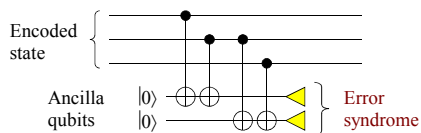


Measure the Error, Not the Data

Use this circuit:



1st bit of error syndrome says whether the first two bits of the state are the same or different.

2nd bit of error syndrome says whether the second two bits of the state are the same or different.

Measure the Error, Not the Data

With the information from the error syndrome, we can determine whether there is an error and where it is:

E.g., $\alpha |010\rangle + \beta |101\rangle$ has syndrome 11, which means the second bit is different. Correct it with a X operation on the second qubit. Note that the syndrome does not depend on α and β .

We have learned about the error without learning about the data, so superpositions are preserved!

Redundancy, Not Repetition

This encoding does not violate the no-cloning theorem:

$$\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |000\rangle + \beta |111\rangle \neq (\alpha |0\rangle + \beta |1\rangle)^{\otimes 3}$$

We have repeated the state only in the computational basis; superposition states are spread out (redundant encoding), but not repeated (which would violate no-cloning).

Update on the Problems

- ✓ 1. Measurement of error destroys superpositions.
- ✓ 2. No-cloning theorem prevents repetition.
- 3. Must correct multiple types of errors (e.g., bit flip and phase errors).
- 4. How can we correct continuous errors and decoherence?

Correcting Just Phase Errors

Hadamard transform H exchanges bit flip and phase errors:

$$H(\alpha |0\rangle + \beta |1\rangle) = \alpha |+\rangle + \beta |-\rangle$$

$X |+\rangle = |+\rangle, X |-\rangle = -|-\rangle$ (acts like phase flip)
 $Z |+\rangle = |-\rangle, Z |-\rangle = |+\rangle$ (acts like bit flip)

Repetition code corrects a bit flip error

➡ Repetition code in Hadamard basis corrects a phase error.

$$\alpha |+\rangle + \beta |-\rangle \rightarrow \alpha |+++ \rangle + \beta |-- \rangle$$

Nine-Qubit Code

To correct both bit flips and phase flips, use both codes at once:

$$\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha(|000\rangle + |111\rangle)^{\otimes 3} + \beta(|000\rangle - |111\rangle)^{\otimes 3}$$

Repetition 000, 111 corrects a bit flip error, repetition of phase +++, --- corrects a phase error

Actually, this code corrects a bit flip and a phase, so it also corrects a Y error:

$$Y = iXZ: Y |0\rangle = i |1\rangle, Y |1\rangle = -i |0\rangle \quad (\text{global phase irrelevant})$$

Update on the Problems

- ✓ 1. Measurement of error destroys superpositions.
- ✓ 2. No-cloning theorem prevents repetition.
- ✓ 3. Must correct multiple types of errors (e.g., bit flip and phase errors).
- 4. How can we correct continuous errors and decoherence?

Correcting Continuous Rotation

Let us rewrite continuous rotation

$$R_\theta |0\rangle = |0\rangle, R_\theta |1\rangle = e^{i\theta} |1\rangle$$

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

$$= \cos(\theta/2) I - i \sin(\theta/2) Z$$

$$R_\theta^{(k)} |\psi\rangle = \cos(\theta/2) |\psi\rangle - i \sin(\theta/2) Z^{(k)} |\psi\rangle$$

($R_\theta^{(k)}$ is R_θ acting on the k th qubit.)

Correcting Continuous Rotations

How does error correction affect a state with a continuous rotation on it?

$$R_\theta^{(k)} |\psi\rangle = \cos(\theta/2) |\psi\rangle - i \sin(\theta/2) Z^{(k)} |\psi\rangle$$

$$\longrightarrow \cos(\theta/2) |\psi\rangle |1\rangle - i \sin(\theta/2) Z^{(k)} |\psi\rangle |Z^{(k)}\rangle$$

↙ Error syndrome ↘

Measuring the error syndrome collapses the state:

Prob. $\cos^2(\theta/2)$: $|\psi\rangle$ (no correction needed)

Prob. $\sin^2(\theta/2)$: $Z^{(k)} |\psi\rangle$ (corrected with $Z^{(k)}$)

Correcting All Single-Qubit Errors

Theorem: If a quantum error-correcting code (QECC) corrects errors A and B, it also corrects $\alpha A + \beta B$.

Any 2x2 matrix can be written as $\alpha I + \beta X + \gamma Y + \delta Z$.

A general single-qubit error $\rho \rightarrow \sum A_k \rho A_k^\dagger$ acts like a mixture of $|\psi\rangle \rightarrow A_k |\psi\rangle$, and A_k is a 2x2 matrix.

Any QECC that corrects the single-qubit errors X, Y, and Z (plus I) corrects every single-qubit error.

Correcting all t-qubit X, Y, Z on t qubits (plus I) corrects all t-qubit errors.

QECC is Possible

- ✓ 1. Measurement of error destroys superpositions.
- ✓ 2. No-cloning theorem prevents repetition.
- ✓ 3. Must correct multiple types of errors (e.g., bit flip and phase errors).
- ✓ 4. How can we correct continuous errors and decoherence?

The Pauli Group

Define the Pauli group P_n on n qubits to be generated by X, Y, and Z on individual qubits. Then P_n consists of all tensor products of up to n operators X, Y, or Z with overall phase $\pm 1, \pm i$.

Any pair M, N of Pauli operators either commutes ($MN = NM$) or anticommutes ($MN = -NM$).

The weight of $M \in P_n$ is the number of qubits in which M acts as a non-identity operator.

Error Syndromes Revisited

Let us examine more closely the error syndrome for the classical repetition code.

A correctly-encoded state 000 or 111 has the property that the first two bits have even parity (an even number of 1's), and similarly for the 2nd and 3rd bits. A state with an error on one of the first two bits has odd parity for the first two bits.

We can rephrase this by saying a codeword is a +1 eigenvector of $Z \otimes Z \otimes I$ and a state with an error on the 1st or 2nd bit is a -1 eigenvector of $Z \otimes Z \otimes I$.

Error Syndromes Revisited

For the three-qubit phase error correcting code, a codeword has eigenvalue +1 for $X \otimes X \otimes I$, whereas a state with a phase error on one of the first two qubits has eigenvalue -1 for $X \otimes X \otimes I$.

Measuring $Z \otimes Z$ detects bit flip (X) errors; measuring $X \otimes X$ detects phase (Z) errors.

Error syndrome is formed by measuring enough operators to determine location of error.

Stabilizer for Nine-Qubit Code

We can write down all the operators determining the syndrome for the nine-qubit code.

M_1	Z Z
M_2	Z Z
M_3	Z Z
M_4	Z Z
M_5	Z Z
M_6	Z Z
M_7	X X X X X X
M_8	X X X X X X

These generate a group, the stabilizer of the code, consisting of all Pauli operators M with the property that $M|\psi\rangle = |\psi\rangle$ for all encoded states $|\psi\rangle$.

Properties of a Stabilizer

The stabilizer is a group:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then $MN|\psi\rangle = |\psi\rangle$.

The stabilizer is Abelian:

If $M|\psi\rangle = |\psi\rangle$ and $N|\psi\rangle = |\psi\rangle$, then

$$(MN - NM)|\psi\rangle = MN|\psi\rangle - NM|\psi\rangle = 0$$

(For Pauli matrices) $\implies MN = NM$

Given any Abelian group S of Pauli operators, define a code space $T(S) = \{|\psi\rangle \text{ s.t. } M|\psi\rangle = |\psi\rangle \forall M \in S\}$.

Then $T(S)$ encodes k logical qubits in n physical qubits when S has $n-k$ generators (so size 2^{n-k}).

Stabilizer Elements Detect Errors

Suppose $M \in S$ and Pauli error E anticommutes with M . Then:

$$M(E|\psi\rangle) = -EM|\psi\rangle = -E|\psi\rangle,$$

so $E|\psi\rangle$ has eigenvalue -1 for M .

Conversely, if M and E commute for all $M \in S$,

$$M(E|\psi\rangle) = EM|\psi\rangle = E|\psi\rangle \quad \forall M \in S,$$

so $E|\psi\rangle$ has eigenvalue +1 for all M in the stabilizer.

The eigenvalue of an operator M from the stabilizer detects errors which anticommute with M .

Distance of a Stabilizer Code

Let S be a stabilizer, and let $T(S)$ be the corresponding QECC. Define

$$N(S) = \{N \in P_n \text{ s.t. } MN = NM \forall M \in S\}.$$

The distance d of $T(S)$ is the weight of the smallest Pauli operator N in $N(S) \setminus S$.

The code detects any error not in $N(S) \setminus S$ (i.e., errors which commute with the stabilizer are not detected).

Why minus S ? "Errors" in S leave all codewords fixed, so are not really errors. (Degenerate QECC.)

Stabilizer Codes Correct Errors

A stabilizer code with distance d will correct $\lfloor (d-1)/2 \rfloor$ errors (i.e., to correct t errors, we need distance $2t+1$):

The error syndrome is the list of eigenvalues of the generators of S . E and F have the same error syndrome iff $E^\dagger F \in N(S)$. (Then E and F commute with the same set of generators of S .)

If $E^\dagger F \notin N(S)$, the error syndrome can distinguish them. When $E^\dagger F \in S$, E and F act the same on codewords, and there is no need to distinguish them.

The code corrects errors for which $E^\dagger F \notin N(S) \setminus S$ for all possible pairs of errors (E, F) .

Application: 5-Qubit Code

We can generate good codes by picking an appropriate stabilizer. For instance:

$X \otimes Z \otimes Z \otimes X \otimes I$	$n = 5$ physical qubits
$I \otimes X \otimes Z \otimes Z \otimes X$	- 4 generators of S
$X \otimes I \otimes X \otimes Z \otimes Z$	$k = 1$ encoded qubit
$Z \otimes X \otimes I \otimes X \otimes Z$	Distance d of this code is 3.

Notation: $[[n,k,d]]$ for a QECC encoding k logical qubits in n physical qubits with distance d . The five-qubit code is a non-degenerate $[[5,1,3]]$ QECC.

CSS Codes

We can then define a quantum error-correcting code by choosing two classical linear codes C_1 and C_2 , and replacing the parity check matrix of C_1 with Z 's and the parity check matrix of C_2 with X 's.

E.g.: $[[7,1,3]]$ QECC

$Z \otimes Z \otimes Z \otimes Z \otimes I \otimes I \otimes I$	} $C_1: [7,4,3]$ Hamming
$Z \otimes Z \otimes I \otimes I \otimes Z \otimes Z \otimes I$	
$Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z$	} $C_2: [7,4,3]$ Hamming
$X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I$	
$X \otimes X \otimes I \otimes I \otimes X \otimes X \otimes I$	
$X \otimes I \otimes X \otimes I \otimes X \otimes I \otimes X$	

Fault-Tolerant Quantum Computation

In order to perform computations while still protected against errors, we need **fault-tolerant quantum computation**, which tells us how to perform gates between qubits encoded in a QECC.

- Error propagation is a problem. We must arrange the gates so that a single error does not cause multiple errors in a single block of the code.
- The seven-qubit code is particularly good for fault-tolerant computation. Many encoded gates can be performed directly for the seven-qubit code, but a few need more complicated procedures involving measurements and special extra ("ancilla") states.

Fault-Tolerant Threshold

A fault-tolerant protocol provides a way to take a quantum computer with imperfect gates and make it more reliable by encoding it in a QECC.

But then we can encode it again to make it even more reliable, and again, and again This is a **concatenated code**.

Threshold theorem: If the error rate per gate or time step is below some threshold value, then arbitrarily long reliable quantum computations are possible.

The value of the threshold is known to be at least 10^{-3} , one error per 1,000 steps.

Summary

- Quantum error-correcting codes exist which can correct very general types of errors on quantum systems.
- A systematic theory of QECCs allows us to build many interesting quantum codes.
- Fault-tolerant protocols enable us to accurately perform quantum computations even if the physical components are not completely reliable, provided the error rate is below some threshold value.

Quantum Error Correction Sonnet

We cannot clone, perforce; instead, we split
Coherence to protect it from that wrong
That would destroy our valued quantum bit
And make our computation take too long.

Correct a flip and phase - that will suffice.
If in our code another error's bred,
We simply measure it, then God plays dice,
Collapsing it to X or Y or Zed.

We start with noisy seven, nine, or five
And end with perfect one. To better spot
Those flaws we must avoid, we first must strive
To find which ones commute and which do not.

With group and eigenstate, we've learned to fix
Your quantum errors with our quantum tricks.

Further Information

- Short intro. to QECCs: quant-ph/0004072
- Short intro. to fault-tolerance: quant-ph/0701112
- Chapter 10 of Nielsen and Chuang
- Chapter 7 of John Preskill's lecture notes:
<http://www.theory.caltech.edu/~preskill/ph229>
- Threshold proof & fault-tolerance: quant-ph/0504218
- My Ph.D. thesis: quant-ph/9705052
- Complete semester course on QECCs:
<http://perimeterinstitute.ca/personal/dgottesman/QECC2007>