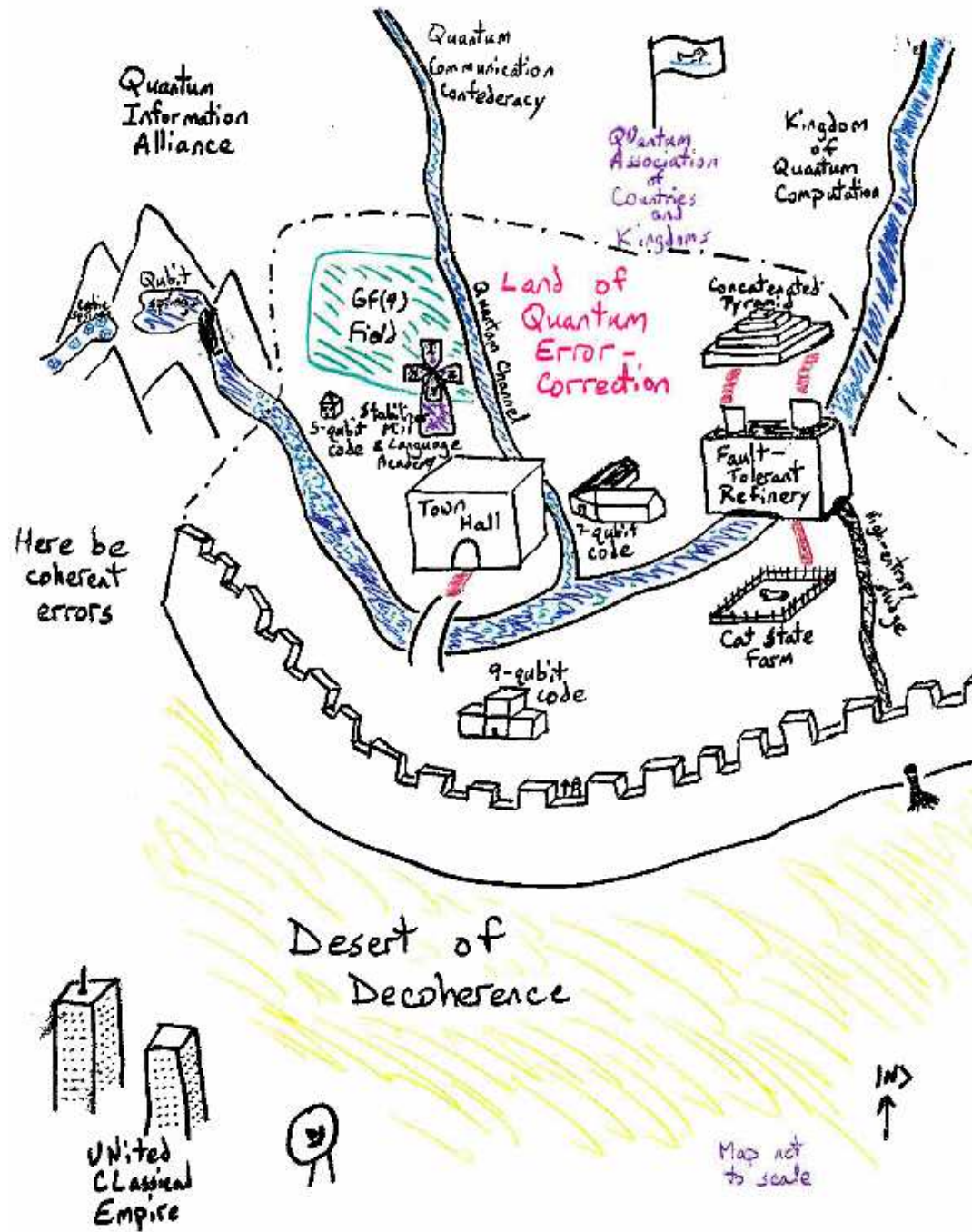


# Quantum Error Correction

Daniel Gottesman  
Perimeter Institute

# The Classical and Quantum Worlds



# Quantum Errors

A general quantum error is a superoperator:

$$\rho \rightarrow \sum A_k \rho A_k^\dagger$$

Examples of single-qubit errors:

**Bit Flip X:**  $X |0\rangle = |1\rangle, X |1\rangle = |0\rangle$

**Phase Flip Z:**  $Z |0\rangle = |0\rangle, Z |1\rangle = -|1\rangle$

**Complete dephasing:**  $\rho \rightarrow 1/2(\rho + Z\rho Z^\dagger)$   
(decoherence)

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

# Classical Repetition Code

To correct a single bit-flip error for classical data, we can use the repetition code:

$$0 \rightarrow 000$$

$$1 \rightarrow 111$$

If there is a single bit flip error, we can correct the state by choosing the majority of the three bits, e.g.  $010 \rightarrow 0$ . When errors are rare, one error is more likely than two.

# Barriers to Quantum Error Correction

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?

# Measurement Destroys Superpositions?

Let us apply the classical repetition code to a quantum state to try to correct a bit flip error:

$$\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |000\rangle + \beta |111\rangle$$

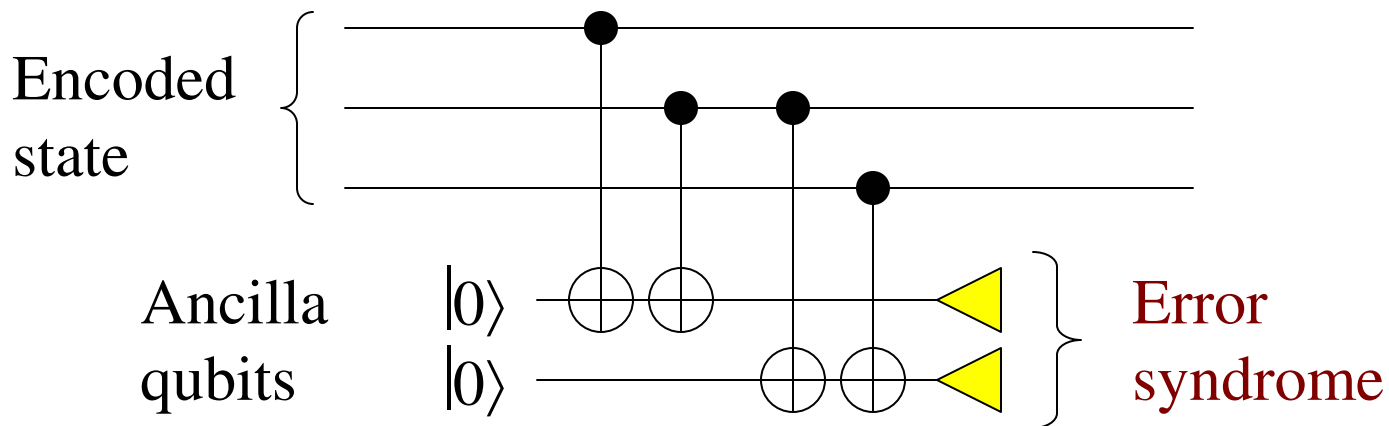
Bit flip error (X) on 2nd qubit:

$$\alpha |010\rangle + \beta |101\rangle$$

2nd qubit is now **different** from 1st and 3rd. We wish to measure that it is different without finding its actual value.

# 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  $\alpha$  and  $\beta$ .

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

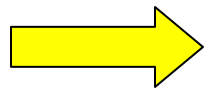
Hadamard transform H exchanges bit flip and phase errors:

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

$$X |+\rangle = |+\rangle, X |-\rangle = -|-\rangle \text{ (acts like phase flip)}$$

$$Z |+\rangle = |-\rangle, Z |-\rangle = |+\rangle \text{ (acts like bit flip)}$$

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:

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

# 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

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

$$\begin{aligned} R_{\theta} &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \\ &= \cos(\theta/2) I - i \sin(\theta/2) Z \end{aligned}$$


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

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

# Correcting Continuous Rotations

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

$$\begin{aligned} R_{\theta}^{(k)} |\psi\rangle &= \cos(\theta/2) |\psi\rangle - i \sin(\theta/2) Z^{(k)} |\psi\rangle \\ \longrightarrow & \cos(\theta/2) |\psi\rangle |I\rangle - i \sin(\theta/2) Z^{(k)} |\psi\rangle |Z^{(k)}\rangle \end{aligned}$$

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.



# Small Error on Every Qubit

Suppose we have a small error  $U_\varepsilon$  on every qubit in the QECC, where  $U_\varepsilon = I + \varepsilon E$ .

Then

$$U_\varepsilon^{\otimes n} |\psi\rangle = |\psi\rangle + \varepsilon(E^{(1)} + \dots + E^{(n)}) |\psi\rangle + O(\varepsilon^2).$$

If the code corrects one-qubit errors, it corrects the sum of the  $E^{(i)}$ s. Therefore it corrects the  $O(\varepsilon)$  term, and the state remains correct to order  $\varepsilon^2$ .

A code correcting  $t$  errors keeps the state correct to order  $\varepsilon^{t+1}$ .

# 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

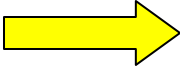
The stabilizer is a group:

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)   $MN = NM$

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:

$$\begin{array}{l} X \otimes Z \otimes Z \otimes X \otimes I \\ I \otimes X \otimes Z \otimes Z \otimes X \\ X \otimes I \otimes X \otimes Z \otimes Z \\ Z \otimes X \otimes I \otimes X \otimes Z \end{array}$$

$n = 5$  physical qubits

- 4 generators of  $S$

$k = 1$  encoded qubit

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.

# Classical Linear Codes

A large and useful family of classical error-correcting codes can be defined similarly, using a **parity check matrix**. Let  $H$  be a  $(n-k) \times n$  binary matrix, and define a classical error-correcting code  $C$  of  $n$ -bit vectors by

$$v \in C \iff Hv = 0.$$

$C$  is linear:  $v, w \in C \Rightarrow v+w \in C$ . Also, let the **distance**  $d$  of  $C$  be the weight (# of non-zero entries) of the smallest non-zero  $v \in C$ . Then **a code with distance  $2t+1$  corrects  $t$  errors**: the error syndrome of error  $e$  is  $He$ , and  $He = Hf$  only if  $e+f \in C$ .

# Classical Hamming Codes

Define a parity check matrix whose columns are all vectors of length  $r$ . E.g., for  $r=3$ :

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

**This code has distance 3:** if error  $e$  has weight 1, the error syndrome  $He$  specifies its location. Thus, the Hamming code for  $r$  is an  **$[n=2^r-1, k=2^r-r-1, d=3]$**  ECC (with  $k$  logical bits encoded in  $n$  physical bits and distance 3).

E.g., for  $r=3$ , we have a  $[7,4,3]$  code.

# Linear Codes and Stabilizers

The classical parity check matrix  $H$  is analogous to the stabilizer  $S$  of a quantum error-correcting code. Indeed, if we **replace all of the 1's of  $H$  with  $Z$  operators**, we get a stabilizer  $S$  defining exactly the same classical code. In particular, it can correct the same number of bit-flip errors.

E.g., Stabilizer of the  $[7,4,3]$  Hamming code:

$$\begin{array}{l} Z \otimes Z \otimes Z \otimes Z \otimes I \otimes I \otimes I \\ Z \otimes Z \otimes I \otimes I \otimes Z \otimes Z \otimes I \\ Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z \end{array}$$

# 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

$$\begin{array}{cccccccc}
 Z \otimes Z \otimes Z \otimes Z \otimes I \otimes I \otimes I \\
 Z \otimes Z \otimes I \otimes I \otimes Z \otimes Z \otimes I \\
 Z \otimes I \otimes Z \otimes I \otimes Z \otimes I \otimes Z \\
 X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I \\
 X \otimes X \otimes I \otimes I \otimes X \otimes X \otimes I \\
 X \otimes I \otimes X \otimes I \otimes X \otimes I \otimes X
 \end{array}$$

$C_1$ : [7,4,3]  
Hamming

$C_2$ : [7,4,3]  
Hamming

# Which CSS Codes Are Possible?

Not all pairs  $C_1$  and  $C_2$  are possible: the stabilizer must be Abelian.

The **dual**  $C^\perp$  of a classical code  $C$  is the set of vectors  $w$  s.t.  $v \cdot w = 0$  for all  $v \in C$ . The rows of the parity check matrix for  $C$  generate  $C^\perp$ .

If  $v \in C_1^\perp$  and  $w \in C_2^\perp$ , the corresponding Pauli operators commute iff  $v \cdot w = 0$ . Thus,  $w \in C_2^\perp$  is also in  $(C_1^\perp)^\perp = C_1$ .

To make a CSS code, we require  $C_2^\perp \subseteq C_1$ .



# Properties of CSS Codes

The parameters of a CSS code made from  $C_1$ , a  $[n, k_1, d_1]$  code, and  $C_2$ , a  $[n, k_2, d_2]$  code, are

$$[[n, k_1 + k_2 - n, d']] \quad \text{with } d' \geq \min(d_1, d_2).$$

Why  $\geq$ ? Because of degeneracy (e.g., 9-qubit code).

Codewords of a CSS code are superpositions of classical codewords: For  $v \in C_1$ ,

$$|\bar{v}\rangle = \sum_{w \in C_2^\perp} |v+w\rangle$$

If  $v-v' \in C_2^\perp$ ,  $|\bar{v}\rangle$  and  $|\bar{v'}\rangle$  are the same state, so  $v$  should run over  $C_1/C_2^\perp$ . (Recall  $C_2^\perp \subseteq C_1$ .)

# 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.
- Stabilizer codes are a large class of codes associated with Abelian groups of operators.
- CSS codes are codes built from pairs of classical linear codes.

# 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
- Longer intro. to QECCs and FT: arXiv:0904.2557 [quant-ph]
- 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>