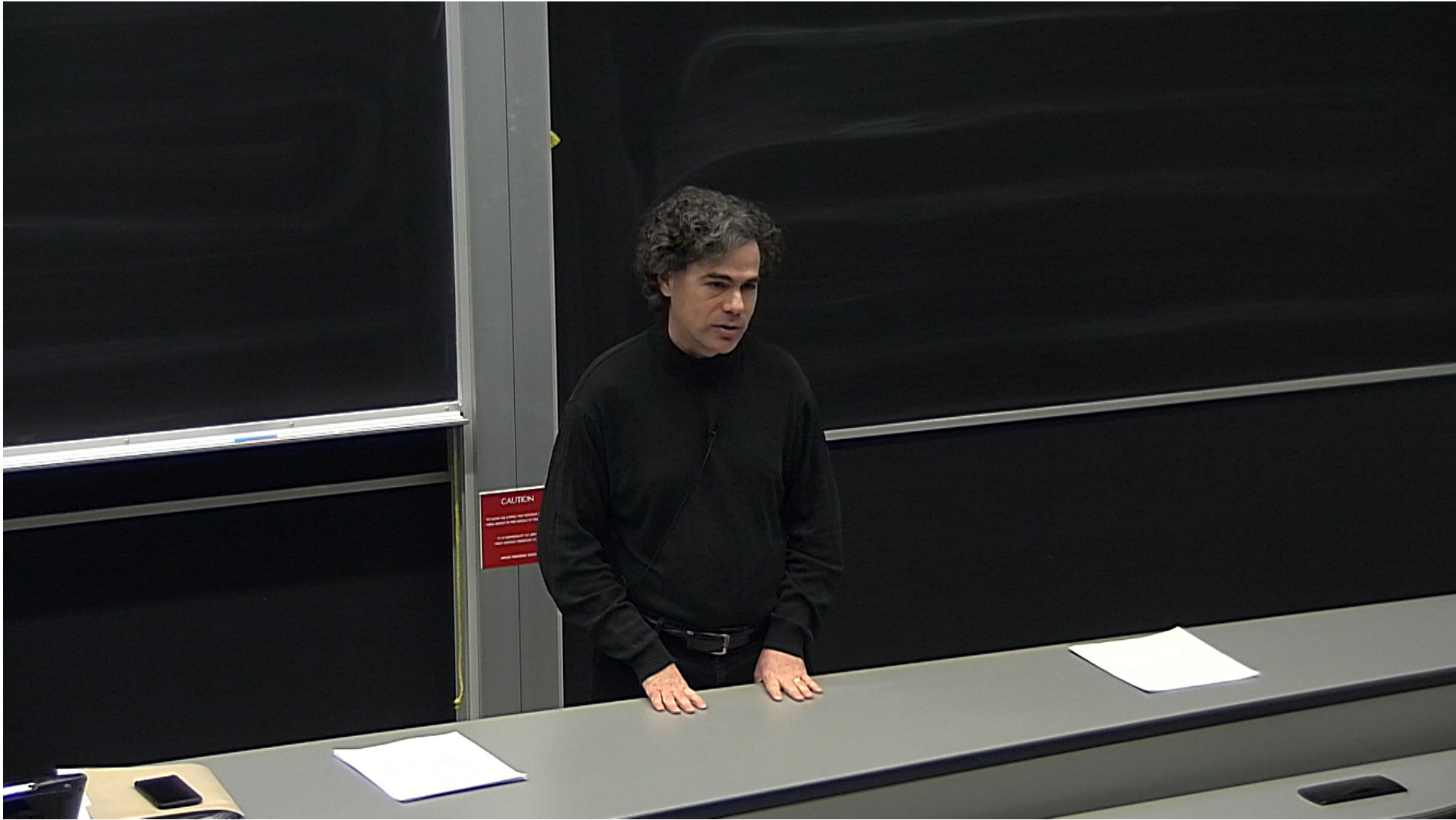


Title: IQC - Quantum Error Correction - Lecture 6

Date: Feb 08, 2018 02:00 PM

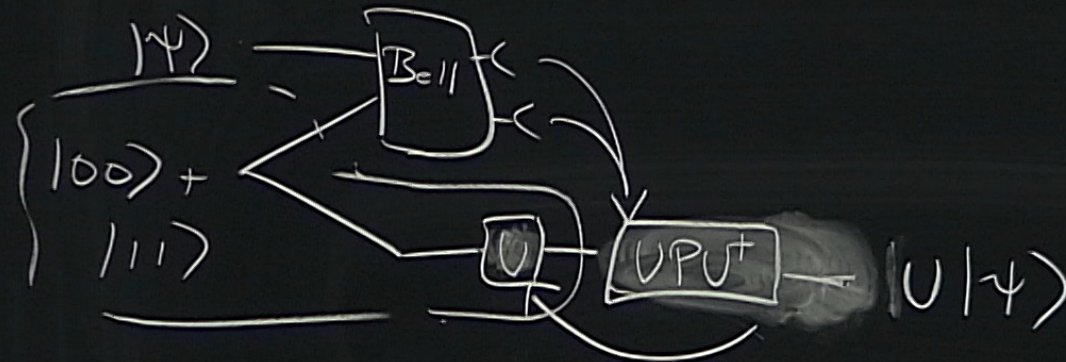
URL: <http://pirsa.org/18020010>

Abstract:



Magic state injection

Th



$$(I \otimes U)(|00\rangle + |11\rangle)$$

$$U \in \mathcal{C}_1 : UPU^\dagger \in \mathcal{P}_1$$

$$\forall P \in \mathcal{P}_1 : UPU^\dagger \in \mathcal{C}_1 \quad (U \in \mathcal{C}_3)$$

injection

Thm.: C_n plus $R_{\pi/8}$ is a universal set of gates

$$U^\dagger \rightarrow |U|4\rangle$$

$|1\rangle$

$\in \mathcal{P}_1$

$$(U \in C_3)$$

$$R_{\pi/8} \in C_3$$

$$R_{\pi/8} X R_{\pi/8}^\dagger = e^{-i\pi/4} R_{\pi/4} X$$

$$R_{\pi/8} Z R_{\pi/8}^\dagger = Z$$

$$Tof \in C_3$$

$$Tof |a, b, c\rangle = |a, b, c+ab\rangle$$

$$(I \otimes U) (|00\rangle + |11\rangle)$$

$$\begin{pmatrix} X & X \\ Z & Z \end{pmatrix}$$

$$\langle X \otimes \underbrace{UXU^\dagger}_{\text{Clifford}}, Z \otimes \underbrace{UZU^\dagger}_{\text{Clifford}} \rangle$$

Can measure using
Shor measurement.

Magic s

Magic state distillation:

15-qubit code - 15-bit Hamming code
& punctured Reed-Muller code (CSS)

Logical $|\bar{0}\rangle$ is superposition of
bit strings of weight 0 mod 8

Logical $|\bar{1}\rangle$ is superposition of bit strings
w/ weight 7 mod 8.

$$R_{\pi/8}^{\otimes 15} |\bar{0}\rangle$$

$$+|111\rangle$$

$$Z \otimes U Z U^\dagger$$

Clifford

reusing
measurement.

Magic state distillation:

15-qubit code - 15-bit Hamming code
& punctured Reed-Muller code (CSS)

Logical $|\bar{0}\rangle$ is superposition of
bit strings of weight 0 mod 8

Logical $|\bar{1}\rangle$ is superposition of bit strings
w/ weight 7 mod 8.

$$R_{\pi/8}^{015} |\bar{0}\rangle$$

$$R_{\pi/8} = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$
$$= e^{-i\pi/8} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$\otimes U^{\dagger} U$
Clifford

Using
element.

Magic state distillation:

15-qubit code - 15-bit Hamming code
 & punctured Reed-Muller code (CSS)

Logical $|\bar{0}\rangle$ is superposition of
 bit strings of weight 0 mod 8

Logical $|\bar{1}\rangle$ is superposition of bit strings
 w/ weight 7 mod 8.

$$\left. \begin{aligned} R_{\pi/8}^{\otimes 15} |\bar{0}\rangle &= |\bar{0}\rangle \\ R_{\pi/8}^{\otimes 15} |\bar{1}\rangle &= e^{-i\pi/4} |\bar{1}\rangle \end{aligned} \right\} R_{\pi/8}^{\dagger}$$

$$R_{\pi/8} = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix} \\ = e^{-i\pi/8} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$\otimes UZU^{\dagger}$
 Clifford

Using
 ent.

Suppose we can do C_n reliably, make $(I \otimes R_{\pi/8})(|00\rangle + |11\rangle)$ unreliably.

→ Do $R_{\pi/8}$ unreliably

→ Create $|00\rangle + |11\rangle$ for 15-qubit code

→ Can create $R_{\pi/8}^{\otimes 15}(|00\rangle + |11\rangle)$ but with $R_{\pi/8}$'s unreliably, with prob p of error

Prob. (2 bad $R_{\pi/8}$ gates) = $O(p^2)$

Prob. (3 bad $R_{\pi/8}$ gates) = $O(p^3)$

Transversal $R_{\pi/8} \Rightarrow \# \text{ errors} = \# \text{ faulty gates}$

→ Correct errors & decode get magic state except w/

$$(I \otimes R_{\pi/8}^{\dagger})(|00\rangle + |11\rangle)$$

logical magic state
for 15-qubit code

Suppose we can do C_n reliably, make $(I \otimes R_{\pi/8})(|00\rangle + |11\rangle)$ unreliably.

→ Do $R_{\pi/8}$ unreliably

→ Create $|00\rangle + |11\rangle$ for 15-qubit code

→ Can create $R_{\pi/8}^{\otimes 15}(|00\rangle + |11\rangle)$ but with $R_{\pi/8}$'s unreliably, with prob. p of error

Prob. (2 bad $R_{\pi/8}$ gates) = $O(p^2)$

Prob. (3 bad $R_{\pi/8}$ gates) = $O(p^3)$

Transversal $R_{\pi/8} \Rightarrow \# \text{ errors} = \# \text{ faulty gates}$

→ Correct errors & decode get magic state except w/ prob. $O(p^2)$

$$(I \otimes R_{\pi/8}^{\dagger})(|00\rangle + |11\rangle)$$

logical magic state
for 15-qubit code

Suppose we can do C_n reliably, make $(I \otimes R_{\pi/8})(|00\rangle + |11\rangle)$ unreliably.

→ Do $R_{\pi/8}$ unreliably

→ Create $|00\rangle + |11\rangle$ for 15-qubit code

→ Can create $R_{\pi/8}^{\otimes 15}(|00\rangle + |11\rangle)$ but with $R_{\pi/8}$'s unreliably, with prob p of error

Prob. (2 bad $R_{\pi/8}$ gates) = $O(p^2)$

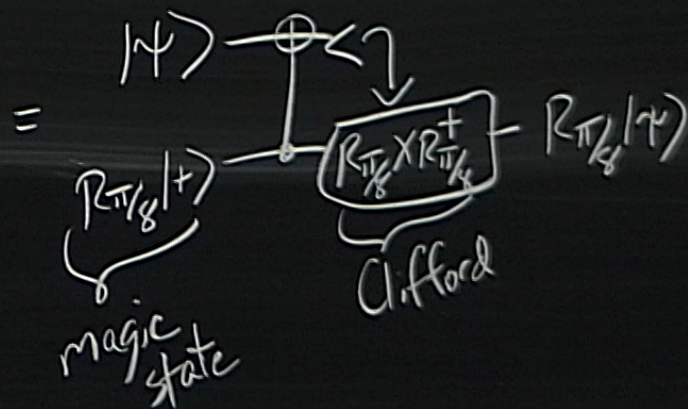
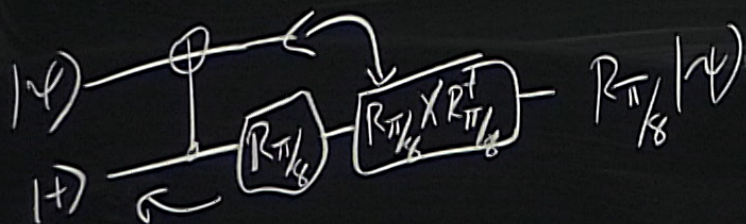
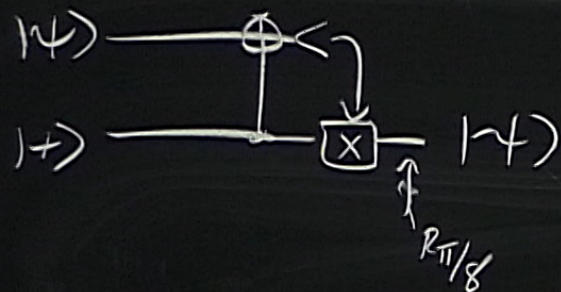
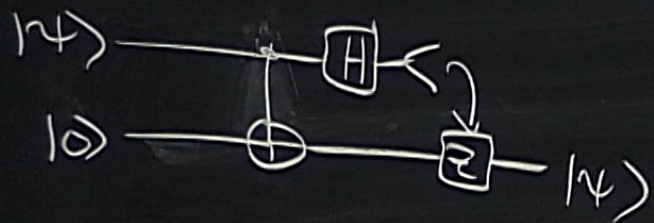
Prob. (3 bad $R_{\pi/8}$ gates) = $O(p^3)$

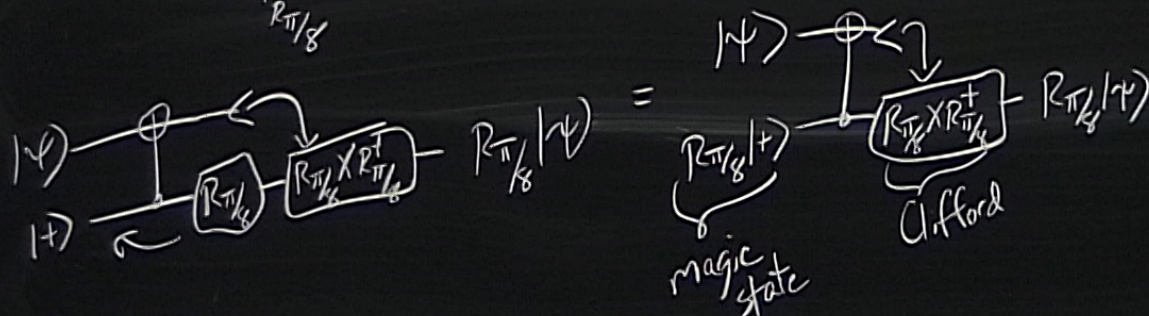
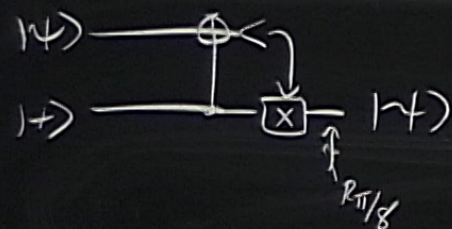
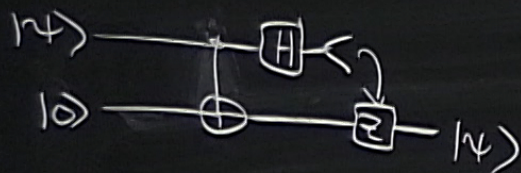
Transversal $R_{\pi/8} \Rightarrow \# \text{ errors} = \# \text{ faulty gates}$

→ Correct errors & decode: get magic state except w/ prob. $O(p^2)$

→ Detect errors & decode: " " " " " $O(p^3)$

$(I \otimes R_{\pi/8}^{\dagger})(|00\rangle + |11\rangle)$
logical magic state
for 15-qubit code





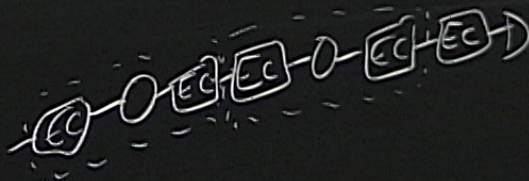
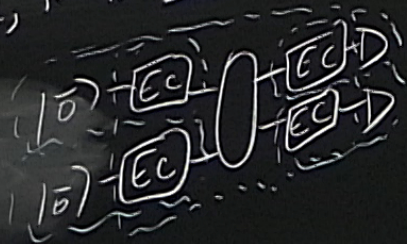
Pauli frame

- keep track of Pauli errors
- update after Clifford group gates
- reset after magic state injection

Def: An exRec (extended rectangle) consists of one of the following:

- A gate or wait gadget plus EC gadgets before & after
- A state preparation gadget plus EC gadget(s) after
- A measurement gadget plus EC gadget(s) before

If the QECC corrects t errors, an exRec is good if it has $\leq t$ faults.
 Otherwise, it is bad.



Def: An exRec for a one-qubit gate gadget is correct if

$$\boxed{\text{EC}} \text{---} \bigcirc \text{---} \boxed{\text{EC}} \text{---} \triangleright = \boxed{\text{EC}} \text{---} \triangleright \text{---} \bigcirc$$

A 2-qubit gate gadget^{exRec} is correct if

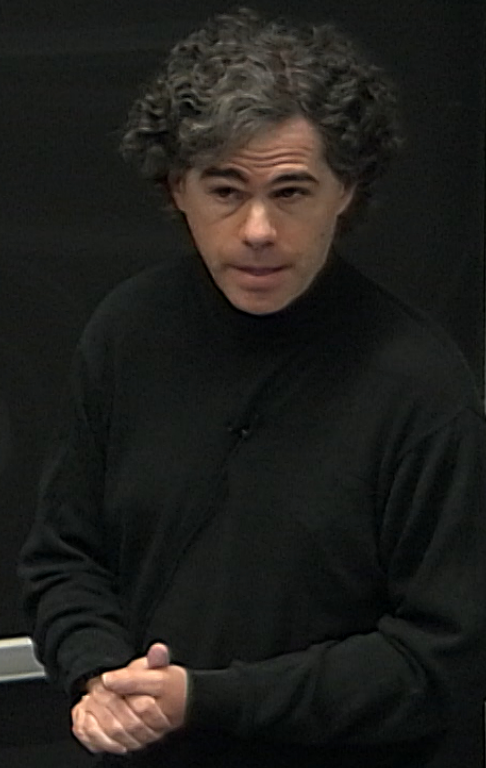
$$\begin{array}{c} \boxed{\text{EC}} \text{---} \triangleright \text{---} \boxed{\text{EC}} \text{---} \triangleright \\ \boxed{\text{EC}} \text{---} \triangleright \text{---} \boxed{\text{EC}} \text{---} \triangleright \end{array} = \boxed{\text{EC}} \text{---} \triangleright \text{---} \boxed{\text{EC}} \text{---} \triangleright$$

A preparation exRec is correct if

$$\bigcirc \text{---} \boxed{\text{EC}} \text{---} \triangleright = \bigcirc$$

A measurement exRec is correct if

$$\boxed{\text{EC}} \text{---} \triangleright \dots = \boxed{\text{EC}} \text{---} \triangleright \text{---} \triangleright \dots$$



Thm: A good exRec is correct.

Proof: $\overset{s_1+s_2+s_3 \leq t}{- \boxed{EC}^{s_1} - \bigcirc^{s_2} - \boxed{EC}^{s_3} \triangleright -} = - \boxed{EC}^{s_1} \parallel^{s_1} - \bigcirc^{s_2} - \boxed{EC}^{s_3} \triangleright -$
 $= - \boxed{EC}^{s_1} \parallel^{s_1} - \bigcirc^{s_2} \parallel^{s_1+s_2} - \boxed{EC}^{s_3} \triangleright - = - \boxed{EC}^{s_1} \parallel^{s_1} - \bigcirc^{s_2} \parallel^{s_1+s_2} \triangleright -$
 $= - \boxed{EC}^{s_1} \parallel^{s_1} - \bigcirc^{s_2} \triangleright - = - \boxed{EC}^{s_1} \parallel^{s_1} \triangleright - \bigcirc - = - \boxed{EC}^{s_1} \triangleright - \bigcirc -$

Thm. A good exRec is correct.

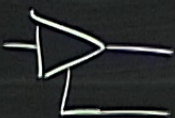
Proof: $s_1 + s_2 + s_3 \leq t$

$$\begin{aligned}
 & \neg \boxed{EC}^{s_1} \circ \boxed{O}^{s_2} \neg \boxed{EC}^{s_3} \triangleright = \neg \boxed{EC}^{s_1} \parallel \boxed{O}^{s_2} \neg \boxed{EC}^{s_3} \triangleright \\
 & = \neg \boxed{EC}^{s_1} \parallel \boxed{O}^{s_2} \parallel \boxed{EC}^{s_3} \triangleright = \neg \boxed{EC}^{s_1} \parallel \boxed{O}^{s_2} \parallel \triangleright \\
 & = \neg \boxed{EC}^{s_1} \parallel \triangleright \circ = \neg \boxed{EC}^{s_1} \triangleright \circ = \neg \boxed{EC}^{s_1} \triangleright \circ
 \end{aligned}$$

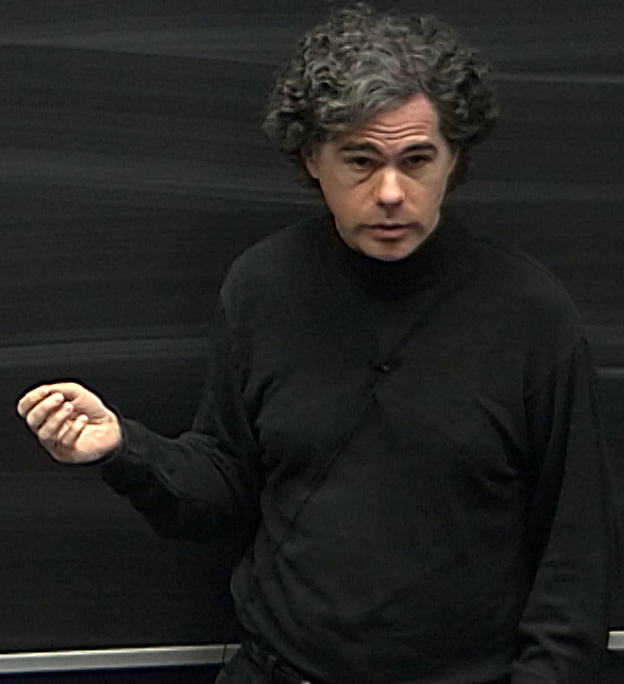
Cor. If all exRecs in a FT circuit are good, the circuit is equivalent to the ideal circuit.

$$(\neg \boxed{EC} \circ \neg \boxed{EC} \circ \neg \boxed{EC}) \triangleright = (\neg \boxed{EC} \circ \neg \boxed{EC}) \triangleright \circ \triangleright = \triangleright \circ \circ \triangleright$$

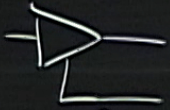
$$- \boxed{\text{EC}} - 0 - \boxed{\text{EC}} - \text{D} - = - \boxed{\text{EC}} - \text{D} - \text{X} -$$

* - decoder: 
 error syndrome

$$- \boxed{\text{EC}} - 0 - \boxed{\text{EC}} - \text{D} - = - \text{D} - \text{X} -$$



$$\boxed{\text{EC}} - \text{O} - \boxed{\text{EC}} - \text{D} = \boxed{\text{EC}} - \text{D} - \text{X}$$

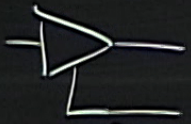
*-decoder: 
error syndrome

$$\boxed{\text{EC}} - \text{O} - \boxed{\text{EC}} - \text{D} = \text{D} - \text{X}$$

Correct for decoder $\Rightarrow$ correct for *-decoder
 Truncated exRecs lack final EC step
 Correct for exRecs $\Rightarrow$ correct for truncated exRecs.

CAUTION

$$\boxed{\text{EC}} - \text{O} - \boxed{\text{EC}} - \text{D} = \boxed{\text{EC}} - \text{D} - \text{X}$$

*-decoder: 

$$\boxed{\text{EC}} - \text{O} - \boxed{\text{EC}} - \text{D} = \text{D} - \text{X}$$

Correct for decoder $\Rightarrow$ correct for *-decoder

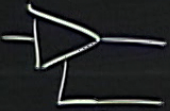
Truncated exRecs lack final EC step

Correct for exRec $\Rightarrow$ correct for truncated exRecs.

Given a fault path (set of faulty locations):

1. Start at end of circuit. Assign measurement exRecs to be good/bad.
2. Truncate any exRec before a bad exRec.
3. Step back one time step & determine if those exRecs are good/bad (including truncation).
4. Repeat 2 & 3 until beginning of circuit.

$$\boxed{\text{EC}} - \text{O} - \boxed{\text{EC}} - \text{D} = \boxed{\text{EC}} - \text{D} - \text{X}$$

*-decoder: 

$$\boxed{\text{EC}} - \text{O} - \boxed{\text{EC}} - \text{D} = \text{D} - \text{X}$$

Correct for decoder $\Rightarrow$ correct for *-decoder

Truncated exRecs lack final EC step

Correct for exRec $\Rightarrow$ correct for truncated exRecs.

Given a fault path (set of faulty locations):

1. Start at end of circuit. Assign measurement exRecs to be good/bad.
2. Truncate any exRec before a bad exRec
3. Step back one time step & determine if those exRecs are good/bad (including truncation)
4. Repeat 2 & 3 until beginning of circuit.

$\Leftarrow$ Circuit is equivalent to unrewired version
w/ good $\rightarrow$ locations w/ faulty, bad $\rightarrow$ faulty locations.

Def: An error model is a local stochastic noise model if w/
probability P_{Φ} we have the fault path Φ , st.

$$\text{Prob.}(S \subseteq \Phi) \leq p^{|S|} \quad \forall S$$

S is a set of locations

$$\text{Prob.}(S \subseteq \Phi) = \sum_{\Phi | S \subseteq \Phi} P_{\Phi}$$

We call p the error probability

The errors can be controlled by a shared persistent environment.

Thm. (level reduction). Suppose we have an FT circuit $\tilde{C}$ simulating unencoded circuit C , $\tilde{C}$ experiences a local stochastic noise model w/ error prob. p . Then $\tilde{C}$ with noise is equivalent to C with a local stochastic noise model with error probability p' ,

$$p' \leq$$

Thm. (level reduction). Suppose we have an FT circuit $\tilde{C}$ simulating unencoded circuit C , $\tilde{C}$ experiences a local stochastic noise model w/ error prob. p . Then $\tilde{C}$ with noise is equivalent to C with a local stochastic noise model with error probability p' ,

$$p' \leq \binom{A}{t+1} p^{t+1}$$

A is # locations in the biggest exec

$$P_{1/2}^{0.5} |1\rangle = e^{-1/2} |1\rangle$$

Thm. (level reduction). Suppose we have an FT circuit $\tilde{C}$ simulating unencoded circuit C , $\tilde{C}$ experiences a local stochastic noise model w/ error prob. p . Then $\tilde{C}$ with noise is equivalent to C with a local stochastic noise model with error probability p' ,

$$p' \leq \binom{A}{t+1} p^{t+1}$$

A is # locations in the biggest exec

Proof: w/ s faulty locations in C , s faulty execs

How many sets of locations in $\tilde{C}$ at most $\binom{A}{t+1}$. Prob of those locations being faulty is $p^{s(t+1)}$

Thm: (Threshold thm): $\exists$ threshold error rate p_T st, in a system subjected to local stochastic noise w/ error prob. $p < p_T$, then $\forall \epsilon > 0$, $\forall$ circuits C w/ T locations, $\exists$ FT encoding $\tilde{C}$ of C st the output probability distribution of $\tilde{C}$ is w/in statistical distance ϵ of that of C , $\tilde{C}$ uses time, gates, # qubits that are greater than C by a $\text{polylog}(T/\epsilon)$ factor.

Proof: Use concatenated FT protocol w/ L levels.

$$P \rightarrow P^{(1)} \leq \left(\frac{A}{t+1}\right)^{t+1} P = P_T \left(\frac{P}{P_T}\right)^{t+1}$$

$$\frac{1}{P_T} = \left(\frac{A}{t+1}\right)^{t+1} \Rightarrow P_T = \left(\frac{1}{\frac{A}{t+1}}\right)^{\frac{1}{t+1}}$$

$$\rightarrow P^{(2)} \leq P_T \left(\frac{P^{(1)}}{P_T}\right)^{t+1} = P_T \left(\frac{P}{P_T}\right)^{(t+1)^2}$$

$$P^{(3)} \leq P_T \left(\frac{P^{(2)}}{P_T}\right)^{t+1} = P_T \left(\frac{P}{P_T}\right)^{(t+1)^3}$$

$$\vdots$$

$$P^{(L)} \leq P_T \left(\frac{P}{P_T}\right)^{(t+1)^L}$$

To get $P^{(L)} \leq \frac{\epsilon}{T}$, choose $L = \left\lceil \frac{\log_2 \frac{\log_2(T P_T / \epsilon)}{\log_2(P_T / \epsilon)}}{\log_2(t+1)} \right\rceil = O(\log \log \frac{T}{\epsilon})$

Proof: Use concatenated FT protocol w/ L levels.

$$P \rightarrow P^{(1)} \leq \binom{A}{t+1} P^{t+1} = P_T \left(\frac{P}{P_T} \right)^{t+1}$$

$$\frac{1}{P_T} = \binom{A}{t+1} \Rightarrow P_T = \left(\frac{1}{\binom{A}{t+1}} \right)^{1/t}$$

$$\rightarrow P^{(2)} \leq P_T \left(\frac{P^{(1)}}{P_T} \right)^{t+1} = P_T \left(\frac{P}{P_T} \right)^{(t+1)^2}$$

$$P^{(3)} \leq P_T \left(\frac{P^{(2)}}{P_T} \right)^{t+1} = P_T \left(\frac{P}{P_T} \right)^{(t+1)^3}$$

$$\vdots$$

$$P^{(L)} \leq P_T \left(\frac{P}{P_T} \right)^{(t+1)^L}$$

Resource overhead $C^L = \text{poly}(\log(T/\epsilon))$.

To get $P^{(L)} \leq \frac{\epsilon}{T}$, choose $L = \left\lceil \frac{\log_2 \frac{\log_2(T P_T / \epsilon)}{\log(P_T / P)}}{\log_2(t+1)} \right\rceil = O(\log \log \frac{T}{\epsilon})$

Thm: (Threshold thm): $\exists$ threshold error rate p_T st., in a system subjected to local stochastic noise w/ error prob. $p < p_T$, then $\forall \epsilon > 0$, $\forall$ circuits C w/ T locations, $\exists$ FT encoding $\tilde{C}$ of C st. the output probability distribution of $\tilde{C}$ is w/in statistical distance ϵ of that of C , $\tilde{C}$ uses time, gates, # qubits that are greater than C by a $\text{polylog}(T/\epsilon)$ factor.

w/ concatenated 7-qubit code, $p_T \geq 2.7 \times 10^{-5}$
best known simulations suggest $p_T \approx 5\%$

Assumptions in threshold theorem:

Gates:

1. Particular set of gates ($H, R_{\pi/8}, CNOT$): not necessary
2. Two-qubit gates between all pairs of qubits: not necessary
3. Produce $|0\rangle$ states on demand: necessary, sort of
4. Measurements during the computation & reliable classical computation: not necessary
5. Maximal parallelism: necessary

Assumptions about errors:

1. Each location has same error rate: not necessary
2. Bounded correlation: necessary
3. No leakage errors: not necessary
4. Adversarial errors: cannot gain advantage
5. Stochastic errors: not necessary, but there are some models of non-Markovian errors for which no proof is known.