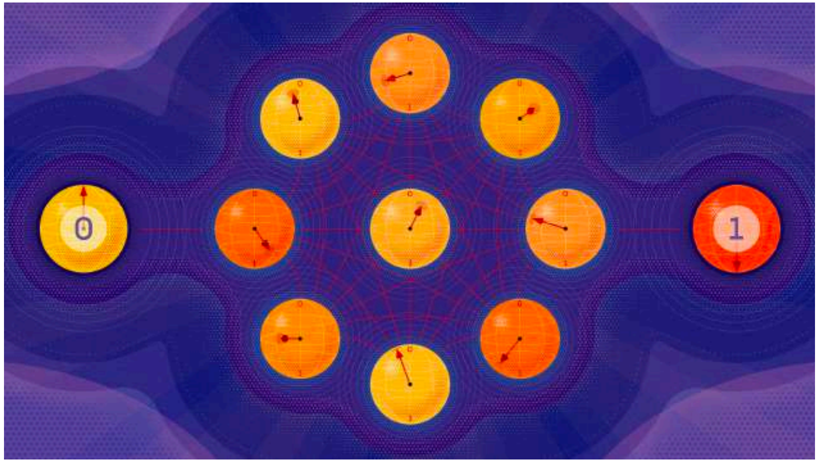
Basics of Quantum Error Correction

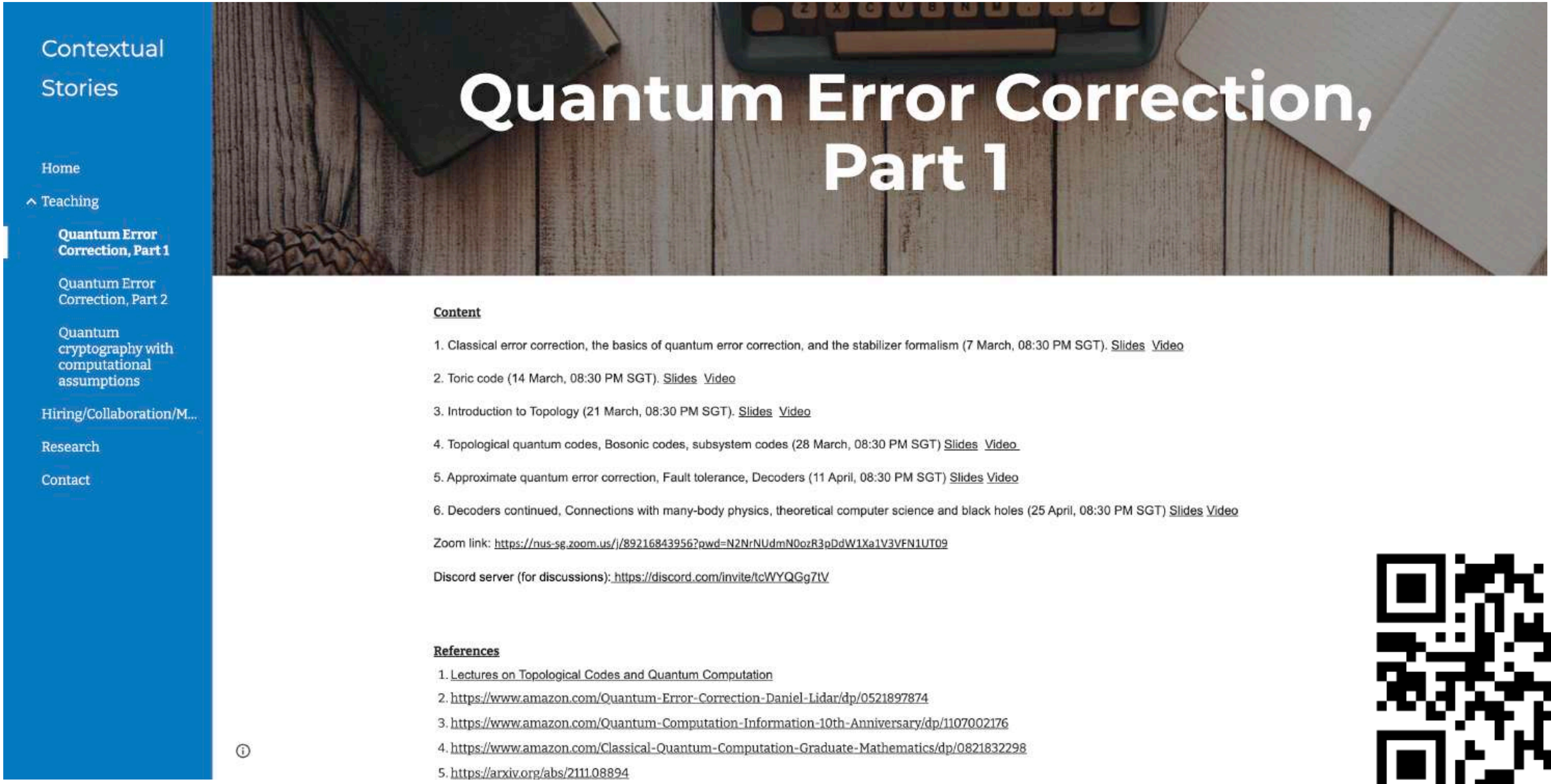
Kishor Bharti



Credits: Samuel Velasco/Quanta Magazine

Asia-Pacific Quantum Error Correction Seminars

QUANTUM ERROR CORRECTION TUTORIALS



Contextual Stories

- Home
- Teaching
  - Quantum Error Correction, Part 1
  - Quantum Error Correction, Part 2
  - Quantum cryptography with computational assumptions
- Hiring/Collaboration/M...
- Research
- Contact

Quantum Error Correction, Part 1

Content

1. Classical error correction, the basics of quantum error correction, and the stabilizer formalism (7 March, 08:30 PM SGT). Slides Video

2. Toric code (14 March, 08:30 PM SGT). Slides Video

3. Introduction to Topology (21 March, 08:30 PM SGT). Slides Video

4. Topological quantum codes, Bosonic codes, subsystem codes (28 March, 08:30 PM SGT) Slides Video

5. Approximate quantum error correction, Fault tolerance, Decoders (11 April, 08:30 PM SGT) Slides Video

6. Decoders continued, Connections with many-body physics, theoretical computer science and black holes (25 April, 08:30 PM SGT) Slides Video

Zoom link: https://nus-sg.zoom.us/j/89216843956?pwd=N2NrNUdmN0ozR3pDdW1Xa1V3VFN1UT09

Discord server (for discussions): https://discord.com/invite/tcWYQGg7tV

References

1. Lectures on Topological Codes and Quantum Computation
2. https://www.amazon.com/Quantum-Error-Correction-Daniel-Lidar/dp/0521897874
3. https://www.amazon.com/Quantum-Computation-Information-10th-Anniversary/dp/1107002176
4. https://www.amazon.com/Classical-Quantum-Computation-Graduate-Mathematics/dp/0821832298
5. https://arxiv.org/abs/2111.08894

CLASSICAL THREE BIT REPETITION CODE

Simplest starting point: Classical three bit repetition code

(A) Classical three-bit repetition code

001
↓
000
000
111

Encodes bits by repeating them

000 000 111

(1) Codewords

$n=3$
$k=1$
$d=3$

$$0_L = 000$$

$$1_L = 111$$

CLASSICAL THREE BIT REPETITION CODE

(2) Bit flip error

$$0 \to 1$$

$$1 \to 0$$

(3) Codewords after a single bit flip error

000

111

$0_L \to 100$	$0_L \to 010$	$0_L \to 001$
$1_L \to 011$	$1_L \to 101$	$1_L \to 110$

(4) Error detection

Bits in the string are not identical $\implies$ Error

CLASSICAL THREE BIT REPETITION CODE

(5) Error correction

Reset all bits to majority value

$$010 \rightarrow 000$$

$$101 \rightarrow 111$$

0 0 0

1 1 0

111

000

111

(6) Code distance

Smallest number of bit flips required to transform any two code words into one another

000

111

3

3-bit repetition code	3
n-bit repetition code	n

CLASSICAL THREE BIT REPETITION CODE

Hamming distance (a,b): minimum number of bit flips to transform bitstring a to bitstring b

a b

Code distance determines:

- Maximum number of errors which can be detected: d-1
- Maximum number of errors that can be corrected: (d-1)/2

a = 0 0 1 0

b = 1 1 1 0

2

(7) [n,k,d] notation

n: number of bits in the codewords

k: number of encoded bits

d: code distance

HD(a,b) =

[3,1,3]

Example: n-bit repetition code [n,1,n]

CLASSICAL THREE BIT REPETITION CODE

(8) Logical operations on the code

Goal: to perform computation on the encoded information

Exa: logical NOT gate

NOT(000) = 111
NOT(111) = 000

000 111

QUANTUM THREE QUBIT REPETITION CODE

(B) Quantum three qubit repetition code

(1) Code words

$$|0\rangle_L = |000\rangle \qquad |1\rangle_L = |111\rangle \qquad\qquad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle_L = \alpha|000\rangle + \beta|111\rangle$$

Codespace $\quad \mathrm{span}(|0\rangle_L, |1\rangle_L)$

Error free encoding of a quantum state lies in this subspace

QUANTUM THREE QUBIT REPETITION CODE

(2) Errors

(a) Bit flip error

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle$$

(b) Phase flip error

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle$$

Remark: If both X and Z errors can be corrected, more general errors can be corrected as well.

QUANTUM THREE QUBIT REPETITION CODE

(3) Encoded state after a single bit flip error

$$|\psi\rangle_L = \alpha|000\rangle + \beta|111\rangle$$

$$(I \otimes X \otimes I)|\psi\rangle_L = \alpha|010\rangle + \beta|101\rangle$$

(4) Error detection

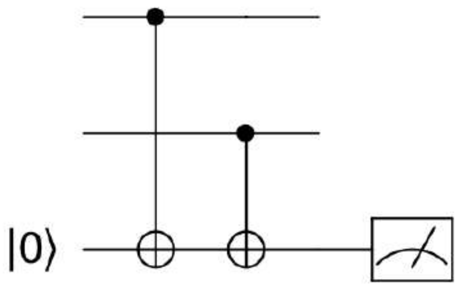
- Do not measure individual qubits in the computational basis
- it would detect the error, it would also result in the collapse of the encoded qubit.

- Measure symmetries of the state rather than individual bits
- Example: parity of any pair of bits

Even parity: 00,11
Odd parity: 01, 10

QUANTUM THREE QUBIT REPETITION CODE

Quantum circuit to measure parity



Equivalent to measuring $Z \otimes Z$ on first two qubits

$$Z \otimes Z|00\rangle = |00\rangle$$

$$Z \otimes Z|11\rangle = |11\rangle$$

$$Z \otimes Z|01\rangle = -|01\rangle$$

$$Z \otimes Z|10\rangle = -|10\rangle$$

Error	$Z \otimes Z \otimes I$	$Z \otimes I \otimes Z$	$I \otimes Z \otimes Z$
$X \otimes I \otimes I$	-1	-1	+1
$I \otimes X \otimes I$	-1	+1	-1
$I \otimes I \otimes X$	+1	-1	-1

(5) Error correction

Apply the inverse of the error operator to correct the error

Error	Correction operator
XII	XII

Paulis are self-inverse!

But..captain..why?

QUANTUM THREE QUBIT REPETITION CODE

(6) Logical operations on encoded states

We want $\bar{X}$ and $\bar{Z}$ such that

$$\bar{X}|0\rangle_L = |1\rangle_L \qquad \bar{X}|1\rangle_L = |0\rangle_L$$

$$\bar{Z}|0\rangle_L = |0\rangle_L \qquad \bar{Z}|1\rangle_L = -|1\rangle_L$$

One possible choice of $\bar{X}$ and $\bar{Z}$

$\alpha|000\rangle + \beta|111\rangle$

$$\bar{X} = XXX$$

$$\bar{Z} = ZII$$

$IIZ \qquad ZZZ$

(7) Distance of a quantum code

Weight of an operator: number of qubits it acts non-trivially on

Operator	Weight
XII	1
IXI	1
XXI	2
ZII	1
ZZZ	3

Distance of a quantum code: minimal weight of any (non-identity) encoded logical operator on the code

QUANTUM THREE QUBIT REPETITION CODE

Minimal weight of encoded $X = 3$ $\quad$ XXX

$Z = 1$ $\quad$ Z11, ZZZ, 1Z1, 11

Remark: the quantum 3-qubit repetition code can detect 2 X errors and no Z errors.

[[n, k, d]]

(C) Stabilizer formalism

- Most error correcting codes can be studied via the stabilizer formalism

Examples:
- Shor code
- Steane code
- 5-qubit code
- All CSS codes
- Toric code
- Planar surface codes

- Widely used formalism to describe topological codes
- Systematic approach to derive encoded logical operators

STABILIZER FORMALISM

Stabilizer code: a quantum error correcting code that can be defined in the stabilizer formalism

Stabilizer codes are defined by specifying two sets of operators

(1) (Stabilizer) generators
(2) Encoded logical operators

(1) The stabilizer group

Let $\{\,|\psi_j\rangle\,\}_j$: code-word basis states

STABILIZER FORMALISM

Let $\{|\psi_j\rangle\}_j$: code-word basis states

Stabilizer group: the set of Pauli operators which leave all codeword basis states $|\psi_j\rangle$ invariant.

$$P_k|\psi_j\rangle = |\psi_j\rangle \quad \forall P_k \in \mathscr{P}$$

Stabilizer operator (or stabilizer element): member of the stabilizer group

Claim: The set of stabilizer operators must commute.

$[P_k, P_l] \neq 0$

$P_k P_l = -P_l P_k$

$P_k P_l|\psi\rangle = P_k|\psi\rangle = -P_l P_k|\psi\rangle$

$= \underline{|\psi\rangle}$ $\qquad = \underline{-|\psi\rangle}$

(2) Stabilizer generators

Any group G can be specified by a set of generators $\{g_j\}_{j=1}^{m}$.

Theorem: For an Abelian group of self-inverse operators, any element $g \in G$ can be written as $g = \prod_{J} g_j^{\alpha_j}$ where $\alpha_j \in \{0,1\}$.

$$|G| = 2^m$$

m

2^m

STABILIZER FORMALISM

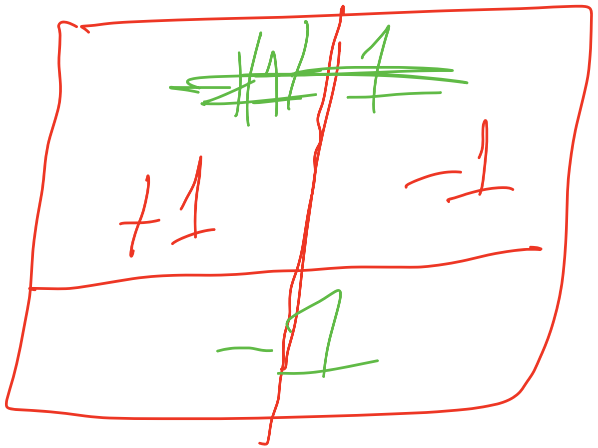
$$|G| = 2^m$$

2^n

k: # of logical qubits

n: # of physical qubits

m: # of stabilizer generators



$$\frac{2^n}{2^m} = 2^k$$

$n = m + k$

$$\boxed{m = n - k}$$

STABILIZER FORMALISM

k: # of logical qubits

n: # of physical qubits

m: # of stabilizer generators

$$m = n - k$$

Three qubit repetition code

$$|0\rangle_L = |000\rangle \qquad |1\rangle_L = |111\rangle$$

$$n = 3 \quad k = 1 \qquad \Longrightarrow \quad m = 3 - 1 = 2$$

$m = 2$

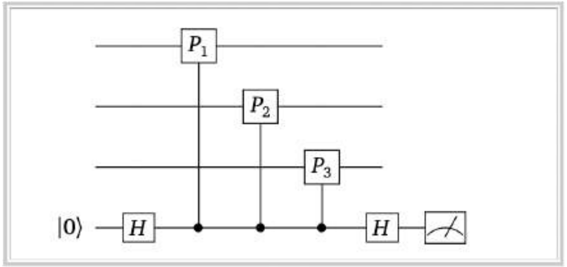
Order of the stabilizer group $= 2^m = 4$

$2^2 = 4$

$$ZZI, ZIZ, IZZ, III$$

(3) Error detection in the stabilizer formalism

- We can detect errors on stabilizer codes by measuring the stabilizer operators
- m measuremnts suffice (corresponding to stabilizer generators)
- Since m = n-k, m scales linearly with the # of physical qubits.
- Syndrome: outcome of the measurement of a given stabilizer generator



Circuit to measure $P_1 \otimes P_2 \otimes P_3$

(4) Encoded logical operators in the stabilizer formalism

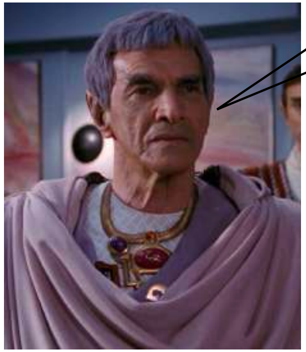
For the three qubit repetition code, we had

$$|0\rangle_L = |000\rangle \qquad |1\rangle_L = |111\rangle \qquad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \to |\psi\rangle_L = \alpha|000\rangle + \beta|111\rangle$$

$$\bar{X} = XXX \qquad \bar{Z} = ZII$$

Instead of ZII, we could have also used IZI and IIZ.

Using stabilizer formalism, we can characterize the equivalent set of logical operators.



STABILIZER FORMALISM

Equivalent set of logical operators

$\mathcal{C}$

- Let S be the stabilizer group
- $|\psi\rangle$ be a state in the codespace
- L be a logical operator

$|\psi\rangle \in \mathcal{C}$

$$S_j|\psi\rangle = |\psi\rangle \quad S_j \in S$$

$$\implies LS_j|\psi\rangle = L|\psi\rangle \quad S_j \in S$$

Remark: Given a logical operator L, there exists a family of $|S| = 2^m$ operators $\{LS_j\}_j$ that act equivalently on the codespace.

STABILIZER FORMALISM

Claim: A logical Pauli operator must belong to the centralizer of the stabilizer group.

Centralizer

The centralizer of an element z of a group G is the set of elements of G which commute with z,

$$C_G(z) = \{x \in G,\ x z = z x\}.$$

Likewise, the centralizer of a subgroup H of a group G is the set of elements of G which commute with every element of H,

$$C_G(H) = \{x \in G,\ \forall\, h \in H,\ x h = h x\}.$$

STABILIZER FORMALISM

(5) Distance

The minimal weight of any operator in the centralizer of the code

STABILIZER FORMALISM

<u>Three qubit repetition code</u>

Stabilizer group S

$$\{ZZI, ZIZ, IZZ, III\}$$

Centralizer of S

III	ZZI	ZIZ	IZZ
XXX	$-YYX$	$-YXY$	$-XYY$
YXX	XYX	XXY	$-YYY$
ZII	IZI	IIZ	ZZZ

[[3,1,1]]

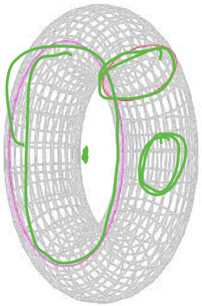
[[5,1,3]]

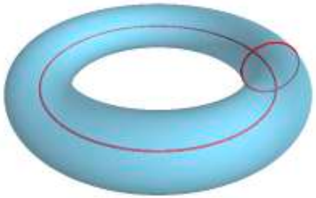
$$XZZXI$$
$$IXZZX$$
$$XIXZZ$$
$$ZXIXZ$$

$n = m + k$

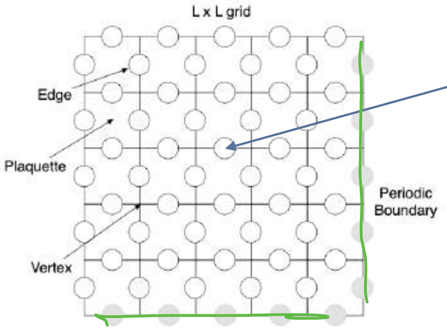
THE TORIC CODE

- Simplest example of a topological code





- The two loops cannot be deformed to a point or to each other.



Qubits

$2L^2$

Kitaev spin liquid
Kitaev's periodic table
Toric code
Sachdev–Ye–Kitaev model
Quantum phase estimation
Solovay–Kitaev theorem
Magic state distillation
Gottesman–Kitaev–Preskill codes
Quantum threshold theorem
QIP
QMA

Fault-tolerant quantum computation by anyons

A. Yu. Kitaev

L.D.Landau Institute for Theoretical Physics, 117940, Kosygina St. 2

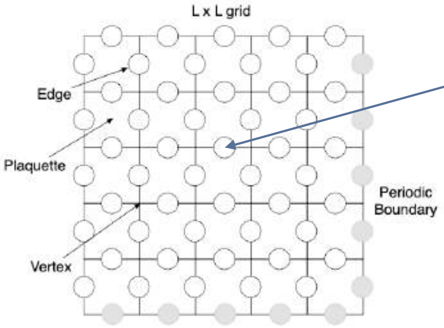
e-mail: kitaev@itp.ac.ru

Annals Phys. 303 (2003) 2-30

arXiv:quant-ph/9707021

THE TORIC CODE

(1) Physical qubits



Qubits

- # of edges = $L^2 + L^2 = 2L^2$
- Each edge corresponds to a physical qubit
- # of physical qubits = $2L^2$

$$[[n, k, d]]$$

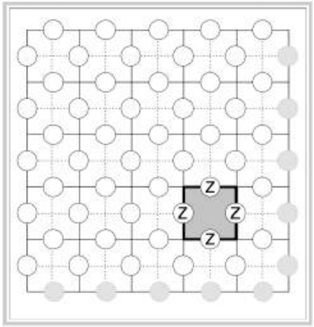
$$n = 2L^2$$

What about k?

....and d?

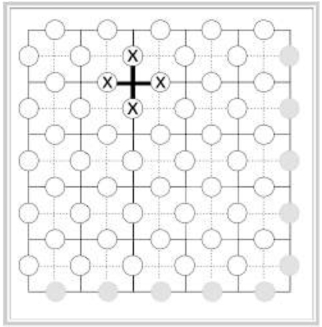
Later!

(2) Stabilizer generators



Plaquette generator

L^2



Vertex generator

L^2

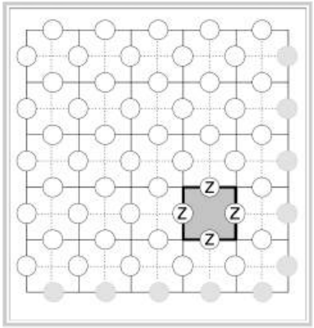
THE TORIC CODE

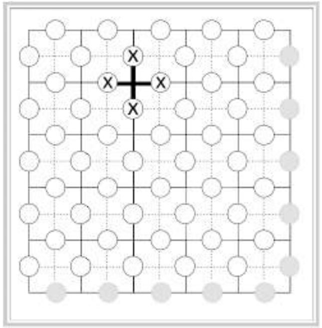
(Baby) claim: Plaquette and vertex operators commute.

Proof:

$[X, Z] \neq 0$

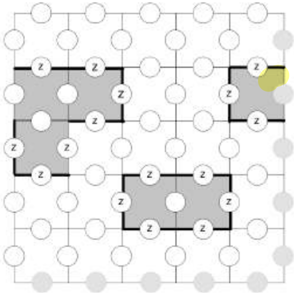
$[XX, ZZ] = 0$



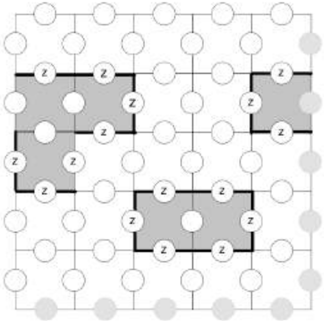


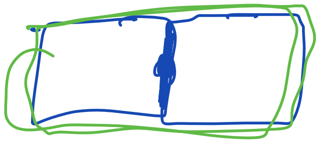
(3) Multiplication of plaquette operators

(Baby) claim: A pair of plaquette operators either do not share a boundary or have only one shared boundary.



(Baby) claim: When we multiply plaquette operators, the resulting operators will include Z operators that act on the boundary of the combined plaquettes.

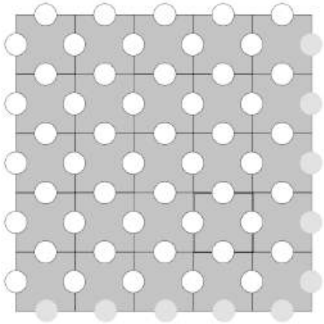




THE TORIC CODE

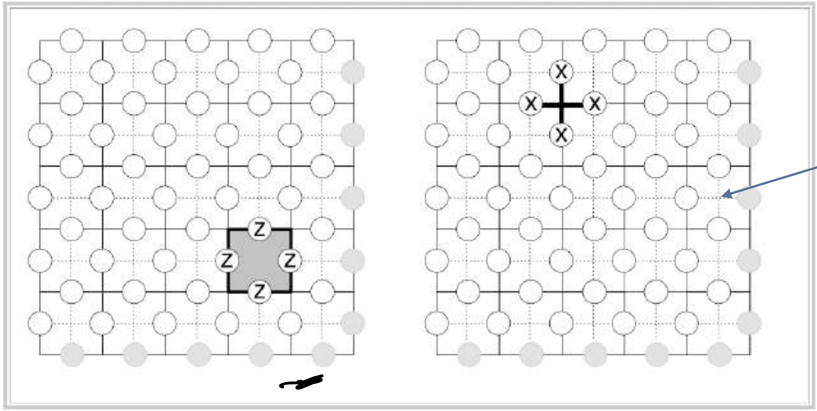
(Baby) claim: # of independent plaquette generators $= L^2 - 1$

Proof:



$$\prod_{\alpha} P_{\alpha} = I$$

(4) Dual lattice



Dashed lines indicate dual lattice.

Plaquette operators are vertex operators in the dual lattice and vice versa.

How to construct dual of a lattice

- Interchange plaquettes with vertices
- Reorient edges accordingly

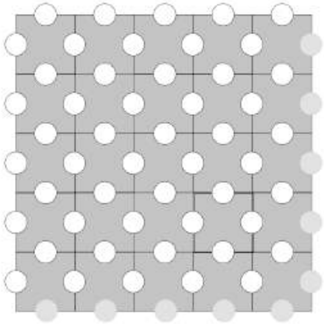
Primal lattice	Dual lattice
Hexagonal	Triangular
Square	Square

Self-dual lattice: primal = dual

THE TORIC CODE

(Baby) claim: # of independent vertex generators $= L^2 - 1$

Proof:



$$\prod_\alpha P_\alpha = I$$

$$\prod_\alpha V_\alpha = I$$

$L^2 - 1$

$+$

$L^2 - 1$

$= 2L^2 - 2$

$m = 2L^2 - 2$

$n = 2L^2$

$n = m + k$

$k = n - m$

$k = 2$

THE TORIC CODE

(5) Encoded qubits

(Baby) claim: # of encoded qubits $= 2$

Proof:

What about k?

2

THE TORIC CODE

(6) Encoded logical operators

$$\bar{Z}_1 \qquad \bar{X}_1$$

$$\bar{Z}_2 \qquad \bar{X}_2$$

<u>Requirements for the encoded logical operators</u>

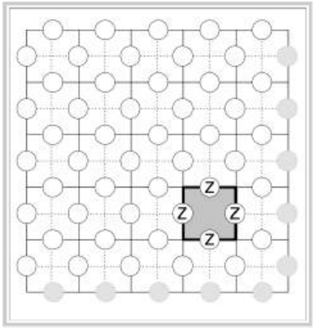
1. Must commute with all elements of the stabilizer group
2. Must not be an element of the stabilizer group
3. Must satisfy the commutation and anti-commutation relations of the Pauli operators they encode

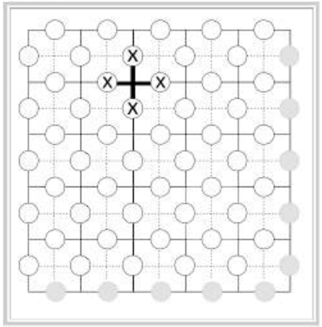
THE TORIC CODE

<u>Requirements for the encoded logical operators</u>

1. Must commute with all elements of the stabilizer group
2. Must not be an element of the stabilizer group
3. Must satisfy the commutation and anti-commutation relations of the Pauli operators they encode

$\bar{Z}_1$



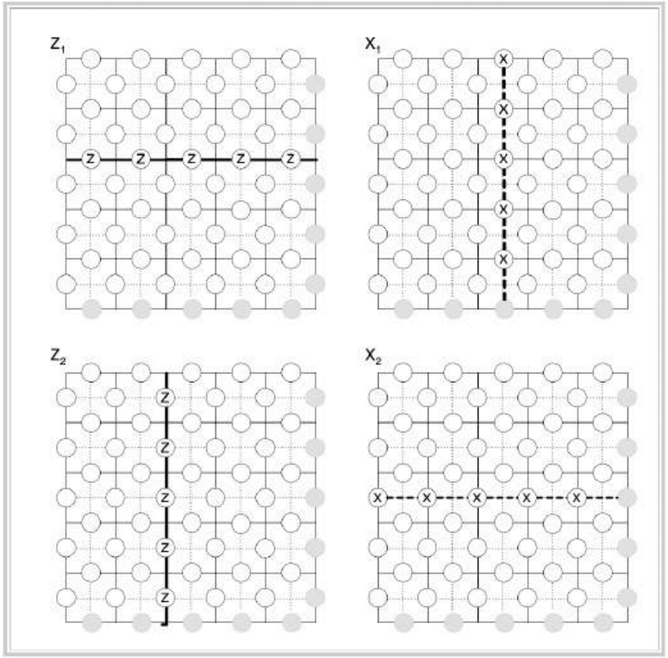


If we form a string of Z operators, regardless of its shape, it will always anticommute with the vertex operators at the ends of the string. The only solution is to find a string of operators which has no end - a loop!

THE TORIC CODE

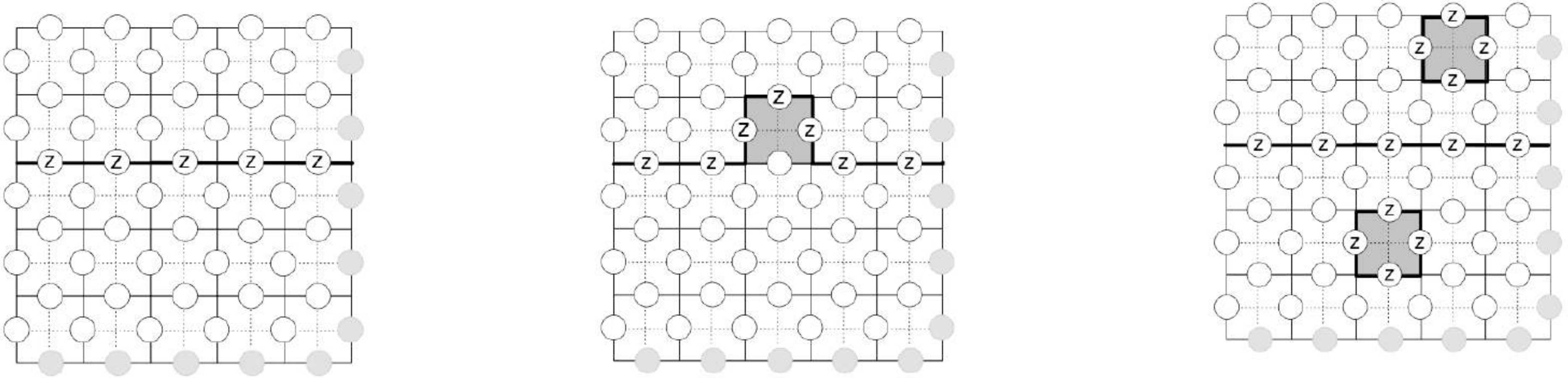
Requirements for the encoded logical operators

1. Must commute with all elements of the stabilizer group
2. Must not be an element of the stabilizer group
3. Must satisfy the commutation and anti-commutation relations of the Pauli operators they encode



THE TORIC CODE

(7) Equivalence of logical operators under stabilizer multiplication



L

$d = L$

(8) Code distance

- Minimum weight of any logical operator in the code
- Lowest weight of any undetectable error

$L \times L$ Lattice: Code distance $= L$

$$[[n = 2L^2, \quad k = 2, \quad d = L]]$$

What about k?

2

....and d?

L

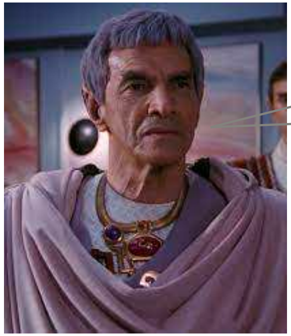
~~Later!~~

ERROR CORRECTION VIA TORIC CODE

ERROR CORRECTION VIA TORIC CODE

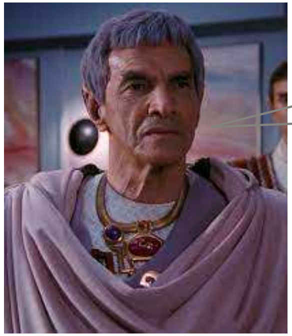
(1) Error detection

- We can detect errors on stabilizer codes by <u>measuring the stabilizer generators</u>
- Syndrome: outcome of the measurement of a given stabilizer generator



When error E happens, the stabilizer generators that don't commute with E will output -1.

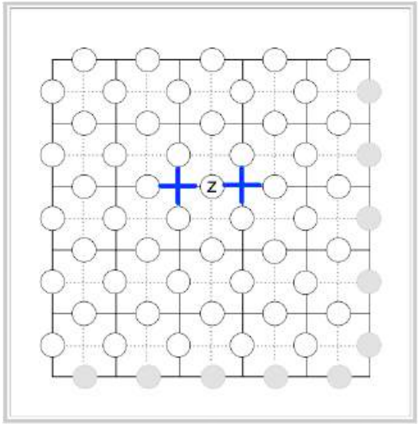
ERROR CORRECTION VIA TORIC CODE



When error E happens, the stabilizer generators that don't commute with E will output -1.

Example: Z error on a single qubit

Which stabilizer generators anticommute with it?

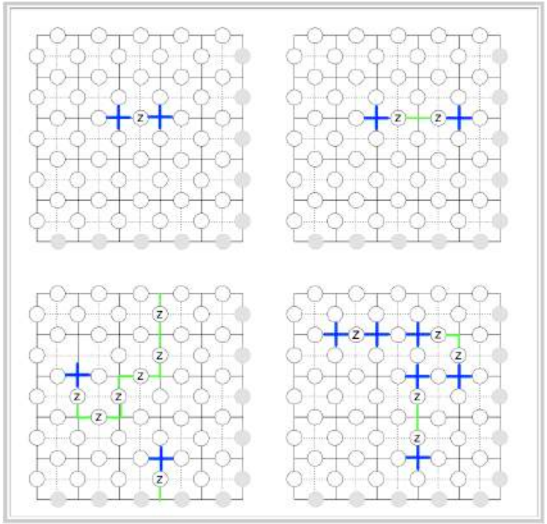


Vertex operators immediately adjacent to it

ERROR CORRECTION VIA TORIC CODE

(Baby) claim: Given any string of errors on the primal lattice, the only stabilizer generators have their outcome -1 are the vertices at the two ends of the string.

Proof:



The ends of a string can be considered its “bounday”

ERROR CORRECTION VIA TORIC CODE

Given any string of errors on the primal lattice, the only stabilizer generators have their outcome -1 are the vertices at the two ends of the string.

What about X errors

Similar analysis can be done for the dual lattice for the X errors.

ERROR CORRECTION VIA TORIC CODE

(2) Error correction

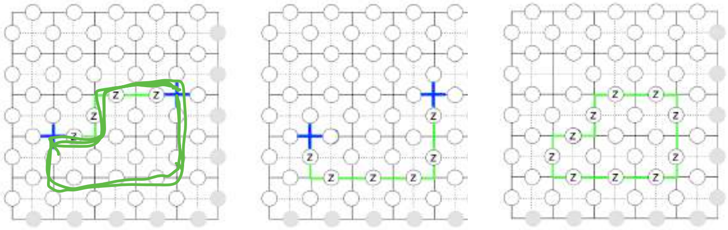
- **Main task in error correction:** identification of the error operator to apply given the syndrome
- For exa: apply the inverse of the error operator
- For self-inverse Pauli errors, apply the same operator

(Baby) claim: If $E'E = S$, where S is a stabilizer, then E' will correct E .

$\underline{E'E|\psi\rangle}$

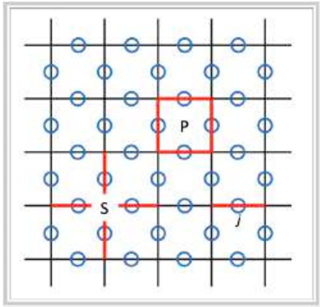
$S|\psi\rangle$

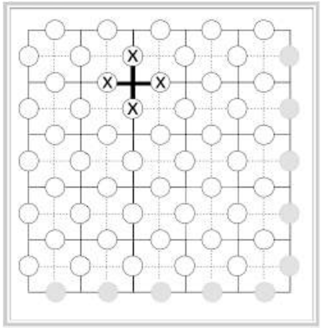
$= |\psi\rangle$

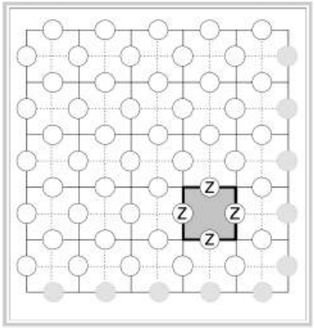


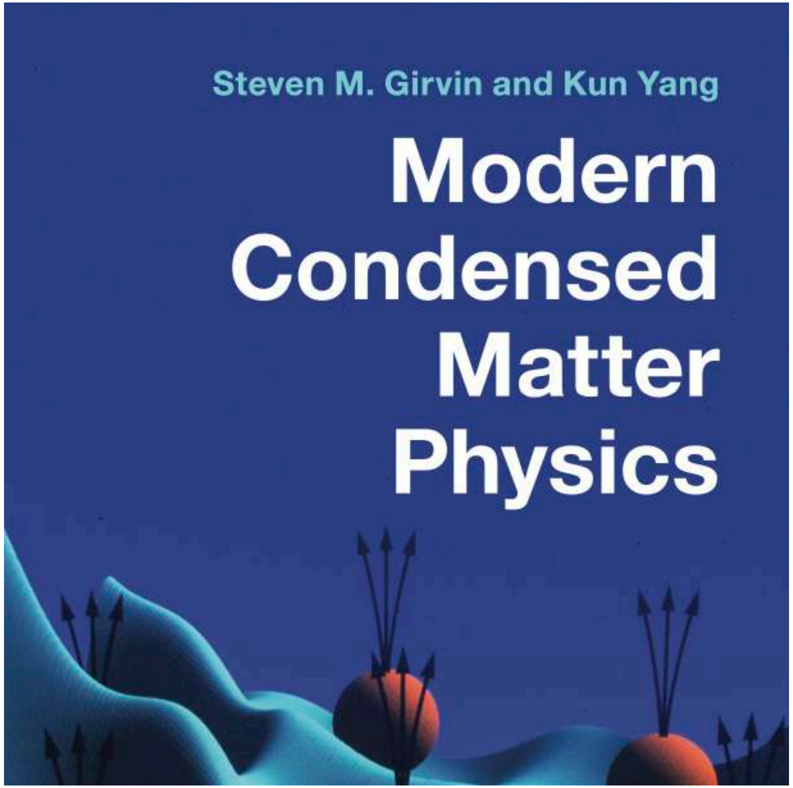
THE TORIC CODE HAMILTONIAN

THE TORIC CODE HAMILTONIAN









spin-$\frac{1}{2}$ particles on the bonds of the lattice

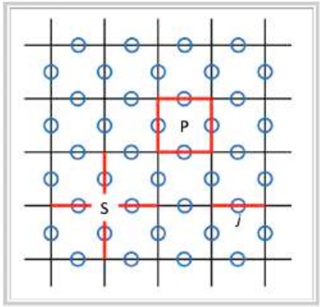
$$A_s = \prod_{j \in s} X_j$$

$$B_p = \prod_{j \in p} Z_j$$

$$H_{tc} = -\sum_s A_s - \sum_p B_p$$

17.8: An Exactly Solvable Model of $\mathbb{Z}_2$ Spin Liquid

THE TORIC CODE HAMILTONIAN

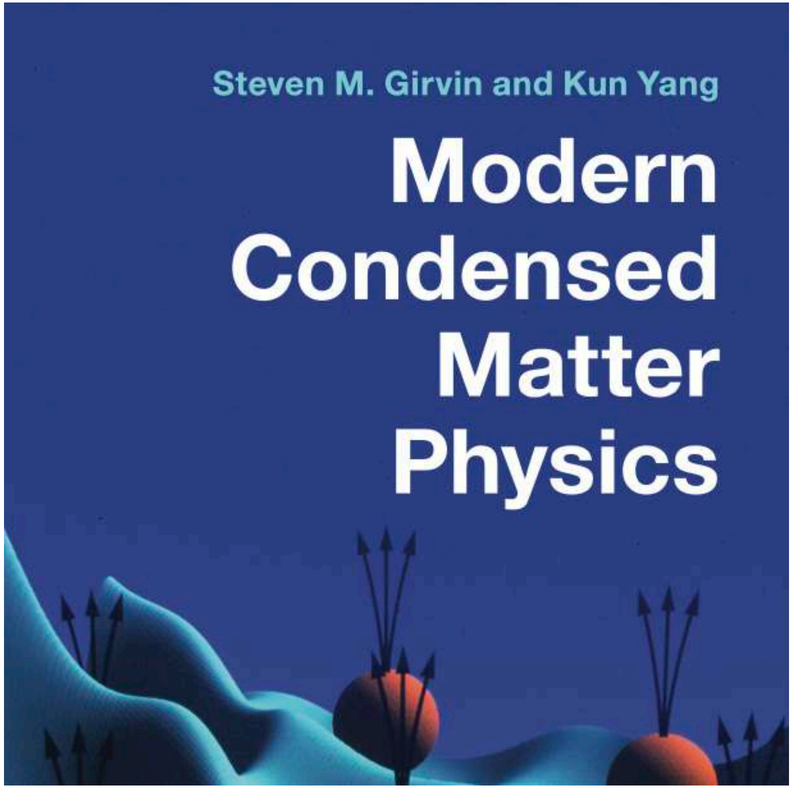


$$A_s = \prod_{j \in s} X_j \qquad B_p = \prod_{j \in p} Z_j$$

$$H_{tc} = -\sum_s A_s - \sum_p B_p$$

$$[A_s, A_{s'}] = [B_p, B_{p'}] = [A_s, B_p] = 0.$$

The ground state has degeneracy $D = 4$.



17.8: An Exactly Solvable Model of $\mathbb{Z}_2$ Spin Liquid