Stabilizer Circuits

CSE 490Q: Quantum Computation
• This will be part 1 of a two-part lecture on simulation of quantum circuits

• Will see a famous and beautiful result in this space

• The simulation result will be a consequence of what we study this time
  • “stabilizer states”
  • “stabilizer circuits”
Stabilizer Circuits

- We discussed how 1-qubit operations + CNOT are universal
  - they form a complete set of operations

- Can be reduced further to CNOT + H + ...

\[
T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}
\]

\[
t|0\rangle = |0\rangle
\]

\[
t|1\rangle = e^{i\pi/4} |1\rangle
\]
• Since $(e^{i\pi/4})^2 = e^{i\pi/2} = i$ and $(e^{i\pi/2})^2 = e^{i\pi} = -1$, we have...

\[
T^2 = \begin{bmatrix}
1 & 0 \\
0 & i
\end{bmatrix} = T \\
T^4 = S^2 = \begin{bmatrix}
1 & 0 \\
0 & -1
\end{bmatrix} = S
\]

$S = \sqrt{2}$

$T = \sqrt{S}$
• \{\text{CNOT, H, T}\} is a complete set of instructions

• \{\text{CNOT, H, }T^2\} = \{\text{CNOT, H, S}\} is not complete
  • potentially only a minor limitation

**Definition:** Circuits using only \text{CNOT, H, and S} are called “stabilizer circuits”

• (We will see that stabilizer circuits are very far from complete.)
• Useful idea from physics: identify a state by the eigenspaces it lies in

• Suppose we know that $U|x> = |x>$ (it is “stabilized by $U$”)
  • I.e., $|x>$ lives in the 1-eigenspace of $U$
  • assume we know the eigenvector decomposition of $U$

• If $U$ has a single eigenvector with eigenvalue 1, then $x$ is that eigenvector.

• But $U$ could have many eigenvectors with eigenvalue 1...
• If $U$ has many eigenvectors with eigenvalue 1, then we only know that $|x\rangle$ lies somewhere in their span.

• Ex: if $U = Z \otimes I \otimes I$, then $|x\rangle = |0\rangle \otimes |y\rangle$ for some $y$.

• Can write $|x\rangle = |0\rangle \otimes |y\rangle + |1\rangle \otimes |z\rangle$.

• Then we have

\[
(Z \otimes I \otimes I)|x\rangle = \begin{bmatrix} z_1 \\
0\end{bmatrix}_1|\langle 1 | y\rangle + \begin{bmatrix} z_1 \\
1\end{bmatrix}_2|\langle 1 | z\rangle
\]

\[
Z_1 = |0\rangle \otimes |y\rangle - |1\rangle \otimes |z\rangle
\]
Example 1

- If U has many eigenvectors with eigenvalue 1, then we only know that $|x>$ lies somewhere in their span.

- Ex: if $U = Z \otimes I \otimes I$, then $|x> = |0> \otimes |y>$ for some $y$.

- Can write $|x> = |0> \otimes |y> + |1> \otimes |z>$.  

- Then we $[Z]_1 |x> = |0> \otimes |y> - |1> \otimes |z>$.  

- So we have $[Z]_1 |x> = |x>$ iff $|z> = 0$, i.e., iff $|x> = |0> \otimes |y>$.  

If $U$ has many eigenvectors with eigenvalue 1, then we only know that $|x\rangle$ lies somewhere in their span.

- Ex: if $U = Z \otimes I \otimes I$, then $|x\rangle = |0\rangle \otimes |y\rangle$ for some $y$.
  - $|x\rangle$ only has coefficients on basis vectors of the form $|0ab\rangle$.

- Ex: if $U = I \otimes I \otimes Z$, then $|x\rangle = |0\rangle \otimes |z\rangle$ for some $y$.
  - $|x\rangle$ only has coefficients on basis vectors of the form $|ab0\rangle$.

- Ex: if $U = I \otimes Z \otimes I$, then ...
  - $|x\rangle$ only has coefficients on basis vectors of the form $|a0b\rangle$. 

Example 1
• If $U$ has many eigenvectors with eigenvalue 1, then we only know that $|x\rangle$ lies somewhere in their span.

• Ex: if $U = Z \otimes I \otimes I$, then only coefficients on basis vectors of the form $|0ab\rangle$.

• Ex: if $U = I \otimes I \otimes Z$, then only coefficients on basis vectors of the form $|ab0\rangle$.

• Ex: if $U = I \otimes Z \otimes I$, then only coefficients on basis vectors of the form $|a0b\rangle$.

• If $|x\rangle$ is in the 1-eigenspace of all three, then $|x\rangle = |000\rangle$.

• If the eigenspaces are bigger, we can identify $|x\rangle$ uniquely as the intersection of the 1-eigenspaces of multiple unitaries.
Heisenberg Representation

• This can be generalized...

• Note that $A \otimes I \otimes I$ and $I \otimes B \otimes I$ and $I \otimes I \otimes C$ all commute
  • since each acts on a different part of the state

• Theorem: if $M_1$, ..., $M_k$ all commute, then they have the same eigenvectors
  • (the eigenvalues can all be different, however.)

  \[ M_1 M = M M_1 \]

• Eigenvectors of $Z$ are $|0\rangle$ and $|1\rangle$

• Eigenvectors of $Z \otimes I \otimes I$ and $I \otimes Z \otimes I$ and $I \otimes I \otimes Z$ are $|000\rangle$ ... $|111\rangle$

  \[ [Z, |ab\rangle\rangle = \pm |abc\rangle \]
• This can be generalized...

• **Theorem**: if $M_1, \ldots, M_k$ all commute, then they have the same eigenvectors
  • (the eigenvalues can all be different, however.)

• If $|x\rangle$ is in the 1-eigenspace of $M_1, \ldots, M_k$, then it is in the span of the eigenvectors with eigenvalue 1 for each of them

• If we include enough matrices, we can get down to a single eigenvector
  • then $|x\rangle$ is uniquely identified
We will use matrices of the form $P_1 \otimes \ldots \otimes P_n$

- where each $P_j$ is one of $\{I, X, Y, Z\}$ scaled by one of $\{1, -1, i, -i\}$

- Ex: saw that $X$, $Z$, and $Y$ all have a $+1$ eigenvalue and a $-1$ eigenvalue
  - hence, any tensor product of the form $[X]_j$, $[Z]_j$, or $[Y]_j$ has half $+1$ eigenvalues

- Each stabilizer cuts the number of remaining $+1$ eigenvectors in half
- With $n$ stabilizers, we uniquely define the vector
• We will use matrices of the form $P_1 \otimes \ldots \otimes P_n$
  • where each $P_j$ is one of \{I, X, Y, Z\} scaled by one of \{1, -1, i, -i\}

• Not every state is stabilized by $n$ commuting matrices of this form

**Definition**: Any state that can be written as the unique state stabilized by $n$ commuting matrices of the form above is called a “stabilizer state”

• These sorts of stabilizer states are frequently used to study *error correcting codes*
  • very important topic for building practical quantum devices
We will use matrices of the form $P_1 \otimes \ldots \otimes P_n$

- where each $P_j$ is one of $\{I, X, Y, Z\}$ scaled by one of $\{1, -1, i, -i\}$

- Possible to form stabilizer states more complicated states

- Ex: $X \otimes X \otimes Z \otimes Z$ commutes with $Z \otimes I \otimes X \otimes I$

- $XZ = -ZX$ but two minus signs cancel
Computing with Stabilizer States

- Suppose that $|x\rangle$ is stabilized by $M_1, \ldots, M_k$ (which all commute)

- What can we say about $U|x\rangle$?

- Then $U|x\rangle$ is stabilized by $U M_1 U^\dagger, \ldots, U M_k U^\dagger$ (which all commute)

\[
(u M_i u^\dagger)(u M_j u^\dagger) = u M_i u = u M_j M_i u = (u M_j u^\dagger)(u M_i u)
\]
• Suppose that $|x\rangle$ is stabilized by $M_1, ..., M_k$ (which all commute)

• What can we say about $U|x\rangle$?

• Then $U|x\rangle$ is stabilized by $U M_1 U^\dagger, ..., U M_k U^\dagger$ (which all commute)

• So $U|x\rangle$ is also the unique state stabilized by some set of $k$ matrices

• BUT its new stabilizers could be very complicated matrices
  • in particular, they are not necessarily these simple tensor products
  • i.e., $U|x\rangle$ is not necessarily a stabilizer state
Suppose that $|x\rangle$ is stabilized by $M_1, ..., M_k$ (which all commute).

What can we say about $U|x\rangle$?

Then $U|x\rangle$ is stabilized by $U M_1 U^\dagger, ..., U M_k U^\dagger$ (which all commute).

**Theorem**: If $|x\rangle$ is a stabilizer state and $U$ is one of \{CNOT, H, S\}, then $U|x\rangle$ is also a stabilizer state.

(I.e., stabilizer circuits take stabilizer states to stabilizer states.)
**Theorem:** If $|x\rangle$ is a stabilizer state and $U$ is one of \{CNOT, H, S\}, then $U|x\rangle$ is also a stabilizer state.

**Proof:** For $U = [\text{CNOT}]_{ij}$, $[\text{H}]_j$, and $[\text{S}]_j$...

- Given a stabilizer of the form $P_1 \otimes ... \otimes P_n$ for some $P_j$'s as above
- Need to show that $U (P_1 \otimes ... \otimes P_n) U$ is also of this form

- Since $U$ is identity on all but 1 or 2 qubits, it leaves the other $P_j$'s unchanged
- E.g.,

\[
(\underbrace{S \otimes I \otimes I}_{P_1}) (P_1 \otimes P_2 \otimes P_3) (\underbrace{S^* \otimes I \otimes I}_{P_1}) = (\underbrace{SP_1S^*}_{P_1}) \otimes P_2 \otimes P_3
\]
**Theorem:** If $|x\rangle$ is a stabilizer state and $U$ is one of \{CNOT, H, S\}, then $U|x\rangle$ is also a stabilizer state.

**Proof:** Reduces to the following...

- For $U$ in \{CNOT, H, or S\}
- For $P$ is one of \{I, X, Z, XZ\} scaled by one of \{1, -1, i, -i\}
  - or a tensor product of two of those when $U = \text{CNOT}$
- Show that $U P U^\dagger$ is of the same form...
• We have seen this already:

\[ H \times H^+ = \mathbb{I} \quad H \geq H^+ = X \]

\[ H \times \mathbb{I} H^+ = H \times H^+ H \geq H^+ = 2X = -XZ \]

• If \( U = wXZ \) where \( w \) is one of \{1, -1, i, -i\}, then

\[ U \left( wXZ \right) U^+ = w \ U^+ XZ \ U^+ = -w \ XZ \]

and \(-w\) is also one of \{1, -1, i, -i\}
• Z and S are both diagonal, so they commute. Hence, \( S Z S^\dagger = Z \).

\[
S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad S Z = Z S
\]

• For X, we see that

\[
S X S^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} S^\dagger = \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} S^\dagger
\]

\[
= \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i X Z \quad (= \gamma)
\]
• Z and S are both diagonal, so they commute. Hence, $S Z S^\dagger = Z$.

• For X, our calculation showed that $S X S^\dagger = iXZ$.

• Combining these, we have

$$S X Z S^\dagger = S X S^\dagger Z = iX Z Z = iX$$

• Thus, $S P S^\dagger$ is also one of \{1, X, Z, XZ\} scaled by one of \{1, -1, i, -i\}.
• Remains to check the CNOT case

• We’ll do that next time...
  • worst case, this is some calculations with 4 x 4 matrices
  • BUT we’ll see that it’s actually much easier than that