Lecture 12
11 May 2026
PHYS 219 (1)

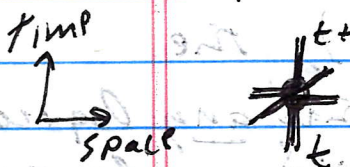
Last Time: Belief propagation

(see Lecture 11 notes)

- Message passing on Tanner graph
- Ideally, want to know $e^* = \arg\max \mathbb{P}(e|s)$. Too hard.
- Instead, estimate log-likelihood ratio of marginals

$$L_i = \ln\left(\frac{P_i(0)}{P_i(1)}\right)$$ Assume no error for $L_i > 0$, Assume error for $L_i < 0$

- Updates assume local independence of messages
- Justified on a tree, violated on graphs with loops
- Bad performance for surface code. Better for expander graphs with "large girth" (not any short loops).
- If $He \neq s$ on BP fails to converge, augment w/ OSD = ordered statistic decoding. Accept e_i^* with large $|L_i|$, solve for rest by Gaussian elimination.
- Syndrome errors? Apply BP to syndrome history.



check nodes triggered where syndrome changes. BP passes messages in both spacelike and timelike directions, seeking locally consistent marginals for both data and syndrome errors

Circuit-based estimates of logical error rate

- Schedule to minimize error propagation during syndrome measurement.
- Consider memory errors (move about logical processing later)
- Surface code: $P_{\text{logical}} \approx 0.1\left(\frac{p}{p_{th}}\right)^{(d+1)/2}$ (dodd) $n = d^2$, $p_{th} \sim .01$

Example: Factoring for RSA 2048 (Gidney 2025)

Keep ~1500 logicals alive for 12 hours

(then do multiple shots for runtime ~ few days)

$P_{logical}^{-1} = (\text{logical error rate per round})^{-1} \sim 1500 \times 12 \times 3600 \times 10^6 \sim 10^{14}$

– assuming a round of syndrome measurement takes ~ 1 microsecond

Suppose $p \sim 10^{-3} \Rightarrow$ want $(d+1)/2 \sim 13 \Rightarrow d = 25$

$\sim 2(25)^2 \sim 1250$ physical qubits per logical

$\Rightarrow (1500)(1250) \approx 1.9$ M physical qubits

(Gidney reduces to ~ 1M via "yoked surface code" for cold storage)

Compare Cain et al. 2026. For $[[5278, 1480, d \le 24]]$ lifted product code ($k \sim 1500$), the block error rate (prob per cycle that any logical qubit fails) is 10^{-11} for $p = 10^{-3}$ physical error rate, with <u>much</u> smaller physical qubit count.

Quantum Computing by Measurement

For logical processing in both the surface code and high-rate codes, performing computation by measurement is a key concept because we know how to measure logical operators (Paulis) fault-tolerantly. We typically use the Clifford + T universal gate set, and track how Pauli operators propagate through Clifford gates (Heisenberg picture — Gottesman-Knill). We'll assume we can do both destructive measurements (which destroy encoded blocks) and nondestructive measurements (revealing Pauli eigenvalue, preserving the encoding).

Clifford unitary acting by conjugation take Pauli P to Pauli P':

$$UPU^\dagger = P' \Rightarrow UP = P'U.$$

U maps P eigenstate to P' eigenstate with the same eigenvalue

$$P|\psi\rangle = \lambda|\psi\rangle \Rightarrow P'U|\psi\rangle = UP|\psi\rangle = \lambda U|\psi\rangle$$

Example: CZ gate. $Z_1 \to Z_1$ $X_1 \to X_1 Z_2$
$Z_2 \to Z_2$ $X_2 \to Z_1 X_2$

(1↔2 symmetry)

$|+\rangle|\psi\rangle \to |0\rangle|\psi\rangle + |1\rangle Z|\psi\rangle$
$|-\rangle|\psi\rangle \to |0\rangle|\psi\rangle - |1\rangle Z|\psi\rangle$
This is $\pm$ eigenstate of $X_1 Z_2$

Other examples $X: X \to X,\ Z \to -Z$

$H: X \to Z,\ Z \to X$

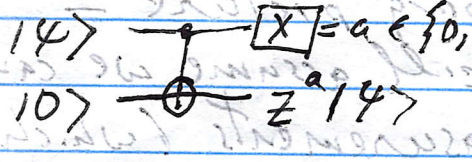
$$S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \Rightarrow SXS^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} X \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = -Y$$

$S: X \to -Y,\ Z \to Z$

Since $\{X_i, Z_i\}$ generate all Paulis, it is enough to know action of U on these.

[For CNOT, see page 9.]

An important primitive: "one-bit teleportation."



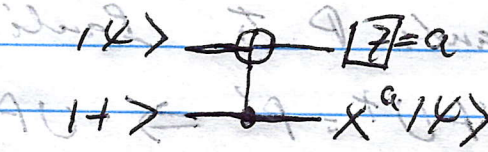
How it works: Stabilizer: $IZ \to ZZ$

$XI \to XX \to (-1)^a X$ ← Apply Z^a to remove phase

$ZI \to ZI \equiv IZ \to Z$

$ZI \equiv IZ$ because $ZZ \in$ Stab.

The dual version:



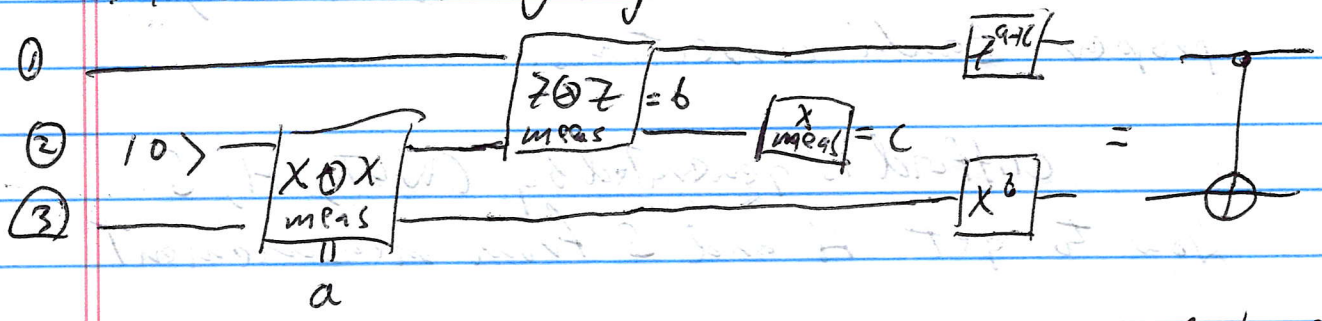
Stabilizer: $IX \to XX$

$XI \to XI \equiv IX \to X$

$ZI \to ZZ \to (-1)^a Z$ ⇐ Apply X^a to remove phase

One-bit teleportation is useful for moving logical info from one block to another. (We don't need to apply the Pauli correction; it suffices to keep track of it in software.)

Measurement gadget for CNOT:



Note: XX and ZZ measurements are nondestructive

How does it work?

Initial stab is $M = IZI$. We want to measure IXX

We want to propagate $X_1 = XII$ $X_3 = IIX$

$Z_1 = ZII$ $Z_3 = IIZ$

Z_3 does not commute with IXX measurement

But $MZ_3 = IIZ$ does commute

Next: Measure ZZI, new stab $M = (-1)^a IXX$

$X_1 = XII$ does not commute with ZZI, but

$X_1 M = (-1)^a XXX$ does

Last step: Measure IXI, new stab $M = (-1)^b ZZI$

Now $Z_3 \to IIZ$ does not commute but $MZ_3 = (-1)^b ZIZ$ does

Summary: $X_1 \to (-1)^a XXX \to (-1)^{a+c} XIX$

$Z_1 \to Z_1$

$X_3 \to X_3$

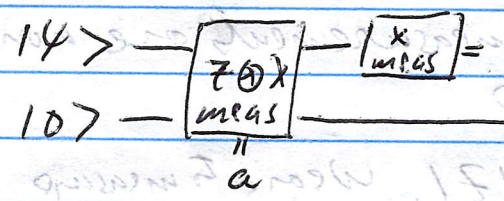
$Z_3 \to (-1)^b ZIZ$

We remove phases with Z_1^{a+c} and $X_3^b \Rightarrow$

$X_1 \to X_1 X_3$, $Z_1 \to Z_1$, $X_3 \to X_3$, $Z_3 \to Z_1 Z_3$. This is CNOT

We need the measurement outcomes to get the proper Pauli corrections.

Clifford is generated by CNOT, H, S.
How to get H and S from measurement



where $H: X \leftrightarrow Z$

Initial stabilizer $M = IZ$

$X_1 = XI \equiv XZ$ commutes with ZX measurement

then $X_{meas} \to (-1)^b Z$

$Z_1 = ZI$ commutes with ZX measurement

After that measurement, new stab $= (-1)^a ZX$

So now $Z_1 \equiv (-1)^a IX$ not affected by XI meas

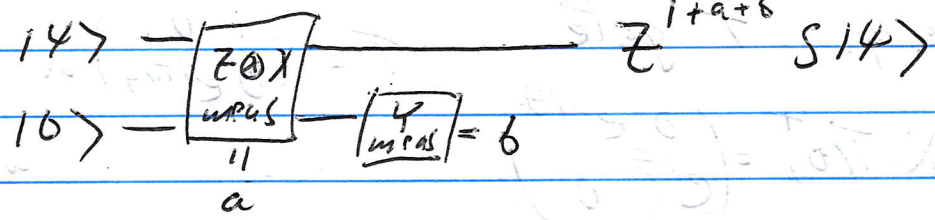
Summary $X \to (-1)^b Z$ $Z \to (-1)^a X$

Hence H after $X^b Z^a$ removes phases.

Note: To toggle basis $X \leftrightarrow Z$, Z-type or X-type measurement does not suffice - we need the mixed $Z \otimes X$ measurement

One more Clifford generator.

$$S: Z \to Z, \quad X \to -Y$$



Initial stab $\mathcal{M} = IZ$

$Z_1 \to Z_1$ commutes with ZX measurement

$X_1 = XI \equiv XZ$ which commutes with ZX meas

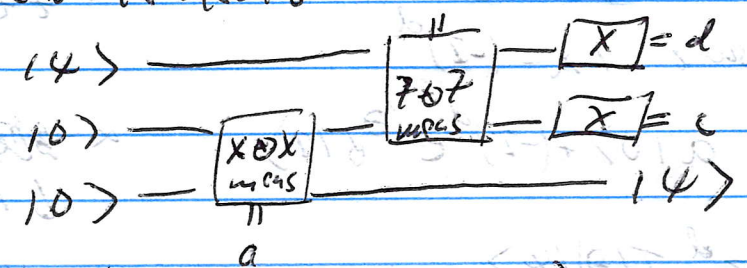
New stab is $\mathcal{M} = (-1)^a ZX$

$$\Rightarrow XZ \equiv (-1)^a (ZX)(XZ) = (-1)^a YY$$

Under Y measurement, this becomes $(-1)^{a+b} Y$, we want $-Y$, so Z^{1+a+b} corrects phase.

Note: To toggle the basis $X \to -Y$, we need Y measurement.

Remark: By combining the CNOT gadget with one-bit teleportation we obtain teleportation via only measurements



(Pauli corrections not shown). We can move quantum states between code blocks if we can measure XX, ZZ across blocks

We've seen that $|0\rangle$ prep and Pauli measurement suffice for Clifford computation. But for universality, we need non-Clifford gate, e.g. T gate. $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ or $T(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$

$T(\theta) X T(\theta)^\dagger = \begin{pmatrix} 0 & e^{-i\theta} \\ e^{i\theta} & 0 \end{pmatrix}$ with $\theta = \pi/4$

For $\theta = \pi/4 \rightarrow \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1-i \\ 1+i & 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(X+Y)$

$TX = \frac{1}{\sqrt{2}}(X+Y)T \Rightarrow$ $T|\pm\rangle$ are $\pm$ eigenstates of $\frac{1}{\sqrt{2}}(X+Y)$

$= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$

Do a T gate with prep of $|T(\theta)\rangle = T(\theta)|+\rangle$ and Pauli measurement

$|T(\theta)\rangle = \frac{1}{\sqrt{2}}|0\rangle + e^{i\theta}|1\rangle$ — $Z\theta Z$ meas — $X_{meas} = d$

$|\psi\rangle = a|0\rangle + b|1\rangle$ — (meas) — c

$\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)(a|0\rangle + b|1\rangle)$

$= \frac{1}{\sqrt{2}}(a|00\rangle + e^{i\theta} b|11\rangle) + \frac{1}{\sqrt{2}}(b|01\rangle + a e^{i\theta}|10\rangle)$

$ZZ = +1$ $\qquad$ $ZZ = -1$

Measure $X = (-1)^d$

$\propto a|0\rangle + (-1)^d e^{i\theta} b|1\rangle$ $\qquad$ $\propto b|1\rangle + (-1)^d e^{i\theta} a|0\rangle$

$= Z^d T(\theta)|\psi\rangle$ $\qquad$ $= (-1)^d e^{i\theta} Z^d T(\theta)^{-1}|\psi\rangle$

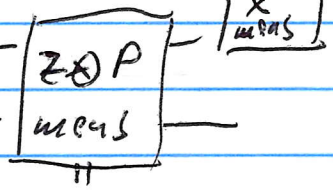
Depending on outcome of $Z\theta Z$ measurement, we have (up to a Pauli correction) $T(\theta)|\psi\rangle$ or $T(\theta)^{-1}|\psi\rangle$

For $ZZ=-1$, we need a Clifford correction $T(\theta)^2 = S^{-1}$ for $\theta = \pi/4$

up to a phase, $T(\theta) = e^{i\frac{\theta}{2}Z}$. We can expand the target state $|\psi\rangle$ in terms of eigenstates of any Pauli operator P.

$$|T(\theta)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$$

$$a|P=1\rangle + b|P=-1\rangle$$



For $c=0$, this applies $\exp(i\frac{\theta}{2}P)$ up to Pauli.

For $c=1$, this applies $\exp(-i\theta/2 P)$ "

The correction for $c=1$, $e^{i\theta P}$, is Clifford for $\theta = \pi/4$.

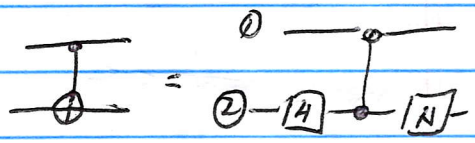
$$e^{i\theta P} = \cos\theta I + i\sin\theta P = \frac{1}{\sqrt{2}}(I + iP) \text{ for } \theta = \pi/4$$

$$\Rightarrow e^{i\theta P} Q e^{-i\theta P} = \frac{1}{\sqrt{2}}(I+iP)Q(I-iP) = Q \text{ if } Q, P \text{ commute}$$

$$\text{or} = \frac{1}{2}(Q + iPQ - iQP + PQP) = iPQ \text{ if anticommute}$$

(and a product of Paulis is Pauli).

Pauli propagation by CNOT



$X_1 \to X_1, Z_2 \to X_1 X_2$

$Z_1 \to Z_1$

$X_2 \to Z_2 \to Z_2 \to X_2$

$Z_2 \to X_2 \to Z_1 X_2 \to Z_1 Z_2$