

Quantum Codes

G. Eric Moorhouse, UW Math

Corrected copies of transparencies for this seminar series should soon be available at

<http://math.uwo.edu/~moorhous/quantum/>

References

P. Shor, 'Quantum computing', proceedings of the International Congress of Mathematicians, 1998.

<http://www.research.att.com/~shor/papers/ICM.pdf>

A.R. Calderbank and P.W. Shor, 'Good quantum error-correcting codes exist', *Phys. Rev. A* **54** (1996), 1098–1105.

A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, 'Quantum error correction via codes over $GF(4)$ ', preprint, 1998.

J. Preskill, 'Fault-tolerant quantum computation', in *Introduction to Quantum Computation and Information*, H.-K. Lo, S. Popescu, and T. Spiller, 1998, pp.213–269.

A.M. Steane, 'Quantum error correction', in *Introduction to Quantum Computation and Information*, H.-K. Lo, S. Popescu, and T. Spiller, 1998, pp.184–212.

The No-Cloning Theorem

Unlike conventional bits, qubits cannot be cloned.

Therefore 'repetition codes' have no analogue in quantum computation. Nevertheless quantum information can be spread throughout many qubits so that a small number of individual qubit errors do not obliterate the data.

Discretized Errors

For simplicity we assume that any qubit error consists in the application of one of the Pauli operators

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (\text{'bit flip error'})$$

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (\text{'phase error'})$$

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i\sigma_x\sigma_z \quad (\text{combination of bit flip and phase errors})$$

and that the three errors σ_x , σ_y , σ_z are all equally likely. Moreover errors in different qubits are statistically independent.

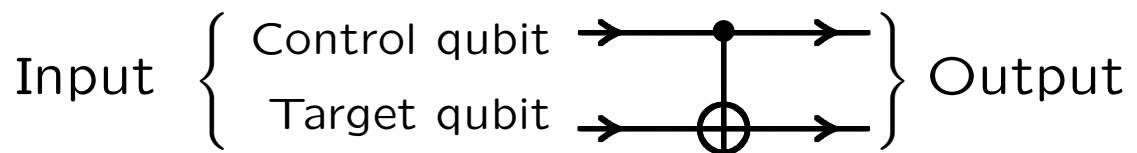
Codes which correct these three errors can also correct more general errors [Bennett, DiVincenzo, Smolin and Wootters (1996); Ekert and Macchiavello (1996); Knill and LaFlamme (1997)].

We'll see how a single qubit can be encoded

(A) as 3 qubits, to allow correction of at most one bit flip error σ_x ; or

(B) as 7 qubits, to allow correction of at most one arbitrary error $\sigma_x, \sigma_y, \sigma_z$.

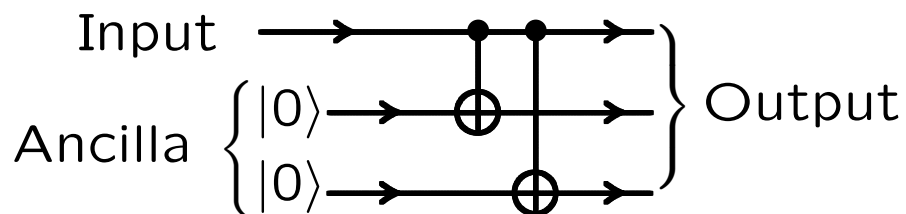
Controlled-Not (CNOT) Gate



$$\begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{array} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

(A) Encoding One Qubit as Three Qubits

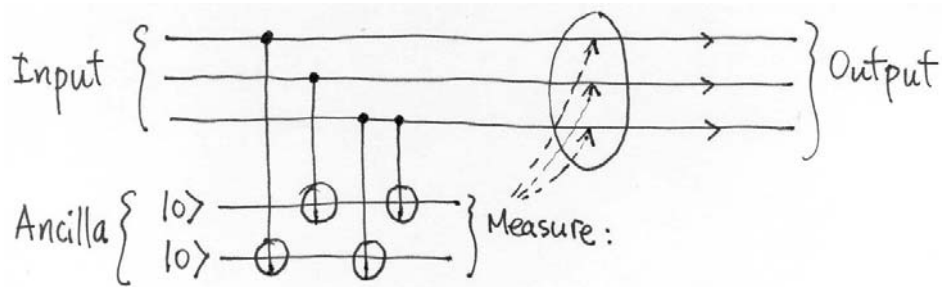
$$|0\rangle \mapsto |000\rangle, \quad |1\rangle \mapsto |111\rangle$$



Ancilla: additional qubits, initialized in state $|0\rangle$

This code corrects up to one bit flip σ_x .

Decoding the Three-Qubit Code (A)



$|00\rangle$: no error
 $|01\rangle$: switch qubit 1
 $|10\rangle$: switch qubit 2
 $|11\rangle$: switch qubit 3

Important: Measuring the ancilla bits reveals the error but not the information qubit.

(B) Encoding One Qubit as Seven Qubits

$$|0\rangle \mapsto \frac{1}{\sqrt{8}} \left(|0000000\rangle + |0001111\rangle + |1100110\rangle \right. \\ \left. + |0111100\rangle + |1010101\rangle + |1101001\rangle \right. \\ \left. + |0110011\rangle + |1011010\rangle \right)$$

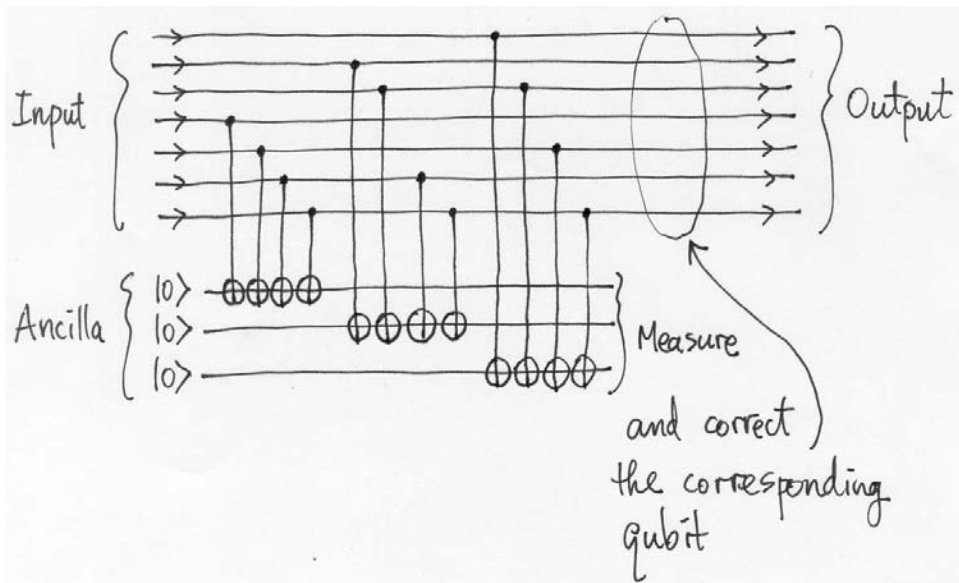
(the sum of all *even*-weight words in the binary Hamming code of length 7)

$$|1\rangle \mapsto \frac{1}{\sqrt{8}} \left(|1111111\rangle + |1110000\rangle + |0011001\rangle \right. \\ \left. + |1000111\rangle + |0101010\rangle + |0010110\rangle \right. \\ \left. + |1001100\rangle + |0100101\rangle \right)$$

(the sum of all *odd*-weight words in the binary Hamming code of length 7)

This code corrects up to one arbitrary bit error σ_x , σ_y or σ_z .

Decoding Bit Flip Errors in the Seven-Qubit Code (B)

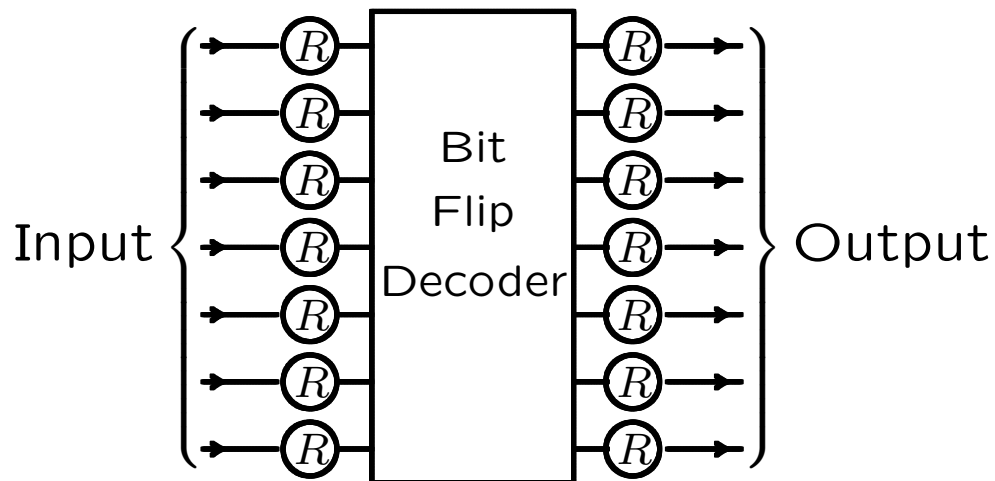


Again, we do not measure the information qubit, only the error.

Decoding Phase Errors in the Seven-Qubit Code (**B**)

Applying $R = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ to an individual qubit transforms phase errors to bit flip errors:

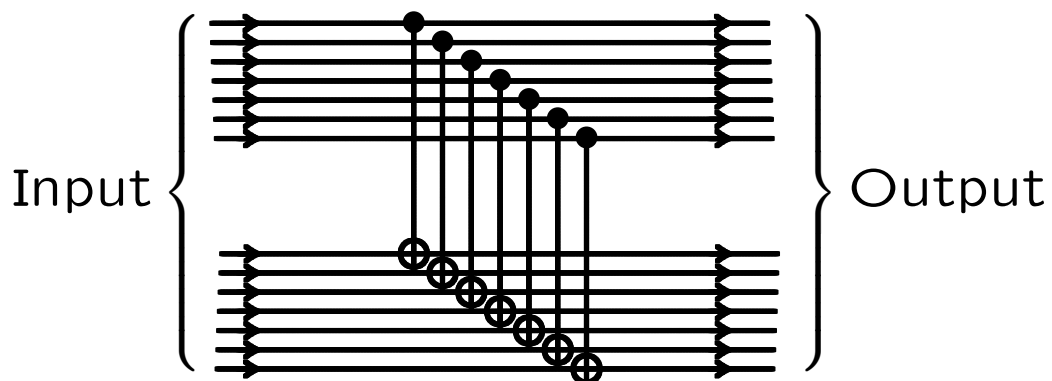
$$\sigma_z = R\sigma_xR$$



Application of Quantum Logic Gates to Encoded Qubits

To apply a CNOT gate to two encoded qubits, for example, to first decode each of the qubits and then apply the single CNOT gate leaves the qubits vulnerable to error.

Instead use seven individual CNOT gates on the seven individual pairs of qubits:



Correcting Many Qubit Errors

A quantum logic circuit of size t requires gates with error rate at most $O(1/(\log t)^c)$. (Shor, 1996)

To achieve fault tolerance with gates of constant error rate, use *concatenated codes*. (Preskill, 1998)