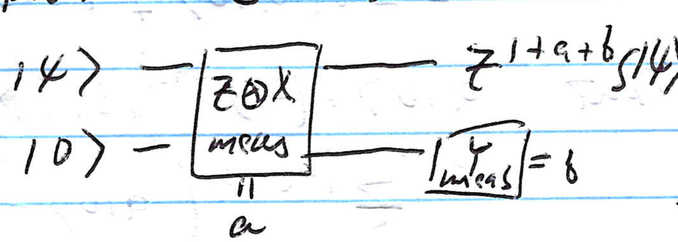
Computing by measurement (continued)

We'd like to leverage ability to perform fault-tolerant measurement of logical Pauli operators in FTQC.

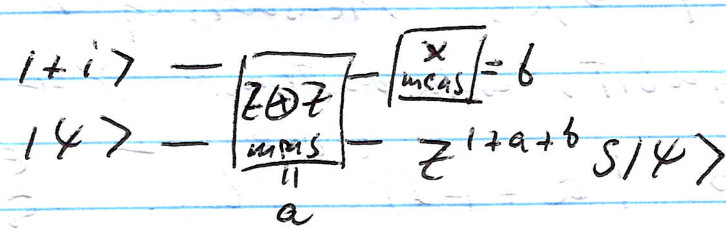
Last time: execution of Clifford generators (CNOT, H, S) via $|0\rangle$ prep and nondestructive Pauli measurement. (And Pauli frame update.)

Example: $S: \; Z \to Z, \quad X \to -Y$ (Heisenberg)



In CSS coding, we might prefer Z-type and X-type meas. But we need to introduce phases

Another way: suppose we can prepare $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, the $Y=+1$ eigenstate. (Maybe by distillation.)



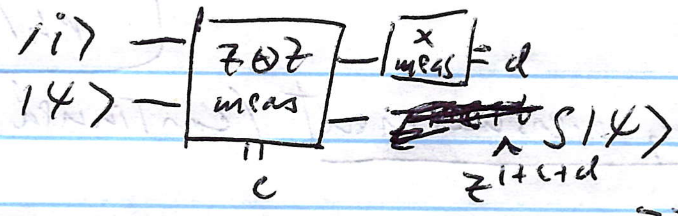
Initial stab is YI

How do X, Z propagate?

$IX \equiv YX$ (commutes w/ ZZ) $\equiv (-1)^a (ZY)(ZX) = (-1)^a XY \to (-1)^{a+b}\, Y$

$IZ \to IZ$ (commutes w/ ZZ).

Let's verify in Schrödinger picture.



$S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$

$$\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)(a|0\rangle + b|1\rangle) \xrightarrow{ZZ=1} a|00\rangle + ib|11\rangle$$

$$\xrightarrow{ZZ=-1} ia|10\rangle + b|01\rangle$$

(equiprobable)

$ZZ = +1$, $X = \pm 1$:

$\longrightarrow a|0\rangle \pm ib|1\rangle$ (equiprob.)

$ZZ = -1$, $X = \pm 1$: $\rightarrow \pm ia|0\rangle + b|1\rangle$ (equiprob.)

$= \pm i(a|0\rangle \mp ib|1\rangle)$

Hence output $a|0\rangle + (-1)^{c+d} ib|1\rangle$

$= Z^{1+c+d}(a|0\rangle - ib|1\rangle)$

Note: If we realize S via measurement as above, using input $|i\rangle$, we can measure Y using ZZ and X measurement, since $S: Y \to X$. Measuring X on second qubit, with outcome $X = (-1)^e$ has Prob $|a + (-1)^{c+d+e} ib|^2$. Equivalent to Y meas, up to outcome flip.

But — For Clifford computation, we can efficiently simulate classically by tracking how Paulis evolve in Heisenberg picture. To give power to QC we need non-Cliffords ("magic"). How to do via measurement?

$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ is non-Clifford: $\quad T X T^\dagger = \frac{1}{\sqrt{2}}(X+Y)$

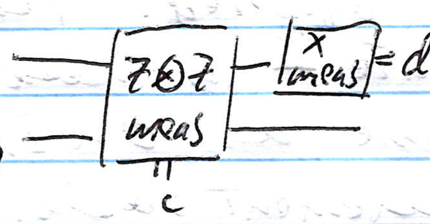
And Clifford + T is <u>universal</u>. $\quad T Y T^\dagger = \frac{1}{\sqrt{2}}(-X+Y)$

We can generalize above Schrödinger picture description.

$$T(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}, \quad |T(\theta)\rangle = T(\theta)|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)$$

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

$|\psi\rangle = a|0\rangle + b|1\rangle$



$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)\left(a|0\rangle + b|1\rangle\right) \xrightarrow{ZZ=1} a|00\rangle + e^{i\theta} b|11\rangle$$
$$\xrightarrow{ZZ=-1} e^{i\theta} a|10\rangle + b|01\rangle$$

$ZZ = +1,\ X = (-1)^d: \quad a|0\rangle + (-1)^d e^{i\theta} b|1\rangle = Z^d T(\theta)|\psi\rangle$

$ZZ = -1,\ X = (-1)^d: \quad (-1)^d e^{i\theta} a|0\rangle + b|1\rangle$

$$= (-1)^d e^{i\theta}\left(a|0\rangle + (-1)^d e^{-i\theta} b|1\rangle\right)$$

$$= \text{phase} \times Z^d\, T(\theta)^{-1}|\psi\rangle$$

$$= \text{phase} \times T(-2\theta)\, Z^d\, T(\theta)|\psi\rangle$$

To get the desired gate, in addition to Pauli correction Z^d, we must apply $T(2\theta)$ for $c = 1$.

For $\theta = \pi/4$ $\quad T(\theta) = T$ and $T(2\theta) = S^{-1}$

The correction $Z^d S^{-1}$ is Clifford but not Pauli. We can efficiently propagate through subsequent Clifford circuit ~~efficiently~~ classically.

Except: Because S toggles between X and Y bases, when qubits are measured downstream from S gate, we need to know outcome $ZZ = (-1)^c$. Hence measurement bases must be adaptive (conditioned on prior measurements), even if S is tracked in software rather than applied. (Contrast with Pauli frame update — we need Pauli frame to interpret outcome as 0 or 1, but not for choice of measurement basis.)

A further generalization: If we can prepare $|T(\theta)\rangle$, we apply (up to Pauli frame) $U = \exp(\pm i \frac{\theta}{2} \underline{P})$

where $\underline{P}$ is any Pauli operator (of arbitrary weight), where now we measure $Z \otimes \underline{P}$ rather than $Z \otimes Z$ (notice that $T(\theta) = e^{i\frac{\theta}{2}Z}$.)

$|T(\theta)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$ — $Z \otimes \underline{P}$ meas. — X meas

$a|\underline{P}=+1\rangle + b|\underline{P}=-1\rangle$ — $Z \otimes \underline{P}$ meas. $= c$

It's the same analysis as before! To correct the $c=1$ outcome, apply

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

This correction is <u>Clifford</u> for $\theta = \pi/4$.

Need to show $\frac{1}{\sqrt{2}}(I+i\underline{P})$ maps Pauli → Pauli. Of course $Q \to Q$ if Q commutes with $\underline{P}$, so suppose $\underline{P}$ and Q anticommute

$$\frac{1}{\sqrt{2}}(I+i\underline{P})Q\frac{1}{\sqrt{2}}(I-i\underline{P})$$
$$= \frac{1}{2}\left(Q-Q+i\underline{P}Q-iQ\underline{P}\right) = i\underline{P}Q,$$ which is Pauli if $\underline{P}$ and Q are.

Pauli-Based Computation

(Bravyi - Smith - Smolin 2016)

Now we've seen that universal computation can be executed replacing Clifford + T by measurement gadgets (including nondestructive Pauli measurement); assume input $|0\rangle$ and $|T\rangle$ are available. But the Clifford comp. can be classically efficiently simulated — only the $|T\rangle$ states seem intrinsically quantum.

In fact, further simplification is possible:

"$|T\rangle$ states and (nondestructive) Pauli measurements are all you need!"

- Measurements are adaptive.
- Pauli + Clifford frame tracked in software.
- Polynomial time classical computation needed.
- Measurements can be chosen to be mutually commuting!

Consider poly(n) size quantum circuit on n qubits with m T gates + Clifford gates. It can be efficiently simulated (including classical processing) by computation with m T state inputs (and no other inputs) and a sequence of Pauli product meas. on the m qubits. Furthermore, these (nondestructive, adaptive) measurements can be chosen to be mutually commuting. Because ~~[illegible]~~ no more than m commuting measurements on m qubits are independent, no more than m measurement rounds are needed.

Let's suppose that, in circuit to be simulated, qubits are initialized as $|0\rangle$ and measured at end in Z basis. We've seen how to simulate with adaptive measurement if we add an input $|T\rangle$ for each T gate, and an input $|0\rangle$ for each Clifford gate. But we don't really need the input $|0\rangle$ for each Clifford because we can simulate Clifford classically by propagating Pauli's through Pauli measurements until the first T gate is encountered. And beyond, because only Pauli measurements are encountered by stabilizer states, even though there are also input T states. We use info to update Clifford frame.

We can choose PPMs (Pauli product meas.) to commute. Here is why. Suppose in round t, P_t is first Pauli measurement that anticommutes with Pauli P_s measured in round $s < t$. The outcome of P_s measurement was $\sigma_s \in \{1, -1\}$. Hence the input state $|\psi\rangle$ to round t satisfies $P_s|\psi\rangle = \sigma_s|\psi\rangle$.

Therefore, $\langle\psi|P_t|\psi\rangle = \langle\psi|P_s^\dagger P_t P_s|\psi\rangle = -\langle\psi|P_t|\psi\rangle$

$$\Rightarrow \langle\psi|P_t|\psi\rangle = 0 \Rightarrow P_t|\psi\rangle = \sigma_t|\psi\rangle$$

outcome is 50-50 random.

After measurement, state has been projected onto $|\psi'\rangle = \frac{1}{2}(P_t + \sigma_t I)|\psi\rangle$

(up to $\sqrt{2}$ norm factor)

Hence

$$|\psi'\rangle = \frac{1}{\sqrt{2}}(P_t + \sigma_s\sigma_t P_s)|\psi\rangle$$

If P_t and P_s anticommute, then $P_t + \sigma P_s$ is Clifford (for $\sigma = \pm 1$). This means we don't need to do the measurement. We can simulate it perfectly by picking $\sigma_t \in \{\pm 1\}$ uniformly at random and inserting the known Clifford $1/\sqrt{2}(P_t + \sigma P_s)$. This Clifford can be propagated forward to the end of the circuit, with Clifford frame update accordingly.

What about the n input states $|0\rangle^{\otimes n}$ to the circuit to be simulated? Think of those as $\sigma = 1$ outcomes of Z measurement ~~on~~ on those n qubits. By the above procedure we choose all subsequent PPM to commute with these — i.e. they act trivially and the qubits themselves are never needed.

What about the measurement of Z_i on each of the simulated circuit's output qubits? We can propagate Z_i backward through the circuit. It becomes the measurement of a Pauli operator acting on the m input T states, up to known Pauli frame updates.

If m independent commuting Paulis have been measured in m rounds, that provides the complete stabilizer of a m-qubit state determined by the measurement outcomes. If the backpropagated Z_i is in this stabilizer, it is determined by the PPM outcomes. Else it anticommutes with some element of stabilizer, has a uniformly random outcome, and I simulate it by flipping a coin.

What if fewer than m independent measurement are performed, and our output observable of interest commutes with stabilizer but is not in stab (hence not determined by PPM outcomes)? Measure additional commuting operators!