# Using Information to measure and manipulate

# Quantum Error Correction

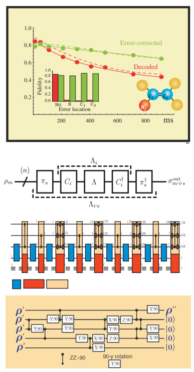

**Raymond Laflamme**

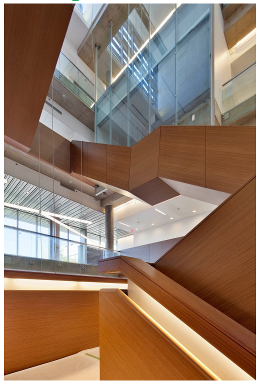
Institute for Quantum Computing

University of Waterloo

laflamme@iqc.ca

www.iqc.ca

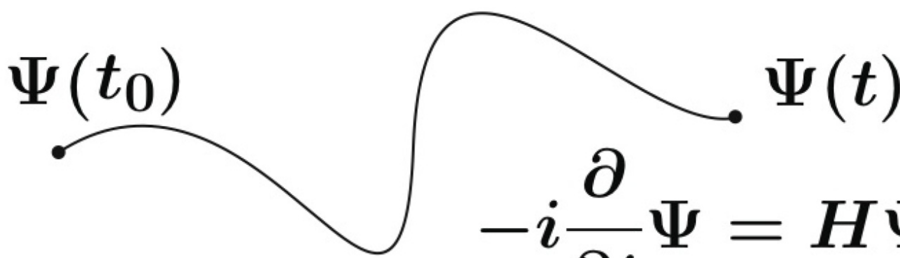





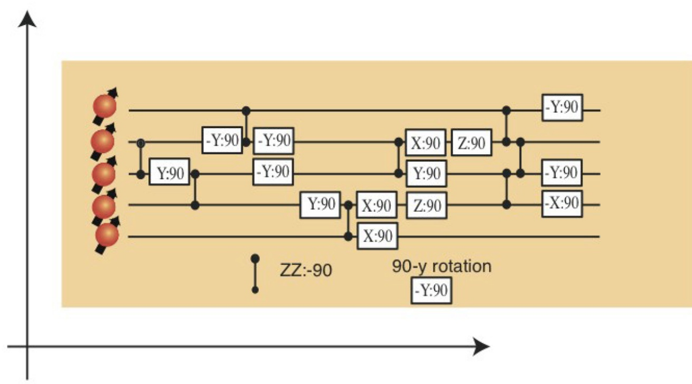
**FQXI, Puerto Rico, 2014**

# Quantum Information Processing

**Goal:**




$$-i\frac{\partial}{\partial t}\Psi = H\Psi$$



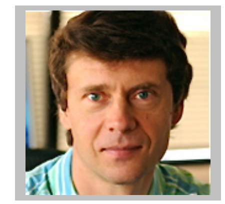

**Probability of success per gate:** $P \approx (1-\epsilon)$

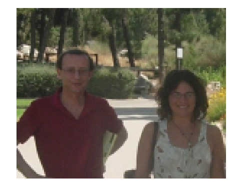
**Probability of success for** $n$ **gates** $P^n \approx (1-\epsilon)^n$

# Threshold theorem

A quantum computation can be as long as required with any desired accuracy using a reasonable amount of resources as long as the noise level is below a threshold value

$P < 10^{-6,-5,-4,-3,-2,\ldots}$





Knill et al.; Science, 279, 342, 1998

Kitaev, Russ. Math Survey 1997

Aharonov & Ben Or,  ACM press

Preskill, PRSL, 454, 257, 1998

...

## Significance:

-imperfections and imprecisions are not fundamental objections to quantum computation

-it gives criteria for scalability

-its requirements are a guide for experimentalists

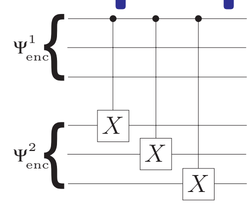
-it is a benchmark to compare different technologies

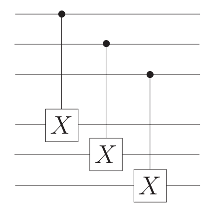
# Assumptions for Accuracy Threshold Theorem

- **Parallel operations**
- **Ability to extract entropy**
- **Knowledge of the noise**
  - **No lost of qubits**
  - **Independent or quasi independent errors**
  - **Depolarising model**
  - **Memory and gate errors**
  - **. . .**

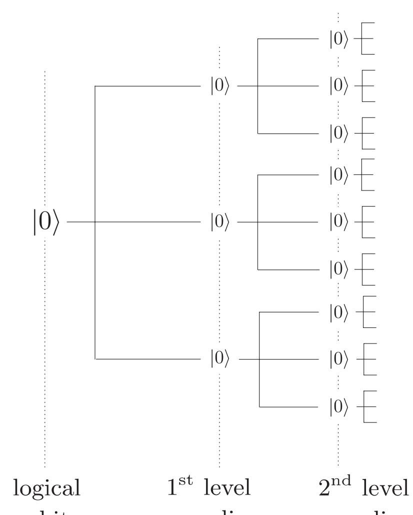
# Ingredients

- **Quantum Error Correcting Codes:**
  **a triplet that includes a noise model $\mathcal{E}$, a subspace $\mathcal{C}$ and a recovery operator $\mathcal{R}$. The latter exist if**
  $$\langle i_j | E_\alpha^\dagger E_\beta | i_k \rangle = \delta_{jk} c_{\alpha\beta}$$
- **Fault tolerant procedure:**
  **a way to forbid bad propagation**



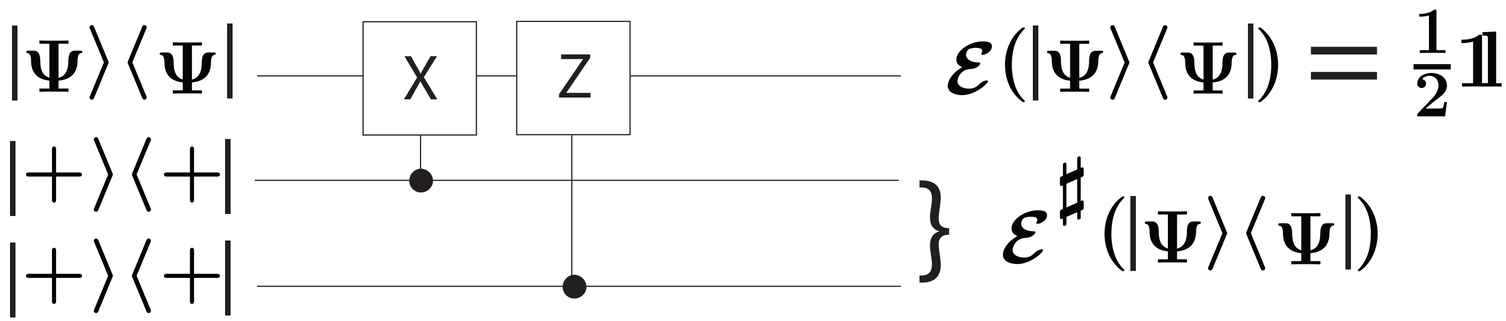

- **Concatenation**



# Quantum private channel

**Find a quantum operation $\mathcal{E}$ such that $\forall|\Psi\rangle \in \mathcal{C}$**

$$\sum_\alpha E_\alpha^\dagger |\Psi\rangle\langle\Psi| E_\alpha = \rho_0$$




**Can we have a private channel with $\mathcal{E}$ made only of $Z$ operators?**

PRL **111,** 030502 (2013) PHYSICAL REVIEW LETTERS week ending 19 JULY 2013

**Private Quantum Subsystems**

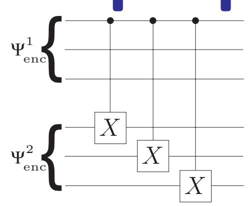
Tomas Jochym-O'Connor,[1,2] David W. Kribs,[1,3] Raymond Laflamme,[1,2,4] and Sarah Plosker[3]
[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[2]*Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[3]*Department of Mathematics and Statistics, University of Guelph, Guelph, Ontario N1G 2W1, Canada*
[4]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada*
(Received 10 August 2012; revised manuscript received 23 January 2013; published 15 July 2013)

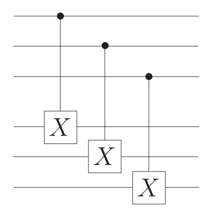
# Ingredients

- **Quantum Error Correcting Codes:**
  **a triplet that includes a noise model $\mathcal{E}$, a subspace $\mathcal{C}$ and a recovery operator $\mathcal{R}$. The latter exist if**

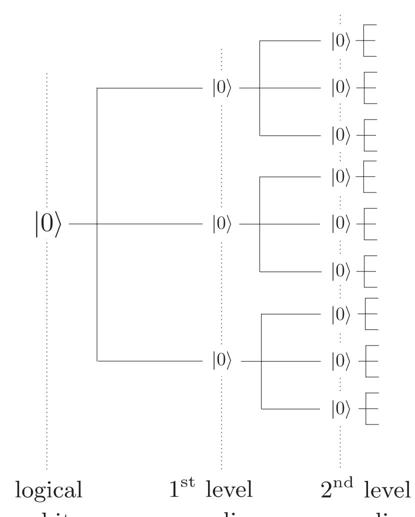
$$\langle i_j | E_\alpha^\dagger E_\beta | i_k \rangle = \delta_{jk} c_{\alpha\beta}$$

- **Fault tolerant procedure:**
  **a way to forbid bad propagation**



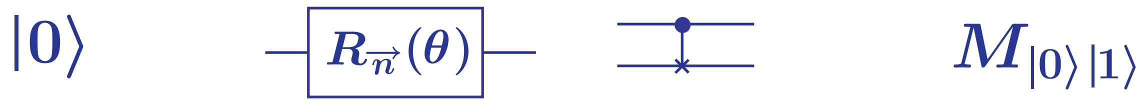




- **Concatenation**

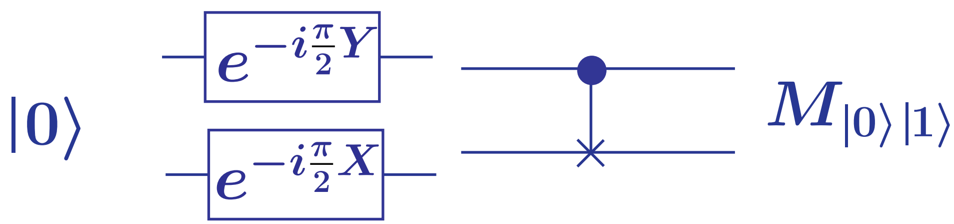


# Fault tolerant gates

**Usually we think of the circcuit model: Prepare a state, compute, measure**




**Other possibility is to use only generators of the Clifford group (generated by Hadamard, Phase gate and CNOT), with state preparation and measuremen in the computational basis:**



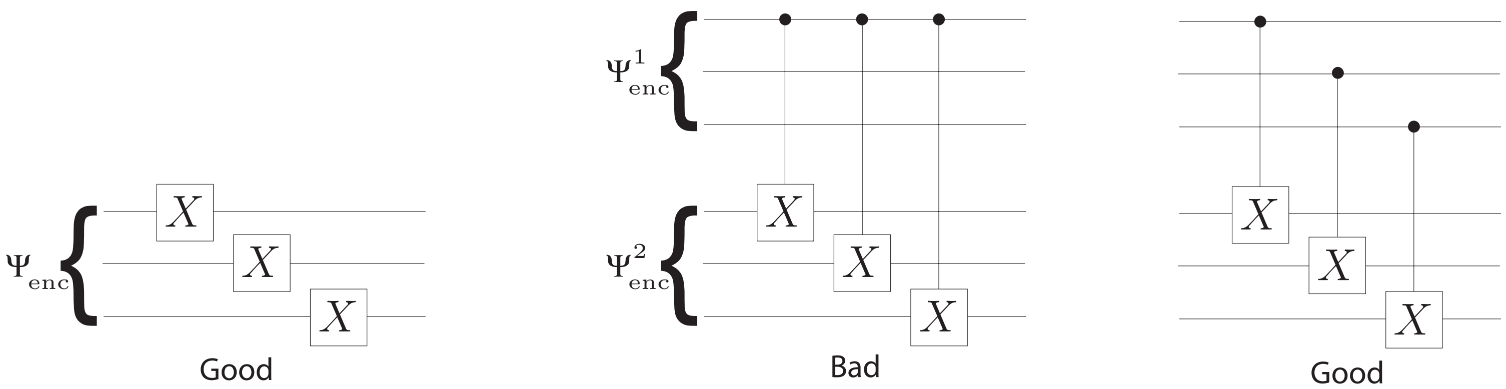

**and include the preparation of the magic state**

$$\rho = \frac{1}{2}\mathbb{1} + \frac{1}{\sqrt{3}}(X + Y + Z)$$

# Transversal gates

**A transversal gate (for a 1 error QEC) is on that does not propagate more than one error per code block**

**E.g. 3 bit code $\mathcal{C} = \{|000\rangle, |111\rangle\}$, encoded NOT and CNOT gates:**




**Transversal have good error propagation properties.**

**Theorem**

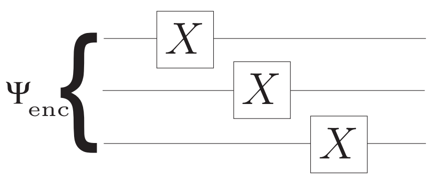
**There exists no quantum error correcting code that exhibits a set of universal transversal gates.**

**B. Eastin, and E. Knill, Phys. Rev. Lett. 102, 110502 (2009)**

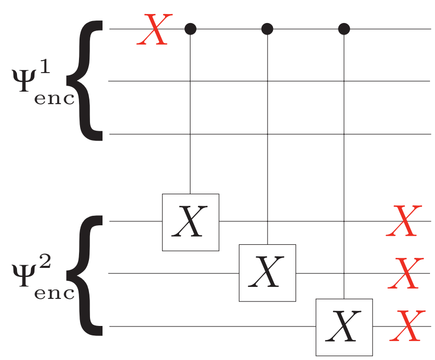
# Transversal gates

**A transversal gate (for a 1 error QEC) is on that does not propagate more than one error per code block**

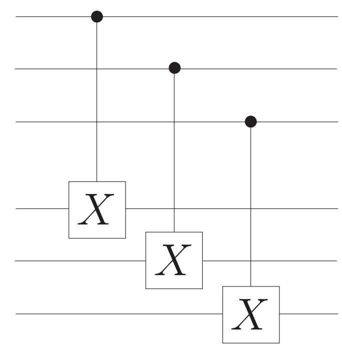
**E.g. 3 bit code $\mathcal{C} = \{|000\rangle, |111\rangle\}$, encoded NOT and CNOT gates:**




Good




Bad




Good

**Transversal have good error propagation properties.**

**Theorem**

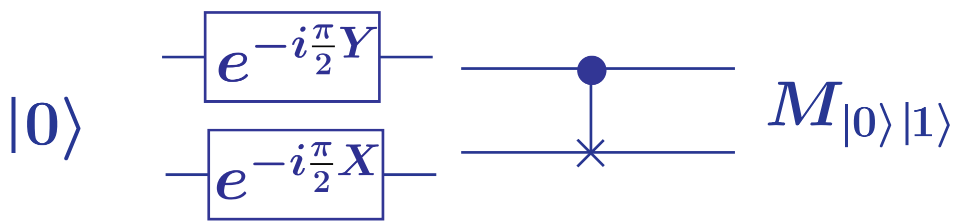
**There exists no quantum error correcting code that exhibits a set of universal transversal gates.**

B. Eastin, and E. Knill, Phys. Rev. Lett. 102, 110502 (2009)

# Fault tolerant gates

**Usually we think of the circcuit model: Prepare a state, compute, measure**


**Other possibility is to use only generators of the Clifford group (generated by Hadamard, Phase gate and CNOT), with state preparation and measuremen in the computational basis:**




**and include the preparation of the magic state**

$$\rho = \frac{1}{2}\mathbb{1} + \frac{1}{\sqrt{3}}(X + Y + Z)$$

# Good propagation without Transversal gates?

**Answer yes! Concatenate two codes**

**•$\mathcal{C}_1$= [[7,1,3]], 7-qubit code**
**This code has transversal gates** $\{H, S, CNOT\}$

**remember** $S = \begin{pmatrix} e^{i\pi/4} & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}$

**•$\mathcal{C}_2$= [15,1,3]], 15-qubit Reed-Muller code**
**This code has transversal gates** $\{T, CNOT\}$

**remember** $T = \begin{pmatrix} e^{i\pi/8} & 0 \\ 0 & e^{-i\pi/8} \end{pmatrix}$

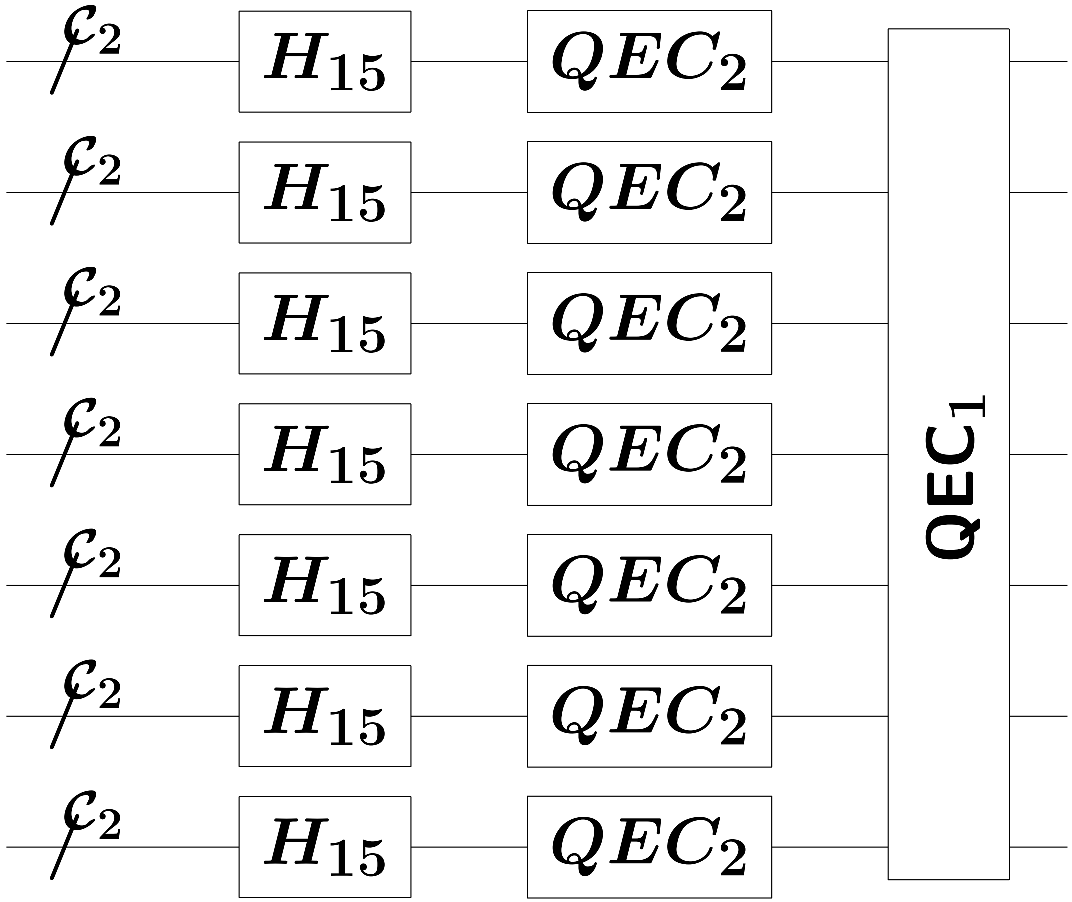
**And the set** $\{H, S, T, CNOT\}$ **is universal**

# Good propagation without Transversal gates?

**Both codes being CSS quantum codes allows for the following:**

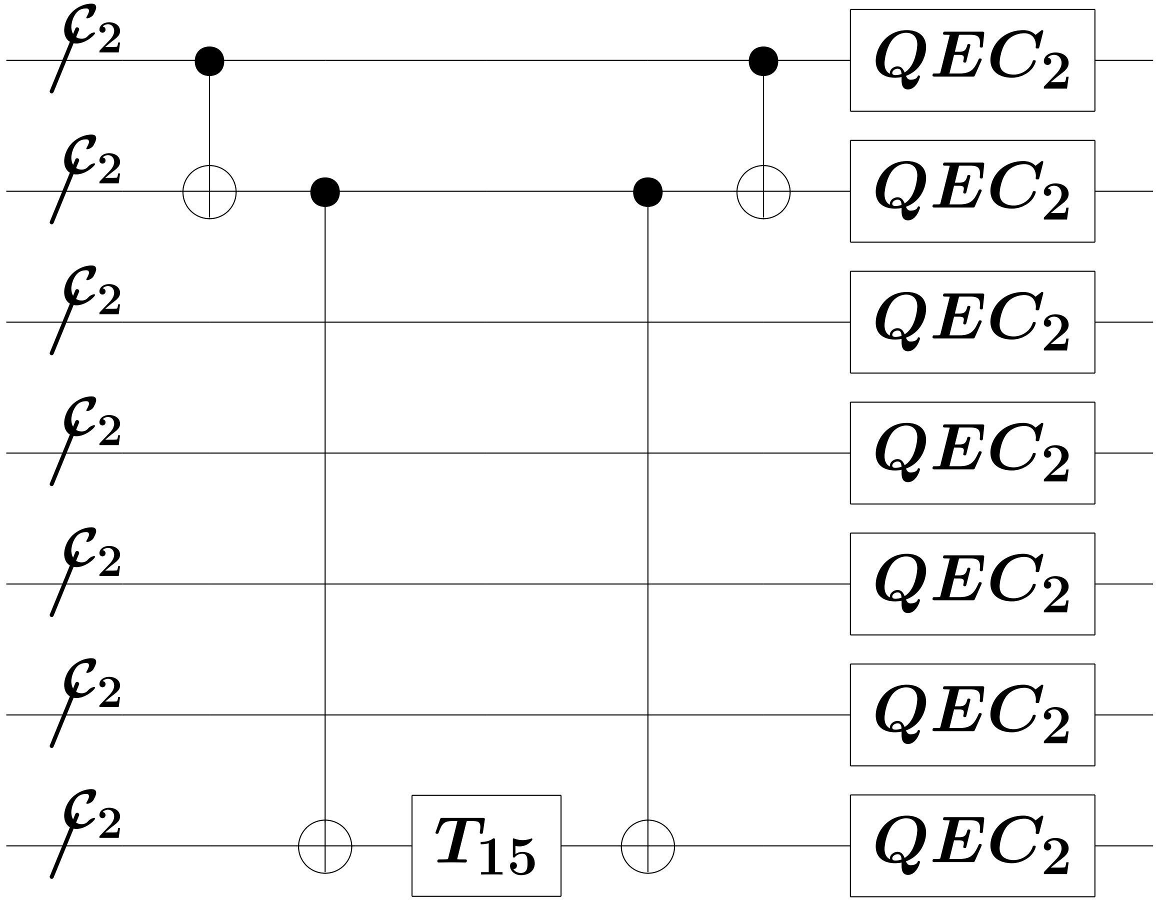
- **Globally transversal CNOT gates**
- **Globally transversal Pauli gates**
- **Transversal syndrome measurements of the logical X and Z stabilizers**
- **Transversal application of error correction post-processing**

# Encoded Hadamard gate




**Non-transversal $H_{15}$ gates can propagate errors, however transversality in $\mathcal{C}_1$ allows for such propagation**

# Encoded T gate




**All logical gates in $\mathcal{C}_2$ are transversal. Any single qubit error will propagate to a correctable error in the concatenated quantum code.**

**T. Jochym-O'Connor, R. Laflamme; arXiv:1309.3310 to appear in PRL**

# Conclusion

- **Quantum error correction**
  - **allows to make quantum information robust**
  - **allows new modalities/implementations e.g. LOQC**
  - **what about adiabatic quantum computing?**
  - **needs experimental implementation...**
- **Ideas can be used to hide information (private quantum subsystems)**
- **New construction that use encoded gates with good propagation**
  - **What is the fault-tolerance threshold for such a scheme?**
  - **Does there exist examples with fewer numbers of qubits?**
  - **Finding examples of concatenated codes protecting against multiple errors fault-tolerantly**