
Quantum error correction

- Error-free quantum computer – from a perspective from a software engineer on the top of the stack, there are no errors
- Error correction – approach to detecting and correcting errors, often phrased as an error-correcting code
- Fault tolerance – if an error appears, it can be detected and corrected

- Error-free quantum computer – from a perspective from a software engineer on the top of the stack, there are no errors
- Error correction – approach to detecting and correcting errors, often phrased as an error-correcting code
- Fault tolerance – if an error appears, it can be detected and corrected

under assumptions about the type of errors that can appear

# Noisy channel

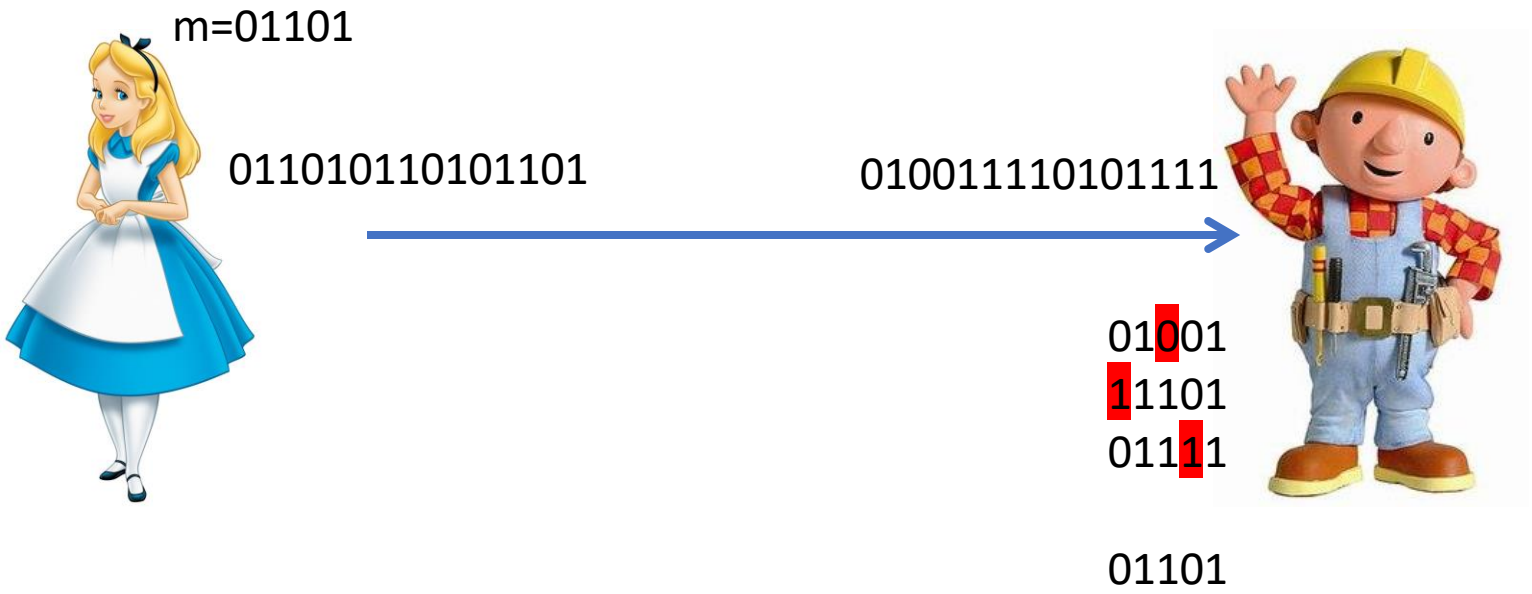
m=01101

m’=01001

The channel might be noisy and with probability p and error will occurs:

$$0 \rightarrow 1$$
$$1 \rightarrow 0$$

# Can you repeat that?




Alice can send the message 3 times which increases the probability that Bob will be able to uncover the meaning.

# Problem

A probability of a bit flip is p. Having three bits, what is the probability that

- No bit flip occurs
- Only the first bit gets flipped.
- At most one bit gets flipped.

How would the probabilities change with n bits?

# Independent errors

We need to make an assumptions that individual errors will be independent of each other. This is not always true in practice (cosmic rays).

# Repetition code

Encode $0_L \rightarrow 000$ (logical 0)

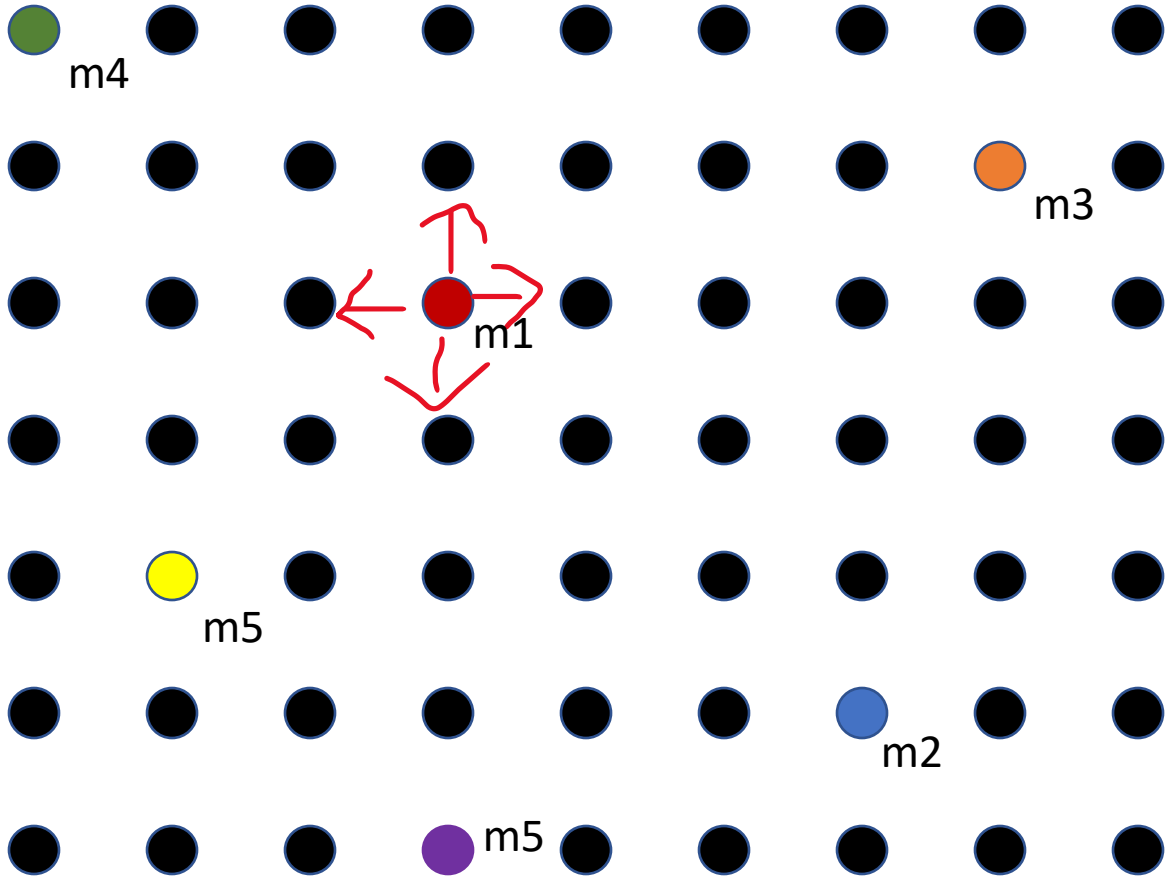
Encode $1_L \rightarrow 111$ (logical 1)

- Decode $000, 001, 010, \ 100 \rightarrow 0$
- Decode $111, 011, 110, \ 101 \rightarrow 1$

Can correct 1 bit-flip.

If the probability of a bit flip is $p < 1/2$, what is the probability of an error before and after decryption with repetition code?

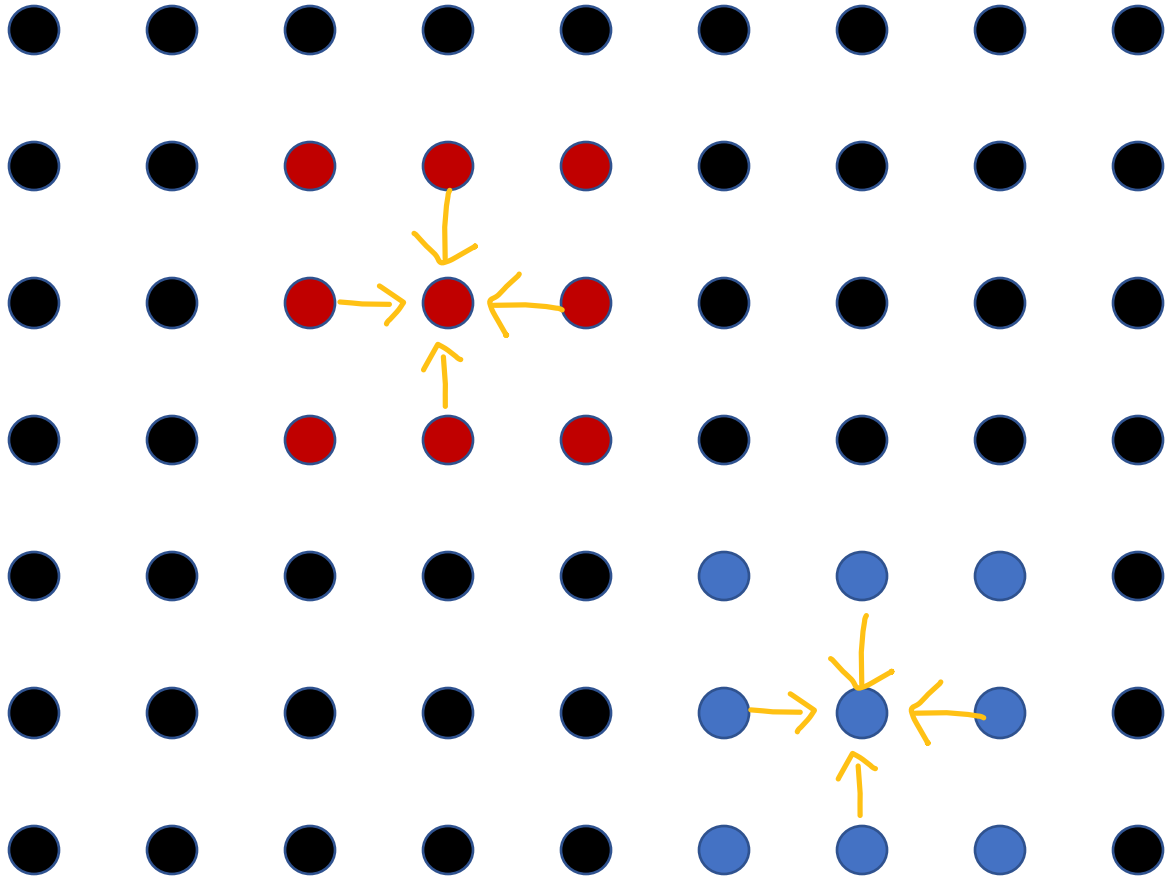
# Hamming distance




Hamming distance between two bitstrings is the number of bits they differ. E.g. 0101, 0011 have Hamming distance 2, 0101 and 1110 have Hamming distance 3.

If the Hamming distance between messages is large,
we can easily correct any errors

# Introduce redundancy

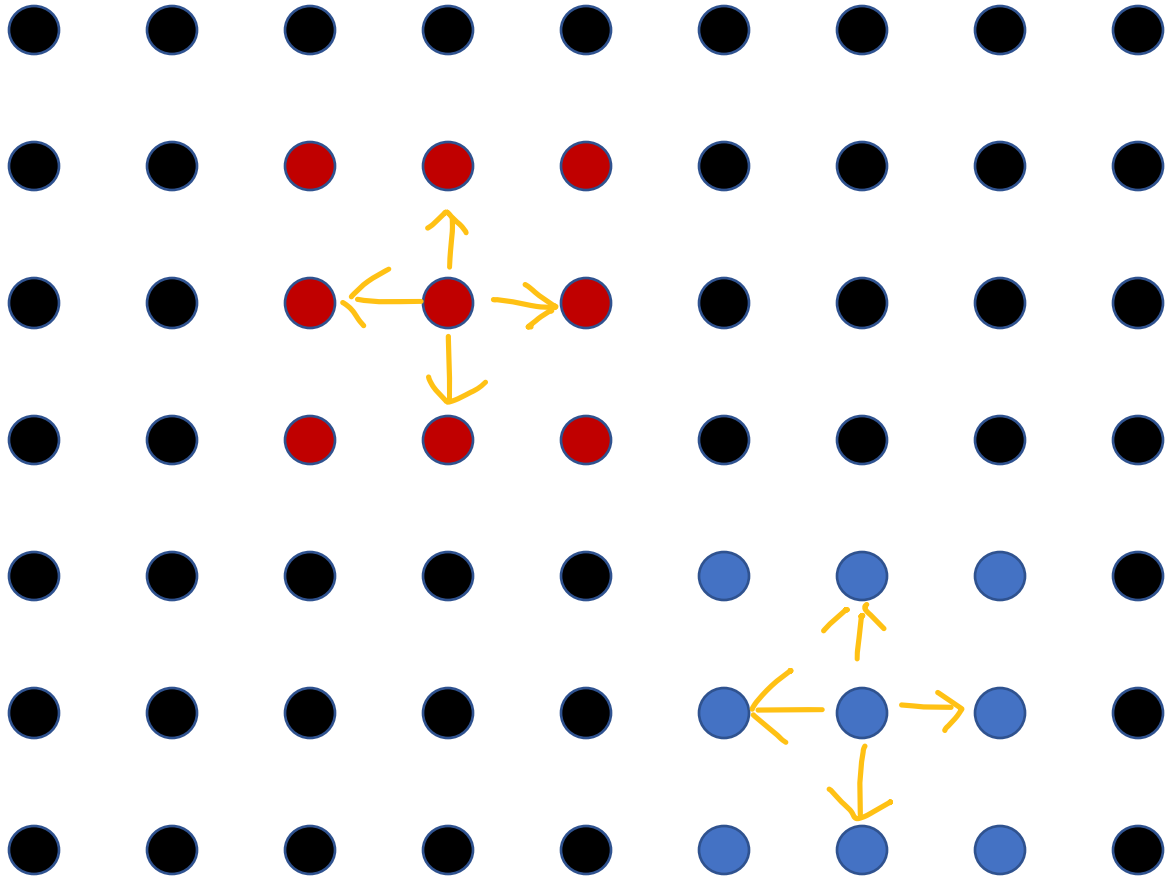


M1 = Errorcorrectingcodes
M2 = Everyonefailstheclass

Errrrcorvctingkodes very likely came from message m1 instead of two m2.

We could send 1 for M1 or M2 for M2 but the redundancy in English allows us to correct for errors

# Codewords



Even if the original messages were close, we can encode them into “codeword” that are far from each other in Hamming distance.

Standard notation: [n,k,d]
Encode n bits/qubits into k bits/qubits with distance d. Distance is the minimum distance between distinct codewords

People use [n,k,d] for classical codes and [[n,k,d]] for quantum ones.

Can we do the same for quantum states?

# Can we do the same for quantum states?

1. No cloning theorem

2. Measuring destroys quantum information

3. Instead of simple bitflips, we have a continuum of errors.

# Yes, but it’s complicated

1. No cloning theorem – only clone orthogonal states
2. Measuring destroys quantum information – measure ONLY errors
3. Instead of simple bitflips, we have a continuum of errors – errors can be discretized

# Quantum errors in the Z basis (bitflips)

- We don’t need to copy an unknown state

$$a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$$

- An error would flip one of the qubits but we still have two to decide majority.

# Decoding

$$a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$$

How do we find out if there is an error without destroying the state? (syndrome extraction)?

Observation: if we measured all three registers, they would always agree.

# Decoding

$$a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$$

Solution: only measure if one of the registers disagrees:

Distinguish between 4 possibilities

- No error $|000\rangle, |111\rangle$
- Error (on the first qubit) $|100\rangle, |011\rangle$
- Error (on the second qubit) $|010\rangle, |101\rangle$
- Error (on the last qubit) $|001\rangle, |110\rangle$

Projective measurement on of the four subspaces

# Parity measurement

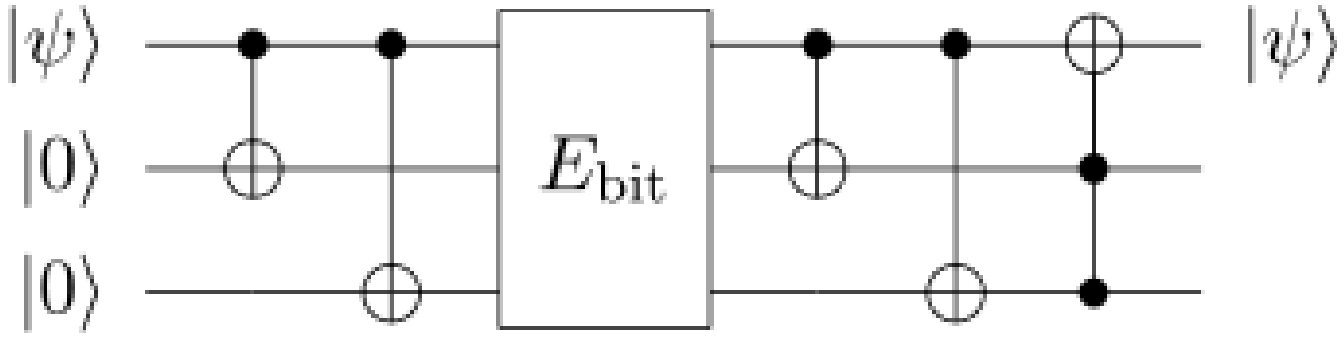
- ZZ return 0 if two bits (qubits) are the same and 1 if they are opposite

$\{|00\rangle,|11\rangle\}$ + 1 subspace

$\{|01\rangle,|10\rangle\}$ - 1 subspace

- Measure $Z_1Z_2$, $Z_1Z_3$, $Z_2Z_3$
- $Z_1Z_2 = Z_1Z_3 = Z_2Z_3 = 1$ no errors
- $Z_1Z_2 = Z_1Z_3 = -1$ and $Z_2Z_3 = 1$ error on the first qubit
- $Z_1Z_2 = 1$, $Z_1Z_3 = -1$ and $Z_2Z_3 = -1$ error on the third qubit
- $Z_1Z_2 = -1$, $Z_1Z_3 = 1$ and $Z_2Z_3 = -1$ error on the second qubit

# Alternative decoding




- No error

$$a|000\rangle + b|111\rangle \rightarrow a|0\rangle + b|1\rangle$$

- Bitflip on the first qubit

$$a|100\rangle + b|011\rangle \rightarrow a|111\rangle + b|011\rangle \rightarrow a|011\rangle + b|111\rangle \rightarrow a|0\rangle + b|1\rangle$$

# Phase flip errors

$$|+\rangle \rightarrow |-\rangle$$
$$|-\rangle \rightarrow |+\rangle$$

- The same in X basis

$$|+\rangle_L \rightarrow |++\,+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$|-\rangle_L \rightarrow |--\,-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

# Can a code correct both Z and X errors?

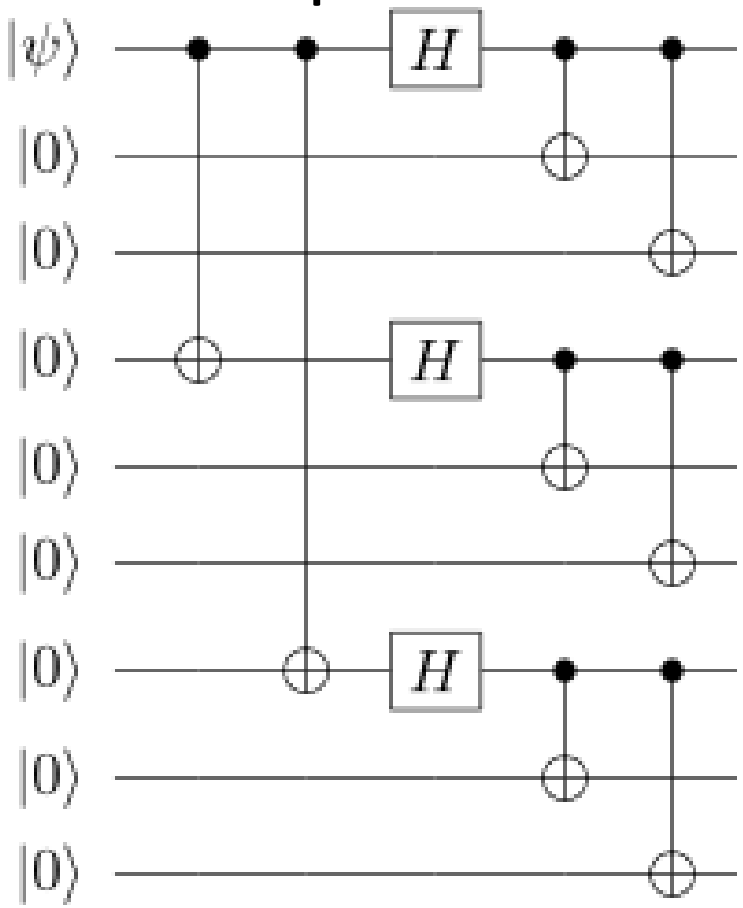
- Concatenate the phase flip and the bitflip code
- First phase flip:

$$|0\rangle_L \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$|1\rangle_L \rightarrow \frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- Then bitflip

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \rightarrow \frac{|000\rangle+|111\rangle}{\sqrt{2}}\frac{|000\rangle+|111\rangle}{\sqrt{2}}\frac{|000\rangle+|111\rangle}{\sqrt{2}}$$
$$\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \rightarrow \frac{|000\rangle-|111\rangle}{\sqrt{2}}\frac{|000\rangle-|111\rangle}{\sqrt{2}}\frac{|000\rangle-|111\rangle}{\sqrt{2}}$$

# Shor's 9 qubit code




encoding

First create the phase flip code.
Then encode each qubit with the bitflip code.

Concatenate codes

# Exercise

- Verify that measuring $Z_1Z_2$ , $Z_2Z_3$, $Z_3Z_1$, $Z_4Z_5$ , $Z_5Z_6$, $Z_6Z_4$, $Z_7Z_8$ , $Z_8Z_9$, $Z_9Z_7$ will detect bitflip errors (just do a few)
- Verify that measuring $X_1$ $X_2$ $X_3$ $X_4$ $X_5$ $X_6$ , $X_4$ $X_5$ $X_6$ $X_7$ $X_8$ $X_9$ and $X_7$ $X_8$ $X_9$ $X_1$ $X_2$ $X_3$ can detect phase flip errors. (just do one)

# Logical operations on the 9-qubit code

- What physical operations do we need to apply to the code to apply logical operations?

- Simplest operations X, Z, other gates can be constructed from them and measurements (fault-tolerant construction)

- Logical X: $|0\rangle_L \rightarrow |1\rangle_L$

$$|0\rangle_L = \frac{|000\rangle+|111\rangle}{\sqrt{2}}\frac{|000\rangle+|111\rangle}{\sqrt{2}}\frac{|000\rangle+|111\rangle}{\sqrt{2}}$$

$$|1\rangle_L = \frac{|000\rangle-|111\rangle}{\sqrt{2}}\frac{|000\rangle-|111\rangle}{\sqrt{2}}\frac{|000\rangle-|111\rangle}{\sqrt{2}}$$

X

Z

# Correcting errors in any basis

- Theorem: If a quantum code can correct errors of type A and type B it can also correct a linear combination of errors aA + bB

- If we know how to correct X, Z and XZ errors we will be able to correct for any unitaries.

# Stabilizer formalism

- Due to Daniel Gottesman.
- A very useful way of representing quantum states for error correction.
- Characterize state/states.
- Language of error correction.

# Groups (abstract algebra refresher)

- set of elements (A,B<C,…) and an operation(∘) between them
- The set is closed wrt the operations, $A \circ B$ always belongs to the set
- Includes an identity $A \circ \mathbb{I} = A$ for all A
- Every element has an inverse in the set $A \circ A^{-1} = \mathbb{I}$

Examples:

- {1,-1}, $\times$
- $\mathbb{Z}, +$
- Unitary matrices with matrix multiplication

# The Pauli group $P_n$

- $P_1$ – single qubit matrices with multiplication

$$\{\pm\mathbb{I}, \pm X, \pm Y, \pm Z, \pm i\mathbb{I}, \pm iX, \pm iY, \pm iZ\}$$

Including $i$ ensures that the set is closed under multiplication. Half of the terms commute and half anti-commute.

Note that $Y = iZX$.

# The stabilizer group

Many states can be described by Paulis that *stabilize* them – if we apply a Pauli on our state, we get the same state back. Take

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

It can be uniquely identified as +1 eigenstate of the operators $X_1X_2$, $Z_1Z_2$, i. e. $X_1X_2\,|\psi\rangle = |\psi\rangle$, $Z_1Z_2\,|\psi\rangle = |\psi\rangle$.

We then say that S is the stabilizer of $V_s$ if S are the Paulis that stabilize as the set of $n$-qubit states $V_s$.

Stabilizers form a group.

# Group generators

- Set of operators $g_1, \ldots, g_m$ such that such that (repeated) application of the generators on themselves and each other is capable of creating all the elements in the group.

- X & Z are generators of the Pauli group.
- E.g. $ZZ = \mathbb{I}, ZX = iY, ZXZ = -X, ZXZX = -\mathbb{I}, \ldots$

# Stabilizers for Shor 9-qubit code

Generators of the stabilizer group

- $Z_1Z_2$ , $Z_2Z_3$, $Z_4Z_5$ , $Z_5Z_6$, $Z_7Z_8$ , $Z_8Z_9$, $X_1\,X_2\,X_3\,X_4\,X_5\,X_6$ , $X_4\,X_5\,X_6\,X_7\,X_8\,X_9$

- These operators uniquely define the error-free subspace.

- Exercise: show that the above operators commute (i.e. AB=BA)

# Normalizer of Paulis

- What unitaries map Paulis onto Paulis under conjugation?

$$UP_nU^+ = P_n$$

- All Paulis have this property.
- Also gates H, CNOT, S (phase)

# Exercise

- Verify $HXH = Z, HZH = X$
- Compute:

$$CNOT\ (X \otimes \mathbb{I})\ CNOT$$
$$CNOT\ (\mathbb{I} \otimes X) CNOT$$

# The Clifford group

The normalizer of $P_n$, includes by X,Z, S,H, CNOT and their product.

Does not include T or Toffoli gates.

Allows us to track quantum states during (certain computation).

# Gottesman-Knill theorem

Circuits that consists only of

- Qubit preparation in the computational basis
- Clifford gates (H,S, CNOT, Paulis)
- Measurement in the computational basis

can be efficiently classically simulated.

Algorithm due to Aaronson and Gottesman.

Very entangled states are classically simulable. Entanglement alone does not lead to quantum speedup.

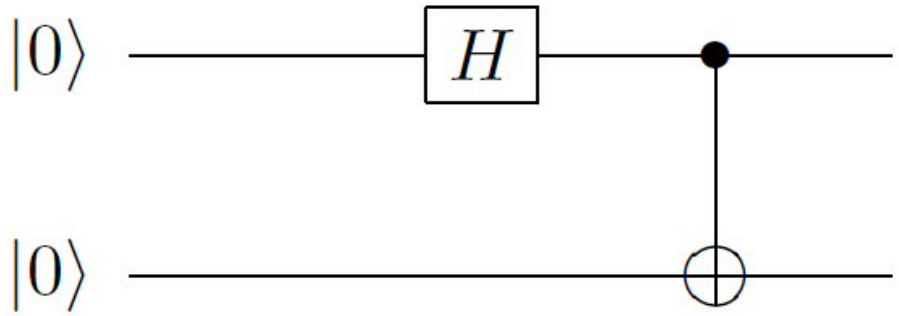
# Example

- Start with $|00\rangle$ stabilized with Z1, Z2.
- Apply Hadamard gate:

$$Z_1 \longrightarrow X_1$$
$$Z_2 \longrightarrow Z_2$$

- Apply CNOT gate

$$X_1 \longrightarrow X_1X_2$$
$$Z_2 \longrightarrow Z_1Z_2$$




Stabilizers of $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ are $X_1X_2$, $Z_1Z_2$ as before

# Fault-tolerant computation

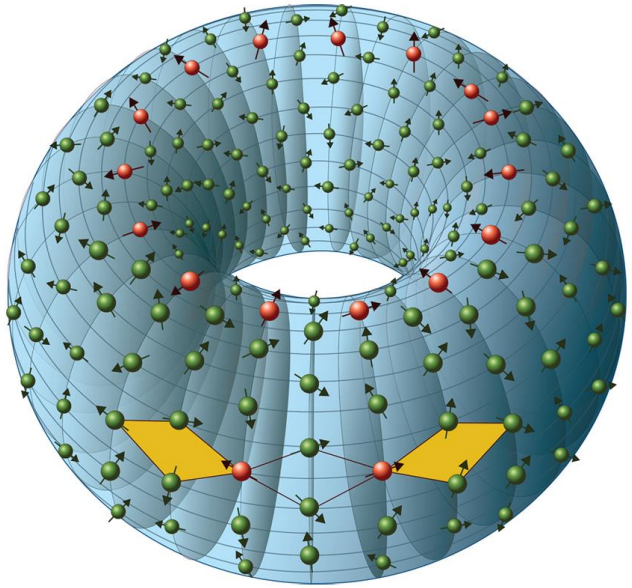
- Errors propagate and accumulate during computation
- If the noise obeys reasonable physical assumptions ( i.e. uncorrelated) and bellow a certain thresholds, we may achieve arbitrarily precise computation using redundancy

- Logical states are encoded into multiple qubits
- Logical gates are performed as fault-tolerant operations requiring more gates and qubits.

# Other error correcting codes

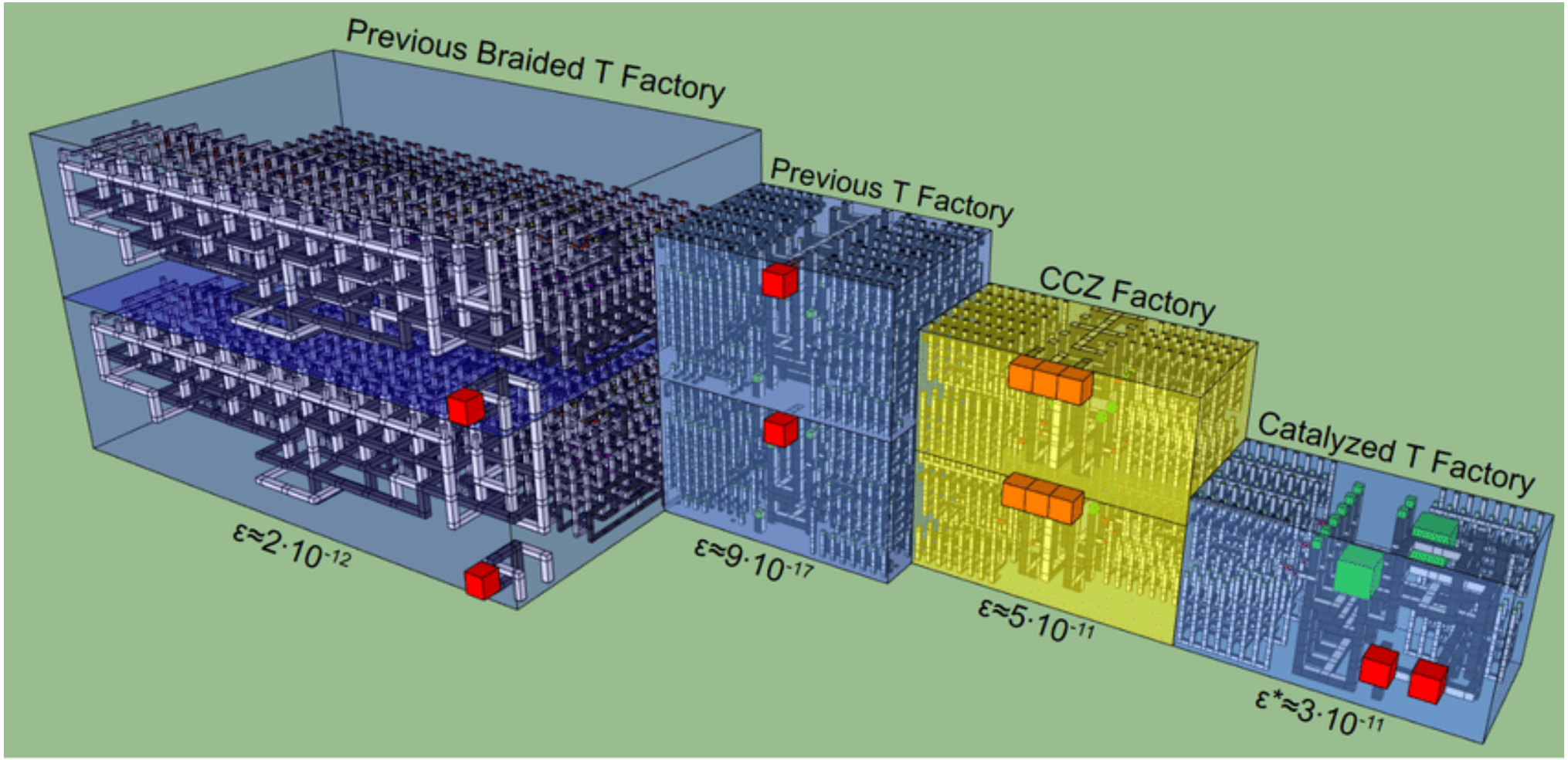
- 5 qubit code – smallest code to correct a single error

- Topological codes
  - Nontrivial loops apply operations



- Surface codes
  - Ideal for qubits on a lattice
  - Expected way to fault-tolerance

# A taste of what is actually required




Gidney and Fowler