We've seen how to implement logical Clifford gates fault-tolerantly & transversally... but these gates are also easy to simulate classically. Universal quantum computation ⇒ another gate?

Def: Clifford hierarchy: defined recursively as

Given $\mathcal{C}_n^{(1)} := \mathcal{P}_n$ and $\mathcal{C}_n^{(2)} = \mathcal{C}_n$

↑ Pauli group ↑ Clifford group,

$$\mathcal{C}_n^{(k)} := \left\{ U \in U(2^n) : U \mathcal{P}_n U^\dagger \subseteq \mathcal{C}_n^{(k-1)} \text{ up to phase} \right\}$$

↑ not a group if $k > 2$ ⇒ important very soon!!

As we shortly justify, we should look for another gate in $\mathcal{C}_n^{(3)}$:

Example: T-gate: $T \in \mathcal{C}_1^{(3)}$:

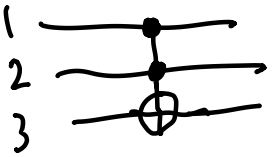
$$T := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8} e^{-i\pi Z/8} \propto \sqrt{S}$$

Since $$TXT^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix} = \begin{pmatrix} 0 & e^{-i\pi/4} \\ e^{i\pi/4} & 0 \end{pmatrix}$$

$$= e^{-i\pi/4} SX \in \mathcal{C}^{(2)}$$

Example: CCNOT-gate: $\text{CCNOT}_{12\to 3} \in \mathcal{C}_3^{(3)}$:

$$\text{CCNOT}_{12\to 3} := I - 2\frac{I-Z_1}{2}\frac{I-Z_2}{2}\frac{I-X_3}{2}$$



T/CCNOT or variants are the most common non-Clifford gates people try to perform fault-tolerantly on a quantum computer

---

Thm: Suppose $G \leq U(2^n)$ is generated [up to phase...] by discrete G_0 if $\mathcal{C}_n \subset G$ [Cliffords are strict subset]

then for any $U \in U(2^n)$, $\exists$ length $\ell(\varepsilon)$ s.t. for any $\varepsilon > 0$.

$$\| U - g_1 \cdots g_\ell \| \leq \varepsilon$$

($g_1 \cdots g_\ell$: each $g_i \in G_0$)

Won't attempt to prove this result but it justifies our earlier claim – access to a fault-tolerant logical T would be enough! This Thm is why it was important $\mathcal{C}_n^{(3)}$ (which is finite) is not a group.

$\Rightarrow$ Cor: $\{H, T, CNOT\}$ is a universal gate set ($T^2 = S$)

Solovay-Kitaev Thm: for $O(1)$ constant $c < 4$ and one qubit

$$\ell(\varepsilon) \lesssim \left(\log \tfrac{1}{\varepsilon}\right)^c$$

Proof sketch: Achieve $\|U - g_1 \cdots g_{\ell_0}\| \lesssim \varepsilon_0^2$ for small but finite ε_0.

if close to I, $e^{i\theta A} \approx I + i\theta A + \cdots$

Suppose: $U_A U_B U_A^{-1} U_B^{-1} = g_C$ (realizable w/ ℓ_0 terms; $g_C \in SU(2)$) w/ $A, B \sim \varepsilon_0$ $\quad C \sim \varepsilon_0^2$

Now approximate $U_A \approx g_A = U_A[I + O(\varepsilon_0^2)]$ (g_A: product of ℓ_0 terms)

Then $g_A g_B g_A^{-1} g_B^{-1} g_C^{-1} \approx I + O(\varepsilon_0^3)$ gives better approx.

$\Rightarrow$ access unitaries at "angle" $\theta \sim \varepsilon_0^{2(3/2)^k}$ w/ $\ell_0 5^k$ gates

$\Rightarrow c \leq \frac{\log 5}{\log 3/2} \approx 4$ ∎

Amazingly, $\exists$ codes w/ a transversal non-Clifford (T) gate:

Prop: 15-qubit quantum Reed-Muller code has a transversal T gate:

I should write this before class

$$H_X = \begin{pmatrix} 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0\\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0\\ 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0\\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix}$$

$$H_Z = \begin{pmatrix} 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0\\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0\\ 1&1&0&0&1&1&0&0&1&1&0&0&1&1&0\\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\ 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\ 1&1&0&0&1&1&0&0&0&0&0&0&0&0&0\\ 1&0&1&0&1&0&1&0&0&0&0&0&0&0&0\\ 1&1&0&0&0&0&0&0&1&1&0&0&0&0&0\\ 1&0&1&0&0&0&0&0&1&0&1&0&0&0&0\\ 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \end{pmatrix}$$

Non-minimial logical generators:

$$G_X = G_Z = (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$$

Proof: All products of X-checks have 8 Paulis, so:

$$T^{\otimes 15}\left[\frac{1}{4}\sum_{v\in \mathrm{im}(H_X^T)} |v\rangle\right] = e^{i\pi/4\cdot(0 \text{ or } 8)}\left[\frac{1}{4}\sum |v\rangle\right] = \frac{1}{4}\sum |v\rangle$$

$|0_L\rangle$

$|1_L\rangle = X^{\otimes 15}|0_L\rangle$ has strings of 7 or 15 1's

so $T^{\otimes 15}|1_L\rangle = e^{i\pi/4(7 \text{ or } 15)}|1_L\rangle = e^{-i\pi/4}|1_L\rangle$

$\Rightarrow \quad T^{\otimes 15} = (T^\dagger)_L$ ∎

But qRM code does NOT have transversal H (it does have $S = T^2$)

Can we fix that?

Eastin-Knill Thm: no quantum code has a universal transversal gate set on partition $R_1 \cup \cdots \cup R_\ell$ if $d > \max |R_j|$

(d: code distance; $\max |R_j|$: largest block size)

Proof sketch:

If transversal gate set, transversal $U_L \sim (e^{i\theta A})_L$ for $\theta \to 0$

[formally, need that closure is a continuous Lie group...]

$\to (I + i\theta A + \cdots)_L$

by taking $\theta \to 0$ arbitrarily small, $\sum_{\text{block } j=1}^{\ell} i(A_L)_j$ is a logical

↳ each Pauli string has weight $< d$

KL $\Rightarrow P_{\mathcal{C}} (A_L)_j P_{\mathcal{C}} \propto P_{\mathcal{C}}$ acts trivially

This is a contradiction; we can only generate non-trivial transversal logicals on discrete orbits... not dense in $U(2^n)$, not universal ∎

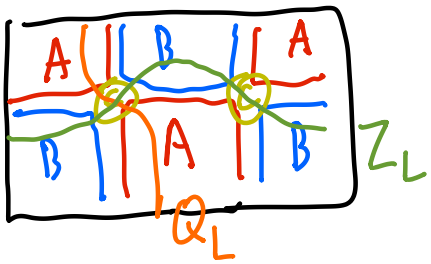
This represents fundamental challenge to FT universal computation!! Most popular way around is magic state distillation; see also HW...

These codes are not qLDPC code families? Manifest FT transversal gates in qLDPC? What about spatial locality?

Bravyi-König Thm: local Pauli stabilizer code in D dimensions only has geometrically local logical gates in $\mathcal{C}^{(D)}$ [D^{th} level of Clifford]

$\Rightarrow$ D=3 minimum for non-Clifford [thankfully we live in D=3...]

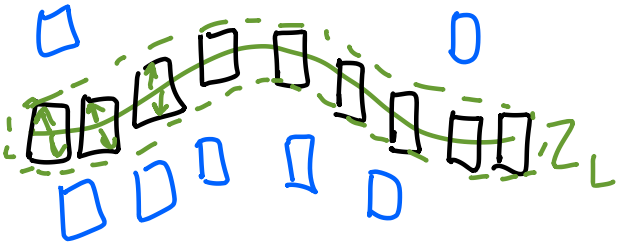
Proof for D=2: Very similar strategy to proving BPT bound.



Clean one X_L logical to A+C
Z_L logical to B+C

Under transversal/spatially local unitary U,
(can also evolve for finite depth circuit...)

operators can't grow too much:

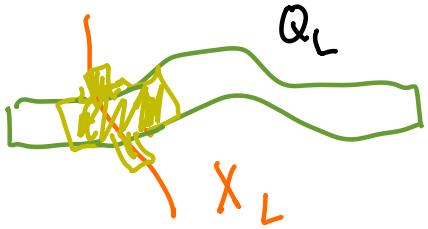


transversal U blocks not overlapping
Z_L just commute through

[baby circuit version of "Lieb-Robinson" Theorem]

Look at commutator:

$$X_L(\underbrace{UZ_LU^\dagger}_{Q_L})X_L^\dagger(U_LZ_L^\dagger U^\dagger)$$

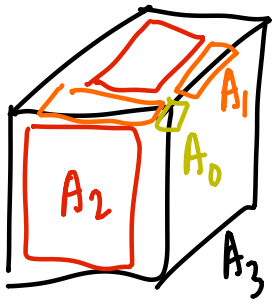


commutator is localized:
only supported near C, O(1) size region

$\Rightarrow P_c[X_LQ_LX_L^\dagger Q_L^\dagger]P_c \propto P_c$ by Knill-Laflamme

so Q_L must be logical Pauli $\Rightarrow$ "$U \in C^{(2)}$" acts as logical Clifford

Extension to D=3 [higher dimensions follow similarly...]



break up into D+1 regions:

clean logical { take to be Pauli: Q_0 away from A_0, Q_1 " " A_1, Q_2 " " A_2 } → evolve to $UQ_0U^\dagger = R_0$

Define $R_1 = Q_1 R_0 Q_1^\dagger R_0^\dagger$

$R_2 = Q_2 R_1 Q_2^\dagger R_1^\dagger \Rightarrow$ has support on A_3

$\Rightarrow$ correctable and acts as identity

So $R_1 \in C^{(1)}$ and $R_0 \in C^{(2)} \Rightarrow U \in C^{(3)}$ ∎

Argument generalizes naturally to higher dimensions.

Since 2D codes are already nice for many expt'l architectures the standard approach is not to implement transversal logical gates, but instead magic state distillation.

The assumption of Pauli stabilizer code was very important...

Thm: ∃ codes (Kitaev quantum double on D_4) w/ transversal CCNOT + locality in 2D

$\Rightarrow$ NOT commuting stabilizer code.

This code is based on discrete lattice gauge theory on dihedral group D_4. A detailed analysis is beyond our scope...