PART 1: SHOR'S ALGORITHM

... IN TWO DIFF. WAYS..

PART 2: course planning mini-topics

Disclaimer: "classical processing" in Shor

is volumenous... "under rug swept"...

PREREQUISITES / REMINDER

QFT

$$|\vec{k}\rangle \xrightarrow{QFT} \frac{1}{2^{n/2}} \sum_{\vec{j} \in \{0,1\}^n} \exp[2\pi i\, kj/2^n]\, |\vec{j}\rangle$$

$\vec{k}$: bitstring, n-bits; $(\vec{x})_2$ integer $0 \dots 2^n-1$

take $\frac{k}{2^n} = \sum_{\ell=1}^{n} k_\ell\, 2^{-\ell}$

Trick: $\equiv \frac{1}{2^{n/2}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + \exp\left[2\pi i \frac{k}{2^\ell}\right] |1\rangle \right)$

- EASY CIRCUIT ($O(n^2)$, approx. $O(n \log n)$)

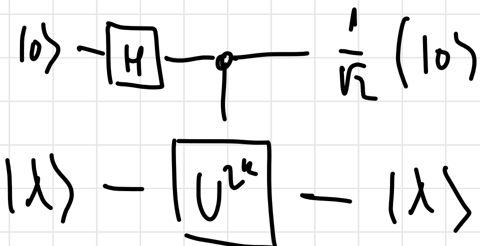
QUANTUM PHASE ESTIMATION. (KITAEV 1995)

Input: ctrl-U, $|\lambda\rangle$ s.t. $U|\lambda\rangle = \lambda|\lambda\rangle = e^{2\pi i\theta}|\lambda\rangle$

Output: $|\psi\rangle|\lambda\rangle$, s.t. $|\langle\psi|\tilde{\theta}\rangle| \geq 0.4$ with $|\hat{\tilde{\theta}} - \theta| \leq \varepsilon$

using $O(1/\varepsilon)$ calls to U

Trick



$\frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left[2\pi i\,(2^k\theta)\right]|1\rangle\right)$

because eigenvector

Phase kick-back in essence...

In other words, outputs $\log_2(1/\varepsilon)$ digits of θ with high probability, using $O(1/\varepsilon)$ calls to ctrl-U

Efficiency important, $\exists$ trivial solutions via "process tomography"

Application Order-finding

$a, b \in \mathbb{Z}$, $a \equiv b \pmod N$ if $N \mid a-b$

$\Rightarrow$ a & b have the same remainder when divided by N.

ORDER FINDING. INPUT: $x, N \in \mathbb{N}$

OUTPUT: smallest r s.t.

$$x^r \equiv 1 \pmod N$$

Note: by Euler's theorem $\exists\, r$ (namely $\phi(N)$)

st $x^{\phi(N)} \equiv 1 \pmod N$ $\forall\, x$, $\gcd(x, N) = 1$

SKIP

Group & Number-theoretic background.

$\mathbb{Z}_N = \{0, \dots, N-1\}$ (group w.r.t. $+$, in general not wrt $\times$)

$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N \mid \gcd(a, N) = 1\}$ => Field !
(group wrt both)

$\varphi(N) = |\mathbb{Z}_N^*|$ "Euler totient function"

note, all operations are mod N

$(\mathbb{Z}_N^*, \times)$: $a \times b := ab \bmod N$

since group: $\forall a \; \exists a^{-1} \quad aa^{-1} \equiv 1 \bmod N$.

Euler's theorem: $a^{\varphi(N)} \equiv 1 \pmod{N}$

good to know.

SKIP

why? a is co-prime to N.

$\Rightarrow \{a^0, a \bmod N, a^2 \bmod N \ldots a^k \bmod N \ldots\} =: \langle a \rangle$
is a (multiplicative) subgroup of $\mathbb{Z}_N^*$

$|\langle a \rangle| = o(a) =: m$ & $\underline{a^m = 1}$

By Lagrange's Theorem $m \mid \varphi(N) \Rightarrow \varphi(N) = g \cdot m$

$\Rightarrow a^{\varphi(N)} = a^{g \cdot m} = (1)^g = 1$.

Back to reality

$$\boxed{\text{No classical algorithm for order-finding in } \underline{\text{poly}(\log_2(N))}}$$

$$\underset{r \in \mathbb{N}}{\operatorname{argmin}} \quad x^r \equiv 1 \pmod N$$

1) $\exists$ efficient quantum algorithm. Two ways of understanding.

2.) It suffices for Factoring.

Shor: the classical bits:

TASK: Find (non-trivial) factors of N

Step 1: check PRIMALITY (2002, ASK. "PRIMES is in P")

Step 2: check prime powers. i.e. $N = p^k$, $k > 1$.

How: let $N = p^k$, note $k \leq \log(N)$

$\rightarrow$ compute $\underbrace{N, \sqrt{N}, N^{\frac{1}{3}}, \dots N^{\frac{1}{\log(N)}}}_{\log(N) \text{ operations.}}$

Not prime power or prime?

Step 3 (N is not a prime power)

1.) choose an arbitrary $a < N$

2.) Compute $\gcd(a, N)$ using Euclid's algorithm

↳ polylog in N.

$\gcd(a,N) > 1 \Rightarrow$ Factor of N, done.

3) [a, N are co-prime] Find order r. a, N

So r is smallest $\mathbb{N}$ st

$$a^r \equiv 1 \pmod N$$

4) IF r is odd, goto (1) [happens $1/2$ OF TIME]

Under rug swept...

Else $r/2 \in \mathbb{N}$.

Spoiler: $\left(a^{\frac{r}{2}}\right)^2 \equiv 1 \pmod N \Rightarrow \left(a^{\frac{r}{2}}\right)^2 - 1 \equiv 0 \pmod N$

$$\Rightarrow N \mid \underbrace{\left(a^{\frac{r}{2}} - 1\right)}_{p} \underbrace{\left(a^{\frac{r}{2}} + 1\right)}_{q} \;;\Rightarrow p \cdot q = \alpha N \Leftrightarrow \gcd(N, q) \text{ or } \gcd(N, p)$$

Almost. can be that

$$a^{\frac{r}{2}} \equiv -1 \pmod{N} \ldots$$

5) check $a^{\frac{r}{2}} \equiv -1 \pmod{N}$

if yes goto 1 (happens rarely)

under rug swept

else

6) $N \mid (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$

$\Rightarrow \gcd(N, a^{\frac{r}{2}} - 1)$ or $\gcd(N, a^{\frac{r}{2}} + 1)$ is a factor

Quantum order finding.

N , a given on input, $\gcd(a, N) = 1$.

consider unitary on n qubits $2^{n-1} \leq N \leq 2^n$,

performing: $$U_a |x\rangle = \underbrace{|x \cdot a \pmod{N}\rangle}_{\text{basis states.}} \quad \forall\, x \leq N$$

for $x \leq N$. We do not care beyond.

Claim 1. . such $\underline{U_a}$ $\underline{\exists}$.

why? $x \overset{f}{\longmapsto} a \cdot x \pmod N$

f: is invertible

NUMBER THEORY WINDOW

if $\gcd(a, N) = 1$, $\exists$
$a^{-1} \in \{1 \ldots N-1\}$
st $a a^{-1} \bmod N = 1$.

$f^{-1}: y \longmapsto a^{-1} y \pmod N$

$\Rightarrow$ f is a permutation $\Rightarrow$ $\exists$ unitary

Note: not difficult to construct; classical circuit $\rightarrow$ Toffoli...

VERSION 1. NOT FULL PROOF, BUT INTUITION

via period finding

$\Rightarrow$ can construct

$$|x\rangle \longmapsto |a^x \pmod N\rangle$$

Assume $x \in [0, \dots, N^2-1]$

Who cares?? We need order finding! $\left(\underset{r}{\operatorname{argmin}}\ a^r \equiv 1 \bmod N\right)$

$$f(x) = a^x \bmod N$$

Let T st $f(x) = f(x+T)\ \forall x$

Specially $f(0) = f(T)$

$$\Rightarrow a^T \bmod N = a^0 \bmod N$$

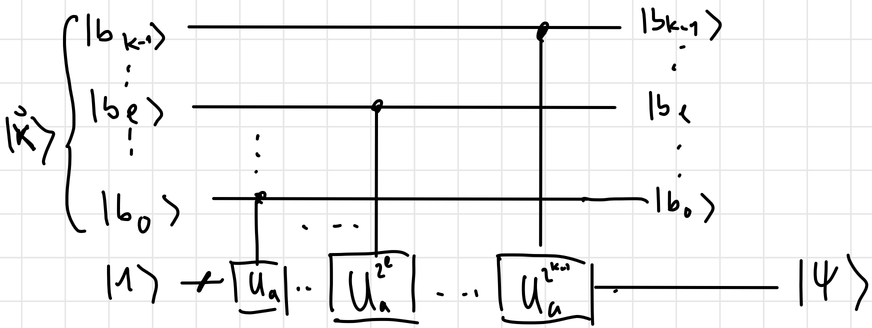
$$\Rightarrow a^T \equiv 1 \pmod N$$

✓ SAME THING

Finding period enough. Constructing $|\tilde{r}\rangle|1\rangle \to |\tilde{r}\rangle|a^r \bmod N\rangle$

Let $\tilde{x} = b_{k-1} b_{k-2} \cdots b_0$

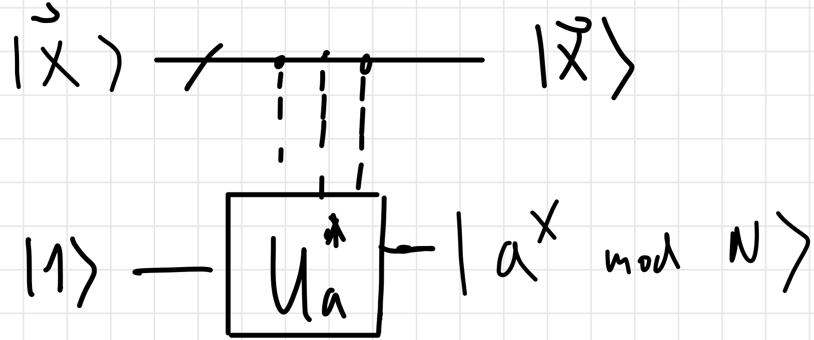
NB: $U_a^k |1\rangle = |\underbrace{a \cdot a \cdots a}_{k} \cdot 1 \pmod N\rangle$



$$|\psi\rangle = \left(U_a^{2^{k-1}}\right)^{b_{k-1}} \left(U_a^{2^{k-2}}\right)^{b_{k-2}} \cdots \left(U_a^{2^l}\right)^{b_l} \cdots \left(U_a\right)^{b_0} |1\rangle =$$

$$= |a^{b_0} a^{2b_1} \cdots a^{2^l b_l} \cdots a^{2^{k-1} b_{k-1}} 1 \pmod N\rangle = |a^x \bmod N\rangle$$

$\Rightarrow$



Next: Period Finding (without detail)

Under rug swept: efficient modular exponentiation

We can compute $a^{2^k} x \bmod N$ more efficiently than 2^k compositions of $f: x \to a^x \bmod N$ ...

Step 1. Do it on uniform superposition of all inputs up to N^2

$$\sum_{x=0}^{N^2-1} |x\rangle_{I} |0\rangle_{II} \xrightarrow{c\text{-}U^{\#}} \sum_{x=0}^{N^2-1} |x\rangle_{I} |a^x \bmod N\rangle_{II} \qquad \text{(ignoring normalization)}$$

Step 2. Measure Register II; get some k, randomly

$$\Rightarrow \sum_{\substack{x \text{ st} \\ a^x \equiv k \bmod N}} |x\rangle |k\rangle \ldots$$

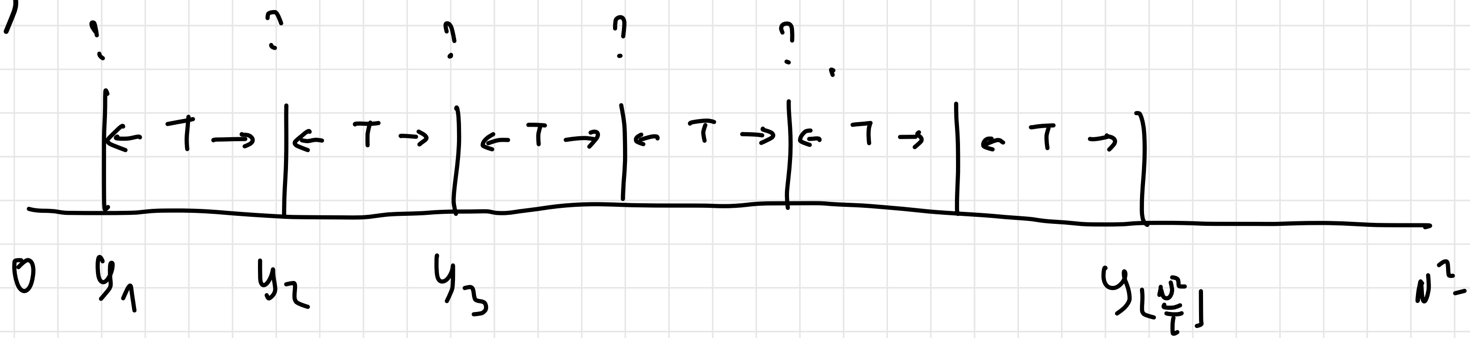
Analyzing the "remaining state"

$$|\psi_k\rangle|k\rangle = \alpha \sum_{\underbrace{x \text{ st } a^x \bmod N = k}} |x\rangle|k\rangle$$

Period

(note $a^x \bmod N = a^{x+T} \bmod N$

$|\psi_k\rangle$



"Spike train"

Suppose I had 2 copies of $|\psi_k\rangle$... could get y_ℓ & $y_{\ell'}$, $\ell \neq \ell'$ (very likely)

$\Rightarrow$ $(y_\ell - y_{\ell'}) = \alpha T$ for some $\alpha \in \mathbb{N}^+$

$\Rightarrow$ possible to get T efficiently.

But to "see" same k twice $(|\psi_k\rangle^{\otimes 2})$, need $O(N)$ samples...

Otherwise classical algo. could do it.

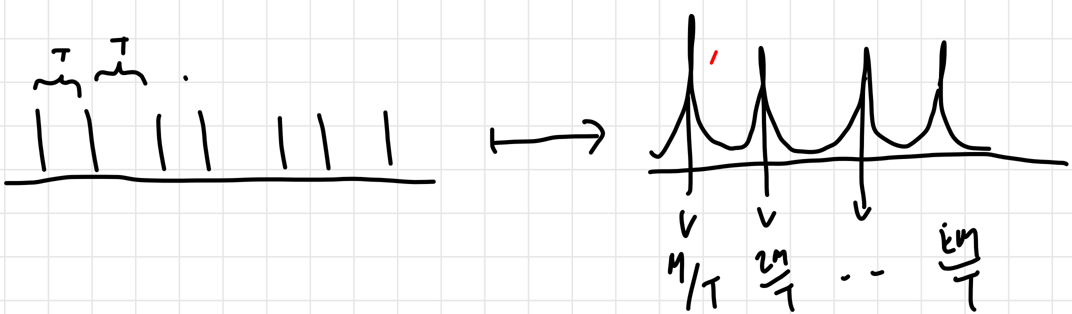
Solution: be Sneaky & treat $|\psi_k\rangle$ as a Signal

with freqency $\frac{1}{T}$ (period T).

Fourier analysis:

If f is periodic with period T $\mathcal{F}(f)(x)$ is periodic with $\frac{M}{T}$

$\Rightarrow$ QFT $|\psi_k\rangle$ is not too far from a spike train.



$M = 2^n$

Measurement reveals $\alpha \in [0 .. 2^n]$

st $\frac{\alpha}{2^n} \approx \frac{S}{T}$ For some S

$\Rightarrow$ can obtain T efficiently

Under rug swept:
"Continued fractions algorithm"

__Recall__: Smallest period T of $x \to a^x \bmod N$

__is__ the order of a in $\mathbb{Z}_N^*$.

$\Rightarrow \underset{r \in \mathbb{N}}{\operatorname{argmin}}\; a^r \equiv 1 \pmod N$ Done.

Shor (version 1)

→ make sure not prime power

→ do period finding on $a^x \bmod N$ via QFT.

→ reveals approximation of $\frac{s}{r}$ for some s

→ sufficient ..

A different perspective

$\Rightarrow$ need $\underset{r \in \mathbb{Z}}{\text{argmin}}\ a^r \equiv 1 \mod (N)$

order finding directly

have $U_a |x\rangle = |a x \pmod N)\rangle$

what are the EIGENVECTORS of U_a ? ?

$$|\psi_0\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + |a\rangle + |a^2\rangle + \dots |a^{r-1}\rangle \right)$$

$$U_a |\psi_0\rangle = |a\rangle + |a^2\rangle + \dots |1\rangle$$

Huh...

$$|\psi_1\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle \dots + \omega^{-(r-1)}|a^{r-1}\rangle \right)$$

$$U_a |\psi_1\rangle = \omega_r |\psi_1\rangle \quad !$$

Let

$$|\psi_j\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-j}|a\rangle + \dots \ \omega_r^{-j(r-1)}|a^{r-1}\rangle\right)$$

$$\Rightarrow \quad U_a|\psi_j\rangle = \omega_r^{j}|\psi_j\rangle$$

[recall $\omega_r = \exp(2\pi i/r)$]

$\Rightarrow$ QUANTUM PHASE ESTIMATION

on U_a, given $|\psi_\ell\rangle$,

will reveal $\frac{\ell}{r}$

$\Rightarrow$ continued fractions gives r.

Don't have $|\psi_\ell\rangle$?

Not a problem:

Check:

$$\frac{1}{r}\sum_{\ell=0}^{r-1}|\psi_\ell\rangle = |1\rangle + \underbrace{\left(\sum_\ell \omega^{-\ell(r-1)}\right)}|a\rangle + \underbrace{\left(\sum_\ell \omega^{-2\ell(r-1)}\right)}|a^2\rangle + \dots (\quad)|a^{r-1}\rangle$$

sums of all powers of roots of unity

$\Rightarrow$ all zero

$$|1\rangle = \sum_{l=0}^{r-1} |\psi_l\rangle$$

$\Rightarrow$ QPE on U_a starting from $|1\rangle$ generates

$$\sum_{l=0}^{r-1} |\text{phase of } \omega_r^l\rangle |\psi_l\rangle$$

$$= \sum |\text{"}\tfrac{l}{r}\text{"}\rangle |\psi_l\rangle$$

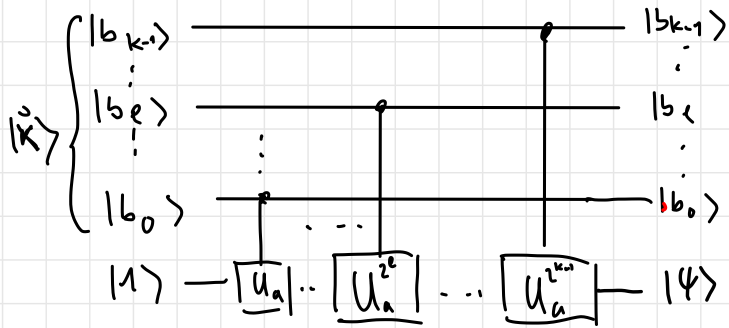
$\Rightarrow$ I will measure one of them.

reveal some $\frac{l}{r}$ $\Rightarrow$ can obtain r

Via Continued Fractions...

Via Period finding

- Let $\tilde{x} = b_{k-1} b_{k-2} \dots b_0$



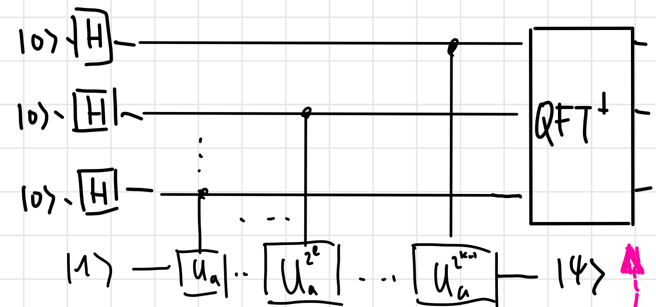
↳ implements $|a^x \bmod N\rangle$

- take as input $\sum_{x=0}^{N^2-1} |x\rangle = H^{\otimes} |0\rangle \sim |0\rangle$

- do QFT† on output

Via Order finding

Do QPE on $|1\rangle$, U_a :



It is the same algorithm.

Measurements?

Note, again we learn some (spectral) property of a unitary ... ($U_a \to \omega_r^e$)

eigenphase

RELEVANCE OF SHOR...

- Factoring & discrete logarithm at basis of RSA & Diffie-Hellman

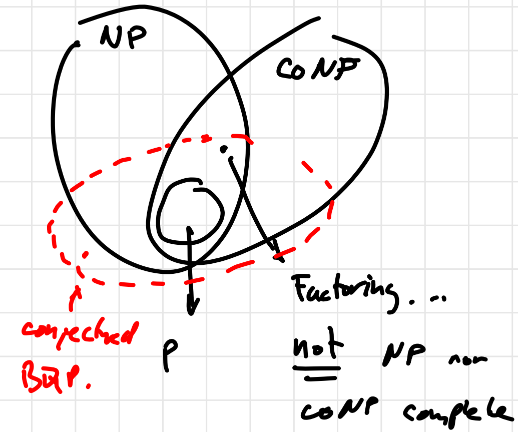
"practical"

- runtime: $O(n^2 \log n)$ vs $\exp(1.9\, n^{1/3})$

  (sub) exponential separation

  → AND WE REALLY TRIED

(Many other algos with exp. separation but we did not try as hard...



WHERE TO NEXT...

In 5 lectures: Basics, Deutsch-Jozsa, Grover + application, QPE & QFT.
Shor

6 lectures remaining (will steal 1 from Casper)

Will cover:

- Hamiltonian simulation + Quantum LINEAR ALGEBRA
- QUANTUM TOPOLOGICAL DATA ANALYSIS (Q. Machine Learning 1)
- QUANTUM APPROXIMATE OPTIMIZATION ALGORITHM (QAOA)
- QUANTUM WALKS FOR QUANTUM BACKTRACKING
- QUANTUM MACHINE LEARNING 2

TWO SLOTS OPEN

- Simon's problem, Bernstein-Vazirani, Hidden Subgroup Problem BUUUUU –
- On Classical Quantum Separations + Quantum complexity Theory YAY
- Quantum Supremacy + Q. complexity theory BUU –
- Quantum error correction + Q. Fault tolerance & a bit about implementations & physics YAY
- Alternative models of Quantum computation & applications YAY
- Quantum Cryptography & Quantum information YAY

D.M. [illegible] + BB 84 + NBRL + D.Q.C.

A bit of Math we skipped:

- Density matrix formalism ,
- Partial trace
- Quantum Channels

→ Stinespring dilation theorem

System $\longleftrightarrow$ $\mathcal{H}$ inner product space, complete w.r.t.

$\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$

$\Leftrightarrow$ has countable orthonormal basis

Operators $T \in \mathcal{L}(H)$

$\to$ "trace class" $\to$ $\mathrm{tr}(T) < \infty$

State space $S(H) = \{ \rho \in T(H) \mid \rho > 0, \ \mathrm{tr}(\rho) = 1 \}$

positive-semidefinite

trace 1.

Quantum states = "density matrices"

NB, $\rho, \sigma \in S(H)$

$\rightsquigarrow \quad p_0 \rho + p_1 \sigma \in S(H)$

$\Rightarrow$ spectral theorem

$$\rho = \sum_i p_i \, \Pi^{|\psi_i\rangle} \quad ; \quad \Pi^{|\psi_i\rangle} = |\psi_i\rangle\langle\psi_i| \in S(H)$$

not ρ ?

$\Rightarrow$ MIXED STATE

$\Rightarrow$ $S(H)$ is a convex set.

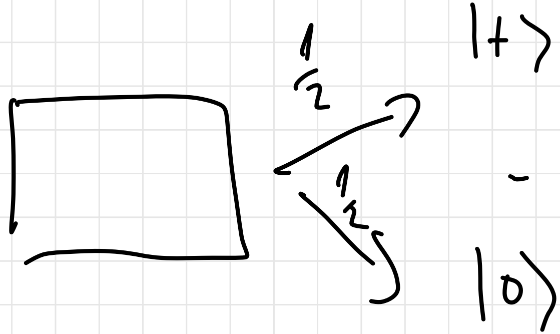
$\Rightarrow$ extremal point: rank-1 projectors

$\Rightarrow$ $|\psi\rangle\langle\psi|$; $|\psi\rangle \in H$

Pure states $|\psi\rangle \longleftrightarrow |\psi\rangle\langle\psi|$ $\qquad \overbrace{\alpha\alpha^{+}}^{1} |\psi\rangle\langle\psi|$

note $(\alpha|\psi\rangle)^{+} = (\alpha^{+}\langle\psi|)$

no global phase



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

$$\rho = \frac{1}{2}\left(\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} + \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\right)$$

$$= \begin{pmatrix}1/4 + \frac{1}{2} & \frac{1}{4}\\ \frac{1}{4} & 1/4\end{pmatrix} = \begin{pmatrix}3/4 & 1/4\\ 1/4 & 1/4\end{pmatrix}$$

$$\text{Purity} = \mathrm{tr}(\rho^2)$$

Note $\frac{1}{2}\left(|+\rangle\langle+| + |-\rangle\langle-| \right) = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| \right)$

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

"maximally mixed state.

→ tensor products.

→ evolution

$$\mathcal{U} : \mathcal{L}(H) \to \mathcal{L}(H)$$

$$\mathcal{U}(\rho) = U \rho U^{\dagger}$$