Quantum error correction tutorial

Monday, August 18, 2014 4:30 PM

Quantum Error Correction Tutorial

Ben Reichardt

Overview of fault-tolerant quantum computation

Why is building a quantum computer hard?

NOISE!

Shor's factoring algorithm

factor a K-bit number using

$72K^3$ gates, (vs. $e^{K^{1/3}}$ classically)

on $5K$ qubits

$K=1024$: 10^{11} gates on 5000 qubits

$\Rightarrow$ need error $<10^{-11}$ per gate

(from environmental noise & control errors)

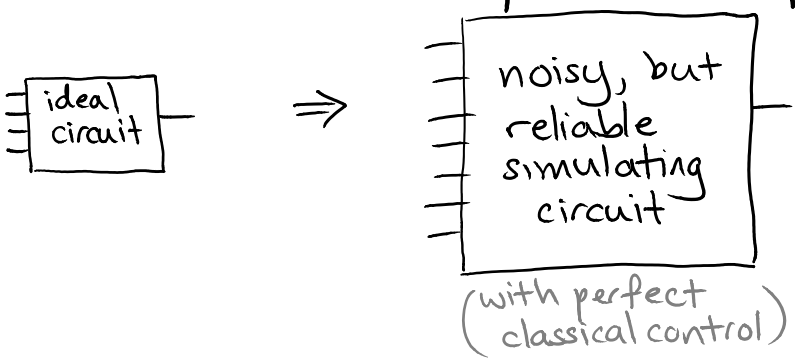
Realistic noise rates: 1% per gate? (maybe 10^{-3} or 10^{-4})

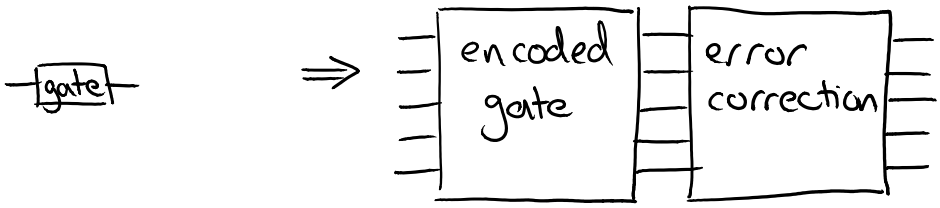
Table 1 | Current performance of various qubits

Type of qubit	T_2	Benchmarking (%)	
		One qubit	Two qubits
Infrared photon	0.1 ms	0.016	1
Trapped ion	15 s	0.48†	0.7*
Trapped neutral atom	3 s	5	
Liquid molecule nuclear spins	2 s	0.01†	0.47†
e^- spin in GaAs quantum dot	3 μs	5	
e^- spins bound to ^{31}P:^{28}Si	0.6 s	5	
^{29}Si nuclear spins in ^{28}Si	25 s	5	
NV centre in diamond	2 ms	2	5
Superconducting circuit	4 μs	0.7†	10*

[Ladd et al., Nature 2010]

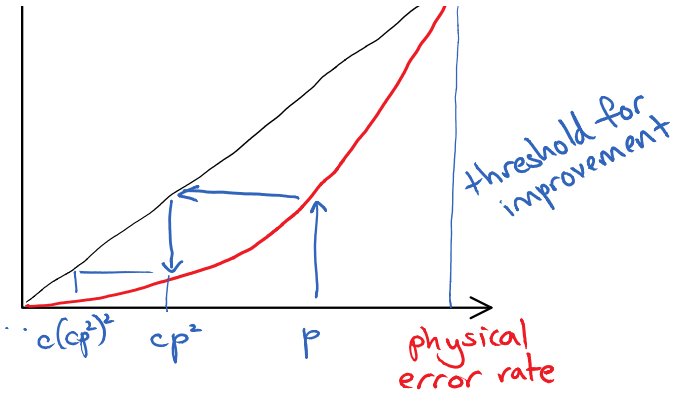
Solution: Fault-tolerant quantum computation





Intuition: Noise threshold

distance-3 code → quadratic reduction in error rate



Concatenate the scheme for arbitrary reliability

"Threshold theorems": For various noise models,

- Tolerable noise rate is a constant > 0 — How high?
- Size overhead is polylogarithmic or constant [Gottesman '13] — How low?

Ingredients:

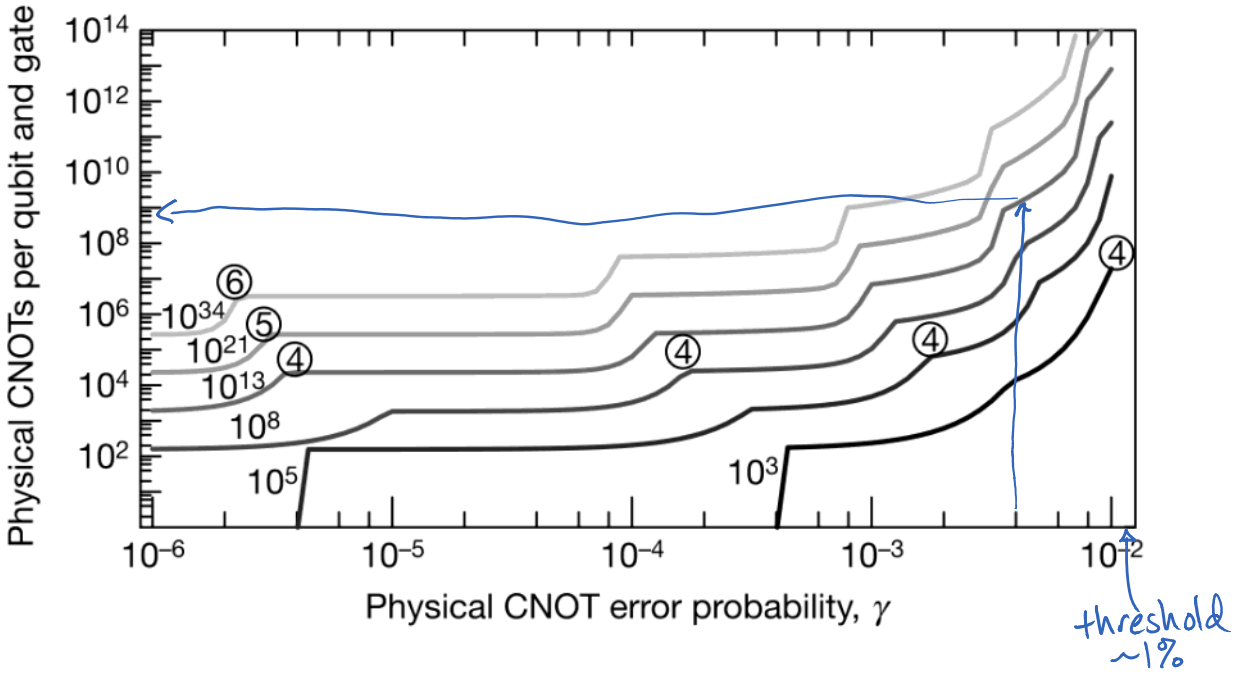
Noise model
- stochastic?
- Hamiltonian coupling to environment?

Quantum error-correcting code

Fault-tolerance scheme

Remark: If you know your noise model well, then you should try to deal with it at the hardware level; techiques for correcting general noise are more expensive.

Example: Knill's postselection-based scheme [Nature '05]



Remark: • Realistically, you'll probably not want to have more than one or two levels of concatenation

• The best scheme depends on the noise rate.

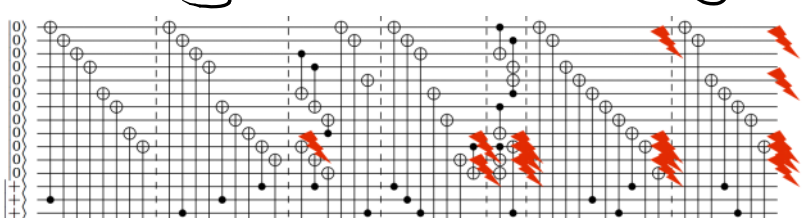
$\Rightarrow$ start with simple, high-threshold code & switch to more efficient, but lower-threshold code once the effective noise rate is low enough

Open problems:

- Develop fault-tolerance schemes that maximize tolerable noise rate with minimal overhead
  - especially schemes based on the surface code or large, efficient QECCs

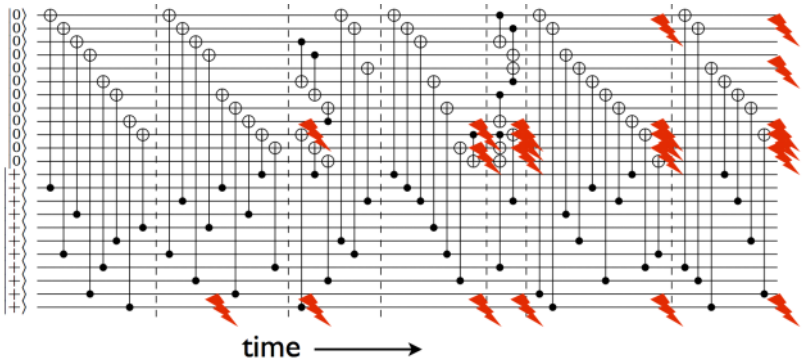
Examples:

- Encoding step bottleneck: how to get data into the code



Control error cascade!

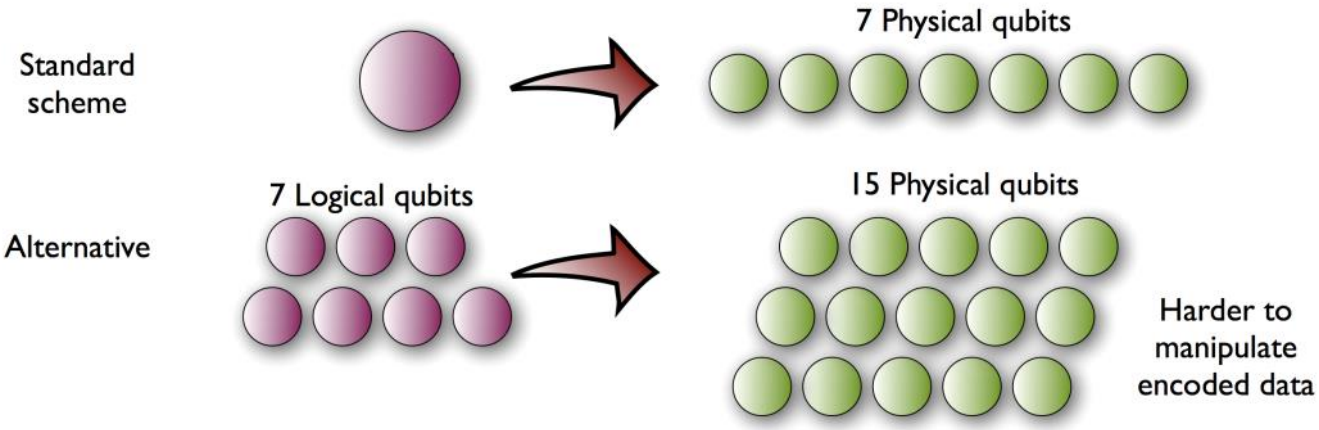
[Paetznick, Reichardt '11]



Control error cascade!

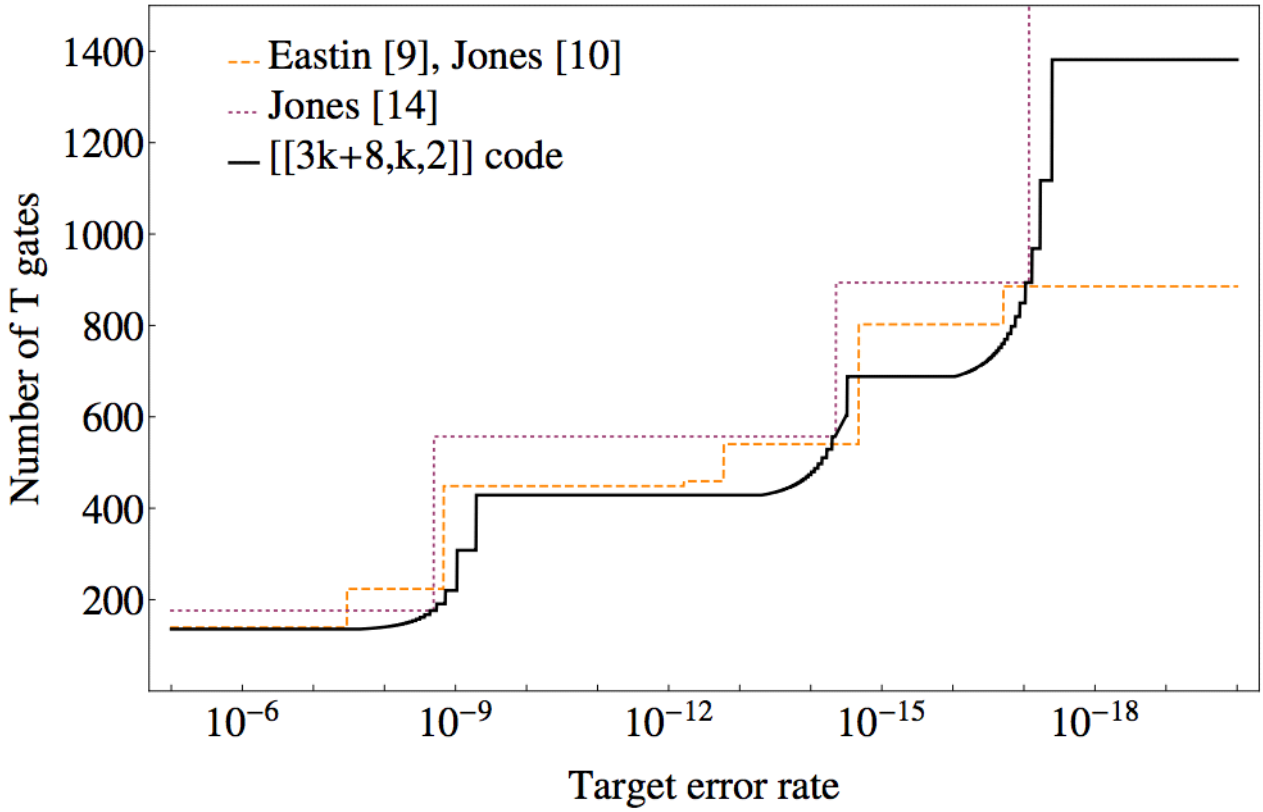
[Paetznick, Reichardt '11]

- Computing with more efficient codes



[Harrington, Reichardt '12]

- More efficient, fault-tolerant, universal computation



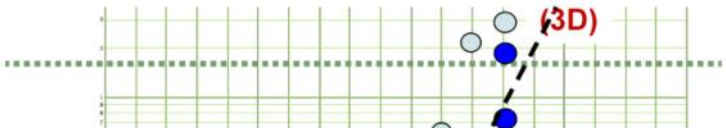
Universal FT computation w/ transversal gates & error correction
[Paetznick, Reichardt '13]

Open:

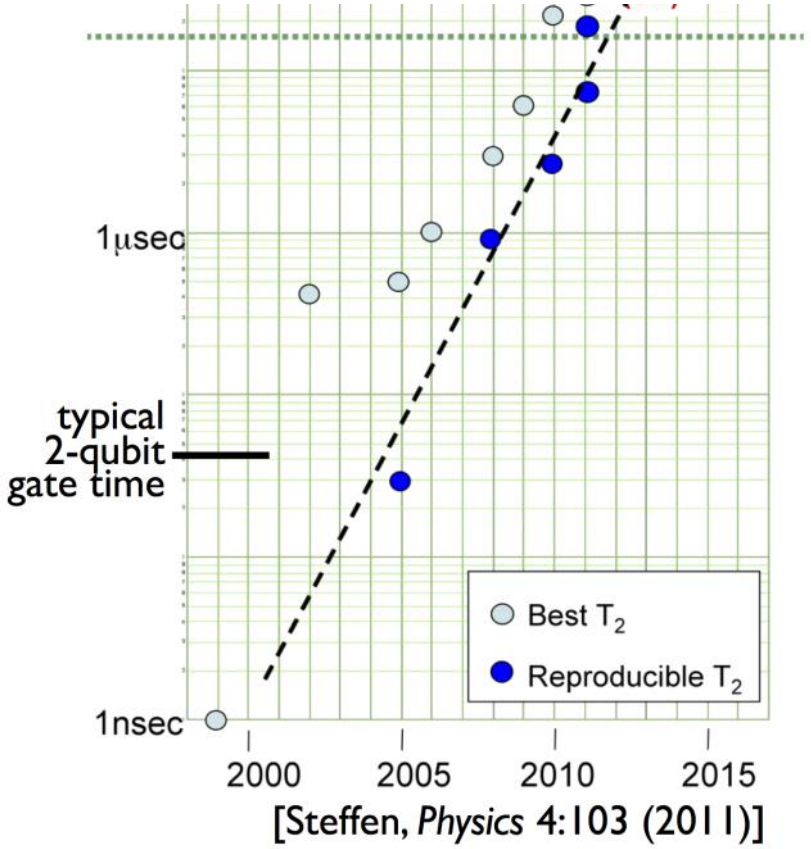
- Can we construct inherently fault-tolerant systems?
  - "self-correcting" quantum codes
  - anyonic systems

Solutions needed!

★ 95 μs [Rigetti et al., 2012]



"This technology [is] a strong candidate for the immediate construction of



strong candidate for the immediate construction of prototype quantum processors with 10-100 qubits."

Course Outline:

1. Quantum codes & stabilizer algebra
2. Fault-tolerance & threshold theorems
3. Surface code

Quantum codes and stabilizer algebra

Monday, August 18, 2014 4:30 PM

Quantum Codes and Stabilizer Algebra

Ben Reichardt

Quantum Codes

$|0\rangle \longmapsto$ |encoded 0⟩

$|1\rangle \longmapsto$ |encoded 1⟩

s.t. looking at only a few qubits of

α |encoded 0⟩ + β |encoded 1⟩

tells you nothing about α, β

"distance d" means nothing is revealed by any subset of $\frac{d-1}{2}$ qubits

Errors are digital

It seems like there are many different kinds of errors that can affect a quantum state.

In fact, infinitely many, since errors can be continuous.

But look closer...

Pauli operators

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad = iXZ$$

Observe:

- These form a basis, over $\mathbb{C}$, for all 2×2 complex matrices
- Their k-fold tensor products form a

basis for all $2^k \times 2^k$ complex matrices

e.g. $k=2$ $\quad I\otimes I$, $I\otimes X$, $I\otimes Y$, $I\otimes Z$

$\vdots$

$Z\otimes I$, ..., $Z\otimes Z$

Corollary: Any error (any operation) on k qubits can be expanded as a linear combination of these Paulis.

$\Rightarrow$ H is enough to protect against X, Y, Z errors.

Why?

Formally $\quad |\psi\rangle$ = codeword

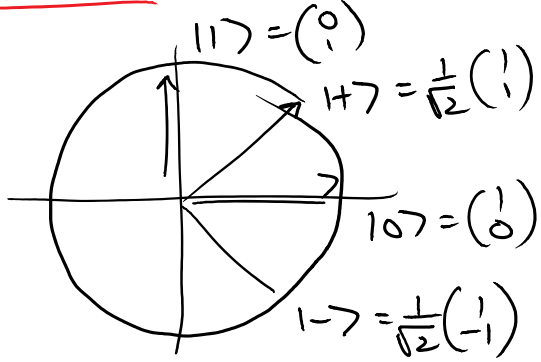
R = recovery procedure

$$R(X_j|\psi\rangle) = |\psi\rangle|\phi_{xj}\rangle$$
$$R(Y_j|\psi\rangle) = |\psi\rangle|\phi_{yj}\rangle$$
$$R(Z_j|\psi\rangle) = |\psi\rangle|\phi_{zj}\rangle$$
$$R(|\psi\rangle) = |\psi\rangle|\phi\rangle$$

if $E_j = \alpha I + \beta X + \gamma Y + \delta Z$

$\Rightarrow R(E_j|\psi\rangle) = |\psi\rangle\otimes(\alpha|\phi\rangle + \beta|\phi_{xj}\rangle + \cdots + \delta|\phi_{zj}\rangle)$

Dual bases



$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The simplest quantum code

$|0\rangle \mapsto |0000\rangle$

$|1\rangle \mapsto |1111\rangle$

$|+\rangle \mapsto |++++\rangle$

$|-\rangle \mapsto |----\rangle$

distance 3 against X errors

$\left(|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \mapsto |++++\rangle + |----\rangle\right.$

$\left.\sqrt{2}|1\rangle = |+\rangle - |-\rangle \mapsto |++++\rangle - |----\rangle\right)$

$|{-}\rangle \mapsto |{---}\rangle$ $\left(\sqrt{2}\,|{-}\rangle = |{+}\rangle - |{-}\rangle \mapsto |{+++}\rangle - |{---}\rangle\right)$

Combine the codes — concatenate one on the other — to protect against both kinds of errors.

Parity checks and logical operators

$Z : |0\rangle \mapsto |0\rangle,\ |1\rangle \mapsto -|1\rangle$

$X : |{+}\rangle \mapsto |{+}\rangle,\ |{-}\rangle \mapsto -|{-}\rangle$

$Z \otimes Z$ measures parity of two qubits

+1	−1
00	10
11	01

Repetition code is "stabilized by" $Z\otimes Z\otimes I$, $I\otimes Z\otimes Z$

$(Z\otimes Z\otimes I)(\alpha|000\rangle + \beta|111\rangle) = \alpha|000\rangle + \beta|111\rangle$

Logical operators $X\otimes X\otimes X : |000\rangle \longleftrightarrow |111\rangle$

$Z\otimes I\otimes I : |{+++}\rangle \longleftrightarrow |{---}\rangle$

Similarly, X measures parity in the $|{+}\rangle/|{-}\rangle$ basis

⇒ Stabilizers/parity checks of 9-qubit code:

```
ZZI
IZZ
      ZZI
      IZZ
            ZZI
            IZZ
XXXXXX      III
IIIXXX      XXX
```

(and everything in the abelian group they generate)

STABILIZER ALGEBRA (Gottesman-Knill theorem)

Pauli operators $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $Y=iXZ$

Pauli operators $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $Y=iXZ$

Stabilizer state = +1 eigenvalue eigenvector of a set of Pauli operator tensor products

Examples:

State	Stabilizers
$\|0\rangle$	Z
$\|+\rangle=\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	X
$\|1\rangle\otimes\|+\rangle$	$\{-Z\otimes I, I\otimes X, -Z\otimes X, I\otimes I\}$
$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$	$\{II, XX, ZZ, -YY\}$
$\frac{1}{\sqrt{2}}(\|01\rangle-\|10\rangle)$	$-XX$, $-ZZ$
?	$XX1$, $ZZ1$, $11X$

An n-qubit stabilizer state has
n independent, pairwise-commuting stabilizers.
(They generate a 2^n element abelian group.)

Commutation relationships:

$XZ = -ZX$ anticommute

$\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$

$XZZX1$, ?
$1XZZX$ commute — even # of different Paulis

$ZZZZZ$, ? anticommute

ZZZZZ, ? anticommute
XXXXX 5 = odd # of different Paulis

Manipulating stabilizer states

State	Stabilizers
$\|\psi\rangle$	$P, Q, \ldots$
$\downarrow$	
$U\|\psi\rangle$	$UPU^\dagger, UQU^\dagger, \ldots$

since $(UPU^\dagger)U|\psi\rangle = UP|\psi\rangle = U|\psi\rangle$ ✓

Def.: A unitary is **Clifford** if it conjugates Pauli operators to Pauli operators.

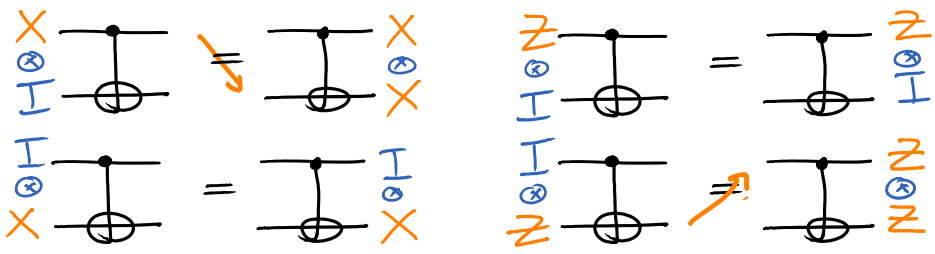
Examples:

- Hadamard $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

  $H|0\rangle = |+\rangle$, $H|+\rangle = |0\rangle$

  $HZH = X$ $HXH = Z$

- CNOT

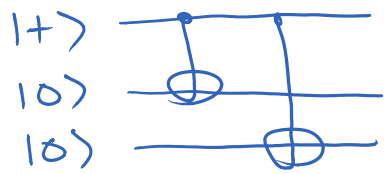


Example: To prepare $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$

Initial stabilizers $\xrightarrow{CNOT_{1,2}}$ $\xrightarrow{CNOT_{1,3}}$ Final stabilizers

XII XXI XXX

Initial stabilizers	$\xrightarrow{CNOT_{1,2}}$	$\xrightarrow{CNOT_{1,3}}$ Final stabilizers
$X\,1\,1$	$X\,X\,1$	$X\,X\,X$
$1\,Z\,1$	$Z\,Z\,1$	$Z\,Z\,1$
$1\,1\,Z$	$1\,1\,Z$	$Z\,1\,Z \sim 1\,Z\,Z$



Stabilizer codes

n qubits, $m \leq n$ independent stabilizers

$\Rightarrow$ $n-m$ encoded qubits (degrees of freedom)

Example:

$n = 3$, $m = 2$

$1\,Z\,Z$

$1\,X\,X$

$\Rightarrow$ one encoded qubit

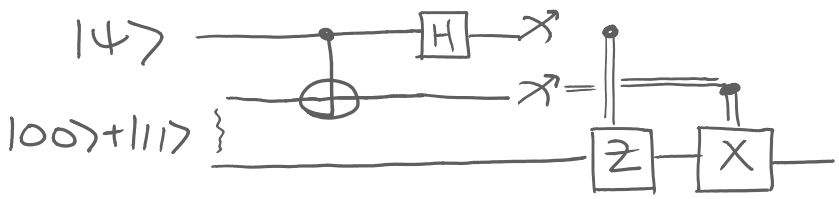
$|+\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

logical X: $X\,1\,1$

logical Z: $Z\,1\,1$

↖ commute with stabilizers, ↙ anticommute with each other

Exercise: Derive quantum teleportation using the stabilizer formalism.



EXAMPLES OF STABILIZER CODES

Examples of Stabilizer Codes

- Shor code $[\![9, 1, 3]\!]$

  n = # physical qubits, k = # logical qubits, d = distance

- $[\![5, 1, 3]\!]$ code

X	Z	Z	X	I
I	X	Z	Z	X
X	I	X	Z	Z
Z	X	I	X	Z
X	X	X	X	X
Z	Z	Z	Z	Z

  – smallest qubit code w/ $d \geq 3$

  – not CSS

- $[\![4,2,2]\!]$ error-detecting code

X	X	X	X
Z	Z	Z	Z
X	X	I	I
I	Z	I	Z
X	I	X	I
I	I	Z	Z

Exercises:

- Generalize to $[\![n, n-2, 2]\!]$ for n even
- Give a $[\![3, 1, 2]\!]_3$ code on qutrits

Hint: Use $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & & \\ & e^{2\pi i/3} & \\ & & e^{-2\pi i/3} \end{pmatrix}$

- Steane code $[\![7, 1, 3]\!]$

  -self-dual CSS code

I	I	I	X	X	X	X
I	X	X	I	I	X	X
X	I	X	I	X	I	X
I	I	I	Z	Z	Z	Z
I	Z	Z	I	I	Z	Z
Z	I	Z	I	Z	I	Z
X	X	X	X	X	X	X
Z	Z	Z	Z	Z	Z	Z

Exercises:

- Give a circuit that prepares $|0\rangle$ encoded

- Give a circuit that prepares $|0\rangle$ encoded in this code.
- Generalize to the family of Hadamard codes

$$[\![2^s-1,\ 2^s-1-2s,\ 3]\!]$$

$s=3$: $[\![7,1,3]\!]$
$s=4$: $[\![15,7,3]\!]$
$s=5$: $[\![31,21,3]\!]$
⋮

- Many other codes

Concatenated, eg. $[\![7,1,3]\!]$ on itself $\rightarrow [\![49,1,9]\!]$

Golay $[\![23,1,7]\!]$ $\rightarrow [\![21,3,5]\!]$

BCH $[\![31,11,5]\!]$
$[\![63,27,7]\!]$
$[\![127,29,15]\!]$

QR $[\![47,1,11]\!]$
$[\![79,1,15]\!]$
$[\![103,1,19]\!]$

RM $[\![7,1,3]\!]$, $[\![31,1,7]\!]$, $[\![127,1,15]\!]$

See [Steane, http://arxiv.org/abs/quant-ph/0207119]

and [Grassl, http://codetables.de/]

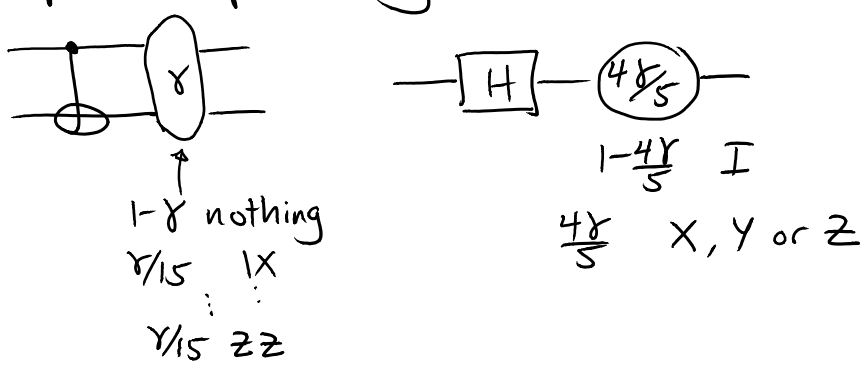
n/k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	1	1																													
2	2	1	1																												
3	2	1	1	1																											
4	2	2	2	1	1																										
5	3	3	2	1	1	1																									
6	4	3	2	2	2	1	1																								
7	3	3	2	2	2	1	1	1																							
8	4	3	3	3	2	2	2	1	1																						
9	4	3	3	3	2	2	2	1	1	1																					
10	4	4	4	3	3	2	2	2	2	1	1																				
11	5	5	4	3	3	3	2	2	2	1	1	1																			
12	6	5	4	4	4	3	3	2	2	2	2	1	1																		
13	5	5	4	4	4	3	3	3	2	2	2	1	1	1																	
14	6	5	5	4-5	4	4	4	3	3	2	2	2	2	1	1																
15	6	5	5	5	4	4	4	3	3	3	2	2	2	1	1	1															
16	6	6	6	5	5	4-5	4	4	3	3	3	2	2	2	2	1	1														
17	7	7	6	5-6	5	4-5	4-5	4	4	4	3	3	2	2	2	1	1	1													
18	8	7	6	5-6	5-6	5	5	4	4	4	3	3	2	2	2	2	2	1	1												
19	7	7	6	5-6	5-6	5-6	5	4-5	4	4	3-4	3	3	2	2	2	2	1	1	1											
20	8	7	6-7	6-7	6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	2	1	1										
21	8	7	6-7	6-7	6-7	6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	3	2	2	2	1	1	1									
22	8	7-8	6-8	6-7	6-7	6-7	5-6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	2	1	1								
23	8-9	7-9	7-8	6-8	6-7	6-7	5-7	5-6	5-6	4-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	1	1	1							
24	8-10	8-9	7-8	7-8	6-8	6-7	6-7	5-7	5-6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	2	1	1						
25	8-9	9	7-8	7-8	7-8	7-8	6-7	5-7	5-7	5-6	5-6	4-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	1	1	1					
26	8-10	9	8-9	8-9	8	7-8	6-8	6-8	6-7	5-7	5-6	5-6	5-6	4-5	4-5	4	4	3-4	3	3	2	2	2	2	2	1	1				
27	9-10	9	9	9	8-9	7-8	6-8	6-8	6-8	6-7	5-7	5-6	5-6	5	4-5	4-5	4	4	3-4	3	3	2	2	2	2	1	1	1			
28	10	10	10	9	8-9	7-9	6-8	6-8	6-8	6-8	6-7	6-7	6	5-6	5-6	4-5	4	4	4	3-4	3	3	2	2	2	2	2	1	1		
29	11	11	10	9-10	8-9	7-9	7-9	6-8	6-8	6-8	6-7	6-7	6	5-6	5-6	4-5	4-5	4	4	4	3-4	3	3	2	2	2	2	1	1	1	
30	12	11	10	9-10	8-10	8-9	7-9	7-9	7-8	6-8	6-8	6-7	6-7	5-6	5-6	5-6	5	4-5	4	4	4	3-4	3	3	2	2	2	2	2	1	1
n/k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

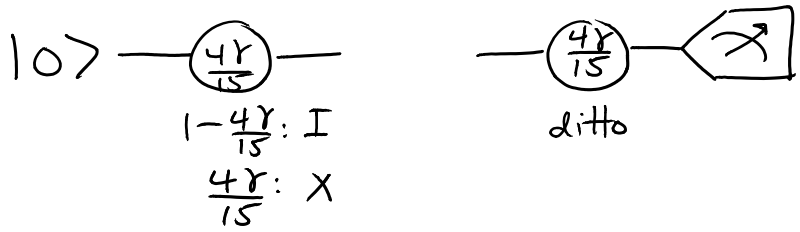
Simulating fault-tolerance schemes

Syndrome extraction and error correction for a stabilizer code only needs Clifford gates.

⇒ Can be efficiently simulated classically for stochastic Pauli noise models

Example: Depolarizing noise model

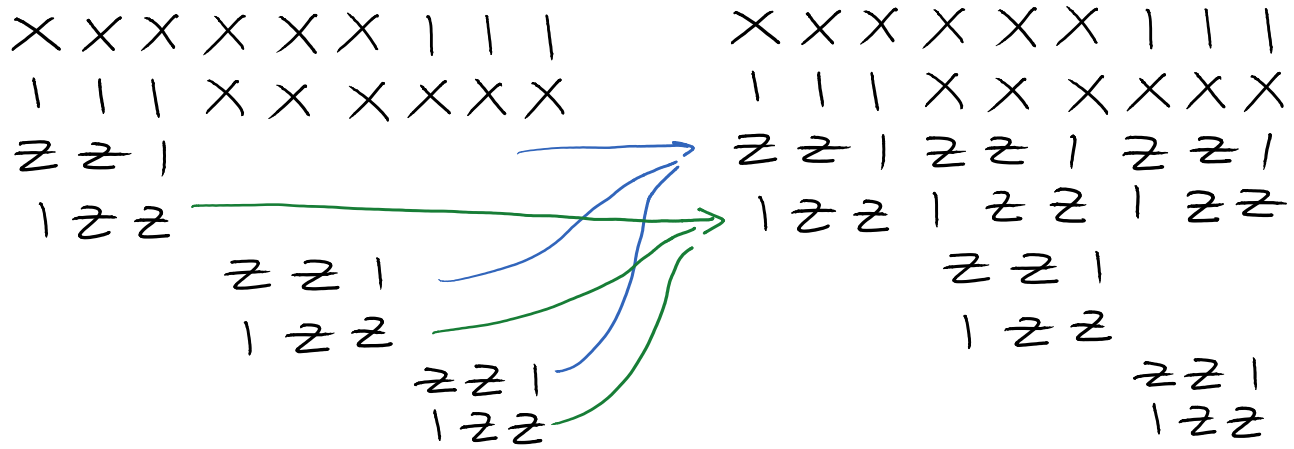


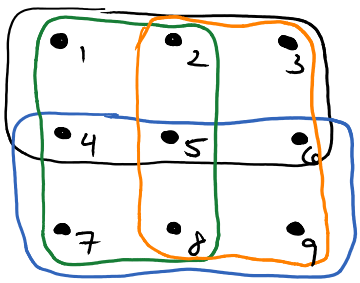


We cannot simulate a universal set of quantum gates, nor Hamiltonian noise models.

THE BACON-SHOR "SUBSYSTEM" CODE

The 9-qubit Shor code is asymmetrical between X and Z. Let's fix this...





Now they are symmetrical, except with 4 extra Z stabilizers. Why do we need them? Get rid of them!

stabilizers

X X X X X X | | |
| | | X X X X X X
Z Z | Z Z | Z Z |
| Z Z | Z Z | Z Z

	Operators
	$Z\,Z\,I\ \ Z\,Z\,I\ \ Z\,Z\,I$
	$I\,Z\,Z\ \ I\,Z\,Z\ \ I\,Z\,Z$
logical operators for encoded qubit 1	$X\,X\,X\ \ X\,X\,X\ \ X\,X\,X$
	$Z\,Z\,Z\ \ Z\,Z\,Z\ \ Z\,Z\,Z$
2	$Z\,Z\,I\ \ I\,I\,I\ \ I\,I\,I$
	$X\,I\,I\ \ X\,I\,I\ \ I\,I\,I$
3	$I\,Z\,Z\ \ I\,I\,I\ \ I\,I\,I$
	$I\,I\,X\ \ I\,I\,X\ \ I\,I\,I$
4	$I\,I\,I\ \ I\,I\,I\ \ Z\,Z\,I$
	$I\,I\,I\ \ X\,I\,I\ \ X\,I\,I$
5	$I\,I\,I\ \ I\,I\,I\ \ I\,Z\,Z$
	$I\,I\,I\ \ I\,I\,X\ \ I\,I\,X$

Observe: The code distance is $d=2$,

but the first qubit is protected to distance 3!

(That is, any operator acting nontrivially on encoded qubit 1 has weight ≥ 3.)

Proof: The two X stabilizers allow for determining which block a Z error occurred on, but not where in the block. If you guess wrong, that just causes a logical error on encoded qubits 2 to 5. ✓ □

Why is this useful?

- Fewer stabilizers ⇒ extracting syndromes is easier.
- Easier to prepare encoded states

eg.,

$$\text{Shor-encoded } |0\rangle = \frac{1}{2}\Big(|0^3 0^3 0^3\rangle + |1^3 1^3 0^3\rangle + |1^3 0^3 1^3\rangle + |0^3 1^3 1^3\rangle\Big)$$

Bacon-Shor encoded $|0\rangle$: many choices, depending on qubits 2 to 5, but

$(\quad\quad)^{\otimes 3}$

on qubits 2 to 5, but

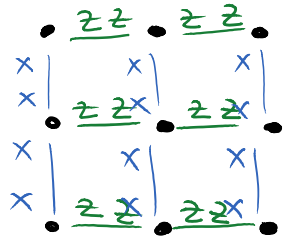
encoded $|0{+}{+}{+}{+}\rangle = \left(\left|{+}{+}{+}\right\rangle + \left|{-}{-}{-}\right\rangle\right)^{\otimes 3}$

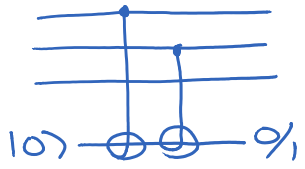
Z X I
Z X X
Z I X

- simpler, easier to prepare fault-tolerantly

- Easier to apply encoded Hadamard H
  - apply $H^{\otimes 9}$, then "transpose" the qubits
- Much easier to extract error syndromes

Measure





one-qubit ancilla is enough
—errors can't spread

Remark: Why isn't noise such a problem for CLASSICAL computation?
"SELF-CORRECTING CODES"

Classical magnets: $\mathcal{H} = \sum_{\text{edges}(i,j)} Z_i \otimes Z_j$

$Z_i \otimes Z_j$: −1 if spins agree (00 or 11)
+1 if they disagree (01 or 10)

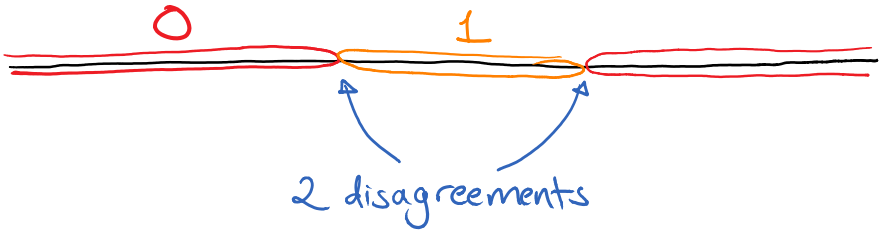
ID: 0 0 0 0 0 0 0 0 0 0 0 0

or

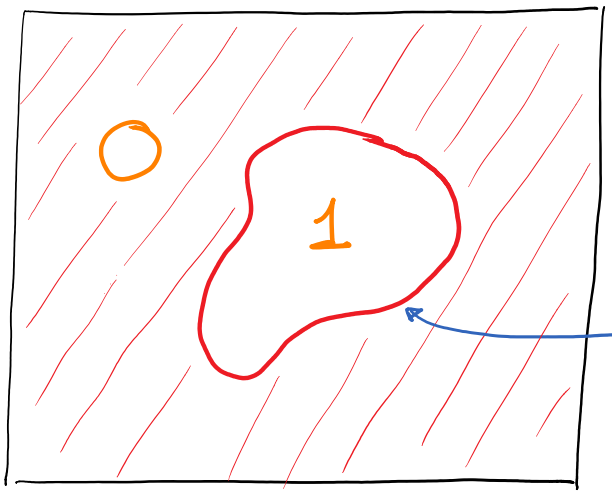
ground states

or

ground states
repetition code codewords

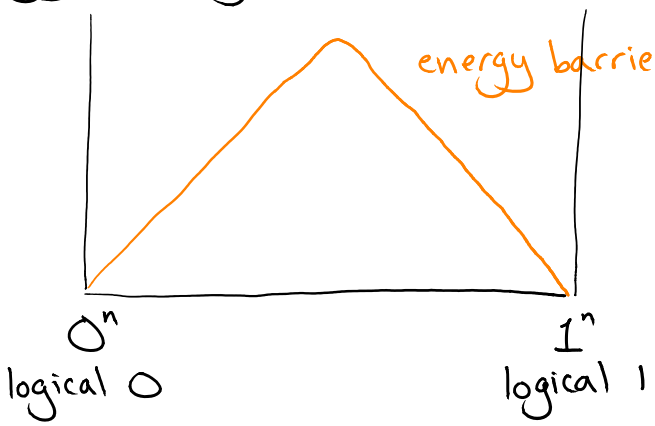


2D:

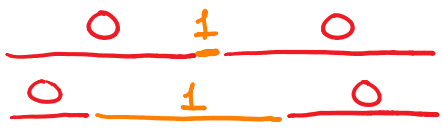


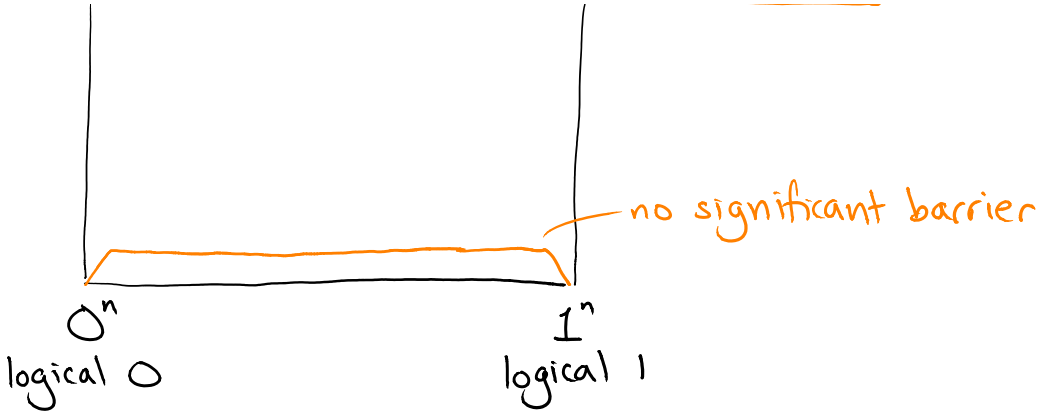
$\Rightarrow$ In 2D or higher, energy cost grows with # of errors

Energy penalty means errors will tend to shrink away.



But not in 1D:





Self-correcting quantum codes?

4D ✓ generalization of surface code

3D lattice ✓? - probably: see Bravyi & Haah

http://arxiv.org/abs/1105.4159

http://arxiv.org/abs/1112.3252

- the "compass model" (Bacon-Shor with Y⊗Y in the 3rd direction) is conjectured to self-correct

2D lattice ? maybe, but probably not

Bravyi & Terhal http://arxiv.org/abs/0810.1983

Kay & Colbeck http://arxiv.org/abs/0810.3557

- impossible for standard stabilizer codes, possible for a subsystem code (like Bacon-Shor)