Introduction to Quantum Error Correction

Jonathan Webb

This note is intended to provide an introduction to quantum error correction accessible to somebody comfortable with linear algebra and the notion of a group. We describe how quantum information is represented, what kinds of errors may affect it, and give a general procedure for quantum error correction. We then provide examples of quantum error correcting codes, eventually arriving at the Shor code. We finish by introducing the stabilizer formalism for quantum error correction.

1. Preliminaries

In this section, we explain the bra-ket, or Dirac, notation commonly used when discussing quantum mechanics and related areas. We also discuss a few items from linear algebra that the reader is not assumed to be familiar with, such as the tensor product.

When using bra-ket notation, the vector v is represented by $|v\rangle$. We use $\langle v|$ to represent the Hermitian adjoint $|v\rangle^\dagger$ of $|v\rangle$. The inner product of two vectors $|v\rangle$ and $|u\rangle$ is given by $\langle v|u\rangle$. Given a matrix A, the inner product between $|v\rangle$ and $A|u\rangle$ is given by $\langle v|A|u\rangle$. Given a Hilbert space $\mathcal{H}$, let $W \subseteq \mathcal{H}$ be a subspace spanned by an orthonormal basis $|1\rangle, \ldots, |n\rangle$. The projector P into W is the operator given by

$$P = \sum_{i=1}^{n} |i\rangle\langle i|.$$

We now explain the tensor product operation informally. Given an $m \times n$ matrix A and a $p \times q$ matrix B, the tensor product $A \otimes B$ is the $pm \times qn$ block matrix:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

We may take tensor products of vector spaces. The tensor product $V \otimes W$ of two vector spaces V and W with bases B_V and B_W, respectively, has as its basis the set

$$\{|v\rangle \otimes |w\rangle : |v\rangle \in B_V, |w\rangle \in B_W\}.$$

When discussing how quantum errors are detected, we will use the following fact often:

$$\text{If } Ax = \lambda x \text{ and } By = \mu y, \text{ then } (A \otimes B)(x \otimes y) = \lambda\mu(x \otimes y). \tag{1}$$

2. Quantum error correction

While classical information is carried by strings of bits, we think of quantum information as being given by the state of a qubit, or quantum bit. We use the common bra-ket notation $|v\rangle$ to represent the vector v. The state of a qubit is given by the vector

$$|\psi\rangle = a|0\rangle + b|1\rangle \in \mathcal{H} \cong \mathbb{C}^2$$

where $|0\rangle = e_1$ and $|1\rangle = e_2$, $a, b \in \mathbb{C}$, and $|a|^2 + |b|^2 = 1$. The complex numbers a and b are called amplitudes. The state $|\psi\rangle$ is said to be in a superposition of the states $|0\rangle$ and $|1\rangle$. The amplitudes a and b are said to differ by a relative phase if there is a real θ such that $a = e^{i\theta}b$. More generally, the state of a system of n qubits is in a superposition of the 2^n bitstrings of length n. Given n qubit states $|\psi_1\rangle, \ldots, |\psi_n\rangle$, the state of the total system of these qubits is given by the simple tensor $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$. For brevity, we may omit tensor product symbols, as in $|00\rangle = |0\rangle \otimes |0\rangle$. Many multi-qubit quantum states relevant to quantum error correction cannot be written as simple tensors; these are called entangled states. A procedure for preparing an entangled state is given later in this section. An example of an entangled state is the Bell state

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

Qubit states are acted on by operators in the space of 2×2 complex matrices. The Pauli matrices I, X, Y, Z are a set of Hermitian, unitary, and involutory matrices which form a basis for $M_{2,2}(\mathbb{C})$.

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The action of each Pauli matrix corresponds to an error on one qubit. For some $|\psi\rangle = a|0\rangle + b|1\rangle$,

$$\begin{aligned} I|\psi\rangle &= |\psi\rangle \\ X|\psi\rangle &= a|1\rangle + b|0\rangle \\ Y|\psi\rangle &= i(a|1\rangle - b|0\rangle) \\ Z|\psi\rangle &= a|0\rangle - b|1\rangle. \end{aligned}$$

Because of their effects, the Pauli X and Z gates are often called the bit flip and phase flip gates, respectively. Operators acting on multiple qubits are given by taking tensor products of the Pauli matrices. For example,

$$(X \otimes Y \otimes Z)(|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle) = X|\psi_1\rangle \otimes Y|\psi_2\rangle \otimes Z|\psi_3\rangle.$$

A notion central to quantum theory is measurement. Given a qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$, there exists a measurement operation which takes $|\psi\rangle$ to $|0\rangle$ with probability $|a|^2$, and to $|1\rangle$ with probability $|b|^2$. A projective measurement is associated with an observable, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

$$M = \sum_{\lambda} \lambda P_{\lambda},$$

where P_λ is the projector into the eigenspace of M with eigenvalue λ. The possible outcomes of the measurement are associated with the eigenvalues λ. Upon measuring the state $|\psi\rangle$, the probability of observing the outcome associated with λ is given by

$$p(\lambda) = \langle\psi|P_\lambda|\psi\rangle.$$

Given that outcome λ occurred, the state of the quantum system immediately after the measurement is

$$\frac{P_\lambda|\psi\rangle}{\sqrt{p(\lambda)}}.$$

In what follows, we invoke the notion of measurement in a particular way: given a state $|\psi\rangle$ and an observable M, we say "measure M" to mean "determine the eigenvalue of $|\psi\rangle$ with respect to M".

We are now ready to discuss quantum codes. The need for quantum error correction is straightforward: quantum information, in storage or transmission, may suffer errors due to noise in its environment. We would like some procedure to correct these errors. Given a state $|\psi\rangle$, the general procedure goes as follows:

1. Encode $|\psi\rangle$ as a state that is more robust to error. This involves introducing redundancy in the sense that the encoded state will be composed of more qubits than $|\psi\rangle$. When working with classical information, it is possible to replicate strings of bits and use a majority voting procedure to correct error. By the no-cloning theorem, it is not possible to replicate an arbitrary quantum state. One way to introduce redundancy is to encode $|\psi\rangle$ as an entangled state. For example, to encode $|1\rangle$ as $|111\rangle$, we take the tensor product $|10\rangle$ and apply to it the CNOT gate, which flips the second qubit only if the first is $|1\rangle$. This yields the state $|11\rangle$. We then take the tensor product $|110\rangle$ and apply the CNOT gate to the first and third qubits, giving the state $|111\rangle$.

The encoded state is called a codeword, and the set of codewords comprises a code.

2. We allow the encoded state to experience error. We then perform measurements on the qubits of the corrupted state to determine which error occurred.

3. We apply a recovery (error correction) procedure informed by the result of the previous step.

Before discussing specific codes, we state an important point: If a code can detect or correct some set $\{E_i\}$ of errors, it can also detect or correct linear combinations of the E_i. In particular, a code capable of correcting the Pauli errors X, Y, and Z on a single qubit is capable of correcting arbitrary errors on that qubit.

3. Three quantum error correcting codes

Suppose we wish to send the qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$ across a noisy channel which will apply the Pauli X gate with probability p while leaving $|\psi\rangle$ unchanged with probability $1 - p$. Following the format given above, we can perform the following procedure to correct this error:

1. Encode $|\psi\rangle$ as $a|000\rangle + b|111\rangle$. Then the code is the space spanned by $\{|000\rangle, |111\rangle\}$, subject to the constraints on the norms of a and b. We may call this code the $|0\rangle, |1\rangle$-repetition code; it is often called the bit flip code as well.

2. We allow the codeword to experience error by sending each of the three qubits through an independent channel. To detect error, we measure the observables $Z \otimes Z \otimes I$ and $I \otimes Z \otimes Z$. By (1), both of these observables have eigenvalues ± 1, so there are four pairs of measurements we may obtain. In particular, the observable $Z \otimes Z$ has eigenvalue $+1$ for the states $|00\rangle$ and $|11\rangle$, and eigenvalue -1 for the states $|01\rangle$ and $|10\rangle$. These measurements amount to a comparison of the first and second qubits, and the second and third qubits, of the corrupted state, without revealing the amplitudes a and b.

3. We use the measurements obtained in the previous step to tell us what procedure to use to recover the initial state. For example, suppose that the measurement result for $(Z \otimes Z \otimes I, I \otimes Z \otimes Z)$ was $(-1, -1)$. Then the first and second qubits differ, and the second and third qubits

differ. Assuming at most one error, it follows that the second qubit flipped. We may correct this by flipping the second qubit again, via an application of the operator $I \otimes X \otimes I$.

Before describing a quantum code capable of correcting phase flip errors, we first consider a certain relationship between the X and Z gates. Define the Hadamard gate,

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

We have that $HXH = Z$. The Z matrix has $|0\rangle$ and $|1\rangle$ as its $+1$ and -1 eigenvectors, respectively. Define the vectors

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}.$$

We have that the X matrix has $|+\rangle$ and $|-\rangle$ as its $+1$ and -1 eigenvalues, respectively. Also,

$$H|0\rangle = |+\rangle \quad \text{and} \quad H|1\rangle = |-\rangle.$$

Then the Hadamard matrix allows us to move between the $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle$ bases, while interchanging the effects of the X and Z matrices.

We now consider a situation which does not have a direct classical analogue. Suppose we wish to send the qubit state $|\psi\rangle$ across a noisy channel which will apply the Pauli Z gate with probability p while leaving $|\psi\rangle$ unchanged with probability $1 - p$. We may perform the following procedure to correct this error:

1. We perform a two-step encoding. First, we map $|\psi\rangle$ to $a|000\rangle + b|111\rangle$, as in the $|0\rangle, |1\rangle$-repetition code. We then apply the Hadamard gate to each qubit, giving the codeword $a|{+}{+}{+}\rangle + b|{-}{-}{-}\rangle$. Then the code is the space spanned by $\{|{+}{+}{+}\rangle, |{-}{-}{-}\rangle\}$, subject to the constraint on the norms of a and b. We may call this code the $|+\rangle, |-\rangle$-repetition code; it is often called the phase flip code as well.

2. We allow the codeword to experience error by sending each of the three qubits through an independent channel. Let

$$H^{\otimes n} = \underbrace{H \otimes \cdots \otimes H}_{n \text{ times}}$$

Then, to detect error, we may measure the observables

$$H^{\otimes 3}(Z \otimes Z \otimes I)H^{\otimes 3} = X \otimes X \otimes I$$

and

$$H^{\otimes 3}(I \otimes Z \otimes Z)H^{\otimes 3} = I \otimes X \otimes X.$$

These measurements perform a task analogous to what was done in the error detection step associated with the $|0\rangle, |1\rangle$-repetition code. By (1), the observable $X \otimes X$ has eigenvalue $+1$ for $|++\rangle$ and $|--\rangle$, and eigenvalue -1 for $|+-\rangle$ and $|-+\rangle$. Then measuring the given observables amounts to comparing the sign of the first and second qubits, and of the second and third qubits. As with the previous code, these comparisons are performed without revealing information about a or b.

3. We use the measurements obtained in the previous step to tell us what procedure to use to recover the initial state. For example, suppose that the measurement result for $(X \otimes X \otimes I, I \otimes X \otimes X)$ is $(1, -1)$. Then the first and second qubits are the same, while the second and third qubits are different. Assuming at most one error, it follows that the phase of the third qubit was flipped. We may correct this by flipping the phase of the third qubit again, via an application of the operator $I \otimes I \otimes Z$.

In summary, the $|+\rangle, |-\rangle$-repetition code is essentially the $|1\rangle, |0\rangle$-repetition code under a change of basis. By combining both codes in what is known as the Shor code, we are able to correct an arbitrary error on one qubit. The procedure for using the Shor code is as follows:

1. As in the $|+\rangle, |-\rangle$-repetition code, we encode $|\psi\rangle = a|0\rangle + b|1\rangle$ as $a|+++\rangle + b|---\rangle$. We then encode each of these three qubits as in the $|0\rangle, |1\rangle$-repetition code: $|+\rangle$ is encoded as $(|000\rangle + |111\rangle)\sqrt{2}$ and $|-\rangle$ is encoded as $(|000\rangle - |111\rangle)\sqrt{2}$. The result is a nine qubit code, with codewords given by:

$$|0\rangle \to \frac{(|000\rangle + |111\rangle)^{\otimes 3}}{2\sqrt{2}}$$
$$|1\rangle \to \frac{(|000\rangle - |111\rangle)^{\otimes 3}}{2\sqrt{2}}.$$

2. We allow the codeword to experience error by sending each of the nine qubits through an independent channel. The Shor code is able to protect against bit and phase flip errors by a simple extension of the procedures associated with the previously discussed codes. We may detect

a bit flip error on, for example, the fifth qubit, by measuring

$$I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I \otimes I$$

and

$$I \otimes I \otimes I \otimes I \otimes Z \otimes Z \otimes I \otimes I \otimes I.$$

For brevity, we adopt a notation whereby Is and tensor product symbols are omitted, and a subscript is used to indicate to which qubit an operator is being applied. The above operators are then written as Z_4Z_5 and Z_5Z_6. By the same argument as for the $|0\rangle, |1\rangle$-repetition code, we use the pair of measurement outcomes to determine whether the fifth qubit flipped.

We detect phase flip errors in a similar way, although we perform measurements on blocks of three qubits rather than on the nine individual qubits. Suppose we wish to detect a phase flip error on one of the first three qubits. Such an error flips the sign of the first block of qubits, changing $|000\rangle \pm |111\rangle$ to $|000\rangle \mp |111\rangle$. Therefore to detect this error it suffices to compare the sign of the first and second blocks of qubits, and the sign of the second and third blocks. This is done by measuring the observables $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$. In general, we may detect bit and phase flips on any one of the nine qubits by measuring the set of observables:

$$\{Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9,$$
$$X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9\}.$$

3. Assuming at most one qubit was affected by bit and/or phase flips, we may correct these errors in the ways described for the previous codes. A bit flip error on the ith qubit is corrected by applying the operator X_i, and a phase flip error on one qubit in the ith block is corrected by applying the operator $Z_{3i-2}Z_{3i-1}Z_{3i}$.

Notice that the procedures for detecting and correcting bit and phase flip errors are distinct. It follows that a simultaneous bit and phase flip error on the same qubit may be corrected by the procedure given above. Furthermore, this procedure corrects an arbitrary error. Let

$$E = a_0I + a_1X + a_2Z + a_3XZ$$

be an arbitrary error affecting one qubit of the codeword $|\psi\rangle$ (note that $Y = iXZ$). Then the unnormalized corrupted state $E|\psi\rangle$ is a superposition of the

four terms

$$|\psi\rangle, X|\psi\rangle, Z|\psi\rangle, XZ|\psi\rangle.$$

Measuring which error occurred collapses this superposition into one of the four states comprising it. Since we may recover $|\psi\rangle$ from each of these four states, it follows that the Shor code can correct an arbitrary error on one qubit.

We now introduce a more general framework for specifying quantum error correcting codes.

4. The stabilizer formalism

The three codes in the previous section had a commonality: they were given by the mutual $+1$-eigenspaces of the operators we measured to detect error. The central idea of the stabilizer formalism is that there are many quantum states which are more easily described in terms of the operators that stabilize them — that is, the operators for which they are a $+1$-eigenstate. The stabilizer formalism relies on group theory; the group of interest to us is the Pauli group,

$$G_n = \left\{ i^k \bigotimes_{j=1}^{n} M_j : k \in \{0,1,2,3\}, M_j \in \{I, X, Y, Z\} \right\}$$

on n qubits. It is evident that G_n consists of all n-fold tensor products of the Pauli matrices, with the multiplicative factors ± 1 and $\pm i$. Any two elements of G_n either commute or anticommute with eachother.

The stabilizer S of a code C is the subgroup of G_n consisting of all Pauli operators M with the property that $M|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in C$. In order for C to be nontrivial, we need $-I \notin S$, as $-I|\psi\rangle = |\psi\rangle$ is satisfied only by $|\psi\rangle = 0$. This further implies $\pm iI \notin S$. Additionally, we need S to be abelian. To see why this is necessary, suppose that $M, N \in S$ anticommute. We will deduce a contradiction. We have $-NM = MN$ by assumption, so

$$-|\psi\rangle = -NM|\psi\rangle = MN|\psi\rangle = |\psi\rangle$$

where the first and last equalities are due to the fact that $M, N \in S$. Then $|\psi\rangle = -|\psi\rangle$, so $|\psi\rangle = 0$. Then S stabilizes a trivial code, giving a contradiction.

It is convenient to specify a stabilizer in terms of its generators. As an example, the $|0\rangle, |1\rangle$-repetition code is stabilized by the group

$$S = \{I, Z_1Z_2, Z_1Z_3, Z_2Z_3\},$$

as the intersection of the $+1$-eigenspaces of the elements of S is the set spanned by $\{|000\rangle, |111\rangle\}$. However, we have that $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$, and $I = (Z_1Z_2)^2$. Then any element of S can be written as a product of powers of Z_1Z_2 and Z_2Z_3, so we write $S = \langle Z_1Z_2, Z_2Z_3\rangle$.

We now discuss the errors that a stabilizer code may detect and correct. Let C be stabilized by S, and suppose E commutes with some $M \in S$, so that $ME|\psi\rangle = EM|\psi\rangle = E|\psi\rangle$ for $|\psi\rangle \in C$. Then $E|\psi\rangle$ is a $+1$ eigenstate of M, so E is not detected as an error. Conversely, suppose E and M anticommute so that $E|\psi\rangle$ is a -1 eigenstate of M. Then E is detected as an error. Let $N(S)$ be the set of operators which commute with all $M \in S$. Then C detects errors outside of $N(S) \setminus S$ because errors outside of $N(S)$ anticommute with $M \in S$ and are detected by measuring observables, while errors in S act like the identity by definition and are thus trivial errors. Then errors may be classified as

- detectable (not in $N(S) \setminus S$),
- undetectable (in $N(S)$), or
- trivial (in S).

Correcting an error requires us to know exactly which observable(s) was (were) measured to have a -1 eigenvalue for the corrupted state. We learn this by measuring the eigenvalues of every generator for the stabilizer, as described in the previous section. It can be shown that E and F have the same eigenvalue measurements, and therefore correspond to the same error, if and only if $E^\dagger F \in N(S)$. Then if $E^\dagger F \notin N(S)$, E and F may be distinguished by measuring eigenvalues. Meanwhile, if $E^\dagger F \in S$ then $E|\psi\rangle = F|\psi\rangle$, and we cannot distinguish between the two errors. However, we do not need to as they have the same effect on a given codeword. Then a stabilizer code corrects all pairs of errors (E, F) such that $E^\dagger F \notin N(S) \setminus S$.

5. References

[1] Preskill, John. "Course Information for Physics 219/Computer Science 219 Quantum Computation." Physics 219 Course Information, http://theory.caltech.edu/~preskill/ph229.

[2] Nielsen, Michael A., and Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2022.