CSE 599d - Quantum Computing
The Quantum Error Correcting Criteria

Dave Bacon
Department of Computer Science & Engineering, University of Washington

Now that we have seen that quantum error correction is possible, it is interesting to try to formalize a criteria for why it was possible. In particular we are interested in understanding when it is possible to encode into a subspace such that, for certain errors on the quantum information, we can fix the quantum information from this error. One thing to note that is in the first lecture we discussed encoding quantum information from a bare, unencoded qubit, into a qubit encoded over the subspace. In practice we really want to never do this but instead we want to be able to prepare an encoded quantum state. We therefore won't spend much time discussing encoding into a quantum error correcting code.

I. THE QUANTUM ERROR CORRECTING CRITERIA

Suppose that we have a quantum system which evolves according to some error process which we will represent by the superoperator $\mathcal{D}$. Now we will assume that this superoperator is given by some operator sum representation

$$\mathcal{D}[\cdot] = \sum_k A_k[\cdot]A_k^\dagger \tag{1}$$

Now, in general, our codes will not be able to reverse the effect of all errors on our system: the goal of quantum error correction is to make the probability of error so small that it is effectively zero, not to eliminate the possibility of error completely (although philosophers will argue about the difference between this two: I'm talking to you Henry James (easy to pick on a dead guy.)) It is therefore useful to assume that the Kraus operators in the expansion for $\mathcal{D}$ are made up of some errors $E_i = A_i$, $i \in S$ which we wish to correct. This will be a good assumption because the real error process will contain these terms, which we will then be certain we have fixed, plus the errors which we might not fix. Thus we may think about $\mathcal{D}$ as have Kraus operators, some of which are error E_k and some of which are not. Define $\mathcal{E}$ as the operator,

$$\mathcal{E}[\cdot] = \sum_i E_i[\cdot]E_i^\dagger \tag{2}$$

Notice that $\mathcal{E}$ will not necessarily preserve the trace of a density matrix. This won't stop us from considering reversing it's operation.

Okay, so given $\mathcal{E}$ with some Kraus operators A_k we can ask, under what conditions is it possible to design a quantum code and a recovery operations $\mathcal{R}$ such that

$$\mathcal{R} \circ \mathcal{E}[\rho_C] \propto \rho_C \tag{3}$$

for ρ_C with support over the code subspace, $\mathcal{H}_C \subseteq \mathcal{H}$? Why do we use $\propto$ here instead of $=$? Well because $\mathcal{E}$ is not trace preserving now. This means that there may be processes which are occurring in the full $\mathcal{D}$ which occur with some probability and we do not need to preserve ρ on these errors.

Lets call a basis for the code subspace $|\phi_i\rangle$. $\mathcal{H}_C = \text{span}\{|\phi_i\rangle\}$. al We will show that a necessary and sufficient condition for the recovery operations to preserve the subspace is that

$$\langle\phi_i|E_k^\dagger E_l|\phi_j\rangle = C_{kl}\delta_{ij} \tag{4}$$

where C_{kl} is a hermitian matrix. This equation is called the quantum error correcting criteria. It tells us when our encoding into a subspace can protect us from quantum errors E_k. As such it is a very important criteria for the theory of quantum error correction. Let's show that this is a necessary and sufficient condition.

A. Sufficiency

Let's begin with showing that if this criteria is satisfied, we can construct a recovery operation $\mathcal{R}$ with the desired properties.

The first thing to do is to change the error operators. Instead of discussing the error operators E_k, define a new set of error operators $F_m = \sum_k u_{mk} E_k$ where u_{lk} is a unitary matrix. We saw in a previous lecture that this means that F_l represents the same superoperator. Now we see that since the E_i satisfy the error correcting criteria,

$$\langle \phi_i | F_m^\dagger F_n | \phi_j \rangle = \sum_{k,l} \langle \phi_i | u_{mk}^* E_k^\dagger u_{nl} E_l | \phi_j \rangle = \sum_{k,l} u_{mk}^* C_{kl} u_{nl} \delta_{ij} \tag{5}$$

Since C_{kl} is hermitian, it is always possible to choose u_{ij} such that it diagonalizes this matrix,

$$\langle \phi_i | F_m^\dagger F_n | \phi_j \rangle = d_m \delta_{m,n} \delta_{i,j} \tag{6}$$

with $d_m \in \mathbb{R}$. Now define the following operators for $d_k \neq 0$

$$R_k = \frac{1}{\sqrt{d_k}} \sum_i |\phi_i\rangle\langle\phi_i| F_k^\dagger \tag{7}$$

and if $d_k = 0$ then let $R_k = 0$. Now we want to show that a recovery superoperator with R_k as it's Kraus operators will correctly recover our erred quantum information:

$$\sum_k R_k \sum_l \left(F_l \rho_C F_l^\dagger \right) R_k^\dagger = \sum_{k|d_k \neq 0} \frac{1}{\sqrt{d_k}} \sum_i |\phi_i\rangle\langle\phi_i| F_k^\dagger \sum_l \left(F_l \rho_C F_l^\dagger \right) \frac{1}{\sqrt{d_k}} \sum_j F_k |\phi_j\rangle\langle\phi_j| \tag{8}$$

If we can show that for $\rho_C = |\phi_m\rangle\langle\phi_n|$ this produces something proportional to ρ_C, then we will have shown that the recovery correctly restores in information in the subspace. Substituting this ρ_C in, we obtain

$$\sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_i |\phi_i\rangle\langle\phi_i| F_k^\dagger \sum_l \left(F_l |\phi_m\rangle\langle\phi_n| F_l^\dagger \right) \sum_j F_k |\phi_j\rangle\langle\phi_j| \tag{9}$$

Using the quantum error correcting criteria, this becomes

$$\sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_{ilj} |\phi_i\rangle d_k \delta_{lk} \delta_{im} d_k \delta_{lk} \delta_{jn} \langle\phi_j| = \sum_k d_k |\phi_m\rangle\langle\phi_n| = \left(\sum_k d_k \right) \rho_C \tag{10}$$

Thus we see that indeed the recovery produces a sate proportional to ρ_C. Notice that if $\mathcal{E}$ is trace preserving, then $\sum_k d_k = 1$ and then we recover exactly ρ_C, as desired.

Now we need to check that R_k forms a valid superoperator. Check,

$$R = \sum_k R_k^\dagger R_k = \sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_{i,j} F_k |\phi_i\rangle\langle\phi_i||\phi_j\rangle\langle\phi_j| F_k^\dagger = \sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_i F_k |\phi_i\rangle\langle\phi_i| F_k^\dagger \tag{11}$$

Now notice, using the quantum error correcting criteria, that this operator is a projector:

$$\begin{aligned} R^2 &= \sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_i F_k |\phi_i\rangle\langle\phi_i| F_k^\dagger \sum_{k'|d_{k'} \neq 0} \frac{1}{d_{k'}} \sum_{i'} F_{k'} |\phi_{i'}\rangle\langle\phi_{i'}| F_{k'}^\dagger \\ &= \sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_i F_k |\phi_i\rangle \sum_{k'|d_{k'} \neq 0} \frac{1}{d_{k'}} \sum_{i'} d_k \delta_{k,k'} \delta_{i,i'} \langle\phi_{i'}| F_{k'}^\dagger = \sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_i F_k |\phi_i\rangle\langle\phi_i| F_k^\dagger = R \end{aligned} \tag{12}$$

Thus if we add one extra (if necessary) projector to the R_k's which is has support on the space orthogonal to this projector, $I - \sum_k R_k^\dagger R_k$, then we will obtain a complete set of Kraus operators which satisfy the proper normalization condition for the Kraus operators. Thus we have seen that we have a valid recovery operator which does the proper recovery and that this valid recovery operator, with addition of possibly one extra Kraus operator, is indeed a valid superoperator.

B. Necessity

Now let's show necessity of the quantum error correcting criteria. Errors followed by recovery produces the following evolution on an encoded state

$$\sum_k R_k \left(\sum_i E_i \rho_C E_i^\dagger \right) R_k^\dagger = c \rho_C \tag{13}$$

We want to show that this implies the error correcting criteria. Note that ρ_C by itself is equivalent to a superoperator in which no evolution has taken place. If we express the above as

$$\sum_{k,l}(R_k E_i)\rho_C(E_i^\dagger R_k^\dagger) = cI\rho_C I \tag{14}$$

Now let P_C be a projector onto the code subspace, $P_C = \sum_i |\phi_i\rangle\langle\phi_i|$. Then the above criteria is that, for all ρ,

$$\sum_{k,l}(R_k E_i P_C)\rho(P_C E_i^\dagger R_k^\dagger) = cP_C\rho P_C \tag{15}$$

Thus by the unitary freedom of the operator sum representation, there must exists an orthogonal vector with with coefficients u_{ki} such that

$$R_k E_i P_C = u_{ki} c P_C \tag{16}$$

Taking the conjugate transpose of this equation and setting $i = j$, yeilds

$$P_C E_j^\dagger R_k^\dagger = u_{kj}^* c^* P_C \tag{17}$$

Multiplying this equation on the left of the original equation yields

$$P_C E_j^\dagger R_k^\dagger R_k^\dagger E_i P_C = u_{kj}^* u_{ki} |c|^2 P_C \tag{18}$$

Summing this equation and using the fact that $\mathcal{R}$ must be a trace preserving operator

$$P_C E_i^\dagger E_j P_C = \sum_k u_{kj}^* u_{ki} |c|^2 P_C \tag{19}$$

Defining $C_{ij} = \sum_k u_{kj}^* u_{ki} |c|^2$, this is just

$$P_C E_i^\dagger E_j P_C = C_{ij} P_C \tag{20}$$

where we see that C_{ij} is hermitian. Taking matrix elements of this equation and relabeling i and j as k and l, then yields,

$$\langle\phi_i|E_k^\dagger E_l|\phi_j\rangle = C_{kl}\delta_{ij} \tag{21}$$

Thus we have established the necessity and sufficiency of the quantum error correcting criteria.

II. CONTENT OF THE QUANTUM ERROR CORRECTING CRITERIA AND THE QUANTUM HAMMING BOUND

What is the content of the quantum error correcting criteria?

$$\langle\phi_i|E_k^\dagger E_l|\phi_j\rangle = C_{kl}\delta_{ij} \tag{22}$$

Well first look at the δ_{ij}. This implies that orthogonal codewords after the error E_l to the codewords after the error E_k. If $l = k$ this implies that the code words are not distorted by the effect of error E_k. They may be rotated, but the inner product between all codewords will be the same before as after (up to a full normalization factor.) In our example of quantum error correcting codes for the bit flip code, we saw that each possible error could act to take the error to an orthogonal subspace. If every such error acts this way for a code, then the code is said to be non-degenerate. In this case, C_{kl} will be diagonal. Some codes, however, do not posses this property: there are multiple errors which can produce the same syndrome, but the recovery procedure works in spite of this.

For non-degenerate codes there is a nice bound on the size of the codes. Suppose that we wish to encode k qubits into n bare qubits in a quantum error correcting code which corrects errors on t or fewer qubits (we call such a code a $[n, k, 2t+1]$ code.) Now in the next section we will discuss how if we can correct any t or less qubit Pauli error (i.e. an error which acts from the set $\{X, Y, Z\}$ on t qubits and is identity on the other qubits), then we can correct all t qubit errors. Now in order for a non-degenerate quantum error correcting code to correct all of these errors, for each

error there must be an orthogonal subspace. There are $\binom{n}{j}$ places where j errors can occur. And in each of these places there are 3 different nontrivial Pauli errors. Thus the total number of errors for such a code we've described is

$$\sum_{j=0}^{t} \binom{n}{j} 3^j \tag{23}$$

Now for each of these errors, there must be a subspace as big as the size of the encoded space, 2^k and these subspaces must be orthogonal. Thus each subspace must fit into the full space of n qubit. Thus we obtain the bound

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n. \tag{24}$$

This is called the quantum Hamming bound. Suppose that we want a code that corrects $t = 1$ error and encodes $k = 1$ qubit. Then we obtain the inequality $(1 + 3n)2 \leq 2^n$. This inequality cannot be satisfied for $n \leq 4$. Thus for non-degenerate codes, the smallest code which can correct a single error and encodes a single qubit has $n = 5$. Indeed we will find that just such a code exists (such codes which saturate this bound are called perfect codes.) Further there is the question of what about degenerate codes. Well for the $k = t = 1$ case there is another bound, the Quantum Singleton bound which implies that even in this case $n = 5$ qubits are needed.

III. DIGITIZING QUANTUM NOISE

Suppose that we have an error correcting code which corrects a set of errors $\{E_k\}$. What other errors will this code correct? It turns out that this code will correct any linear combination of these errors. To do this, work with the errors which satisfy the diagonal error correcting criteria, like in the sufficiency construction above (the F_l's). Now suppose that the actual F_ls are written as a sum over the F_ls we can correct: $G_l = \sum_p f_{lp} F_p$. Then using the recovery operation we defined in the sufficiency proof, we obtain that the action of recovery after the error is

$$\sum_k R_k \sum_l \left(G_l \rho_C G_l^\dagger \right) R_k^\dagger = \sum_{k|d_k \neq 0} \frac{1}{\sqrt{d_k}} \sum_i |\phi_i\rangle\langle\phi_i| F_k^\dagger \sum_l \left(G_l \rho_C G_l^\dagger \right) \frac{1}{\sqrt{d_k}} \sum_j F_k |\phi_j\rangle\langle\phi_j| \tag{25}$$

We wish to show that if we operator on $\rho_C = |\phi_m\rangle\langle\phi_n|$, that we will again obtain something proportional to ρ_C. Thus we obtain

$$\sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_i |\phi_i\rangle\langle\phi_i| F_k^\dagger \sum_l \left(G_l |\phi_m\rangle\langle\phi_n| G_l^\dagger \right) \sum_j F_k |\phi_j\rangle\langle\phi_j| \tag{26}$$

Substituting in our expression for G_l as a sum F_k's yields

$$\sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_i |\phi_i\rangle\langle\phi_i| F_k^\dagger \sum_l \left(\sum_p f_{lp} F_p |\phi_m\rangle\langle\phi_n| \sum_q f_{lq}^* F_q^\dagger \right) \sum_j F_k |\phi_j\rangle\langle\phi_j| \tag{27}$$

Using the quantum error correcting criteria, we see that this becomes

$$\sum_{k|d_k \neq 0} \frac{1}{d_k} \sum_{ilpq} |\phi_i\rangle d_k \delta_{pk} \delta_{im} d_k \delta_{qk} f_{lp} f_{lq}^* \delta_{jn} \langle\phi_j| = \sum_{kl} d_k f_{lk} f_{lk}^* |\phi_m\rangle\langle\phi_n| = \left(\sum_{kl} d_k f_{lk} f_{lk}^* \right) \rho_C \tag{28}$$

So even for this linear sum of errors, we correctly restore the coded subspace.

What have we done? We have shown that even though we have designed a code to correct E_k operators, it can in fact correct any linear sum of these operators. This is great! Why? Because, for example if we want to correct a superoperator which has one qubit which has been arbitrarily erred (and only one qubit), then we need only consider a code which corrects X, Y, and Z errors, since every single qubit error operator can be written as a sum of these errors (plus identity, which we, by default almost always include in our possible errors.) This is what is known as make the errors discrete or digital. This discovery, that a code which was designed to correct a discrete set of errors can also correct a continuous set of errors, is one of the worst understood properties of quantum error correction among certain skeptics who shall remain nameless. The reason for this property is that quantum theory is linear. This linearity has a lot to do with why we can treat amplitudes like fancy probabilities and indeed when we view quantum theory this way, we aren't quite as surprised as if we thought about the components of a wave function as being some parameters with a reality all their own.