D.5 Quantum error correction

D.5.a Motivation

Quantum coherence is very difficult to maintain for long.[19] Even weak interactions with the environment can affect the quantum state, and we've seen that the amplitudes of the quantum state are critical to quantum algorithms. On classical computers, bits are represented by very large numbers of particles (but that is changing). On quantum computers, qubits are represented by atomic-scale states or objects (photons, nuclear spins, electrons, trapped ions, etc.). They are very likely to become entangled with computationally irrelevant states of the computer and its environment, which are out of our control. Quantum error correction is similar to classical error correction in that additional bits are introduced, creating redundancy that can be used to correct errors. It is different from classical error correction in that: (a) We want to restore the entire quantum state (i.e., the continuous amplitudes), not just 0s and 1s. Further, errors are continuous and can accumulate. (b) It must obey the no-cloning theorem. (c) Measurement destroys quantum information.

D.5.b Effect of decoherence

Ideally the environment $|\Omega\rangle$, considered as a quantum system, does not interact with the computational state. But if it does, the effect can be categorized as a unitary transformation on the environment-qubit system. Consider decoherence operator D describing a bit flip error in a single qubit (Fig. III.36):

$$D : \left\{ \begin{array}{lcl} |\Omega\rangle|0\rangle & \Longrightarrow & |\Omega_{00}\rangle|0\rangle + |\Omega_{10}\rangle|1\rangle \\ |\Omega\rangle|1\rangle & \Longrightarrow & |\Omega_{01}\rangle|0\rangle + |\Omega_{11}\rangle|1\rangle \end{array} \right. .$$

In this notation the state vectors $|\Omega_{xy}\rangle$ are not normalized, but incorporate the amplitudes of the various outcomes. In the case of no error, $|\Omega_{00}\rangle = |\Omega_{11}\rangle = |\Omega\rangle$ and $|\Omega_{01}\rangle = |\Omega_{10}\rangle = \mathbf{0}$. If the entanglement with the environment is small, then $\|\Omega_{01}\|, \|\Omega_{10}\| \ll 1$ (small exchange of amplitude).

Define *decoherence operators* $D_{xy}|\Omega\rangle \stackrel{\text{def}}{=} |\Omega_{xy}\rangle$, for $x, y \in \mathbf{2}$, which describe the effect of the decoherence on the environment. (These are not unitary, but are the products of scalar amplitudes and unitary operators for the various

[19] This section follows Rieffel & Polak (2000).

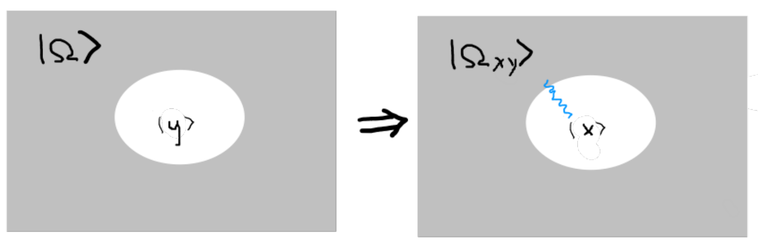

Figure III.36: Effects of decoherence on a qubit. On the left is a qubit $|y\rangle$ that is mostly isoloated from its environment $|\Omega\rangle$. On the right, a weak interaction between the qubit and the environment has led to a possibly altered qubit $|x\rangle$ and a correspondingly (slightly) altered environment $|\Omega_{xy}\rangle$.

outcomes.) Then the evolution of the joint system is defined by the equations:

$$\begin{aligned}
D|\Omega\rangle|0\rangle &= (D_{00} \otimes I + D_{10} \otimes X)|\Omega\rangle|0\rangle, \\
D|\Omega\rangle|1\rangle &= (D_{01} \otimes X + D_{11} \otimes I)|\Omega\rangle|1\rangle.
\end{aligned}$$

Alternately, we can define it:

$$D = D_{00} \otimes |0\rangle\langle 0| + D_{10} \otimes |1\rangle\langle 0| + D_{01} \otimes |0\rangle\langle 1| + D_{11} \otimes |1\rangle\langle 1|.$$

Now, it's easy to show (Exer. III.20):

$$|0\rangle\langle 0| = \frac{1}{2}(I+Z), |0\rangle\langle 1| = \frac{1}{2}(X-Y), |1\rangle\langle 0| = \frac{1}{2}(X+Y), |1\rangle\langle 1| = \frac{1}{2}(I-Z),$$

where $Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Therefore

$$\begin{aligned}
D &= \frac{1}{2}[D_{00} \otimes (I+Z) + D_{01} \otimes (X-Y) + \\
&\quad D_{10} \otimes (X+Y) + D_{11} \otimes (I-Z)] \\
&= \frac{1}{2}[(D_{00}+D_{11}) \otimes I + (D_{10}+D_{01}) \otimes X + \\
&\quad (D_{10}-D_{01}) \otimes Y + (D_{00}-D_{11}) \otimes Z].
\end{aligned}$$

Therefore the bit flip error can be described as a linear combination of the Pauli matrices. It is generally the case that the effect of decoherence on a single qubit can be described by a linear combination of the Pauli matrices, which is important, since qubits are subject to various errors beside bit flips. This is a distinctive feature about quantum errors: they have a finite basis, and because they are unitary, they are therefore invertible. In other words, single-qubit errors can be characterized in terms of a linear combination of the Pauli matrices (which span the space of 2×2 self-adjoint unitary matrices: C.2.a, p. 112): I (no error), X (bit flip error), Y (phase error), and $Z = YX$ (bit flip phase error). Therefore a single qubit error is represented by $e_0\sigma_0 + e_1\sigma_1 + e_2\sigma_2 + e_3\sigma_3 = \sum_{j=0}^{3} e_j\sigma_j$, where the σ_j are the Pauli matrices (Sec. C.2.a, p. 111).

D.5.c Correcting the quantum state

We consider a basis set of unitary "error operators" E_j, so that the error transformation is a superposition $E \stackrel{\text{def}}{=} \sum_j e_j E_j$. In the more general case

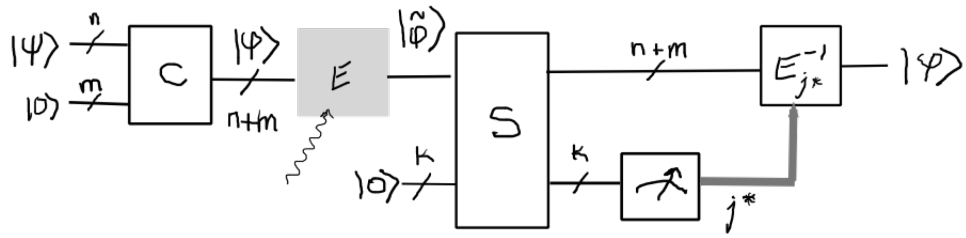

Figure III.37: Circuit for quantum error correction. $|\psi\rangle$ is the n-qubit quantum state to be encoded by C, which adds m error-correction qubits to yield the encoded state $|\phi\rangle$. E is a unitary superposition of error operators E_j, which alter the quantum state to $|\tilde{\phi}\rangle$. S is the syndrome extraction operator, which computes a superposition of codes for the errors E. The syndrome register is measured, to yield a particular syndrome code j^*, which is used to select a corresponding inverse error transformation $E_{j^*}^{-1}$ to correct the error.

of quantum registers, the E_j affect the entire register, not just a single qubit.

algorithm quantum error correction:

Encoding: An n-bit register is encoded in $n+m$ bits, where the extra bits are used for error correction. Let $y \stackrel{\text{def}}{=} C(x) \in \mathbf{2}^{m+n}$ be the $n+m$ bit code for $x \in \mathbf{2}^n$. As in classical error correcting codes, we embed the message in a space of higher dimension.

Error process: Suppose $\tilde{y} \in \mathbf{2}^{m+n}$ is the result of error type k, $\tilde{y} = E_k(y)$.

Syndrome: Let $k = S(\tilde{y})$ be a function that determines the error syndrome, which identifies the error E_k from the corrupted code. That is, $S(E_k(y)) = k$.

Correction: Since the errors are unitary, and the syndrome is known, we can invert the error and thereby correct it: $y = E_{S(\tilde{y})}^{-1}(\tilde{y})$.

Quantum case: Now consider the quantum case, in which the state $|\psi\rangle$ is a superposition of basis vectors, and the error is a superposition of error types, $E = \sum_j e_j E_j$. This is an orthogonal decomposition of E (see Fig. III.37).

Encoding: The encoded state is $|\phi\rangle \stackrel{\text{def}}{=} C|\psi\rangle|\mathbf{0}\rangle$. There are several requirements for a useful quantum error correcting code. Obviously, the codes for orthogonal inputs must be orthogonal; that is, if $\langle\psi \mid \psi'\rangle = 0$, then $C|\psi, \mathbf{0}\rangle$ and $C|\psi', \mathbf{0}\rangle$ are orthogonal: $\langle\psi, \mathbf{0}|C^\dagger C|\psi', \mathbf{0}\rangle = 0$. Next, if $|\phi\rangle$ and $|\phi'\rangle$ are the codes of distinct inputs, we do not want them to be confused by the error processes, so $\langle\phi|E_j^\dagger E_k|\phi'\rangle = 0$ for all i, j. Finally, we require that for each pair of error indices j, k, there is a number m_{jk} such that $\langle\phi|E_j^\dagger E_k|\phi\rangle = m_{jk}$ for every code $|\phi\rangle$. This means that the error syndromes are independent of the codes, and therefore the syndromes can be measured without collapsing superpositions in the codes, which would make them useless for quantum computation.

Error process: Let $|\tilde{\phi}\rangle \stackrel{\text{def}}{=} E|\phi\rangle$ be the code corrupted by error.

Syndrome extraction: Apply the syndrome extraction operator to the encoded state, augmented with enough extra qubits to represent the set of syndromes. This yields a superposition of syndromes:

$$S|\tilde{\phi}, \mathbf{0}\rangle = S\left(\sum_j e_j E_j|\phi\rangle\right) \otimes |\mathbf{0}\rangle = \sum_j e_j(SE_j|\phi\rangle|\mathbf{0}\rangle) = \sum_j e_j(E_j|\phi\rangle|j\rangle).$$

Measurement: Measure the syndrome register to obtain some j^* and the collapsed state $E_{j^*}|\phi\rangle|j^*\rangle$.[20]

Correction: Apply $E_{j^*}^{-1}$ to correct the error.
$\square$

[20] As we mentioned the discussion of in Shor's algorithm (p. 150), it is not necessary to actually perform the measurement; the same effect can be obtained by unitary operations.

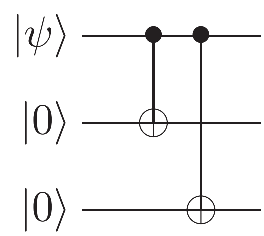

Figure III.38: Quantum encoding circuit for triple repetition code. [source: NC]

Note the remarkable fact that although there was a superposition of errors, we only have to correct one of them to get the original state back. This is because measurement of the error syndrome collapses into a state affected by just that one error.

D.5.d Example

We'll work through an example to illustrate the error correction process. For an example, suppose we use a simple triple redundancy code that assigns $|0\rangle \mapsto |000\rangle$ and $|1\rangle \mapsto |111\rangle$. This is accomplished by a simple quantum gate array:

$$C|0\rangle|00\rangle = |000\rangle, \quad C|1\rangle|00\rangle = |111\rangle.$$

This is not a sophisticated code! It's called a *repetition code*. The three-qubit codes are called *logical zero* and *logical one* (See Fig. III.38). This code can correct single bit flips (*by majority voting*); the errors are represented by the operators:

$$\begin{aligned} E_0 &= I \otimes I \otimes I \\ E_1 &= I \otimes I \otimes X \\ E_2 &= I \otimes X \otimes I \\ E_3 &= X \otimes I \otimes I. \end{aligned}$$

The following works as a syndrome extraction operator:

$$S|x_3, x_2, x_1, 0, 0, 0\rangle \stackrel{\text{def}}{=} |x_3, x_2, x_1, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3\rangle.$$

The $\oplus$s compare each pair of bits, and so the $\oplus$ will be zero if the two bits are the same (the majority). The following table shows the bit flipped (if any), the corresponding syndrome, and the operator to correct it (which is the same as the operator that caused the error):

bit flipped	syndrome	error correction
none	$\|000\rangle$	$I \otimes I \otimes I$
1	$\|110\rangle$	$I \otimes I \otimes X$
2	$\|101\rangle$	$I \otimes X \otimes I$
3	$\|011\rangle$	$X \otimes I \otimes I$

(Note that the correction operators need not be the same as the error operators, although they are in this case.)

For an example, suppose we want to encode the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Its code is $|\phi\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. Suppose the following error occurs: $E = \frac{4}{5}X \otimes I \otimes I + \frac{3}{5}I \otimes X \otimes I$ (that is, the bit 3 flips with probability 16/25, and bit 2 with probability 9/25). The resulting error state is

$$
\begin{aligned}
|\tilde{\phi}\rangle &= E|\phi\rangle \\
&= \left(\frac{4}{5}X \otimes I \otimes I + \frac{3}{5}I \otimes X \otimes I\right)\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \\
&= \frac{4}{5\sqrt{2}}X \otimes I \otimes I(|000\rangle - |111\rangle) + \frac{3}{5\sqrt{2}}I \otimes X \otimes I(|000\rangle - |111\rangle) \\
&= \frac{4}{5\sqrt{2}}(|100\rangle - |011\rangle) + \frac{3}{5\sqrt{2}}(|010\rangle - |101\rangle).
\end{aligned}
$$

Applying the syndrome extraction operator yields:

$$
\begin{aligned}
S|\tilde{\phi}, 000\rangle &= S\left[\frac{4}{5\sqrt{2}}(|100000\rangle - |011000\rangle) + \frac{3}{5\sqrt{2}}(|010000\rangle - |101000\rangle)\right] \\
&= \frac{4}{5\sqrt{2}}(|100011\rangle - |011011\rangle) + \frac{3}{5\sqrt{2}}(|010101\rangle - |101101\rangle) \\
&= \frac{4}{5\sqrt{2}}(|100\rangle - |011\rangle) \otimes |011\rangle + \frac{3}{5\sqrt{2}}(|010\rangle - |101\rangle) \otimes |101\rangle
\end{aligned}
$$

Measuring the syndrome register yields either $|011\rangle$ (representing an error in bit 3) or $|101\rangle$ (representing an error in bit 2). Suppose we get $|011\rangle$. The state collapses into:

$$
\frac{1}{\sqrt{2}}(|100\rangle - |011\rangle) \otimes |011\rangle.
$$

Note that we have projected into a subspace for just one of the two bit-flip errors that occurred (the flip in bit 3). The measured syndrome $|011\rangle$ tells us to apply $X \otimes I \otimes I$ to the first three bits, which restores $|\phi\rangle$:

$$(X \otimes I \otimes I)\frac{1}{\sqrt{2}}(|100\rangle - |011\rangle) = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = |\phi\rangle.$$

We can do something similar to correct single phase flip (Z) errors by using the encoding $|0\rangle \mapsto |+++\rangle$, $|1\rangle \mapsto |---\rangle$ (Exer. III.55). To see this, recall that Z in the sign basis is the analog of X is the computational basis.

D.5.e Discussion

There is a nine-qubit code, called the *Shor code*, that can correct arbitrary errors on a single qubit, even replacing the entire qubit by garbage (Nielsen & Chuang, 2010, §10.2). The essence of this code is that triple redundancy is used to correct X errors, and triple redundancy again to correct Z errors, thus requiring nine code qubits for each logical qubut. Since $Y = ZX$ and the Pauli matrices are a basis, this code is able to correct all errors.

Quantum error correction is remarkable in that an entire continuum of errors can be corrected by correcting only a discrete set of errors. This works in quantum computation, but not classical analog computing. The general goal in syndrome extraction is to separate the syndrome information from the computational information in such a way that the syndrome can be measured without collapsing any of the computational information. Since the syndrome is unitary, it can be inverted to correct the error.

What do we do about noise in the gates that do the encoding and decoding? It is possible to do *fault-tolerant quantum computation*. "Even more impressively, fault-tolerance allow us to perform logical operations on encoded quantum states, in a manner which tolerates faults in the underlying gate operations." (Nielsen & Chuang, 2010, p. 425) Indeed, "provided the noise in individual quantum gates is below a certain constant threshold it is possible to efficiently perform an arbitrarily large quantum computation." (Nielsen & Chuang, 2010, p. 425)[21]

[21] See Nielsen & Chuang (2010, §10.6.4).