{1}{\sqrt{2^m}} \sum_k \omega_M^{j\cdot k} |k\rangle \right\}$$

$j \in \{0, \ldots, 2^m - 1\}$

$M = 2^m$

$\omega_M = e^{2\pi i/M}$

$j \cdot k \mod M$

$$F_M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 \cdots & \omega^{M-1} \\ \vdots & \vdots & & \\ 1 & \omega^{M-1} & \cdots & \omega^{(M-1)^2} \end{bmatrix}$$

- Discrete F transform
- FFT : $O(M \log M)$
- Quantum ckt : QFT_M $O(\log^2 M)$

4. Factoring

a. Overview :

<u>Given</u>: $N = p \cdot q$ $\quad$ ($n = \log N$ input size)

<u>Goal</u>: find p.

- Classical : superexp(n)
- Quantum : poly(n)

$$\boxed{\text{factoring}} \xrightarrow{\text{classical}} \boxed{\text{ORDER finding}} \longrightarrow \boxed{\text{QFT}}$$

$\xrightarrow{\qquad\qquad\qquad\qquad}$ Shor

$\left(\longrightarrow \boxed{\text{Ph. Est.}} \right)$

b. ORDER finding.

- $a \in \mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$.

  $\mathrm{ord}_N(a) = \min\{r : a^r = 1 \bmod N\}$.

- <u>Given</u> : N, $a \in \mathbb{Z}_N^*$

  <u>Goal</u> : $\mathrm{ord}_N(a)$

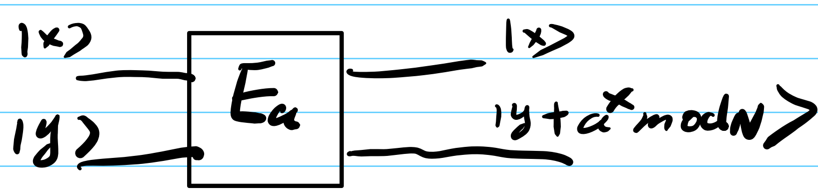
  <u>Thm</u> : $\boxed{\text{Factoring} \equiv \text{ORDER Finding}}$

- Modular exponentiation

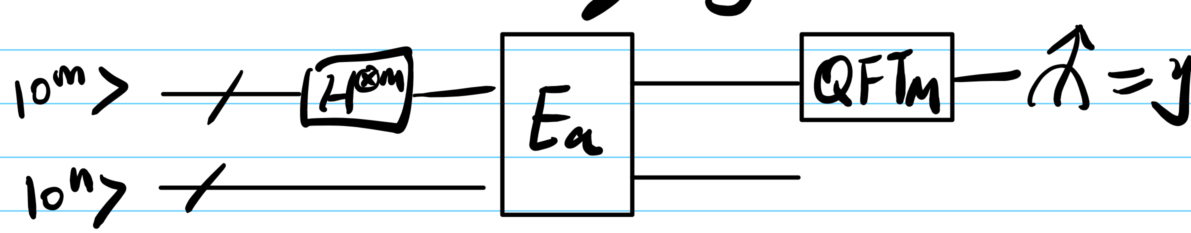
$$E_a : \mathbb{Z} \longrightarrow S \qquad r = \mathrm{ord}_N(a)$$

$$x \longmapsto a^x \bmod N$$

- <u>OBS</u> : $f(x) = f(y)$ <u>iff</u>. $r \mid x - y$

- 

- Shor's ORDER Finding Alg.

① 

② $y_i \rightarrow r$ (Continued fraction)

5. Hidden Subgroup Problem (HSP)
[period finding].

a. <u>DEF.</u>: G: group. S: set

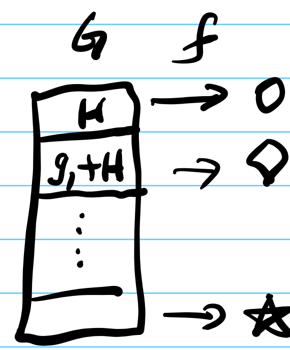
<u>Given</u>: B.B. $f: G \to S$

<u>promise</u>: $\exists H \leq G$, s.t. $\forall x, y \in G$

$$\boxed{f(x) = f(y) \text{ iff. } x \in y + H}$$

i.e.
① (periodic): $\forall x \in G$, $h \in H$
$f(x) = f(x+h)$

② (injective) if $x \notin y + H$
~~then~~ $f(x) \neq f(y)$.



<u>Goal</u>: Find H.

b. Examples

	G	H
Deutsch	$\mathbb{Z}_2 = \{0,1\}$ $\oplus$	$\{0\}$ OR G → Balanced, constant
SIMON	$\mathbb{Z}_2^n, \oplus$	$\{0, s\}$
Factoring OBER Finding	$\mathbb{Z}, +$	$r\mathbb{Z} = \{0, \pm r, \pm 2r, \dots\}$.
DLog	$\mathbb{Z}_N \times \mathbb{Z}_N$	

Pell's equ.	$\mathbb{R}$ [Hallgren '02 '05]	
High-deg number fields	continuous HSP $\mathbb{R}^n$ [EHKS'14] BS'16	PIP $\downarrow$ Break lattice CRYPTO [Chris's Lec.]

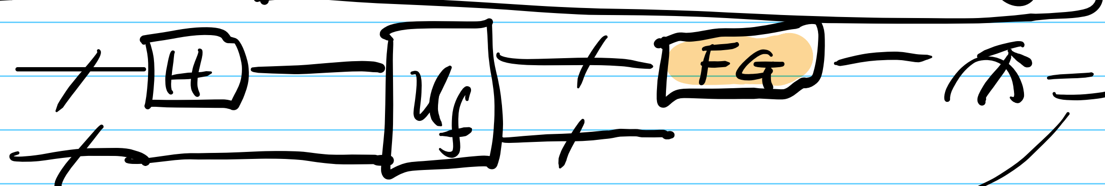
- Some non-abelian HSP.

Graph iso problem	S_N (symmetric group)
unique shortest vector problem	D_N (dihedral group)

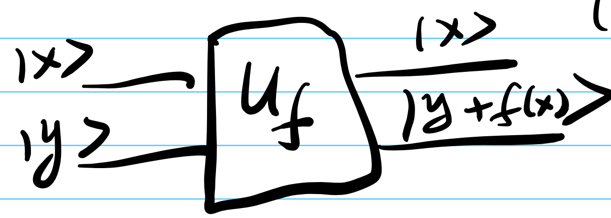
efficient QAlg's unknown

C. Quantum Algs. on Abelian HSP.

$\boxed{\text{key technique : Q Fourier Sampling}}$

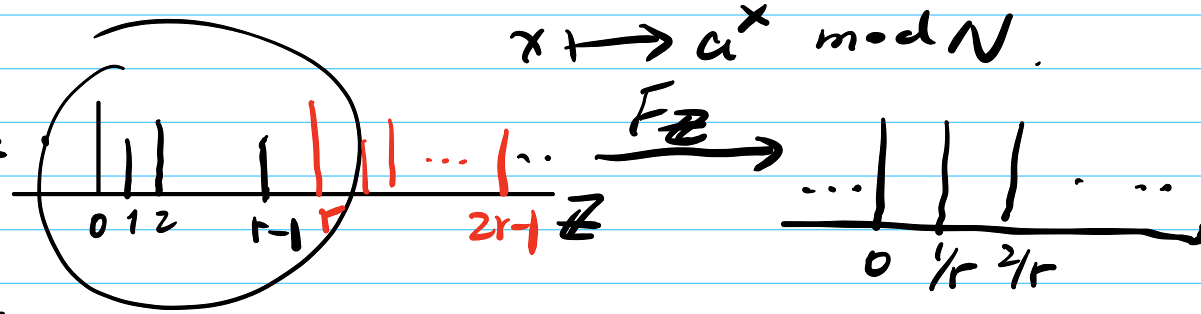


Random Samples from $H^\perp$ (dual) $\to H$



- Recall: $f(E_a): \mathbb{Z} \to S$ $\quad r = \mathrm{ord}_N(a)$

$x \mapsto a^x \bmod N.$



1. Quantum Search.

a. **Given**: $f: \{0,1\}^n \to \{0,1\}$.

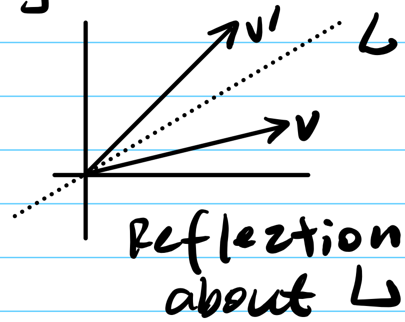
Goal: find x s.t. $f(x) = 1$ (if exists)

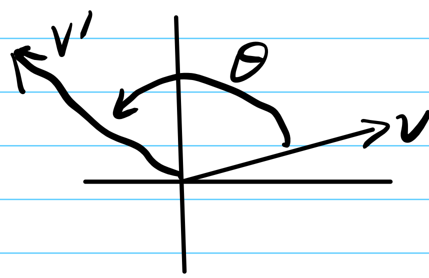
(a marked item)

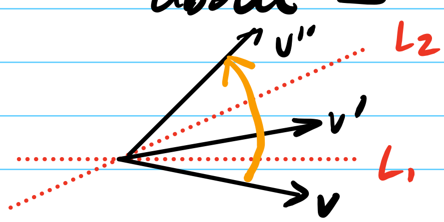
- **Classical**: $\Omega(2^n)$ queries.
- **Quantum**: $O(\sqrt{2^n})$ Q queries.

b. Grover's alg.

- geometric Lemma



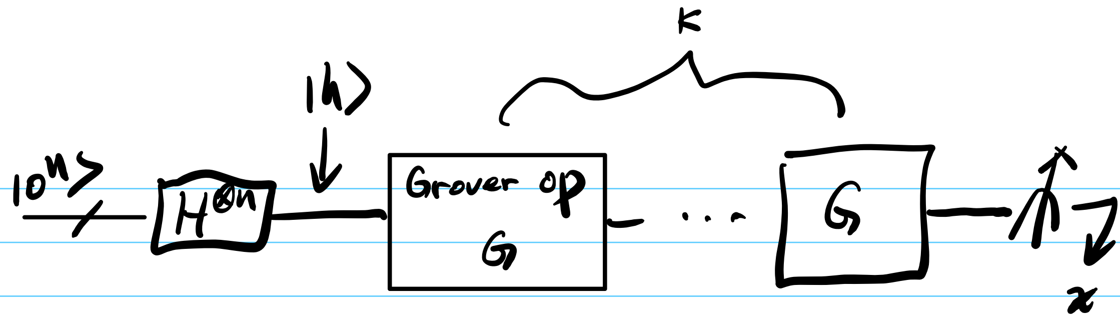




$\angle(L_1, L_2) = \theta$

$\mathrm{Ref}(L_1/L_2)$

$\equiv \mathrm{Rot}(2\theta)$

• 

$$|h\rangle := \frac{1}{\sqrt{N}} \sum_x |x\rangle \quad (N = 2^n)$$

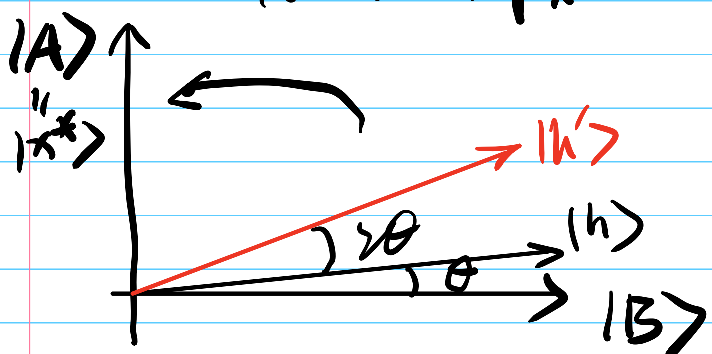
x^*: marked item (unique)

$$|A\rangle := |x^*\rangle$$

$$|B\rangle := \frac{1}{\sqrt{N-1}} \sum_{x \neq x^*} |x\rangle$$

$$\angle(|h\rangle, |B\rangle) = \theta$$

$$\theta = \sin^{-1}\left(\frac{1}{\sqrt{N}}\right) \approx \frac{1}{\sqrt{N}}$$



G: Two reflections about $|B\rangle$ then $|h\rangle$

<u>WANT</u>: $k \cdot 2\theta \approx \frac{\pi}{2}$

$$\Rightarrow k \approx \frac{\pi}{4\theta} = O(\sqrt{N})$$

c. Remarks

• q. a marked items $\quad p_{succ} = \Omega\left(\frac{a \cdot q^2}{N}\right)$

Lec 3.

1. Density matrices.

$|\psi\rangle \in \mathbb{C}^2 \longrightarrow |\psi\rangle\langle\psi|$

Ex1. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$

$\langle\psi| = (\bar{\alpha} \quad \bar{\beta})$

$\Rightarrow |\psi\rangle\langle\psi| = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}(\bar{\alpha} \quad \bar{\beta})$ $\quad \alpha = \beta = \frac{1}{\sqrt{2}}$

$= \begin{pmatrix}|\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2\end{pmatrix} \quad \begin{pmatrix}\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2}\end{pmatrix}$

$\boxed{\text{density matrix}}$

Ex2: $|\psi\rangle = |+\rangle \xrightarrow{\text{meas.}} \begin{cases} |0\rangle & \text{w.p } \frac{1}{2} \\ |1\rangle & \text{w.p } \frac{1}{2} \end{cases}$

$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \begin{pmatrix}\frac{1}{2} & 0 \\ 0 & \frac{1}{2}\end{pmatrix}$

$\equiv$ flip a coin $\begin{cases} \text{HEADS} & \text{prep. } |0\rangle \\ \text{TAILS} & \text{prep } |1\rangle \end{cases}$

- In general:
  - $p_1 \cdots p_k \quad \sum p_i = 1$
  - $|\psi_1\rangle \cdots |\psi_k\rangle$

  pick j w.p p_j

  then prep $|\psi_j\rangle$

$\{p_j, |\psi_j\rangle\} \qquad \rho := \sum p_j |\psi_j\rangle\langle\psi_j|$

$|\psi\rangle\langle\psi|$ vs. $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

pure state — mixed state

- Ex 3. \$ $\begin{cases} H : & |+\rangle \\ T : & |-\rangle \end{cases}$

$$\sigma = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| \qquad \underline{\begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1 & 1\end{pmatrix}}$$

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

$$= \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

- Ex 4. $\rho = \begin{pmatrix} p_1 & & 0 \\ & \ddots & \\ 0 & & p_N \end{pmatrix}$ $\quad \sum p_i = 1$, $p_i \geq 0$

Subsumes classical distr.

- Ex 5. Alice sample $x \leftarrow p_x$
then prep. ρ_x on a Q reg.

Joint system: $\rho = \sum_x p_x \underbrace{|x\rangle\langle x| \otimes \rho_x}_{\text{c-q state}}$

b. Op's.

- Unitary. $|\psi\rangle \xmapsto{U} \boxed{U|\psi\rangle}$

$$\rho = \underline{|\psi\rangle\langle\psi|} \xmapsto{U} U|\psi\rangle(U|\psi\rangle)^\dagger$$

$$= \underbrace{U|\psi\rangle\langle\psi|}_{\rho}U^\dagger$$

$$= U\rho U^\dagger$$

- meas. $\rho \xmapsto{\text{meas}}$ "see x" w.p. $\langle x|\rho|x\rangle$

post state $|x\rangle\langle x|$

c. General Q operations

$$\rho \;—\; \boxed{\Phi} \;—\; \rho'$$

- Quantum channel.

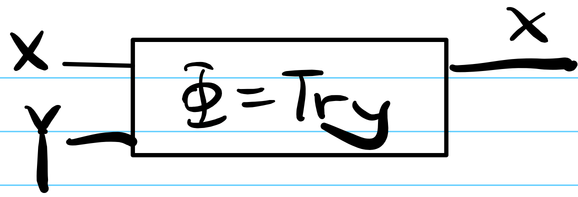
$$\boxed{\begin{array}{l} A_1 \cdots A_m \quad \text{s.t.} \quad \sum_j A_j^\dagger A_j = \mathbb{1} \\ \rho \longmapsto \sum_j A_j \rho A_j^\dagger \quad \text{is Q channel} \end{array}}$$

- Example

Partial trace

X (ξ)

Y (ξ) — discard.



$$A_0 = \mathbb{1}_X \otimes \langle 0|_Y \qquad A_1 = \mathbb{1}_X \otimes \langle 1|_Y$$

- Validity: ✓

★: Apply to $\rho = |\phi^+\rangle\langle\phi^+|$ (EPR)

$$= \frac{1}{2}\Big(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\Big)$$

$$\mathrm{Tr}_Y(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger$$

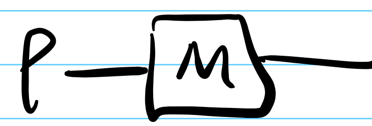
$$= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

$$= \frac{1}{2}\mathbb{1}.$$

d. General meas.

- $M = \{M_a : a \in \Gamma\}$

a ↑ possible outcome



outcome	w.p	post. state
a	$\mathrm{Tr}(M_a \rho M_a^\dagger)$	$\dfrac{M_a \rho M_a^\dagger}{\mathrm{Tr}(M_a \rho M_a^\dagger)}$

- Ex: $M_0 = |0\rangle\langle 0|$ $M_1 = |1\rangle\langle 1|$
- Proj. meas.
  - Each M_a is projection. $M_a^2 = M_a$, $M_a^\dagger = M_a$
- POVM (Positive-Operator Valued meas.)

→ don't care about the post. state only the statistics.

$$a \text{ w.p } \mathrm{Tr}(M_a \rho M_a^\dagger)$$
$$= \mathrm{Tr}(\underbrace{M_a^\dagger M_a}_{E_a} \rho)$$

POVM: $\{E_a : a \in \Gamma\}$.

"a" w.p $\mathrm{Tr}(E_a \rho)$.

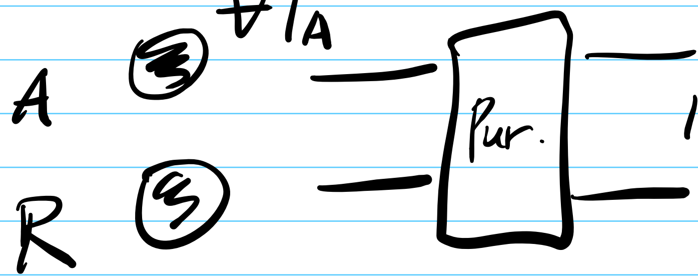
3. <u>Purification.</u>

Schmidt decomp. <u>Thm</u>: $\|\psi\rangle_{AB}$ pure. $\exists$ orth basis $\{\|i_A\rangle\}$ $\{\|i_B\rangle\}$. s.t. $\|\psi\rangle = \sum \lambda_i \|i_A\rangle\|i_B\rangle$ λ_i : sch.. coeff. $\lambda_i \geq 0$ $\sum \lambda_i^2 = 1$.

21

b. Purification of mixed states

$\forall \rho_A$



$|\psi\rangle_{AR}$ pure

s.t. $\mathrm{Tr}_R(|\psi\rangle\langle\psi|_{AR}) = \rho_A$

- proof sketch.
  - $\rho \Rightarrow$ speztral dezomp.

$\rho = \sum_i p_i |i_A\rangle\langle i_A|$ $\quad$ i_A orth basis

- introduze R. $\{|i_R\rangle\}$.

$$|\psi\rangle_{AR} := \sum_i \sqrt{p_i}\, |i_A\rangle |i_R\rangle$$

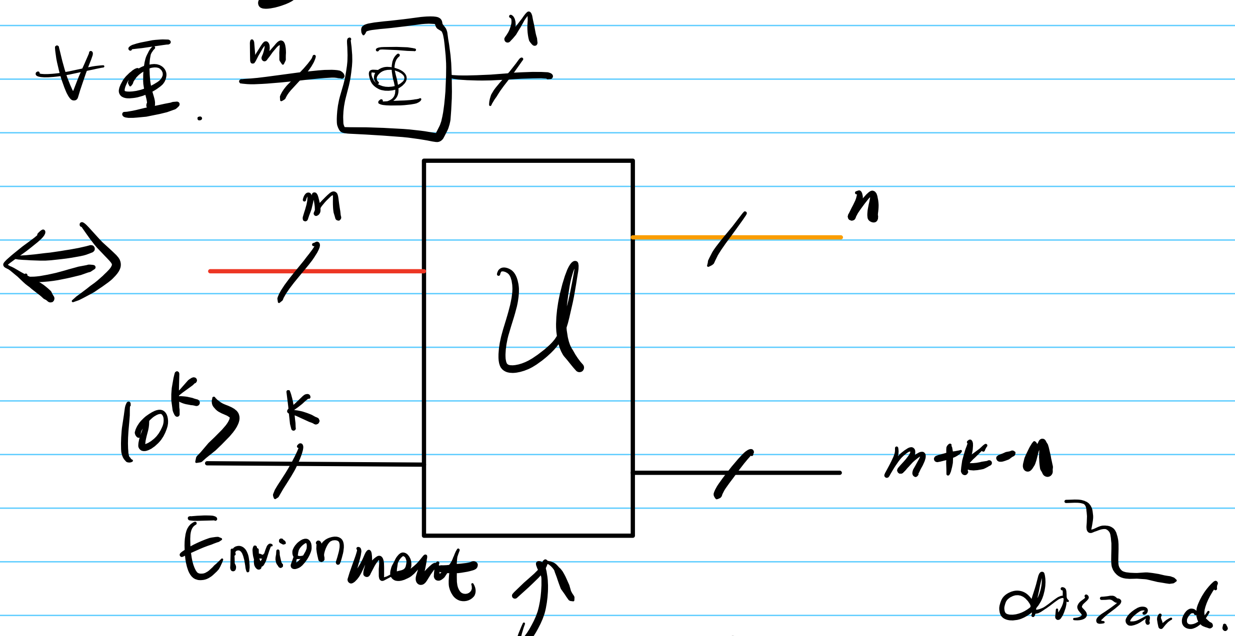
- OBS: $\dim(R) \geq \dim(A)$.
  - unitary equivalenze.

$|\psi\rangle_{AR_1}$ $\quad$ $|\psi\rangle_{AR_2}$ $\quad$ ρ_A

then $\exists\, U_{R_2}$ <u>acting on R_2 only</u>

s.t. $|\psi\rangle_{AR_1} = \mathbb{1}_A \otimes U_{R_2} |\psi\rangle_{AR_2}$

c. Unitary simulation of general ops.



Stinespring form of a Q channel.

Epilogue.

QC./QI.

Quantum Reductions

? NPC ⇒ OWF

Q Money

QKD

[Anne]

superposition

no-cloning

(des. meas.)

[Q side info.]

entanglement

+ Comp. assumption

Quantum Alg. → solve hard problems [CRAZG CHZZS]

break PKC

New Attacks.

CB~~C~~-MAC

[CSST'11]

Multi-prover Commit

Ext~~r~~actor

new security models & analysis

[Domingue & Fermi]

QRO ZK

OWF + QI ⇒ QMPC

PRS [JLS'18]

(Pesudorandom states)

[Dakshita]

Designer's perspective

(QCRYPTO)

Attacker's perspective

(PQC)

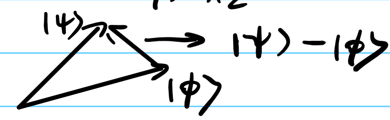
Supplement

* Distances on Quantum States & Channels

a. Simple distances on states

[As vectors, Euclidean is natural]

- Euclidean : $\| |\psi\rangle - |\phi\rangle \|_2$



[Another indicator of the distance is how much they overlap]

- Fidelity : $|\langle\psi|\phi\rangle|$ (inner product)

[how to generalize to mixed states ?]

b. Trace norm / distance

- <u>DEF.</u> $\|M\|_{tr} = \|M\|_1 := \mathrm{Tr}\sqrt{M^\dagger M}$

  - 1-norm of eigenvalues (if M normal)
  - 1-norm of singular values (if M non-normal)

- <u>DEF.</u>

  Trace distance $TD(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1$

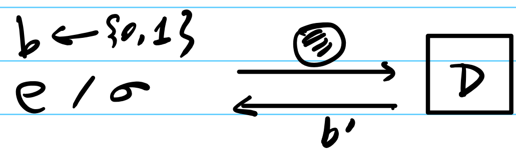
  - <u>OBS</u>: if ρ, σ classical $\begin{pmatrix} p_1 & & \\ & \ddots & \\ & & p_N \end{pmatrix} \begin{pmatrix} q_1 & & \\ & \ddots & \\ & & q_N \end{pmatrix}$

    $TD(\rho, \sigma) = SD(p, q)$

[we know SD captures optimal advantage]
of distinguishing 2 distributions. This generalizes to TD.

-

Thm (Helstrom-Holevo) $\forall \rho, \sigma$, optimal measurement procedure distinguishes them w. prob $\frac{1}{2} + \frac{1}{4}\|\rho - \sigma\|_1$



$P_{succ} = \Pr[b = b']$

$$\delta_D(\rho, \sigma) := \Pr[D(\rho) = 1] - \Pr[D(\sigma) = 1] \leq c \cdot TD(\rho, \sigma)$$

* D needs NOT be efficient.

[Now we generalize fidelity based on trace norm]

c. Fidelity

$$F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$$
$$= \mathrm{Tr}\sqrt{(\sqrt{\rho}\sqrt{\sigma})^{\dagger}\sqrt{\rho}\sqrt{\sigma}}$$
$$= \mathrm{Tr}\sqrt{\sqrt{\sigma}\,\rho\sqrt{\sigma}}$$

- Properties
  - symmetric [Although NOT evident esp. from last exp.] $\|M\|_2 = \|M^{\dagger}\|$
  - $F(\rho,\sigma) \in [0,1]$ $\begin{cases} 1 & \text{iff } \rho = \sigma \\ 0 & \text{iff } \rho\sigma = 0 \text{ (ortho images)} \end{cases}$
  - [multiplicative wrt tensor product]
  $$F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1,\sigma_1)\cdot F(\rho_2,\sigma_2)$$
  - Uhlman's theorem [Explains — how this generalized Fid. for pure — I.P. is called Fidelity] depending on your perspective

$$\boxed{F(\rho,\sigma) = \max_{\substack{|\psi\rangle,|\phi\rangle \\ \text{purifications of } \rho,\sigma}} |\langle\psi|\phi\rangle|}$$

- Relation between Fid. / TD

Thm (Fuchs - van de Graff)

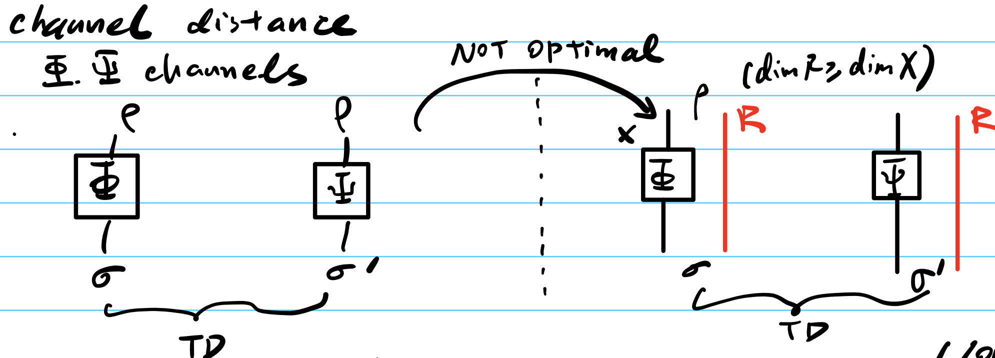
$$\boxed{1 - F(\rho,\sigma) \le TD(\rho,\sigma) \le \sqrt{1 - F(\rho,\sigma)}}$$

[vdG also among the first to notice the issue of q. rewinding]

[Sometimes. Fid. easier to calculate & manipulate] relate back to TD afterwar.

e. channel distance

Φ, Ψ channels



- Formally this is $\|\Phi - \Psi\|_{\diamond}$: diamod norm (completely bounded trace norm)

* Computational analogue can be derived [Wat '09]

References

1. Watrous qc notes 1 - 4; Childs note Chapter 1.
2. Watrous qc notes 6, 8, 12; Childs note Chapter 5, 9, 18.
3. Watrous qc notes 14, 15; Watrous qi note 3,4.

Watrous QC note link: https://cs.uwaterloo.ca/~watrous/QC-notes/
Watrous QI note link: https://cs.uwaterloo.ca/~watrous/TQI-notes/
Childs note link: https://www.cs.umd.edu/~amchilds/qa/qa.pdf