Classical Simulation

CSE 490Q: Quantum Computation

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
- Can uniquely identify $|x\rangle$ by a set of stabilizers $U_1, \ldots, U_n$

Stabilizer States

- 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

Example

- Consider states of three qubits
- 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>, |a0b>, and |ab0>
- The unique state stabilized by all three is |000>

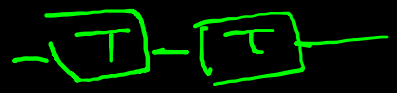
Classical Simulation

- 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

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.)

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)

Computing with Stabilizer States

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

$P_1 \otimes \cdots \otimes P_n$

- 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.)

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 = $[\text{CNOT}]_{ij}$, $[H]_j$, 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

$P_1 \otimes \cdots \otimes P_{n-1} \otimes (\_\_)$

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: 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).

Stabilizer States and Circuits

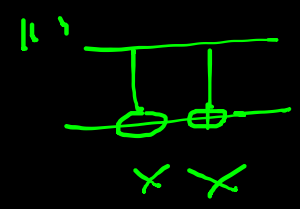
Theorem: If |x> is a stabilizer state and U is one of {CNOT, H, S},
then U|x> is also a stabilizer state.

Proof: Reduces to the following for U = CNOT…

- P and Q are each one of {I, X, Z, XZ} scaled by one of {1, -1, i, -i}
- Show that CNOT (P ⊗ Q) CNOT is of the same form

$CNOT^2 = I$

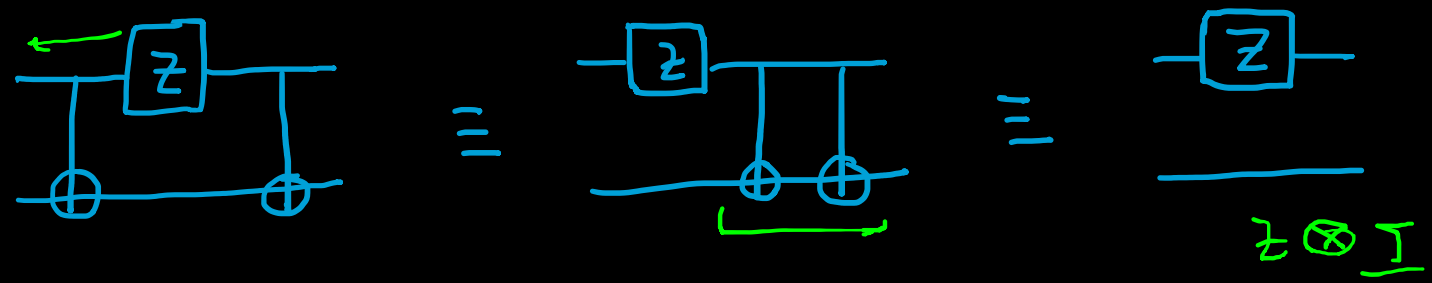
- We have done a lot of the work already (see circuit equivalences)…



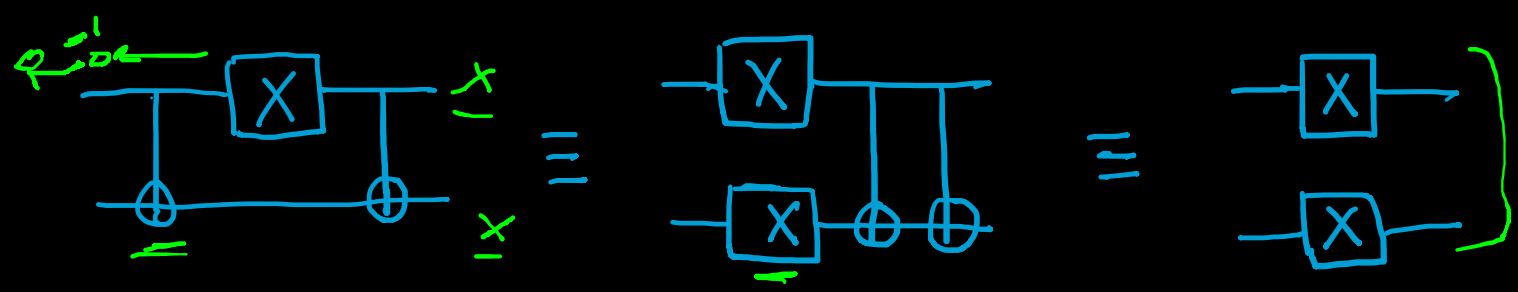
$I \otimes I$

Stabilizer States and Circuits

$Z \otimes I$

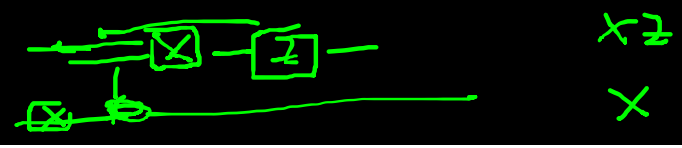


$X \otimes I$



$P \otimes I$

$I \otimes Q$

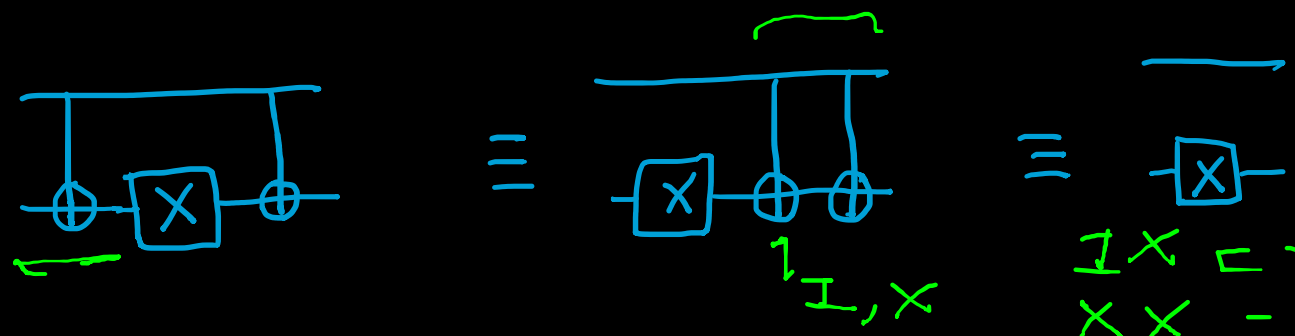


XZ

X

Stabilizer States and Circuits

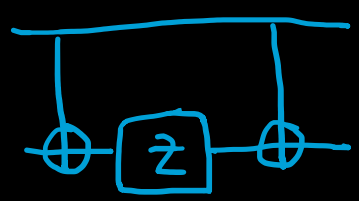
$I \otimes X$



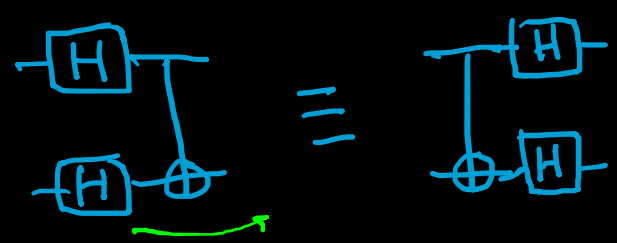
$IX = XI$

$XX = -XX$

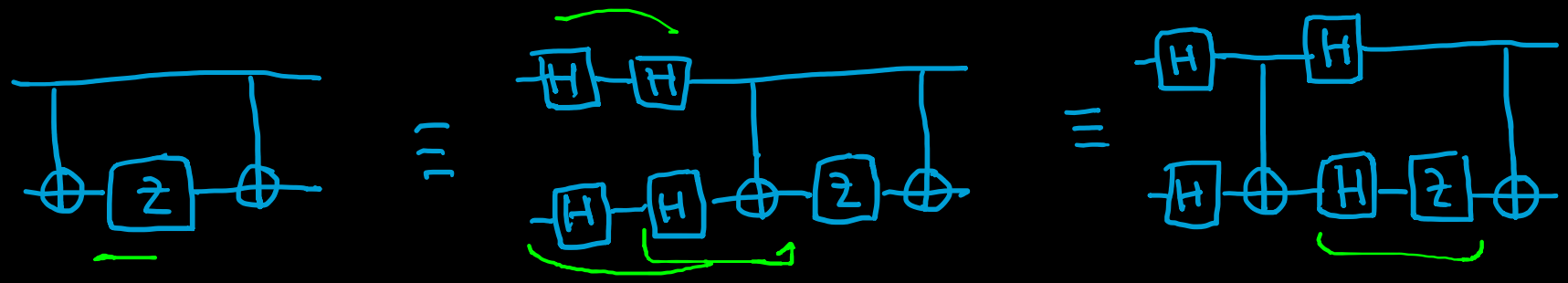
$I \otimes Z$



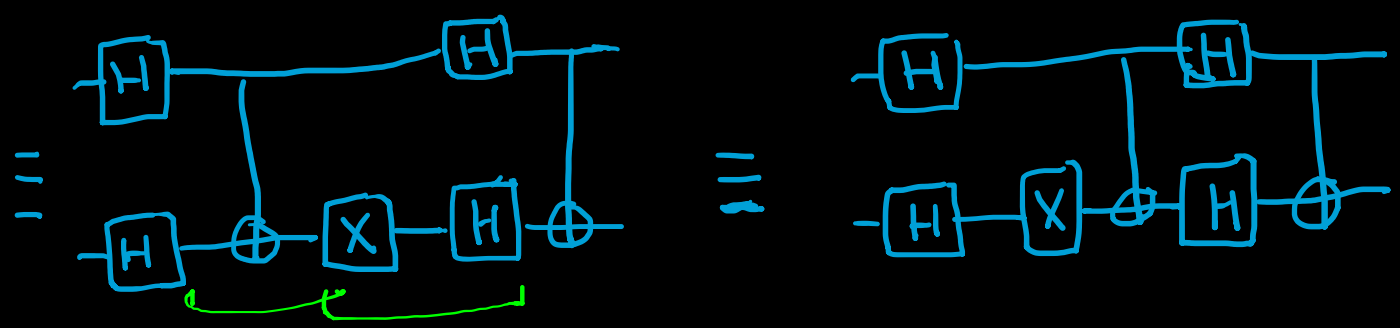
use the fact that



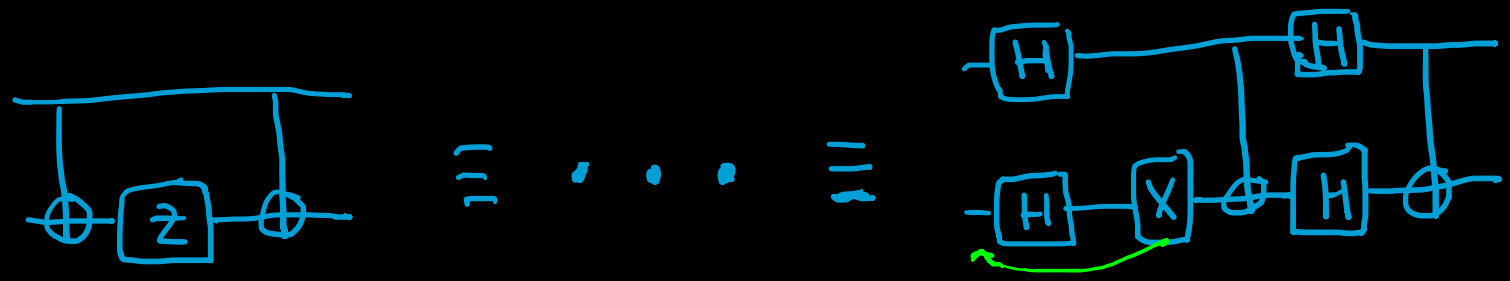
Stabilizer States and Circuits



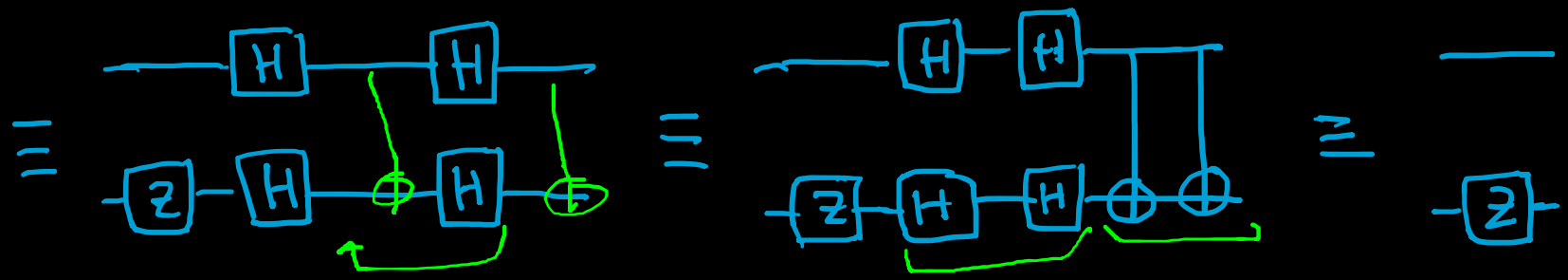
$$HZH^{H} = X^{H}$$ or equiv. $$HZ = XH$$



Stabilizer States and Circuits



$$\overset{+1}{H} Z H = \overset{+1}{X} \quad \text{or equiv.} \quad Z H = H X$$



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 = CNOT…

- P and Q are each one of {I, X, Z, XZ} scaled by one of {1, -1, i, -i}
- Show that CNOT (P ⊗ Q) CNOT is of the same form

XZ ⊗ I I ⊗ XZ

- We've done X ⊗ I, Z ⊗ I, I ⊗ X, and I ⊗ Z.
- The other ones are just combinations of these.
  - (The constants {1, -1, i, -i} all pass through unchanged.)

Normalizers

Theorem: If |x> is a stabilizer state and U is one of {CNOT, H, S},
then U|x> 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}

Stabilizer States and Circuits

	H	S
I	I	I
⋮	⋮	⋮
X	Z	iXZ
−X	−Z	−iXZ
iX	iZ	−XZ
⋮	⋮	⋮
−iXZ	iXZ	X

16 rows

Stabilizer States and Circuits

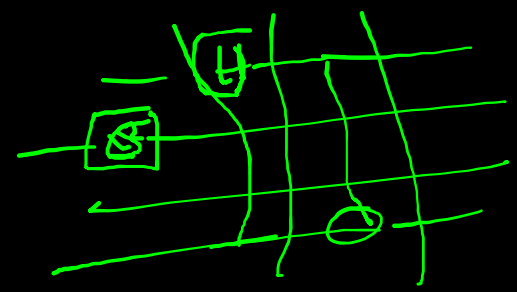
	CNOT
$I \otimes I$	$I \otimes I$
$I \otimes -I$	$I \otimes -I$
$I \otimes iI$	$I \otimes iI$
$\vdots$	
$-iXZ \otimes -iXZ$	$-iXZ \otimes -iZ$

256 rows

Gottesman-Knill Theorem

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…

Measuring a Stabilizer State

- Suppose that all the stabilizers are of the form $[\pm Z]_j$ 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

1 0

- 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 $[\pm X]_j$ for some j's

- The 1 eigenvector for +X is |+>
- The 1 eigenvector for –~~X~~ is |–>

$\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

- Either one has a 50% chance of measuring as |0> and 50% as |1>

- We can simulate this just by flipping a coin and returning |0> or |1>
  - that produces the same distribution of outcomes as the measurement

Measuring a Stabilizer State

- We can combine these approaches for a mix of $[\pm Z]_j$ and $[\pm X]_j$ 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 $|1\rangle$
  - $I \otimes -X \otimes I$ tells us that the second qubit must be $|-\rangle$
  - $I \otimes I \otimes Z$ tells us that the third qubit must be $|0\rangle$

- To simulate:
  - flip a 50/50 coin to get a random 0/1 value b
  - return $|1b0\rangle$ as the measurement

Measuring a Stabilizer State

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

$$UV|x\rangle = U|x\rangle = |x\rangle$$

$$|x\rangle = U^\dagger U|x\rangle = U^\dagger|x\rangle$$

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

$$\begin{bmatrix} I & & \\ & \ddots & \\ & & I \end{bmatrix}$$

$$\begin{array}{ccc} I & Z & I \\ \end{array}$$
$$\begin{bmatrix} I & Z & X \\ I & I & X \\ X & I & I \end{bmatrix}$$

- 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 ±Z qubits and uniformly random for the ±X and ±iXZ qubits

I

$T \to T^2$

Gottesman-Knill Theorem

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