Quantum Code Properties. (Source Gottesman thesis)

Note Title 5/22/2012

A code that uses n qubits to encode k qubits will have a basis of 2^k codewords in a Hilbert space of dimension 2^n.

Linear combination of codewords is also a codeword which comes from a linear combination of basis states from unencoded basis states.

$\Rightarrow$ Coding Space: space spanned by basis of codewords.

If we can correct $E+F$, we can correct $aE+bF$, so we only need to consider a basis of coding errors.

We will use tensor products of $I, \sigma_x, \sigma_y, \sigma_z$ with an overall phase of $\pm 1, \pm i$. The weight of an operator of this form is the # ops which are not I.

Forms a group G under multiplication.

If we have two different basis codewords $|\psi_i\rangle$ & $|\psi_j\rangle$ which each incur an error: $E_a|\psi_i\rangle$ & $E_b|\psi_j\rangle$

The error detection & recovery procedure must return them to their original (orthogonal) states, so it must be that for $i \neq j$ $\quad \langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = 0$

otherwise the codewords could not be reliably distinguished.

Also, when the error syndrome is measured, we must gain no information about $|\psi_i\rangle$.

Intuitively, we learn information about the error by measuring $\langle\psi_i|E_a^\dagger E_b|\psi_i\rangle$ so this quantity must be independent of i: $\quad \langle\psi_i|E_a^\dagger E_b|\psi_i\rangle = C_{ab}$ ← C forms a Hermitian matrix.

We can put these together in the following theorem:

Theorem: There is an Error Correcting Code for codewords spanned by $\{|\psi_j\rangle\}$ that corrects errors spanned by $\{E_a\}$ if and only if

$$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = \delta_{ij} C_{ab} \quad \forall a,b,i,j$$

for Hermitian matrix C.

Proof $\Leftarrow$ Suppose $\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = \delta_{ij} C_{ab}$.

Since C is Hermitian, it can by diagonalized $D = U C U^\dagger$

Let $\begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix} = U^* \begin{pmatrix} E_1 \\ \vdots \\ E_s \end{pmatrix}$ the F's span the same space of errors as the E's.

$$F_l^\dagger F_m = \sum_{ab} E_a^\dagger U_{la} U_{mb}^* E_b$$

[Note that the F's are not necessarily tensors of Pauli operators on individual qubits.]

$$\langle \psi_i | F_l^\dagger F_m | \psi_j \rangle = \sum_{ab} U_{la} U_{mb}^* \langle \psi_i | E_a^\dagger E_b | \psi_j \rangle$$

$$= \delta_{ij} \sum_{ab} U_{la} C_{ab} U_{mb}^* = d_a \delta_{ij} \delta_{ab}$$

Thus we have mutually orthogonal subspaces

H_a : span of $\{E_a |\psi_i\rangle\}_i$

Measure using projections $P_a = \sum_i E_a |\psi_i\rangle\langle\psi_i|$

then correct.

Proof of $\Rightarrow$ Suppose that there is an error correcting procedure for $\{|\psi_i\rangle\}_i$ that corrects $\{E_a\}_a$

Our recovery procedure consists of a measurement (error detection) followed by a unitary error correction. We can make the whole process unitary by storing the results of the measurement in an ancilla register. If the set of projections associated with the measurement are $\{P_m\}$ $\sum_m P_m = I$

$$U_{\text{detection}}\left(|\psi\rangle|\vec{0}\rangle\right) = \sum_m P_m|\psi\rangle\,|\vec{0}\oplus m\rangle$$

Then error correction is controlled by the ancilla.
Apply U_m-correct if ancilla is $|m\rangle$ $\forall m$.

We can bundle the whole set of unitaries in U_r (r for recovery)

For any $|\psi\rangle$ in the code space and any E in the error space $U_r E\left(|\psi\rangle|0\rangle\right) = a|\psi\rangle|\text{anc}\rangle$

there is a constant a because E is not necessarily unitary.

For $|\phi\rangle$ also in the code space we have

$$U_r E\left(|\phi\rangle|0\rangle\right) = b|\phi\rangle|\text{anc}'\rangle$$

Also $U_r E\left(\frac{1}{\sqrt{2}}(|\psi\rangle+|\phi\rangle)|0\rangle\right) = c\,\frac{1}{\sqrt{2}}(|\psi\rangle+|\phi\rangle)|\text{anc}''\rangle$

$$= \frac{1}{\sqrt{2}}\left(a|\psi\rangle|\text{anc}\rangle + b|\phi\rangle|\text{anc}'\rangle\right)$$

Since $|\psi\rangle$ & $|\phi\rangle$ are orthogonal: $a = b = c$.

$$\langle\psi|E^\dagger E|\psi\rangle = \langle\psi|E^\dagger U^\dagger U E|\psi\rangle = |a^2|$$

c independent of $|\psi\rangle$ but possibly dependent on E.

Define $\langle\psi|E^\dagger E|\psi\rangle = C(E)$.

Now let $E = (E_a + E_b)$:

$$C(E_a+E_b) = \langle\psi|\,(E_a^\dagger + E_b^\dagger)(E_a+E_b)\,|\psi\rangle$$
$$= \underbrace{C(E_a) + C(E_b)}_{\text{indep of } |\psi\rangle} + \underbrace{\langle\psi|E_a^\dagger E_b|\psi\rangle}_{X} + \underbrace{\langle\psi|E_b^\dagger E_a|\psi\rangle}_{X^*} = 2\,\mathrm{Re}(X)$$

Let $E = (E_a + iE_b)$.

$$C(E_a+iE_b) = \langle\psi|\,(E_a^\dagger - iE_b^\dagger)(E_a+iE_b)\,|\psi\rangle$$
$$= \underbrace{\langle\psi|E_a^\dagger E_a|\psi\rangle + \langle\psi|E_b^\dagger E_b|\psi\rangle}_{\text{indep of } |\psi\rangle} + i\langle\psi|E_a^\dagger E_b|\psi\rangle - i\langle\psi|E_b^\dagger E_a|\psi\rangle$$
$$i(X - X^*) = i\,2\,\mathrm{Im}(X)$$

$\Rightarrow$ X is independent of $|\psi\rangle$ $\quad \langle\psi|E_a^\dagger E_b|\psi\rangle = C_{ab}$

Similarly, plug in $|\psi_i\rangle + |\psi_j\rangle$ and $|\psi_i\rangle - |\psi_j\rangle$ for $i \neq j$

$$\langle\psi_j|E^\dagger E|\psi_i\rangle + \langle\psi_i|E^\dagger E|\psi_j\rangle = -C(E).$$
$$-\langle\psi_j|E^\dagger E|\psi\rangle - \langle\psi_i|E^\dagger E|\psi_j\rangle = -C(E).$$
$$\Rightarrow \mathrm{Re}\left(\langle\psi_j|E^\dagger E|\psi_i\rangle\right) = 0.$$

Using $|\psi_i\rangle + i|\psi_j\rangle$ and $|\psi_i\rangle - i|\psi_j\rangle$

shows $\mathrm{Im}\left(\langle\psi_j|E^\dagger E|\psi_i\rangle\right) = 0.$

The operator $E = E_a^\dagger E_b$ is still in the group G.
The weight of the smallest E in G for which (*) does not hold is the distance of the code.

A quantum code to correct up to t errors must have distance at least $t+1$.

A distance d code that encodes k qubits using n qubits is an $[n, k, d]$ code.

Error model assumption:
An error occurs independently on each qubit with probability ϵ and is equally likely to be $\sigma_x, \sigma_y, \sigma_z$.
We will deal with codes that handle up to t errors (since ϵ^{t+1} will be small).