Lecture 7

Oct 17, 2024

<u>Thm</u> (Schmidt Decomposition)

Any pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be expressed as

$$\sum_{i=1}^{d} \lambda_i |u_i\rangle |v_i\rangle$$

Schmidt coefficients

where $d \leq \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B)$, $\lambda_i \geq 0$, $\sum \lambda_i^2 = 1$,

$\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ are orthonormal vectors within $\mathcal{H}_A, \mathcal{H}_B$, respt.

This is a special case of singular value decomposition.

Recall SVD, for any matrix $M: \mathcal{H}_B \to \mathcal{H}_A$, $\quad M = \mathcal{U}\Lambda\mathcal{V}$

$$\mathcal{U} = \sum_i |u_i\rangle\langle i| \ , \quad \Lambda = \sum_i \lambda_i |i\rangle\langle i| \ , \quad \mathcal{V} = \sum_i |i\rangle\langle v_i| .$$

orthonormal basis of $\mathcal{H}_A$. , $\Lambda \geq 0$, orthonormal basis of $\mathcal{H}_B$.

so $\quad M = \sum_i \lambda_i |u_i\rangle_A \langle v_i|_B .$

Pf of Schmidt Decomposition:

Let T be the map $\langle v| \mapsto |v\rangle$ for any $|v\rangle \in \mathcal{H}_B$.

For any vector $|\psi\rangle = \sum_{jk} \psi_{jk} |j\rangle|k\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$

Consider $M = \sum_{jk} \psi_{jk} |j\rangle\langle k|$.

Then,
$$|\psi\rangle = T \circ M$$
$$= T\left(\sum_i \lambda_i |u_i\rangle\langle v_i|\right)$$
(by SVD)
$$= \sum_i \lambda_i |u_i\rangle\langle v_i|. \quad \blacksquare$$

Schmidt decompositions are very useful.

Given $|\psi\rangle_{AB} = \sum_i \lambda_i |u_i\rangle|v_i\rangle$, it is easy to check

$$\psi_A := \mathrm{tr}_B(|\psi\rangle\langle\psi|) = \sum \lambda_i^2 |u_i\rangle\langle u_i|$$

$$\psi_B := \mathrm{tr}_A(|\psi\rangle\langle\psi|) = \sum \lambda_i^2 |v_i\rangle\langle v_i|$$

Def. (Purification)

given a density matrix $\rho_A \in \mathcal{H}_A$, a purification is <u>any</u> state $|\varphi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_{A'}$ s.t. $\mathrm{tr}_{A'}(|\varphi\rangle\langle\varphi|) = \rho_A$.

A purification is a pure state whose statistics when acting only on A mirror that of ρ_A.

① A purification always exists when $\mathcal{H}_{A'} \cong \mathcal{H}_A$.

$\rho = \sum_i p_i |u_i\rangle\langle u_i|$ then $|\varphi\rangle = \sum_i \sqrt{p_i}\, |u_i\rangle_A |u_i\rangle_{A'}$

is a purification.

(Uhlmann's Thm)

② Let $|\varphi\rangle_{AA'}$ and $|\tau\rangle_{AA''}$ be two purifications of ρ. Then

$$\exists\, V : \mathcal{H}_{A'} \to \mathcal{H}_{A''} \text{ s.t. } \mathbb{1}_A \otimes V\, |\varphi\rangle = |\tau\rangle$$

(Pf sketch) Consider the Schmidt decompositions of $|\varphi\rangle$ and $|\tau\rangle$

$$|\varphi\rangle = \sum_i \lambda_i |u_i\rangle|v_i\rangle$$

$$|\tau\rangle = \sum_i \mu_i |w_i\rangle|z_i\rangle$$

The Schmidt coefficients of both are the roots of the eigenvalues of ρ.

So $\lambda_i = \mu_i$.

$|u_i\rangle$ and $|w_i\rangle$ must be eigenvectors of ρ.

If distinct (easy case), then $|u_i\rangle = |w_i\rangle$ up to global phase.

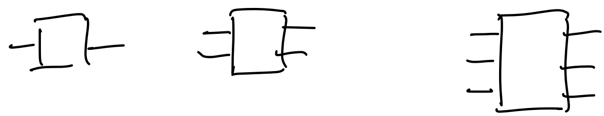
Then it remains only to identify a mapping $|v_i\rangle \mapsto |z_i\rangle$. ∎

Today:

- The circuit model
- A faster search algorithm (Grover's)

We need a way to describe a sequence of elementary quantum operations.

Quantum gate: a $1, 2, 3, \dots O(1)$ qubit unitary.

Depicted as 

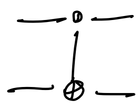
<u>Ex.</u>

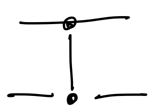
$-\boxed{Z}-$ $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$

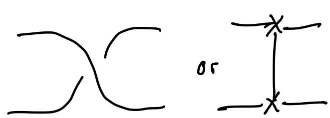
$-\boxed{H}-$ $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

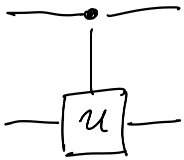
$-\boxed{T}-$ $\begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$

$-\boxed{X}$ $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$

 $\begin{pmatrix}1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1\\ & & 1 & 0\end{pmatrix}$ CNOT

 $\begin{pmatrix}1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1\end{pmatrix}$ CZ

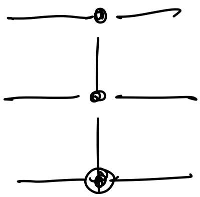
 $\begin{pmatrix}1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1\end{pmatrix}$



C-U

"control-U"

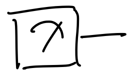
$$\begin{pmatrix} \mathbb{1} & 0 \\ 0 & U \end{pmatrix}$$



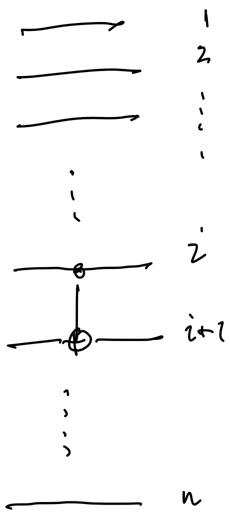
CCX

(Toffoli)

Measurement:



measurement in the standard basis.



CNOT gate between i and $i+1$ qubits, $\mathbb{1}$ on rest.

we can allow gates between any $O(1)$ qubits.

Initialize a qubit:

$-|0\rangle$ or $-|+\rangle$, etc.

Def. A quantum circuit is a classical description of a sequence of gates.

quantities of interest:

# of gates, # of wires, # of uninitialized qubits.

description complexity in terms of # of bits.

Recall, from classical complexity theory:

A <u>language</u> $\mathcal{L}$ is a subset $\mathcal{L} \subseteq \{0,1\}^*$.

A <u>promise language</u> is a pair $\mathcal{L}_{yes}$ & $\mathcal{L}_{no} \subseteq \{0,1\}^*$ s.t.

$$\mathcal{L}_{yes} \cap \mathcal{L}_{no} = \emptyset.$$

A language $\mathcal{L}$ is in $DTIME(t(n))$ if $\exists$ a turing machine which decides if $x \in \mathcal{L}$ and halts in time $t(|x|)$.

Equivalently, for $t(n) \geq n$, a language $\mathcal{L}$ is in $DTIME(t)$ if $\exists$ a logspace uniform turing machine M s.t.

(i) $M(1^n) = \langle C_n \rangle \leftarrow$ Description of classical reversible circuit on n-bits + $t(n)$ ancilla.

② $C_n(x, 0^{t(n)}) = \mathbb{1}\{x \in \mathcal{L}\}$.

This second def is helpful for defining $\mathrm{BQTIME}[t(n)]$.

For $t(n) \geq n$, a promise language $\mathcal{L}_{yes}, \mathcal{L}_{no}$ is in $\mathrm{BQTIME}(t)$ if $\exists$ a logspace uniform Turing machine M s.t.

① $M(1^n) = \langle C_n \rangle \leftarrow$ Description of quantum circuit on n-qubits + $t(n)$ ancilla, with 1 measument gate.

② if $x \in \mathcal{L}_{yes}$, $\Pr[\chi = 1 \text{ on input } (x, 0^t)] \geq 2/3$
if $x \in \mathcal{L}_{no}$, $\Pr[\chi = 1 \text{ on input } (x, 0^t)] \leq 1/3$

Common misconception: "Factoring $\in$ BQP"

① Factoring is not a decision problem.

② Primes is a decision problem: Decide if $x \in \{0,1\}^n$ representing an int in binary is prime or not.

PRIMES $\in$ P (Agrawal-Kayak-Saxena)

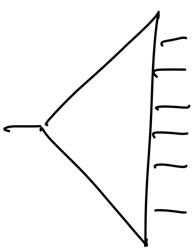
2006 Gödel & Fulkerson prize

(3) We can use PRIMES to generate factors for composite numbers since factoring isn't self-reducible

Today: 3-SAT on n variables, m clauses is in $\mathrm{BQPTIME}\left[O(m \cdot \sqrt{2^n})\right]$

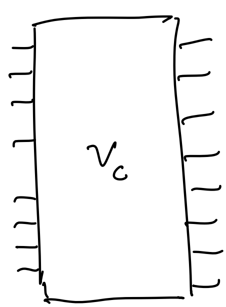
Precusor: classical computation as a reversible ckt.

Pset 1 problem 8 had you show that any classical bool. ckt. can be converted into one that was reversible, used and reset ancillas, and not too much larger.



$C: \{0,1\}^n \to \{0,1\}$

$\Longrightarrow$



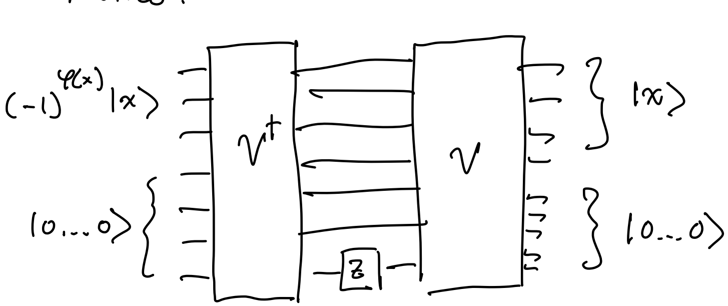
$V: \{0,1\}^{n+|C|+1} \to \{0,1\}^{n+|C|+1}$

where every gate of V is diagonal (i.e. classical).
and # of gates in V = $2 \cdot$ # of gates in C

$$V(x, 0^{|C|}, b) = (x, 0^{|C|}, b + C(x)).$$

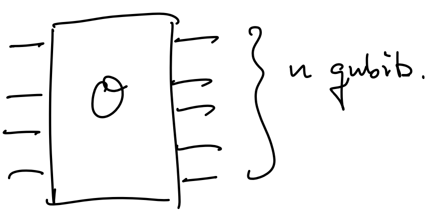
For any 3-SAT formula φ, then $\exists$ a reversible ckt V which computes if x satisfies φ.

Notice:



"Compute the fn φ in the phase"

Use this transformation as a "black-box" transformation



$\varphi \in$ 3-SAT if $\exists\, x$ s.t. $\varphi(x) = 1$ i.e. $\qquad \mathcal{O} \neq \mathbb{1}$

$\varphi \notin$ 3-SAT if $\forall\, x$, $\varphi(x) = 0$. $\qquad \mathcal{O} = \mathbb{1}$.

Claim $\exists$ an alg deciding if

- (yes) $\quad \mathcal{O} = \mathbb{1} - 2|x_1\rangle\langle x_1| - 2|x_2\rangle\langle x_2|$
  $- 2|x_k\rangle\langle x_k|$
  for $x_1, \dots, x_k \in \{0,1\}^n$
- (no) $\quad \mathcal{O} = \mathbb{1}$

with a runtime of $O(\sqrt{2^n})$ calls to $\mathcal{O}$ + $O(\sqrt{2^n})$ additional gates.

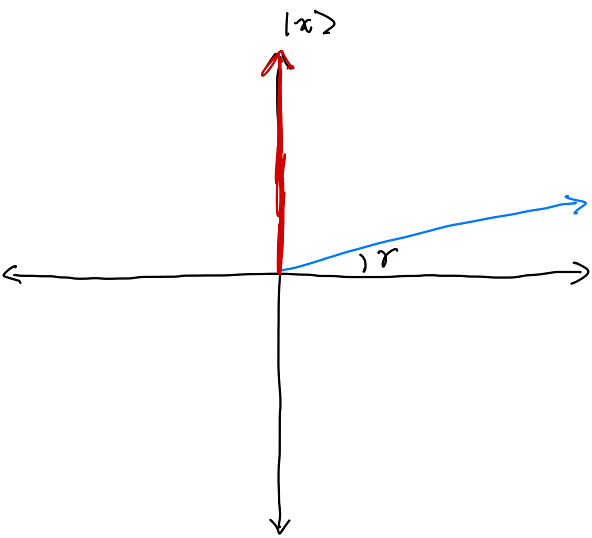
In class: we will only consider

$\mathcal{O} = \mathbb{1} - 2|x\rangle\langle x|$ vs $\mathcal{O} = \mathbb{1}$.

This "oracular" version is also known as unconstrained search, since O is basically an oracle identifying 1 marked string x or no marked strings.

Classically: Any alg takes time $\Omega(2^n)$ even with randomness (we will prove).

Lets create an alg which when $O = \mathbb{1} - 2|x\rangle\langle x|$ finds x (which we can then check).



$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_y |y\rangle .$$

$$\sin \gamma = \frac{1}{\sqrt{2^n}} .$$

$F = \mathbb{1} - 2|+\rangle^{\otimes n}\langle +|^{\otimes n}$ is implementable.

Pf. $H^{\otimes n} F \cdot H^{\otimes n} = \mathbb{1} - 2|0^n\rangle\langle 0^n|$

This is a classical phase computation whether input $= 0^n$.

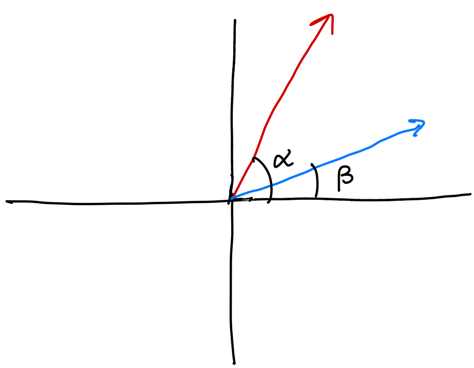
So to implement F, ① implement $H^{\otimes n}$

② run classical phase computation

③ implement $H^{\otimes n}$.

Properties: Both $\mathcal{O}$ and R preserve identified 2-dim subspace spanned by $|x\rangle$ and $|+\rangle^{\otimes n}$.

Observation:



Red + Blue Reflection:

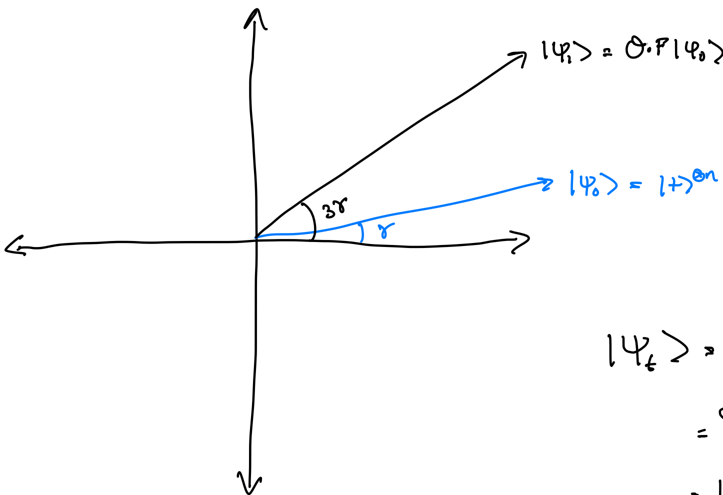
$$
\begin{aligned}
|\theta\rangle &\longmapsto |\alpha + (\alpha - \theta)\rangle \\
&= |2\alpha - \theta\rangle \\
&\longmapsto |\beta - (2\alpha - \theta - \beta)\rangle \\
&= |\theta + 2(\beta - \alpha)\rangle
\end{aligned}
$$

equals rotation by $2(\beta - \alpha)$.

In this case $\alpha = \pi/2$, $\beta = \arcsin\left(\frac{1}{\sqrt{2^n}}\right)$

rotation by $2\beta - \pi$

which is equivalent to rotation by 2β up to phase.



$$|\varphi_t\rangle = O \cdot F\, |\varphi_{t-1}\rangle$$
$$= R_{2\gamma} |\varphi_{t-1}\rangle$$
$$= |2\gamma t + \gamma\rangle$$

For T s.t. $(2\gamma + 1)T \approx \pi/2$, $|\varphi_T\rangle$ has good overlap with $|x\rangle$

so measuring in standard basis outputs solution x

since $\sin \gamma = \frac{1}{\sqrt{2^n}}$, $\quad T \approx \frac{\pi}{4\gamma + 2} \approx \frac{\pi}{4}\sqrt{2^n}$.

<u>Notice</u> when $O = \mathbb{1}$, $|\varphi_t\rangle = F^t |\varphi_0\rangle = |\varphi_0\rangle = |+\rangle^{\otimes n}$

so measuring produces uniformly random basis vector.

Replacing O with verification algorithm for 3-SAT formula gives the $\mathrm{BQTIME}\left[O(m\sqrt{2^n})\right]$ runtime.

Could we have done better?

Answer: <u>NO</u> (provably) in the case that we are deciding

$O = \mathbb{1} - 2|x\rangle\langle x|$ vs O.

This is the Bernstein, Bennett, Brassard & Vazirani query lowerbound for unconstrained search.