We've seen how to store logical qubits safely. Want to discuss how it's done in experiment + how to apply logical gates safely.

To get there, need to introduce a bit of formalism, which is today's goal

Def: **Clifford group**

$$\mathcal{C}_n := \{ U \in U(2^n) : U^\dagger P_n U = P_n \}$$

$U \in U(2^n)$: unitary matrix on n qubits

$U^\dagger P_n U = P_n$: U-conjugation takes Pauli strings to themselves.

$U \in \mathcal{C}_n \Rightarrow U$ is a "Clifford gate"

Clifford gates preserve structure of Pauli stabilizer codes, so they're a natural set of gates to study.

Prop: $\mathcal{C}_n$ is a group.

Proof: $U_1^\dagger P_n U_1 = U_2^\dagger P_n U_2 = P_n$

$$\Rightarrow U_1^\dagger U_2^\dagger P_n U_2 U_1 = (U_2 U_1)^\dagger P_n (U_2 U_1) = P_n$$ ∎

also easy to check identity/inverses etc.

Prop: $P_n \leq \mathcal{C}_n$ [Paulis are Clifford]

Proof: if $P, Q \in P_n$, $Q^\dagger P Q = \eta P$ where $\eta = \pm 1$ as discussed previously

Example: **Hadamard gate H** on a single qubit:

$$H := \frac{X+Z}{\sqrt{2}} \quad \text{is unitary}$$

$$H^\dagger X H = \tfrac{1}{2}(X+Z)X(X+Z) = \tfrac{1}{2}(X + ZXZ + Z + Z) = Z$$

$H^\dagger Z H = X$ similarly. So H permutes Paulis, but does take $P_n \to P_n$

How does Clifford group act on $\mathbb{F}_2^{2n}$ rep. of Paulis?

If $U \in C_n$ and $P_1, P_2 \in \mathcal{P}_n$: $(U^\dagger P_1 U)(U^\dagger P_2 U) = U^\dagger (P_1 P_2) U$

$\Rightarrow \varphi(U^\dagger P_1 U) + \varphi(U^\dagger P_2 U) = \varphi(U^\dagger (P_1 P_2) U)$

(φ: map from $\mathcal{P}_n \to \mathbb{F}_2^{2n}$)

conjugation by U preserves linearity $\Rightarrow$ $\varphi(U^\dagger P U) = M_U \varphi(P)$

($M_U \in \mathbb{F}_2^{2n \times 2n}$ is a matrix)

Since $P_1 P_2 = \eta P_2 P_1 \Rightarrow (U^\dagger P_1 U)(U^\dagger P_2 U) = \eta (U^\dagger P_2 U)(U^\dagger P_1 U)$

we need: $(M_U \varphi(P_1))^T J (M_U \varphi(P_2)) = \varphi(P_1)^T J \varphi(P_2)$

($J = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$)

or M_U is <u>symplectic</u>: $M_U \in Sp(2n, \mathbb{F}_2) := \{M \in \mathbb{F}_2^{2n \times 2n} : M^T J M = J\}$

Hadamard gate $M_H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in Sp(2, \mathbb{F}_2)$ for a single qubit

Since any 1-Pauli Clifford gate can only permute X, Y, Z, there must be one additional single-qubit Clifford gate...

<u>Example</u>: <u>S gate</u>: $M_S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ or $S = e^{-i\pi/4 Z}$

$S^\dagger X S = -Y, \quad S^\dagger Y S = X, \quad S^\dagger Z S = Z.$

Once $n > 1$, there are also entangling Clifford gates:

<u>Example</u>: $CNOT_{i \to j} = \frac{I + Z_i}{2} + \frac{I - Z_i}{2} X_j$ generates entanglement b/c

$CNOT_{1 \to 2} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ creates Bell pair from a product state.

A short calculation shows that:

$$\mathrm{CNOT}_{i\to j}^{\dagger} Z_i \mathrm{CNOT}_{i\to j} = Z_i \qquad \mathrm{CNOT}_{i\to j}^{\dagger} X_j \mathrm{CNOT}_{i\to j} = X_j$$

$$\mathrm{CNOT}_{i\to j}^{\dagger} X_i \mathrm{CNOT}_{i\to j} = X_i X_j \qquad \mathrm{CNOT}_{i\to j}^{\dagger} Z_j \mathrm{CNOT}_{i\to j} = Z_i Z_j$$

in $\mathbb{F}_2$ formalism,

$$M_{\mathrm{CNOT}_{1\to 2}} = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right) \begin{matrix} X_1 \\ X_2 \\ Z_1 \\ Z_2 \end{matrix}$$

It turns out that these gates suffice to generate all Clifford gates!

Thm: Define $\hat{\mathcal{C}}_n := (\mathcal{C}_n / U(1)\mathcal{P}_n)$

i.e. identify $U \sim e^{i\theta} P U$ (phase, Pauli string)

Then $\hat{\mathcal{C}}_n$ is generated by $\langle H_i, S_i, \mathrm{CNOT}_{1\to i} \rangle$

If $U \in \hat{\mathcal{C}}_n$ it is a product of...

Moreover: $\hat{\mathcal{C}}_n \cong Sp(2n, \mathbb{F}_2)$ [all possible symplectic transforms are realized by Cliffords].

Proof sketch: A bit tedious so we'll be brief

Lemma: If $U \in \mathcal{C}_n / U(1)$ obeys $U^\dagger P U = e^{i\theta_P} P \ \forall P \in \mathcal{P}_n$ then $U \in \mathcal{P}_n / U(1)$.

Proof sketch: if $P^2 = I \Rightarrow e^{i\theta_P} \in \{\pm 1\} \to \mathbb{F}_2$! (can always choose such a P)

$U^\dagger P Q U = U^\dagger P U (U^\dagger Q U) = e^{i(\theta_P + \theta_Q)} PQ$ [phases add...]

$\Rightarrow \theta_P = \varphi(R)^T J \varphi(P)$ for some Pauli string R

$\Rightarrow U = R$ (up to phase) ∎

Then one does Gaussian elimination to show ∃ sequence of

$$\cdots S_7 \, CNOT_{3\to 2} \, H_3 \, M = I$$

(arbitrary symplectic) ∎

Now that we've classified all the possible Clifford circuits, our second main result is

Def: Let $\mathcal{S} = \langle S_1, \ldots, S_m \rangle$ be a stabilizer group. Given $\vec{\eta} \in \{\pm 1\}^m$, stabilizer mixed state

$$\rho_{\vec{\eta}} := 2^{m-n} \prod_{i=1}^{m} \frac{I + \eta_i S_i}{2}.$$

Gottesman–Knill Thm: ∃ polynomial runtime algorithm for dynamics of stabilizer states under Clifford circuits, including measurement/feedforward

So if quantum computers are more powerful than classical, Clifford circuits won't be enough... we'll return to that point later.

We can actually build this algorithm directly!

Step 1: dynamics w/o measurement: given Clifford U:

$$U \rho_{\vec{\eta}} U^\dagger = \prod_{i=1}^{m} \frac{I + \eta_i (U S_i U^\dagger)}{2}$$

→ store stabilizers via $\mathbb{F}_2$ formalism!

since Clifford $\in Sp(2n, \mathbb{F}_2)$

$$S = \left(\varphi(S_1) \cdots \varphi(S_m)\right) \in \mathbb{F}_2^{2n \times m}$$

and $\vec{\eta} \in \{\pm 1\}^m$

⇒ update: $S \to M_U S$

also update $\vec{\eta}$ [e.g. $S \, Y S^\dagger = -X$] flips component of η?

Step 2: measure a Pauli operator P.

if $P \in \mathcal{S}$, outcome deterministic [$P = S_1 S_2 \Rightarrow$ measurement outcome $\eta_1 \eta_2$ etc.]

else do each of: ① if any prior $\{S_i, P\} = 0 \ldots$

Suppose $\{S_1, P\} = \cdots = \{S_r, P\} = 0$.

Replace: $\mathcal{S} \to \big(\varphi(S_2)\varphi(S_1) \cdots \varphi(S_r)\varphi(S_1) \;\; \varphi(S_{r+1}) \cdots\big)$

$\vec{\eta}^T \to \big(\eta_2\eta_1 \cdots \eta_r\eta_1 \;\; \eta_{r+1} \cdots\big)$

$\to$ S_1S_2 commutes w/ P so not disturbed

$\to$ and has eigenvalue $\eta_1\eta_2$

② add P to $\mathcal{S}$ (new $\mathcal{S}$): $\mathcal{S} \to (\mathcal{S} \mid \varphi(P))$

$\vec{\eta} \to \begin{pmatrix}\vec{\eta} \\ \eta_P\end{pmatrix}$ where $\mathbb{P}[\eta_P = \pm 1] = \frac{1}{2}$.

$p_{\vec{\eta}}$ contains both e-values, measurement collapses...

Matrix manipulations above require polynomial classical resources ☒

Key: we can simulate (highly) entangled states, if stabilizer. This will be crucial for understanding QEC!

Short example: consider measuring Z_2 in $CNOT_{1\to 2} H_1 |00\rangle$:

$$\mathcal{S} \to \begin{pmatrix}0&0\\0&0\\1&0\\0&1\end{pmatrix} \xrightarrow{H_1} \begin{pmatrix}1&0\\0&0\\0&0\\0&1\end{pmatrix} \xrightarrow{CNOT_{1\to 2}} \begin{pmatrix}1&0\\1&0\\0&1\\0&1\end{pmatrix} \xrightarrow{\text{measure } Z_2} \begin{pmatrix}1&0&0\\1&0&0\\0&1&0\\0&1&1\end{pmatrix}$$

$Z_1 \; Z_2$ $\qquad$ $X_1 \; Z_2$ $\qquad$ $X_1X_2 \; Z_1Z_2$ $\qquad$ $Z_1Z_2 \; Z_2$

$\vec{\eta} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ——until measurement——→ $\vec{\eta} = \begin{pmatrix} 1 \\ \pm 1 \end{pmatrix}$

↖ each w/ 50% prob

G-K gives us another way to understand why it's possible to simulate dynamics (e.g. for threshold...) of QEC at scale!

measure stabilizers of QEC code ⇒ $S = H^T$

Keep track of $\vec{\eta} \to \vec{s}$ (syndrome)

There's a useful idea here:

Def: Pauli frame tracking:

if (noisy) syndrome extraction ⇒ (likely) error E,

store suitable recovery R in software w/o physically correcting.

We already implicitly did this in discussion of spacetime decoding!

in $\mathbb{F}_2$ formalism: Let r = Pauli frame

applying Clifford gate U: $r \to M_U r$ [$R \to URU^\dagger$]

measure Pauli P: reinterpret measurement outcome

$\eta \to \eta (-1)^{\varphi(P)^T J r}$ [measured $R^\dagger P R$]