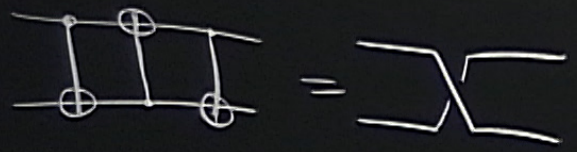
Title: IQC - Quantum Error Correction - Lecture 4

Speakers: Daniel Gottesman, Beni Yoshida
Date: January 25, 2018 - 2:00 PM

URL: https://pirsa.org/18010050



$$\begin{array}{cccc} X\otimes I & X\otimes X & I\otimes X & I\otimes X \\ I\otimes X & I\otimes X & X\otimes X & X\otimes I \\ Z\otimes I \rightarrow & Z\otimes I \rightarrow & Z\otimes Z \rightarrow & I\otimes Z \\ I\otimes Z & Z\otimes Z & Z\otimes I & Z\otimes I \end{array}$$

**Thm** Given an initial stabilizer state and circuit consisting of Clifford group gates, Pauli basis measurements, & Clifford group gates conditioned on classical information. Then the circuit can be simulated on a classical computer with $O(n^2)$ gates per quantum gate.

Measure eigenvalue of $P$: Stabilizer $S = \langle W_i \rangle$ in sympl., $\langle M_i \rangle$ otherwise

Case 1: $\pm P \in S$ — In binary symplectic rep., $\bigvee_P \odot W_i = 0 \ \forall i \Leftrightarrow P \in N(S) = S / \{\pm 1, \pm i\}$

Need to determine $\pm P$

$V_P = \sum_i c_i W_i \Rightarrow$ determine $c_i \Rightarrow \pm P = \prod_i M_i^{c_i}$ → If $+$, then $+1$ output; → If $-$, then $-1$ output

Case 2: $\pm P \notin S$

$P \notin N(S) \Rightarrow \exists\, i$ s.t. $\{M_i, P\} = 0$

$$P_r(+) - P_r(-) = \langle \psi | P | \psi \rangle = \langle \psi | P M_i | \psi \rangle = -\langle \psi | M_i P | \psi \rangle = -\langle \psi | P | \psi \rangle = 0$$

$$\Rightarrow P_r(+) = P_r(-) = \tfrac{1}{2}.$$

What is in $S'$?

Measure eigenvalue of $P$: Stabilizer $S = \langle W_i \rangle$ in symp., $\langle M_i \rangle$ otherwise

Case 1: $\pm P \in S$ — In binary symplectic rep., $v_P \odot w_i = 0 \ \forall i \Leftrightarrow P \in N(S) = S$ $\{\pm 1, \pm i\}$

Need to determine $\pm P$

$v_P = \sum_i c_i w_i \Rightarrow$ determine $c_i \Rightarrow \pm P = \prod_i M_i^{c_i}$ → If $+$, then $+1$ output; → If $-$, then $-1$ output

Case 2: $\pm P \notin S$

$P \notin N(S) \Rightarrow \exists\, i$ s.t. $\{M_i, P\} = 0$

$$Pr(+) - Pr(-) = \langle \psi | P | \psi \rangle = \langle \psi | P M_i | \psi \rangle = -\langle \psi | M_i P | \psi \rangle = -\langle \psi | P | \psi \rangle = 0$$

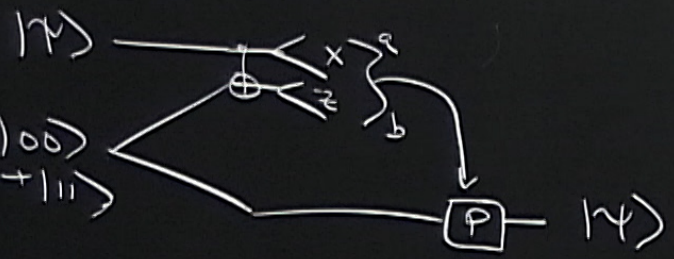
$$\Rightarrow Pr(+) = Pr(-) = \tfrac{1}{2}.$$

What is in $S'$? (State is $\frac{1}{2}(I \pm P)|\psi\rangle) = |\psi'\rangle$)

a) $\pm P \in S'$

$n-1$ gen. { b) $M_j \in S'$ with $[M_j, P] = 0$ : $M_j |\psi'\rangle = \frac{1}{2}(M_j \pm M_j P)|\psi\rangle = \frac{1}{2}(I \pm P) M_j |\psi\rangle = |\psi'\rangle$

c) $M_i M_j \in S'$ when $\{M_j, P\} = 0$: $[M_i M_j, P] = 0$, $M_i, M_j \in S$




| | I | X | X |
|---|---|---|---|
| I | I | Z | Z |
| X | X | I | I |
| Z | Z | I | I |

→

| | I | X | X |
|---|---|---|---|
| Z | Z | Z | Z |
| X | X | X | I |
| Z | Z | I | I |

→

| | I | X | X |
|---|---|---|---|
| $(-1)^q$ | X | I | I |
| X | X | X | I |
| I | Z | Z | |

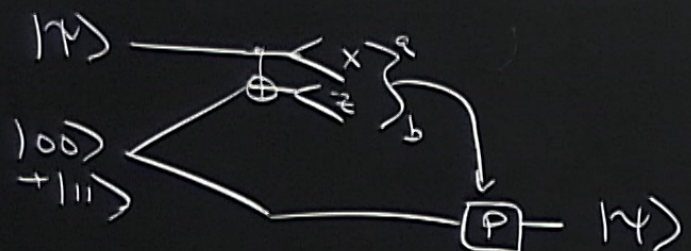
→

| | $(-1)^b$ | I | Z | I |
|---|---|---|---|---|
| $(-1)^q$ | X | I | I | |
| X | I | X | | |
| I | Z | Z | | |

=

| | $(-1)^b$ | I | Z | I |
|---|---|---|---|---|
| $(-1)^a$ | X | I | I | |
| ~~$(-1)^a$~~ | ~~I~~ | ~~I~~ | ~~X~~ | |
| ~~$(-1)^b$~~ | ~~I~~ | ~~I~~ | ~~Z~~ | |

Thm: $\forall U \in SU(2^n)$, $\langle C_n, U \rangle$ is a group which is dense in $SU(2^n)$.




$$\begin{array}{c|cc} & I & X \\ \hline I & I & Z \\ X & X & I \\ Z & Z & I \end{array} \longrightarrow \begin{array}{cc} I & X \\ Z & Z \\ \hline X & I \\ Z & I \end{array} \longrightarrow \begin{array}{cc} I & X \\ \hline (-1)^q X & I \\ X & I \\ I & Z \end{array} \longrightarrow \begin{array}{cc} (-1)^b I & Z I \\ \hline (-1)^q X & I \\ X & I \\ I & Z \end{array} = \begin{array}{cc} (-1)^b I & Z I \\ \hline (-1)^q X & I \\ (-1)^a I & I \\ (-1)^b I & I \end{array} \begin{array}{c} X \\ \hline I \\ X \\ Z \end{array}$$

**Thm:** $\forall\, U \in SU(2^n)$, $\langle C_n, U \rangle$ is a group which is dense in $SU(2^n)$

E.g. $\langle C_1, R_{\pi/8} \rangle$

Generators of $C_n$:

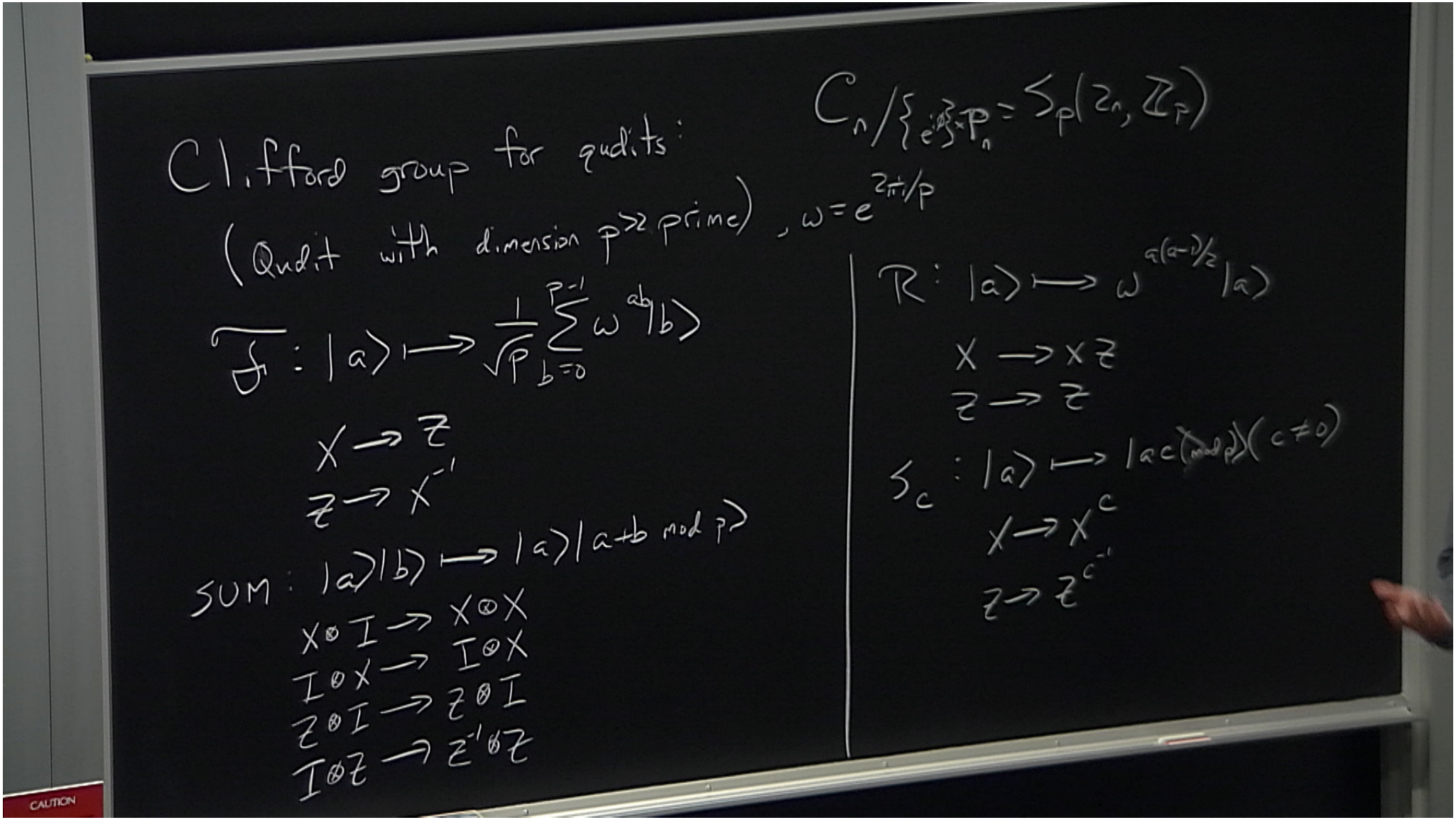
CNOT, H, $R_{\pi/4}$ - can do with $O(n^2/\log n)$

1 qubit H: $X \leftrightarrow Z$

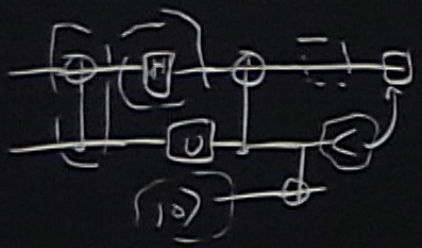
$R_{\pi/4}$: $X \to Y$

$$U = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) \quad \text{Find } V_i, W_j \text{ s.t. } \left(\prod_i V_i\right) U \left(\prod_j W_j\right) = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & I \end{array}\right)$$

| Gate | L mult | R mult |
|---|---|---|
| $H_i$ | Switches $i$th rows of $(A\|B)$ & $(C\|D)$ | Switches $i$th columns of $A \& C$ with $B \& D$ columns |
| $R_{\pi/4,i}$ | Adds $i$th row of $(A\|B)$ to $i$th row of $(C\|D)$ | |
| $CNOT_{ij}$ | Adds $i$th row of $(A\|B)$ to $j$th row of $(A\|B)$ & adds $j$th row of $(C\|D)$ to $i$th row of $(C\|D)$ | |
| $C\text{-}Z_{ij}$ | Add $i$th row of $(A\|B)$ to $j$th row of $(C\|D)$ & $j$th row of $(A\|B)$ to $i$th row of $(C\|D)$ | |


Clifford group for qudits:
(Qudit with dimension $p \geq 2$ prime), $\omega = e^{2\pi i/p}$
$C_n / \{e^{i\theta} I_n\} = S_p(2n, \mathbb{Z}_p)$
$F : |a\rangle \longmapsto \frac{1}{\sqrt{p}} \sum_{b=0}^{p-1} \omega^{ab} |b\rangle$
$X \to Z$
$Z \to X^{-1}$
SUM : $|a\rangle|b\rangle \longmapsto |a\rangle|a+b \bmod p\rangle$
$X \otimes I \to X \otimes X$
$I \otimes X \to I \otimes X$
$Z \otimes I \to Z \otimes I$
$I \otimes Z \to Z^{-1} \otimes Z$
$R : |a\rangle \longmapsto \omega^{a(a-1)/2} |a\rangle$
$X \to XZ$
$Z \to Z$
$S_c : |a\rangle \longmapsto |ac \bmod p\rangle \ (c \neq 0)$
$X \to X^c$
$Z \to Z^{c^{-1}}$
CAUTION

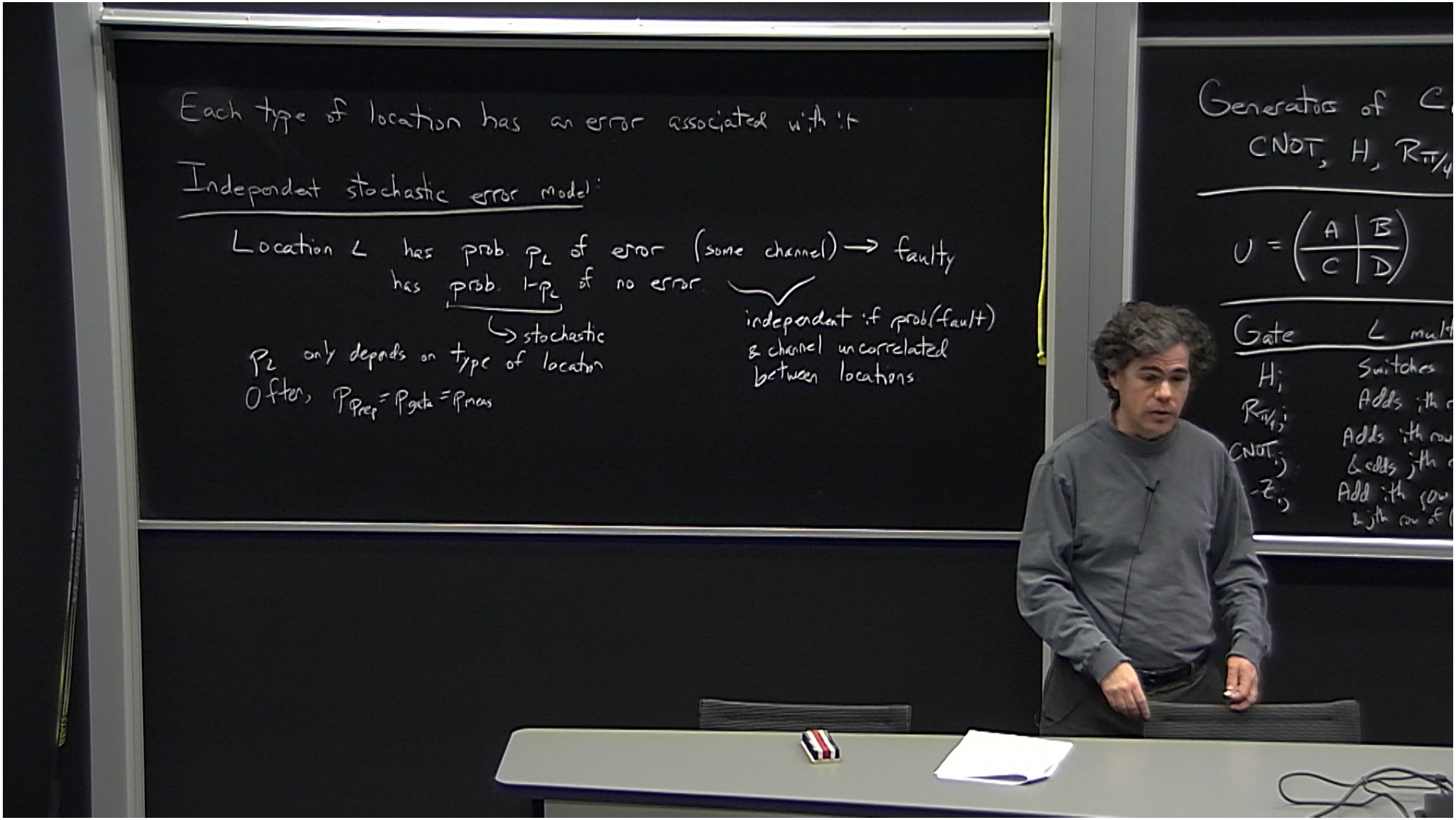
# Basic model of fault tolerance:




**locations** – all take 1 time step

- gate locations (1-qubit, 2-qubit, )
- state preparation locations
- measurement locations
- wait/storage locations

- No classical computation location (Classical gates perfect)


Each type of location has an error associated with it
Independent stochastic error model:
Location ℓ has prob. $p_\ell$ of error (some channel) → faulty
has prob. $1-p_\ell$ of no error
↳ stochastic
independent: if prob(fault) & channel uncorrelated between locations
$p_\ell$ only depends on type of location
Often, $p_{Prep} = p_{gate} = p_{meas}$
Generation of
CNOT, H, $R_{\pi/4}$
$U = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$
Gate
ℓ mult
$H_j$
Switches
$R_{\pi/4,j}$
CNOT
$Z_j$

Fault-tolerant protocol is a circuit encoding

$C \longmapsto FT(C)$

unencoded (ideal) circuit → encoded circuit

→ measurements

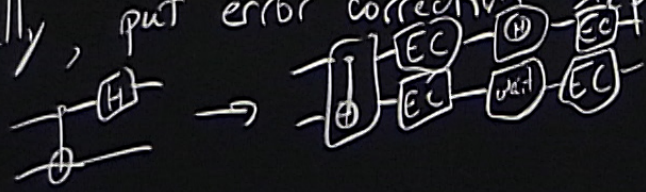
qubits → QECC logical qubits | classical decoding ↪ if no errors, output of ideal circuit

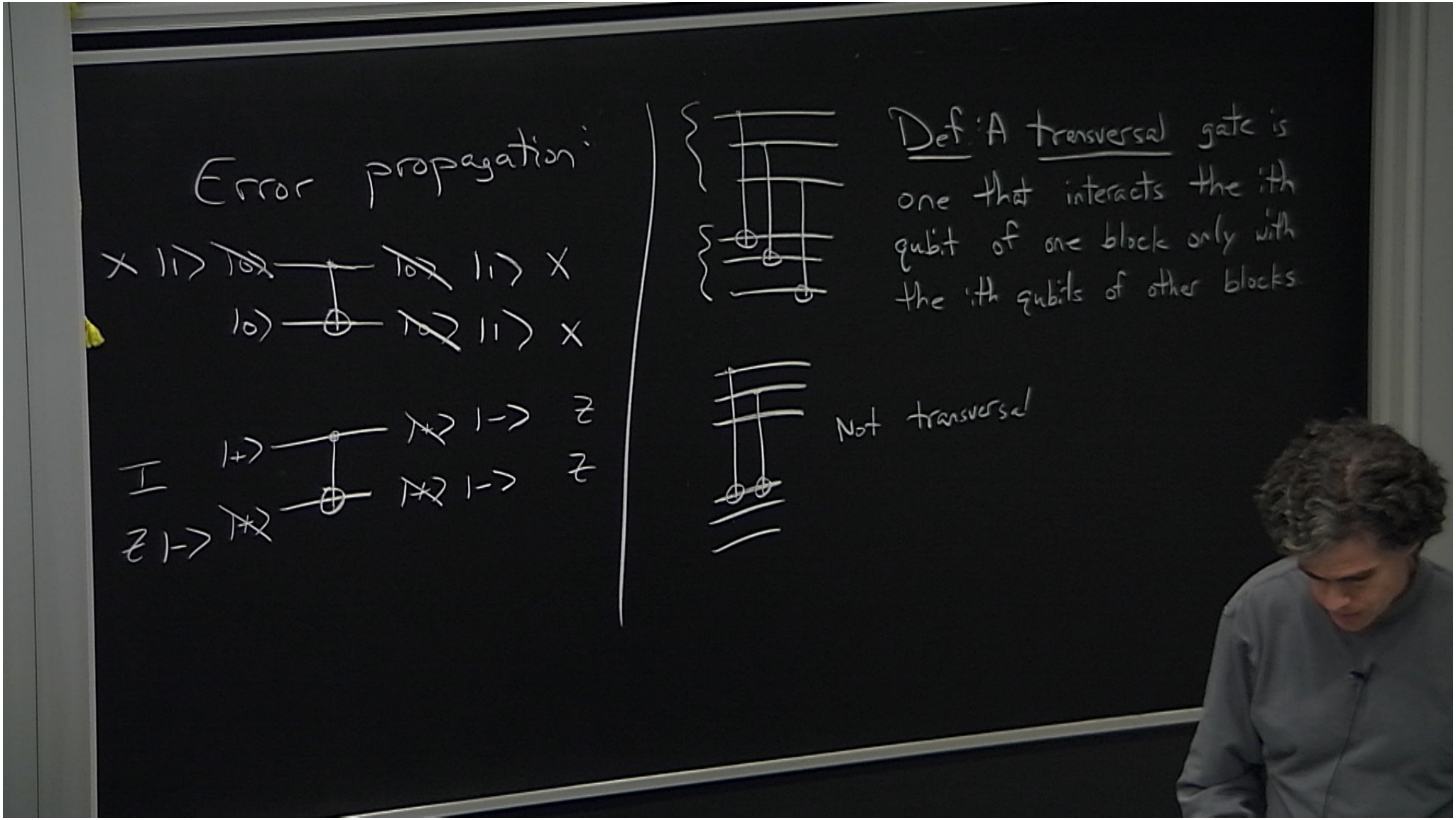
→ measurements

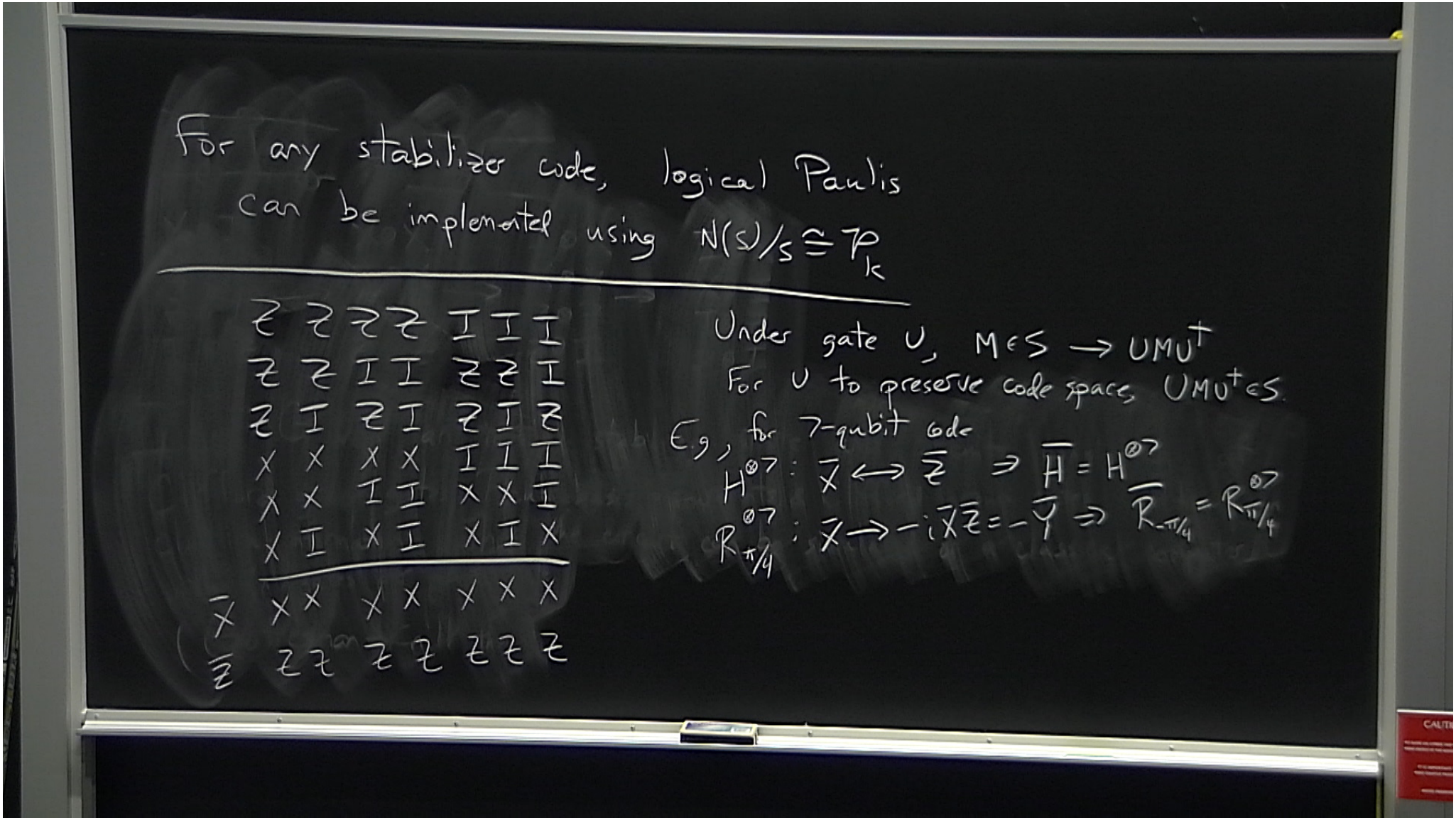
~~ideal~~ logical locations → gadget

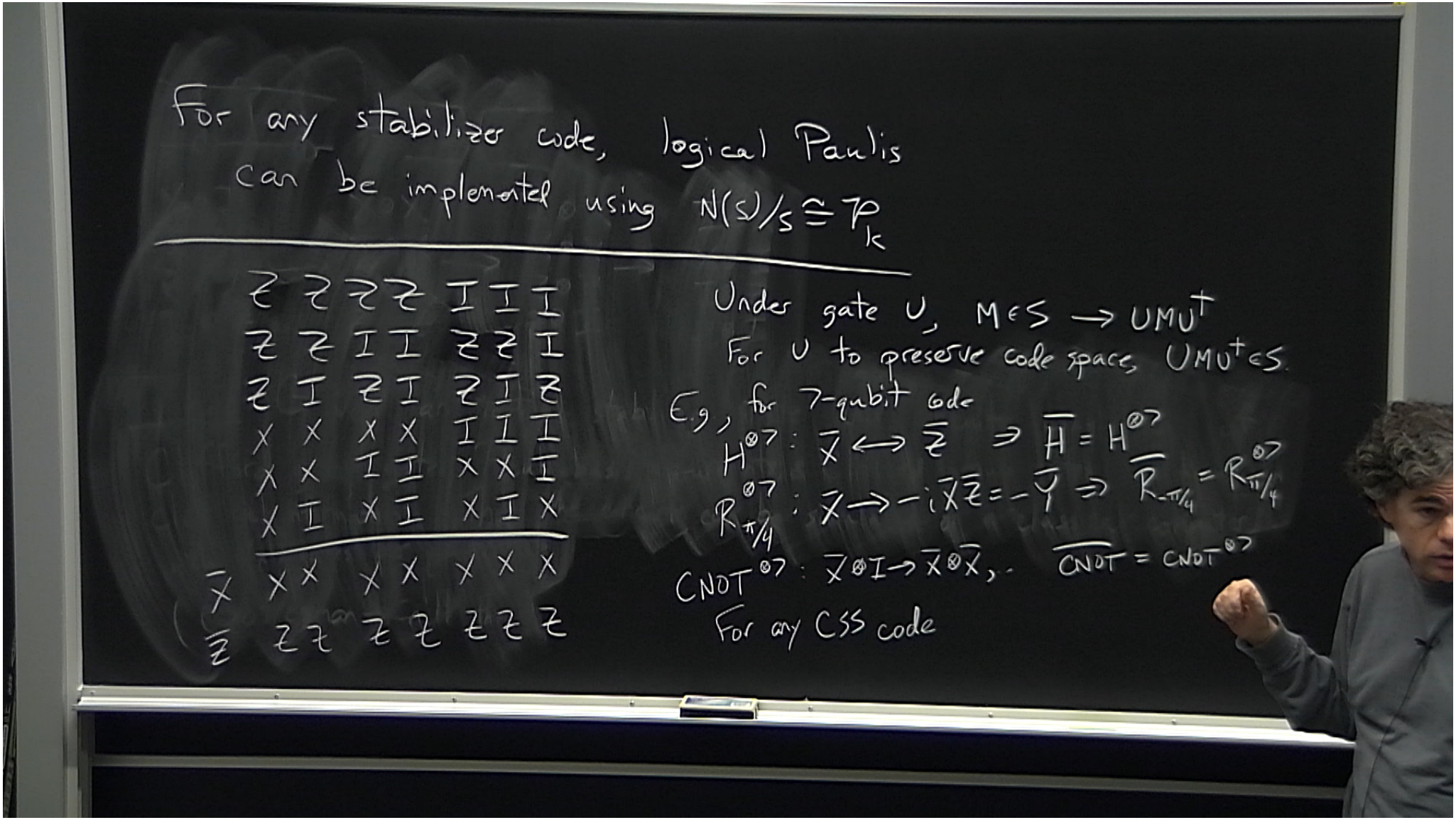
↖ composed of physical locations

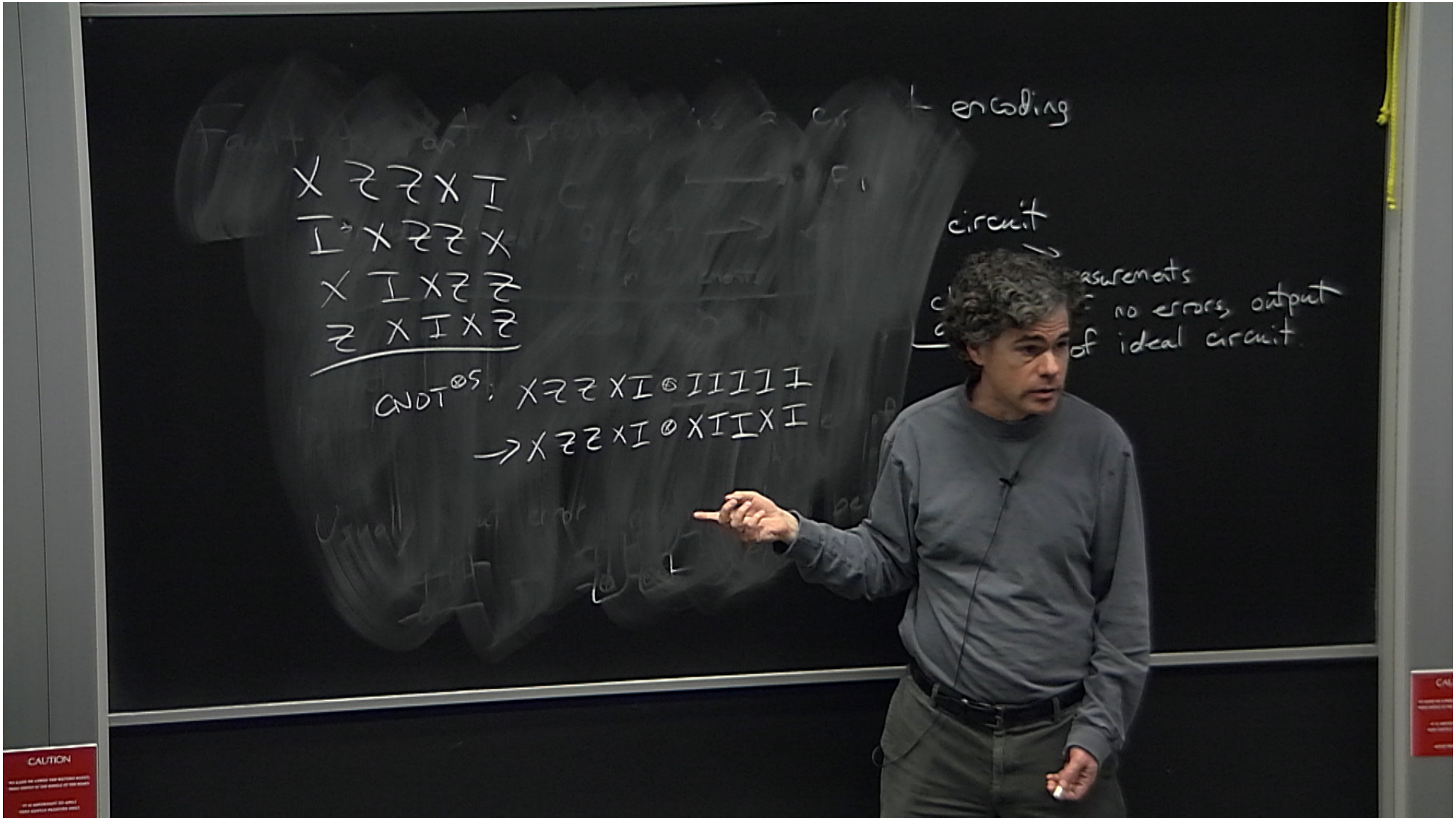
Usually, put error correction steps between gadgets




Error propagation:
Def: A transversal gate is one that interacts the ith qubit of one block only with the ith qubits of other blocks
Not transversal


For any stabilizer code, logical Paulis can be implemented using $N(S)/S \cong \mathcal{P}_k$
Z Z Z Z I I I
Z Z I I Z Z I
Z I Z I Z I Z
X X X X I I I
X X I I X X I
X I X I X I X
$\bar{X}$ X X X X X X X
$\bar{Z}$ Z Z Z Z Z Z Z
Under gate $U$, $M \in S \rightarrow UMU^\dagger$
For $U$ to preserve code space, $UMU^\dagger \in S$.
E.g., for 7-qubit code
$H^{\otimes 7}$: $\bar{X} \leftrightarrow \bar{Z} \Rightarrow \bar{H} = H^{\otimes 7}$
$R_{\pi/4}^{\otimes 7}$: $\bar{X} \rightarrow -i\bar{X}\bar{Z} = -\bar{Y} \Rightarrow \bar{R}_{-\pi/4} = R_{\pi/4}^{\otimes 7}$


For any stabilizer code, logical Paulis can be implemented using $N(S)/S \cong \mathcal{P}_k$
Z Z Z Z I I I
Z Z I I Z Z I
Z I Z I Z I Z
X X X X I I I
X X I I X X I
X I X I X I X
$\bar{X}$ X X X X X X X
$\bar{Z}$ Z Z Z Z Z Z Z
Under gate U, $M \in S \rightarrow UMU^\dagger$
For U to preserve code space, $UMU^\dagger \in S$.
E.g., for 7-qubit code
$H^{\otimes 7}$ : $\bar{X} \leftrightarrow \bar{Z} \Rightarrow \bar{H} = H^{\otimes 7}$
$R_{\pi/4}^{\otimes 7}$ : $\bar{X} \rightarrow -i\bar{X}\bar{Z} = -\bar{Y} \Rightarrow \overline{R_{-\pi/4}} = R_{\pi/4}^{\otimes 7}$
$CNOT^{\otimes 7}$ : $\bar{X} \otimes I \rightarrow \bar{X} \otimes \bar{X}$, . $\overline{CNOT} = CNOT^{\otimes 7}$
For any CSS code


encoding
circuit
no errors, output
of ideal circuit
CNOT^⊗5 : XZZXI ⊗ IIIII
→ XZZXI ⊗ XIIXI
CAUTION

Measure eigenvalue of $P$: Stabilizer $S = \langle W_i \rangle$ in sympl., $\langle M_i \rangle$ otherwise

Case 1: $\pm P \in S$ — In binary symplectic rep., $V_P \odot W_i = 0 \ \forall i \Leftrightarrow P \in N(S) = S / \{\pm 1, \pm\}$

Need to determine $\pm P$

$V_P = \sum_i c_i W_i \Rightarrow$ determine $c_i \Rightarrow \pm P = \prod_i M_i^{c_i}$ ⇒ If $+$, then $+1$ output; ⇒ If $-$, then $-1$ output

Case 2: $\pm P \notin S$

$P \notin N(S) \Rightarrow \exists\, i$ s.t. $\{M_i, P\} = 0$

$$Pr(+) - Pr(-) = \langle \psi | P | \psi \rangle = \langle \psi | P M_i | \psi \rangle = -\langle \psi | M_i P | \psi \rangle = -\langle \psi | P | \psi \rangle = 0$$

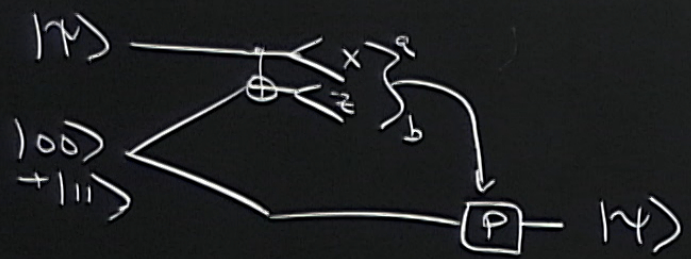
$$\Rightarrow Pr(+) = Pr(-) = \tfrac{1}{2}$$

What is in $S'$? (State is $\frac{1}{2}(I \pm P)|\psi\rangle) = |\psi'\rangle$

a) $\pm P \in S'$

$n-1$ gen. { b) $M_j \in S'$ with $[M_j, P] = 0$ : $M_j |\psi'\rangle = \frac{1}{2}(M_j \pm M_j P)|\psi\rangle = \frac{1}{2}(I \pm P) M_j |\psi\rangle = |\psi'\rangle$

c) $M_i M_j \in S'$ when $\{M_j, P\} = 0$: $[M_i M_j, P] = 0$, $M_i, M_j \in S$




$$\begin{array}{c|cc} & I & X \\ \hline I & I & Z \\ X & X & I \\ Z & Z & I \end{array} \longrightarrow \begin{array}{cc} I & X \\ Z & Z \\ \hline X & I \\ Z & I \end{array} \longrightarrow \begin{array}{cc} I & X \\ \hline (-1)^q X & I \\ X & I \\ I & Z \end{array} \longrightarrow \begin{array}{cc} (-1)^b I & Z \\ (-1)^q X & I \\ \hline X & I \\ I & Z \end{array} = \begin{array}{cc} (-1)^b I & Z \\ (-1)^q X & I \\ \hline (-1)^a I & I \\ (-1)^b I & Z \end{array}$$

**Thm:** $\forall U \in SU(2^n)$, $\langle C_n, U \rangle$ is a group which is dense in $SU(2^n)$.

E.g. $\langle C_1, R_{\pi/8} \rangle$

Generators of $C_n$:

CNOT, $H$, $R_{\pi/4}$ - can do with $O(n^2/\log n)$

1 qubit $H$: $X \leftrightarrow Z$

$R_{\pi/4}$: $X \to Y$

$U = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$ Find $V_i, W_j$ s.t. $\left(\prod_i V_i\right) U \left(\prod_j W_j\right) = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & I \end{array}\right)$

| Gate | $\mathbb{Z}$ mult | $\mathbb{R}$ mult |
|---|---|---|
| $H_i$ | Switches $i$th rows of $(A\|B)$ & $(C\|D)$ | Switches $i$th columns of $A \& C$ with $B \& D$ columns |
| $R_{\pi/4,i}$ | Adds $i$th row of $(A\|B)$ to $i$th row of $(C\|D)$ | |
| $CNOT_{ij}$ | Adds $i$th row of $(A\|B)$ to $j$th row of $(A\|B)$ & adds $j$th row of $(C\|D)$ to $i$th row of $(C\|D)$ | |
| $C\text{-}Z_{ij}$ | Add $i$th row of $(A\|B)$ to $j$th row of $(C\|D)$ & $j$th row of $(A\|B)$ to $i$th row of $(C\|D)$ | |

Clifford group for qudits:

(Qudit with dimension $p \geq 2$ prime), $\omega = e^{2\pi i/p}$

$C_n / \{e^{i\theta} I_n\} = S_p(2n, \mathbb{Z}_p)$

$F : |a\rangle \longmapsto \frac{1}{\sqrt{p}} \sum_{b=0}^{p-1} \omega^{ab} |b\rangle$

$X \to Z$

$Z \to X^{-1}$

SUM : $|a\rangle|b\rangle \longmapsto |a\rangle|a+b \bmod p\rangle$

$X \otimes I \to X \otimes X$

$I \otimes X \to I \otimes X$

$Z \otimes I \to Z \otimes I$

$I \otimes Z \to Z^{-1} \otimes Z$

$R : |a\rangle \longmapsto \omega^{a(a-1)/2} |a\rangle$

$X \to XZ$

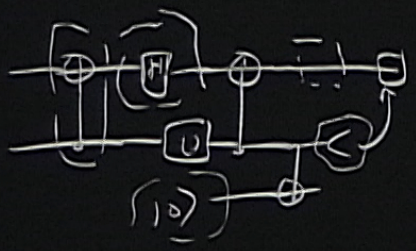
$Z \to Z$

$S_c : |a\rangle \longmapsto |ac \bmod p\rangle \ (c \neq 0)$

$X \to X^c$

$Z \to Z^{c^{-1}}$

# Basic model of fault tolerance:




**locations** – all take 1 time step

- gate locations (1-qubit, 2-qubit, ...)
- state preparation locations
- measurement locations
- wait/storage locations

- No classical computation location (Classical gates perfect) fast

Fault-tolerant protocol is a circuit encoding

$C \longmapsto FT(C)$

unencoded (ideal) circuit → encoded circuit

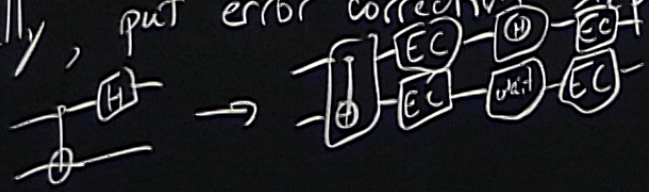
→ measurements → measurements

qubits → QECC logical qubits | classical decoding → if no errors, output of ideal circuit

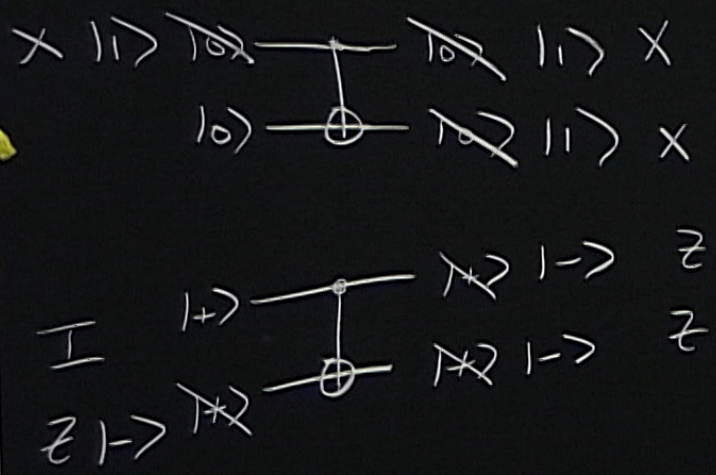
~~ideal~~ logical locations → gadget

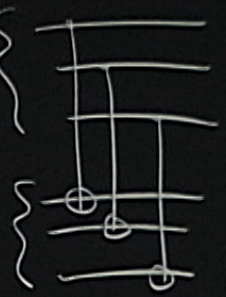
composed of physical locations

Usually, put error correction steps between gadgets

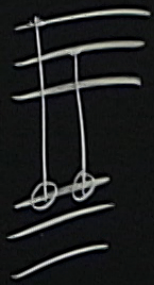


Error propagation:



Def: A transversal gate is one that interacts the ith qubit of one block only with the ith qubits of other blocks.



Not transversal

For any stabilizer code, logical Paulis can be implemented using $N(S)/S \cong \mathcal{P}_k$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Z | Z | Z | Z | I | I | I |
| | Z | Z | I | I | Z | Z | I |
| | Z | I | Z | I | Z | I | Z |
| | X | X | X | X | I | I | I |
| | X | X | I | I | X | X | I |
| | X | I | X | I | X | I | X |
| $\bar{X}$ | X | X | X | X | X | X | X |
| $\bar{Z}$ | Z | Z | Z | Z | Z | Z | Z |

Under gate $U$, $M \in S \rightarrow UMU^\dagger$

For $U$ to preserve code space, $UMU^\dagger \in S$.

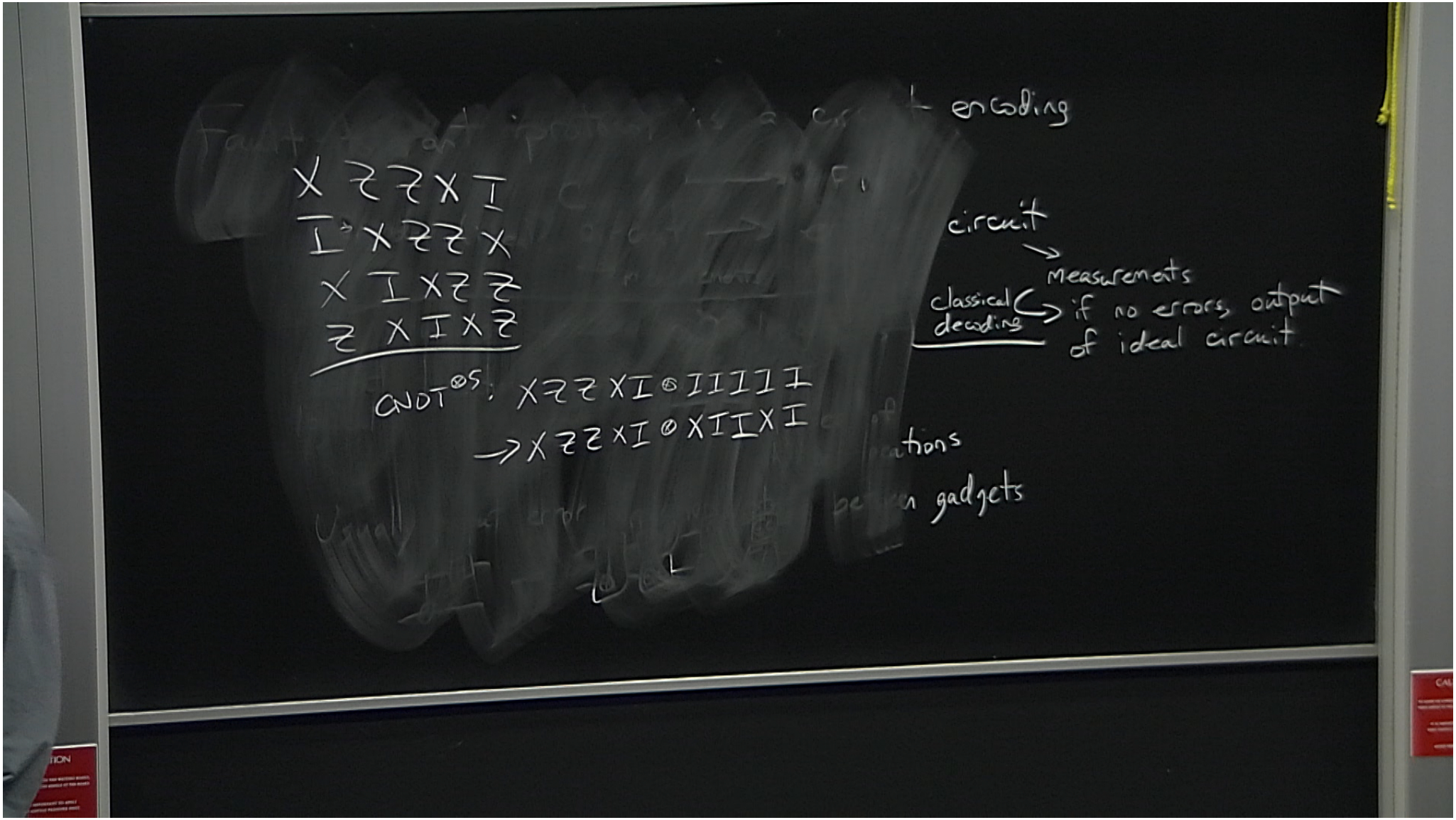
E.g., for 7-qubit code

$H^{\otimes 7}$: $\bar{X} \leftrightarrow \bar{Z} \Rightarrow \bar{H} = H^{\otimes 7}$

$R_{\pi/4}^{\otimes 7}$: $\bar{X} \rightarrow -i\bar{X}\bar{Z} = -\bar{Y} \Rightarrow \overline{R_{-\pi/4}} = R_{\pi/4}^{\otimes 7}$

$CNOT^{\otimes 7}$: $\bar{X} \otimes I \rightarrow \bar{X} \otimes \bar{X}$, . $\overline{CNOT} = CNOT^{\otimes 7}$

For any CSS code


encoding
XZZXI
IXZZX
XIXZZ
ZXIXZ
circuit
measurements
classical decoding
if no errors, output of ideal circuit
CNOT^⊗5 : XZZXI ⊗ IIIII
→ XZZXI ⊗ XIIXI
gadgets