# Stabilizer Circuits

CSE 490Q: Quantum Computation

# Classical Simulation

- 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

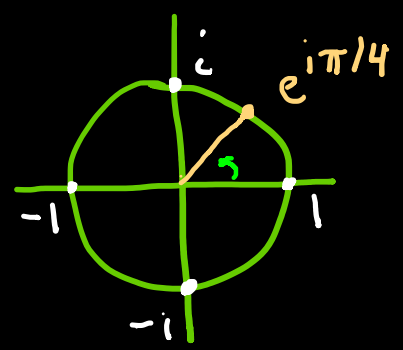
- Can be reduced further to CNOT + H + …

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

$$T|0\rangle = |0\rangle$$

$$T|1\rangle = e^{i\pi/4}|1\rangle$$

# T Gate




- Since $(e^{i\pi/4})^2 = e^{i\pi/2} = i$ and $(e^{i\pi/2})^2 = e^{i\pi} = -1$, we have…

$$T^2 = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} =: S$$

$$T^4 = S^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

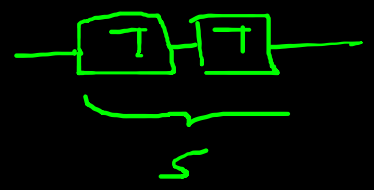
$S = \sqrt{Z}$

$T = \sqrt{S}$

# Stabilizer Circuits

- {CNOT, H, T} is a complete set of instructions

- {CNOT, H, $T^2$} = {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.)

# Heisenberg Representation

- Useful idea from physics: identify a state by the eigenspaces it lies in
- Suppose we know that $U|x\rangle = |x\rangle$ (it is "stabilized by U")
  - I.e., $|x\rangle$ 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…

# 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 ⊗ I ⊗ I, then |x> = |0> ⊗ |y> for some y

- Can write |x> = |0> ⊗ |y> + |1> ⊗ |z>.
- Then we have

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$(Z \otimes I \otimes I)|x\rangle = [Z]_1 |x\rangle = [Z]_1 (|0\rangle \otimes |y\rangle) + [Z]_1 (|1\rangle \otimes |z\rangle)$$

$$Z_1 \qquad = |0\rangle \otimes |y\rangle - |1\rangle \otimes |z\rangle$$

# Example 1

- If U has many eigenvectors with eigenvalue 1,
  then we only know that $|x\rangle$ 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 $[Z]_1|x\rangle = |0\rangle \otimes |y\rangle - |1\rangle \otimes |z\rangle$.

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

# 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 ⊗ I ⊗ I, then |x> = |0> ⊗ |y> for some y
  - |x> only has coefficients on basis vectors of the form |0ab>

- Ex: if U = I ⊗ I ⊗ Z, then |x> = |0> ⊗ |z> for some y
  - |x> only has coefficients on basis vectors of the form |ab0>

- Ex: if U = I ⊗ Z ⊗ I, then …
  - |x> only has coefficients on basis vectors of the form |a0b>

# Example 1

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

|abc>

- Ex: if U = Z ⊗ I ⊗ I, then only coefficients on basis vectors of the form |0ab>
- Ex: if U = I ⊗ I ⊗ Z, then only coefficients on basis vectors of the form |ab0>
- Ex: if U = I ⊗ Z ⊗ I, then only coefficients on basis vectors of the form |a0b>

- If |x> is in the 1-eigenspace of all three, then |x> = |000>

- If the eigenspaces are bigger, we can identify |x> uniquely as the intersection of the 1-eigenspaces of multiple unitaries

# Heisenberg Representation

- This can be generalized…
- Note that A ⊗ I ⊗ I and I ⊗ B ⊗ I and I ⊗ I ⊗ C all *commute*
  - since each acts on a different part of the state

$M_1 M_2 = M_2 M_1$

- **Theorem**: if $M_1$, …, $M_k$ all commute, then they have the same eigenvectors
  - (the eigenvalues can all be different, however.)
- Eigenvectors of Z are |0> and |1>

+1 −1

$X \to$ $|+\rangle$ $|-\rangle$ (+1, −1)

- Eigenvectors of Z ⊗ I ⊗ I and I ⊗ Z ⊗ I and I ⊗ I ⊗ Z are |000> … |111>

$[Z]_1 |abc\rangle = \pm |abc\rangle$

# Heisenberg Representation

- 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> 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

$|x\rangle = c_1(v_1) + \cdots + c_n(v_n)$

- If we include enough matrices, we can get down to a single eigenvector
  - then |x> is uniquely identified

# Stabilizer States

$Y = iXZ$

- 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

# Stabilizer States

- 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

# Stabilizer States

- 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

$Z \otimes I \otimes I$

Z I X I

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

$XZ = -ZI$

  - 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)

$$(U M U^\dagger)\, U|x\rangle = U M|x\rangle = U|x\rangle$$

$$(U M_i U^\dagger)(U M_j U^\dagger) = U M_i M_j U = U M_j \overset{U^\dagger U}{} M_i U$$

$$= (U M_j U^\dagger)(U M_i U)$$

# 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)
- 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*

# 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)

**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.

applied to some qubit

(I.e., stabilizer circuits take stabilizer states to stabilizer states.)

# Stabilizer States and Circuits

**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 = $[CNOT]_{ij}$, $[H]_j$, and $[S]_j$…

- 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
- E.g.,

$$(S \otimes \cancel{I \otimes I})(P_1 \otimes P_2 \otimes P_3)(S^\dagger \otimes I \otimes I) = (S P_1 S^\dagger) \otimes P_2 \otimes P_3$$

# Stabilizer States and Circuits

**Theorem**: If |x> is a stabilizer state and U is one of {CNOT, H, S},
then U|x> 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 = CNOT
- Show that U P $U^{\dagger}$ is of the same form…

16 poss.

# $\boxed{U = H}$

- We have seen this already:

$$HXH^\dagger = Z \qquad HZH^\dagger = X$$

$$HXZH^\dagger = \overbrace{HXH^\dagger}\,\overbrace{HZH^\dagger} = ZX = -XZ$$

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

$$U(wXZ)U^\dagger = w\,UXZU^\dagger = -w\,XZ$$

and -w is also one of {1, -1, i, -i}

# $\boxed{U = S}$

- Z and S are both diagonal, so they commute. Hence, $S\,Z\,S^\dagger = Z$ $SS^\dagger = Z$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad SZ = ZS$$

- For X, we see that

$$SXS^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} S^\dagger = \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} S^\dagger$$

$$= \begin{bmatrix} 0 & 1 \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \underline{iXZ} \quad (= Y)$$

# $\boxed{U = S}$

- 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

$$S\,X\,Z\,S^\dagger = S\,X\,S^\dagger\,Z = iXZZ = \boxed{iX}$$

- Thus, $S\,P\,S^\dagger$ is also one of {I, X, Z, XZ} scaled by one of {1, -1, i, -i}

# U = CNOT

- 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