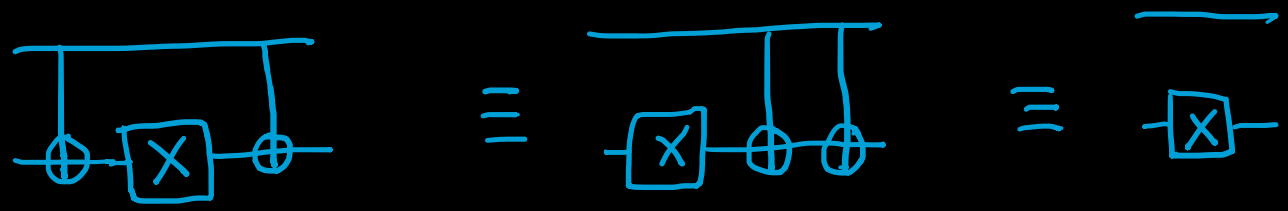
# Classical Simulation

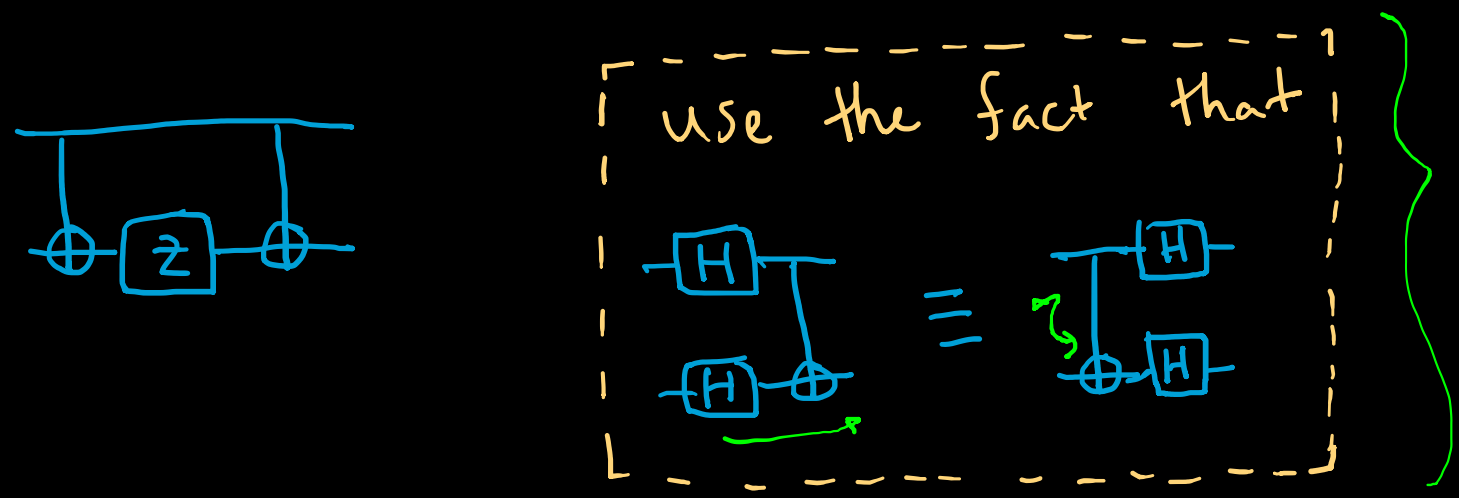
CSE 490Q: Quantum Computation

# Stabilizer States and Circuits

$I \otimes X$

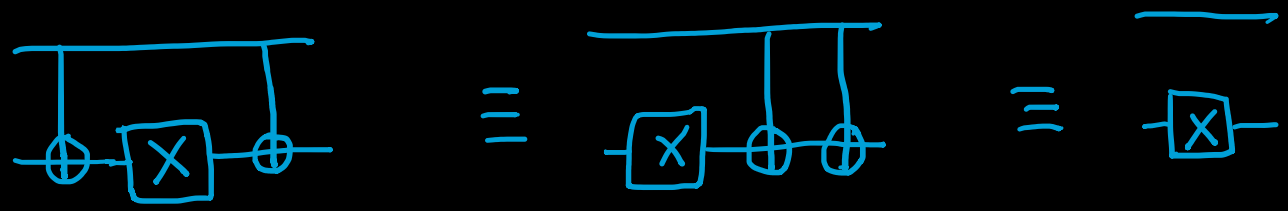



$I \otimes Z$

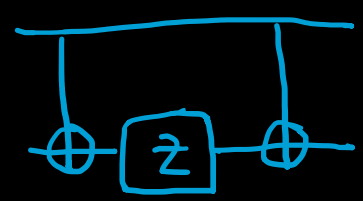


# Stabilizer States and Circuits

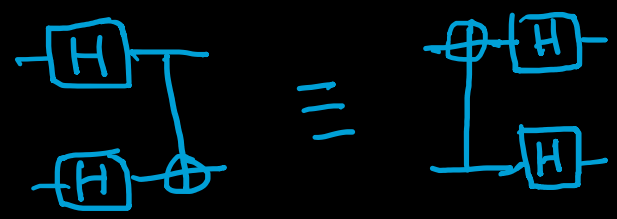
$I \otimes X$



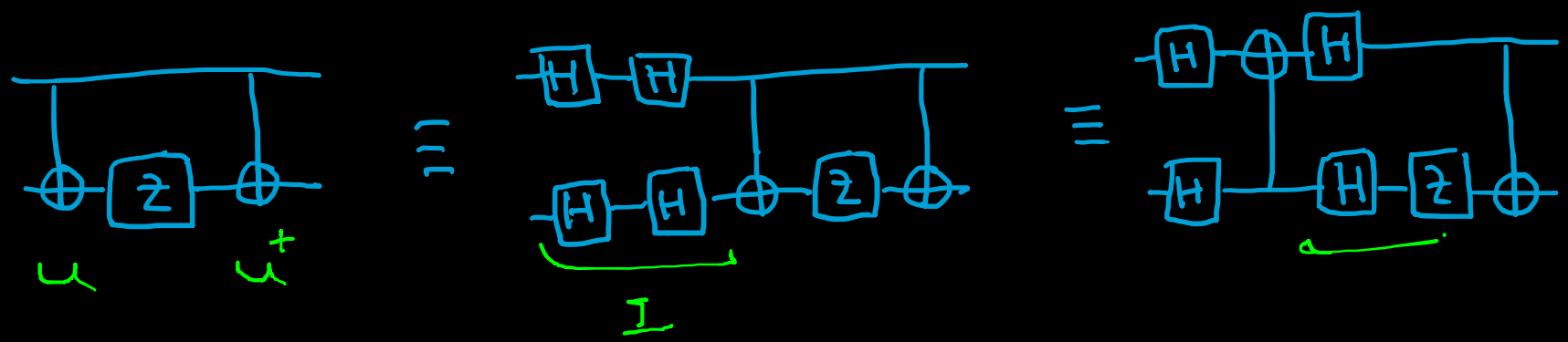

$I \otimes Z$



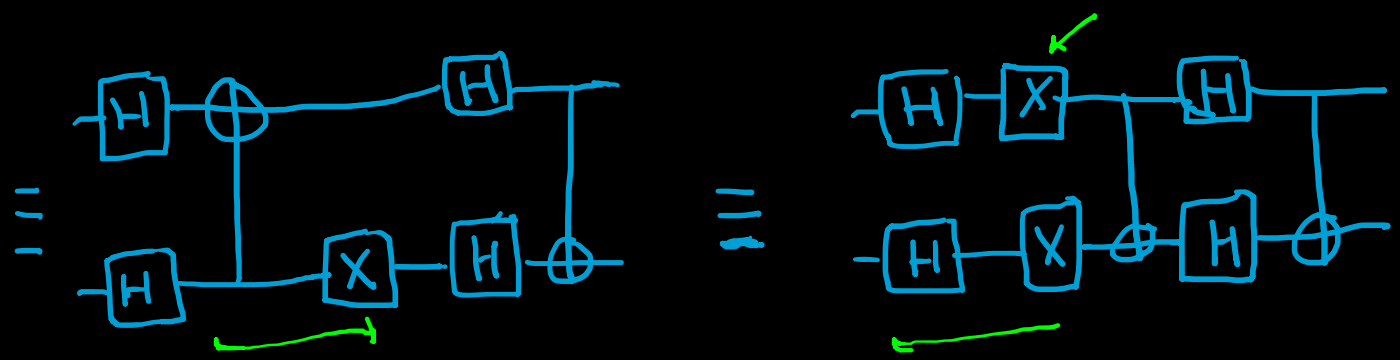

use the fact that



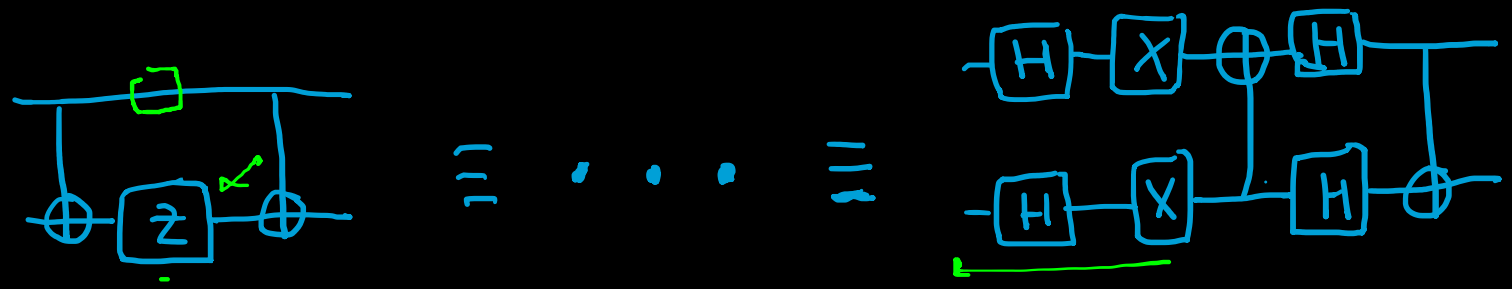
# Stabilizer States and Circuits



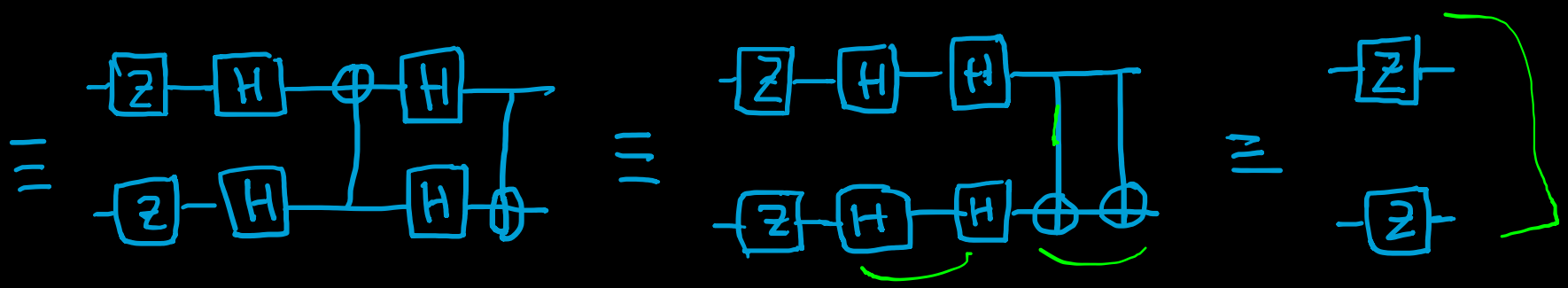

$HZH = X$ or equiv. $HZ = XH$



# Stabilizer States and Circuits




$$HZH = X \quad \text{or equiv.} \quad ZH = HX$$



# The Hidden Subgroup Problem

CSE 490Q: Quantum Computation

# Shor's Algorithm

- Shor's (1994) breakthrough result was an efficient q. algorithm for **factoring**
  - strongly believed to be classically hard
    - 200+ years of failed attempts to solve it
    - hardness is *assumed* by cryptosystems like RSA
  - not a toy problem, not a black box

- Fastest classical algorithm runs in $O(2^{n/3})$ time
- Shor's algorithm is $O(n^3)$

# Post-Shor Algorithms

- Much later work focused on *generalizing* it
  - we will look at some of the generalizations (more than one!)
  - Shor's paper still has insights that may not be fully understood still

- First generalization was the phase estimation algorithm

# Phase Estimation History

Alexei Kitaev, in Russia at the time, heard about Shor's result. Unable to get the paper, he re-derived how he thought it must work. His result was actually a significant generalization of Shor's.

The technique he invented is called "phase estimation"

(He also generalized the problem solved.)

# Groups

# Groups

**Definition**: A group G is a set with…

- a special element $e \in G$
- an operation taking any $x, y \in G$ to some $xy \in G$ multiplication
- an operation taking any $x \in G$ to some $x^{-1} \in G$

satisfying certain rules…

- $ex = x = xe$ for all $x \in G$ ("identity")
- $x x^{-1} = e = x^{-1} x = e$ for all $x \in G$ ("inverses")
- $(xy)z = x(yz)$ for all $x, y, z \in G$ ("associativity")

# Groups in Java

```
public interface Group {
  Collection<Element> elements();
  Element identity();
}

public interface Element {
  Element multiply(Element y);      // returns xy
  Element inverse();                // returns x^-1
}

// Specification would list the rules from the prior page…
```

x.multiply(y)

x.inverse()

# Groups

**Definition**: A group G is a set with…

- a special element $e \in G$
- an operation taking any $x, y \in G$ to some $xy \in G$
- an operation taking any $x \in G$ to some $x^{-1} \in G$

satisfying the following rules…

Abel

**Definition**: A group G is abelian if $xy = yx$ for all $x, y \in G$.

- (In this case, we often write $x+y$ instead of $xy$.)

$uv \neq vu$

# Group Examples

$\mathbb{Q}$

- $\mathbb{R}$ is a group under multiplication, where 1 is identity and the inverse of x is 1/x.

$\frac{p}{q} \to \frac{q}{p}$

- $\mathbb{Z}$ is not a group under multiplication because, e.g., 2 has no inverse.

- $\mathbb{Z}$ is a group under addition, where 0 is the identity and the inverse of x is –x.
  - x + (-x) = 0 = (-x) + x

$0 + x = x = x + 0$

$\mathbb{R}$

- $\mathbb{Z}_N$ is a group under addition, where ~~multiplication~~ addition is modulo N.
  - Set is {0, 1, …, N-1}
  - 0 is still the identity
  - the inverse of x is N – x since x + (N – x) = N ≡ 0 (mod N)

# Group Examples

- $\mathbb{Z}_N$ is a group under addition, where multiplication is modulo N.
  - Set is {0, 1, …, N-1}
  - 0 is still the identity

$\neg\exists$ (t divider x and N)

- If gcd(x, N) = 1, then x has a multiplicative inverse $x^{-1}$.
  - Bezout's Theorem says there exist a and b such that ax + bN = 1, which says that ax ≡ 1 (mod N)

$a = x^{-1}$

$\mathbb{Z}_N^x$

- $(\mathbb{Z}_N)^x$ is a group under multiplication.
  - Set is { x ∈ $\mathbb{Z}_N$ : gcd(x, N) = 1 }
  - 1 is the identity

$\mathbb{Z}_p$ p prime

← either + or x

# Non-Abelian Group Examples

Those groups are all abelian. Here are some non-abelian groups.

- 2 x 2 unitary matrices form a group under multiplication
  - the identity is I
  - the inverse of U is $U^\dagger$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- The Pauli group is a (finite!) group under multiplication
  - elements are one of {I, X, Y, Z} scaled by one of {1, -1, i, -i}
  - inverses… homework problem

$$XZ \neq \underbrace{ZX}_{= -XZ.}$$

# Products of Groups

If G and H are groups, we can combine them to form a new group.

$n_1 \; n_2 \to n_1 n_2$

**Definition**: $G \times H$ is the group with elements $\{ (x, y) : x \in G \text{ and } y \in H \}$

- identity is $(e_G, e_H)$, where $e_G$ is the identity of G and $e_H$ of H
- multiplication is $(u, v)(x, y) = (ux, vy)$
- inverse is $(x, y)^{-1} = (x^{-1}, y^{-1})$

$(x, y)(x^{-1}, y^{-1}) = (xx^{-1}, yy^{-1})$

$= (e_G, e_H)$

- Can take more products to build vectors.
- E.g., $G^4 = G \times G \times G \times G$, whose elements are of the form $(w, x, y, z)$

# Finitely Abelian Groups

- Finite abelian groups are actually not that complicated…

**Theorem**: If G is a finite abelian group, then there are integers $N_1, \ldots, N_K$ $\in \mathbb{Z}$
such that $G = \mathbb{Z}_{N1} \times \ldots \times \mathbb{Z}_{Nk}$

- Here "=" is not really equal but rather "isomorphism".
- There is a correspondence between elements of G and $\mathbb{Z}_{N1} \times \ldots \times \mathbb{Z}_{Nk}$
  - for every $g \in G$, there is an $f(g) \in \mathbb{Z}_{N1} \times \ldots \times \mathbb{Z}_{Nk}$ that behaves identically
- Can do the arithmetic in $\mathbb{Z}_{N1} \times \ldots \times \mathbb{Z}_{Nk}$ instead of G:
  - $f^{-1}(f(g)f(h)) = gh$ for all $g, h \in G$

$$\begin{array}{ccc} gh & \xrightarrow{f} & f(g)f(h) \\ \| & & \| \\ f^{-1}(x) & \xleftarrow{f^{-1}} & x \end{array}$$

# Non-Abelian Groups

- This theorem gives us a great understanding of abelian groups. $\mathbb{Z}_n \times \mathbb{Z}_m$
  - any abelian group is just a vector of numbers using modular arithmetic
  - if we can solve a problem for vectors and modular arithmetic, then in principle, we can solve that problem for all abelian groups (hint hint)

- Non-abelian groups can have much complex behavior…

# Dihedral Group

- Element are $r^i s^j$ for some $i \in \mathbb{Z}_N$ and $j \in \mathbb{Z}_2$, where $r^N = 1$ and $s^2 = 1$
  - identity is $(1, 1) = (r^0, s^0)$
  - r and s satisfy $sr = r^{-1} s$

- Correspondence with $\mathbb{Z}_N \times \mathbb{Z}_2$, but multiplication is more complicated…
  - $(r^i s)(r^j s^k) = r^i r^{-j} s^k = r^{i-j} s^k$
  - c.f. $(r^i)(r^j s^k) = r^{i+j} s^k$

- The inverse of $r^i$ is $r^{N-i}$
- The inverse if $r^i s$ is $r^i s$ !!

# Heisenberg Group

- 3 x 3 matrices with entries from $\mathbb{Z}_p$, with p prime

$$\begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \qquad (a, b, c)$$

$AB \neq BA$

- Can check that a product of these is also of this form.
- Can check that this is the inverse:

$$\begin{bmatrix} 1 & -a & -c+ab \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix}$$

- (Can generalize all of this to k x k matrices for k > 3.)

# Subgroups

# Subgroups

- A subgroup is a subset of a group that is itself a group
- In particular, $S \subseteq G$ is a subgroup iff
  - $e \in S$
  - if $x \in S$, then $x^{-1} \in S$
  - if $x \in S$ and $y \in S$, then $xy \in S$
- So you can perform group operations on elements of S and you will never see an element outside of S (i.e., from $G - S$)

# Cosets

- If $S \subseteq G$ is a subgroup, then a coset of $S$ is a set of the form

$$gS = \{ gs : s \in S \} \qquad \text{for some } g \in G$$

$S = \{a, b, c\}$

$gS = \{ga, gb, gc\}$

- This is not a subgroup (e.g, we do not have $e \in gS$).
- It is just a subset of $G$.

# Cosets

- Let $S \subseteq G$ be a subgroup.

**Theorem**: If $g, h \in G$, then we either have $gS = hS$ or $gS \cap hS = \emptyset$.

**Proof**: If $gS \cap hS$ is not empty, then there is some element in both sets that are the same. I.e., we have $gx = hy$ for some $x, y \in S$.

Multiplying on the right by $x^{-1}$, we have $g = hyx^{-1}$.

Hence, for any $s \in S$, we have $gs = hyx^{-1}s \in hS$ since $x, y, s \in S$.

This shows that $gS \subseteq hS$. Analogous argument shows $hS \subseteq gS$, so $gS = hS$. **Q.E.D.**

# Cosets

**Theorem**: If $g, h \in G$, then we either have $gS = hS$ or $gS \cap hS = \emptyset$.

- So $gS$ and $hS$ are either the same set or completely disjoint. $e \in S$
- And every element in $G$ is in some coset of $S$ (e.g., $g \in gS$ since it is $g = ge$).
- Hence, $n$ the cosets of $S$ partition $G$. I.e., we can write

$$G = g_1S \cup g_1S \cup \ldots \cup g_kS$$

$gS = hS$

$g_1$

for some choice of $g_1, \ldots, g_k \in G$.

# Hidden Subgroup Problem (HSP)

# HSP

**Problem**: Given a function $f : G \to \{0,1\}^k$ (via an oracle) that is constant on cosets of some subgroup $H$, find the subgroup $H$.

- I.e., we are promised that $f(gh_1) = f(gh_2)$ for all $h_1, h_2 \in H$ and $g \in G$.
- Equivalently, $f(g) = f(gh)$ for all $h \in H$ and $g \in G$.

- Outputs need not have any meaning.

- To "find" the subgroup, we usually ask for a "generating set" for it
  - set of elements such that any $h \in H$ can be written as a product of those
  - (usually done when we have informationally "determined" H)

# HSP

**Problem**: Given a function $f : G \to \{0,1\}^k$ (via an oracle) that is constant on cosets of some subgroup H, find the subgroup H.

$y + y = (2y_1, \ldots, 2y_n) = (0, \ldots, 0)$

- Requires exponential time classically.

$(a_1, \ldots, a_n)$

- E.g., consider $G = Z_2^n = Z_2 \times \ldots \times Z_2$

$H = \{(0, \ldots, 0), (y_1, \ldots, y_n)\}$

- Promised that $f(x_1 + y_1, \ldots, x_n + y_n) = f(x_1, \ldots, x_n)$ for *some* vector $(y_1, \ldots, y_n)$ and all vectors $(x_1, \ldots, x_n)$

$y$

$(0, H)$

- But there are $2^n$ choices for what $(y_1, .., y_n)$ could be.
- We'll have to try all of them in the worst case to find the one that works.

# HSP

**Problem**: Given a function $f : G \to \{0,1\}^k$ (via an oracle) that is constant on cosets of some subgroup H, find the subgroup H.

- Requires exponential time classically.
- E.g., consider $G = (Z_N)^x$ and $f(x) = y^x \pmod N$ $\quad 1 = y^0, y^1, y^2 \ldots, y^r = 1$
- If y has ~~period r~~ order r, then $f(x+r) = y^{x+r} = y^x y^r = y^x = f(x)$. $\quad f(x+kr) = f(x)$
- So f is constant on cosets of $Z_r$ $\quad \{ k : k \in Z_r \}$
- This is the ~~period~~ order finding problem, so we have generalized Shor's problem.

# HSP

**Problem**: Given a function $f : G \to \{0,1\}^k$ (via an oracle) that is constant on cosets of some subgroup H, find the subgroup H.

- Requires exponential time classically.
- We will see an efficient quantum algorithm for a *large* number of cases.
  - handle all abelian groups using on phase estimation
- (This is essentially what that Kitaev did after hearing about Shor's result.)