Classical Simulation

CSE 490Q: Quantum Computation
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 $U$

Can uniquely identify $|x>$ by a set of stabilizers $U_1, ..., U_n$
We will use unitaries 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\}
- these are the 16 elements of the “Pauli group”

Not every state is stabilized by \( n \) commuting matrices of this form

**Definition**: Any state that can be uniquely identified by a set of commuting unitaries of the form above is called a “stabilizer state”

- Stabilizer states are frequently used to study error correcting codes
  - very important topic for building practical quantum devices
Consider states of three qubits

\[
\begin{bmatrix}
Z_1 \\
Z_2
\end{bmatrix}
\]

The unitaries \{Z \otimes I \otimes I, I \otimes Z \otimes I, I \otimes I \otimes Z\} all commute

They stabilize states with non-zero coefficients only on \(|0ab\rangle, |a0b\rangle, and |ab0\rangle\n
The unique state stabilized by all three is \(|000\rangle\)
Simulating quantum systems is an extremely important problem.

Look at where classical computers can efficiently simulate quantum ones.

Such algorithms would have practical applications:
- designing new drugs or vaccines
- designing new chemical processes

They are also important theoretically:
- can’t understand where quantum computers have an advantage without understanding what classical computers can and cannot do.
• \{\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 CNOT, H, and S are called “stabilizer circuits”

• (We will see that stabilizer circuits are very far from complete.)
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 $UM_1U^\dagger, \ldots, UM_kU^\dagger$ (which all commute).
• 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)

**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 $P_1 \otimes \ldots \otimes P_n$ for some $P_j$’s as above
- Need to show that $U (P_1 \otimes \ldots \otimes P_n) U^\dagger$ is also of this form

- Since $U$ is identity on all but 1 or 2 qubits, it leaves the other $P_j$’s unchanged
**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 $U = H$ or $U = S$...

- $P$ is one of \{I, X, Z, XZ\} scaled by one of \{1, -1, i, -i\}
- Show that $U P U^\dagger$ is of the same form...
- We did this last time (short calculations).
**Theorem:** If $|x\rangle$ is a stabilizer state and $U$ is one of $\{\text{CNOT, H, S}\}$, then $U|x\rangle$ is also a stabilizer state.

**Proof:** Reduces to the following for $U = \text{CNOT}$...

- $P$ and $Q$ are each one of $\{I, X, Z, XZ\}$ scaled by one of $\{1, -1, i, -i\}$
- Show that $\text{CNOT} (P \otimes Q) \text{CNOT}$ is of the same form
- We have done a lot of the work already (see circuit equivalences)...

\[ \text{CNOT}^2 = I \]
Stabilizer States and Circuits

\[ Z \otimes I \quad \equiv \quad \begin{array}{c}
\text{Diagram 1} \\
\text{Diagram 2} \\
\text{Diagram 3}
\end{array} \quad \equiv \quad \begin{array}{c}
\text{Diagram 4} \\
\text{Diagram 5} \\
\text{Diagram 6}
\end{array} \quad \equiv \quad \begin{array}{c}
\text{Diagram 7} \\
\text{Diagram 8}
\end{array} \]

\[ X \otimes I \quad \equiv \quad \begin{array}{c}
\text{Diagram 9} \\
\text{Diagram 10} \\
\text{Diagram 11}
\end{array} \quad \equiv \quad \begin{array}{c}
\text{Diagram 12} \\
\text{Diagram 13} \\
\text{Diagram 14}
\end{array} \quad \equiv \quad \begin{array}{c}
\text{Diagram 15} \\
\text{Diagram 16}
\end{array} \]
Stabilizer States and Circuits

$I \otimes X$

$\text{use the fact that}$

$I \otimes Z$

$\text{I}_{I,X}$

$\text{I}_{X} = \text{I}_{X}$

$\text{X}_{X} = \text{X}_{X}$
Stabilizer States and Circuits

$H \otimes H = X \otimes X$ or equiv. $H \otimes Z = X \otimes H$
Stabilizer States and Circuits

\[ H^2 = 1 \]

or equiv.

\[ Z H = H X \]
**Theorem:** If $|x>\rangle$ is a stabilizer state and $U$ is one of $\{\text{CNOT, H, S}\}$, then $U|x>\rangle$ is also a stabilizer state.

**Proof:** Reduces to the following for $U = \text{CNOT}$...

- $P$ and $Q$ are each one of $\{I, X, Z, XZ\}$ scaled by one of $\{1, -1, i, -i\}$
- Show that $\text{CNOT} (P \otimes Q) \text{CNOT}$ is of the same form
  \[ XZ \otimes I \quad I \otimes XZ \]
- We’ve done $X \otimes I$, $Z \otimes I$, $I \otimes X$, and $I \otimes Z$.
- The other ones are just combinations of these.
  - (The constants $\{1, -1, i, -i\}$ all pass through unchanged.)
**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.

- Can consider a set $S$ of stabilizers other than tensor products of Paulis.

**Definition:** the matrices $U$ such that, for all $M$ in $S$, we have $U M U^\dagger$ in $S$ are called “normalizers” of $S$.

- Particularly, nice in this case because
  - only 16 stabilizer matrices
  - normalizers include \{CNOT, H, $T^2$\}
<table>
<thead>
<tr>
<th>H</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>x</td>
<td>i x^2</td>
</tr>
<tr>
<td>i x</td>
<td>i^2</td>
</tr>
<tr>
<td>-x</td>
<td>- i x^2</td>
</tr>
<tr>
<td>- i x^2</td>
<td>x</td>
</tr>
<tr>
<td>_</td>
<td>_</td>
</tr>
</tbody>
</table>

14 rows
Stabilizer States and Circuits

\[
\begin{align*}
I \otimes I &= I \\
I \otimes -I &= -I \\
I \otimes iI &= iI \\
\vdots \\
-xz &\otimes -iI \\
-xz &\otimes -iI \\
-xz &\otimes iI \\
-xz &\otimes iI \\
256 \text{ rows}
\end{align*}
\]
Theorem: There is an efficient classical algorithm for simulating circuits made up of only CNOT, H, and S gates.

Idea: Keep track of the current state via its stabilizers

Algorithm
- Initial state $|0^n\rangle$ is stabilized by $[Z]_1, \ldots, [Z]_n$
- For each gate
  - update the current stabilizers from $M_1, \ldots, M_n$ to $M_1', \ldots, M_n'$ using the tables from the prior slides
- All that remains is to simulate the final measurement...
• Suppose that all the stabilizers are of the form \([±Z]_j\) for some \(j\)’s

• The 1 eigenvector for \(+Z\) is \(|0>\)
  • as we saw before, a \([Z]_j\) stabilizer means the \(j\)-th bit is 0

• The 1 eigenvector for \(-Z\) is \(|1>\)
  • so a \([-Z]_j\) stabilizer means the \(j\)-th bit is a 1

• Example: \(Z \otimes I \otimes I\) and \(I \otimes -Z \otimes I\) and \(I \otimes I \otimes -Z\)
  • the unique state stabilized by all three is \(|011>\)

• Hence, we know the measurement outcome with certainty
Measuring a Stabilizer State

• Suppose that all the stabilizers are of the form $[±X]_j$ for some $j$’s

• The $1$ eigenvector for $+X$ is $|+\rangle$

• The $1$ eigenvector for $-Z$ is $|→\rangle$

• Either one has a $50\%$ chance of measuring as $|0\rangle$ and $50\%$ as $|1\rangle$

• We can simulate this just by flipping a coin and returning $|0\rangle$ or $|1\rangle$
  • that produces the same distribution of outcomes as the measurement
We can combine these approaches for a mix of $[\pm Z]_j$ and $[\pm Z]_j$ stabilizers.

Example: $-Z \otimes I \otimes I$ and $I \otimes -X \otimes I$ and $I \otimes I \otimes Z$

- $-Z \otimes I \otimes I$ tells us that the first qubit must be $\ket{1}$
- $I \otimes -X \otimes I$ tells us that the second qubit must be $\ket{-}$
- $I \otimes I \otimes Z$ tells us that the third qubit must be $\ket{0}$

To simulate:
- flip a 50/50 coin to get a random 0/1 value $b$
- return $\ket{1b0}$ as the measurement
Measuring a Stabilizer State

- It is possible to reduce any set of stabilizers to this last case:
  \[
  |x\rangle = u|x\rangle = u^\dagger|x\rangle
  \]

- Key Ideas:
  - if A and B are stabilizers, then so is AB
  - if A is a stabilizer, then so is \( A^\dagger \)

- Reduction:
  - Write out the stabilizers as a matrix
  - Using the ideas above, we can perform Gaussian Elimination
  - ...
Measuring a Stabilizer State

• It is possible to reduce any set of stabilizers to this last case

• Reduction:
  • Write out the stabilizers as a matrix
  • Using the ideas above, we can perform Gaussian Elimination
  • Result will be a diagonal matrix, which means the j-th row is \([\pm Z]_j\) or \([\pm X]_j\)
    • the other possibility is \([\pm iXZ]_j\), but that is just like the X case
    • no other Pauli matrix is possible (Why not?)
  • Return a measurement result that is 0/1 for the \(\pm Z\) qubits and uniformly random for the \(\pm X\) and \(\pm iXZ\) qubits

\[ T = T^2 \]
Theorem: There is an efficient classical algorithm for simulating circuits made up of only CNOT, H, and S gates.

• Construction shows that we can simulate the circuit, in principle, without determining what the final state is

• Simulations possible for other normalizer circuits
  • e.g., Bermejo-Vega and Z. on certain hypergroup matrices

• But G-K is the original and nicest one
  • another demonstration of the beautiful algebra of Pauli matrices