Introduction to quantum information processing

Quantum codes

Brad Lackey

8 November 2016

Outline

LAST TIME...

- Quantum channels have Kraus forms $\mathcal{C}(\rho) = \sum_j A_j \rho A_j^\dagger$.
- An error channel is just a quantum channel whose Kraus operators are the possible errors in the error model.
- For example the bit-flip (qubit) channel is given by Kraus form

$$\mathcal{B}_p(\rho) = (1-p)\rho + pX\rho X.$$

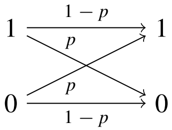
- The fidelity has formula $F(\rho, \sigma) = \sqrt{\sigma^{\frac{1}{2}} \rho \sigma^{\frac{1}{2}}}$.
- If $\sigma = |\psi\rangle\langle\psi|$ is pure this is easier to evaluate:

$$F(\rho, |\psi\rangle\langle\psi|) = \sqrt{\langle\psi|\rho|\psi\rangle}.$$

Outline

THE REPETITION CODE

Classically, the "standard" error models is independent bit flips:



This is identical to the bit flip channel (albeit classical).

The main idea in (forwared) error correction:

- use redundancy to protect information.

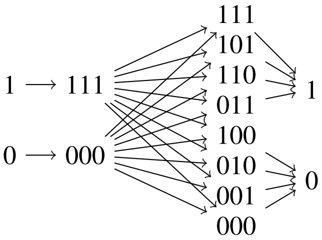
The simplest nontrivial way to protect a bit is repetition.

- Encoding: $0 \mapsto 000$ and $1 \mapsto 111$.
- Decoding: take the "majority vote" of the bits.

Analysis of the repetition code

Bit flips are assumed independent.

- No flips: probability $(1-p)^3$.
- One flip: probability $3p(1-p)^2$.
- Two flips: probability $3p^2(1-p)$.
- Three flips: probability p^3.



Majority vote decoding:

- 0 or 1 flip: correct decoding.
- 2 or 3 flips: wrong decoding.

So the probability of decoding correctly is $(1-p)^3 + 3p(1-p)^2$.

- Without coding, the correct bit is received with probability $(1-p)$.
- As long as $p < \frac{1}{2}$, we have $(1-p)^3 + 3p(1-p)^2 > 1-p$.

The probability of an error is $O(p^2)$.

- Correcting a single bit-flip error gives "quadratic error suppression."

Syndromes

Let's instead correct error without decoding.

- We define two "check equations" on our three bits:

$$x_1x_2x_3 \mapsto x_1 \oplus x_2 \text{ and } x_1x_2x_3 \mapsto x_2 \oplus x_3.$$

- These are called *syndrome* bits $s_1 = x_1 \oplus x_2$ and $s_2 = x_2 \oplus x_3$.
- Note that $s_1 = s_2 = 0$ for *both* 000 and 111.

These two equations test for a single bit flip error,

- *and* the location of the error.
- We tabulate syndromes to error locations.
- Correction is just re-flipping the erred bit.

So we can correct an error without decoding.

Syndrome s_1s_2	Error location
00	–
10	1
01	3
11	2

What happens with multiple bit flips?

- Bad things: one corrects to the wrong codeword.

Outline

Quantum codes

How do we encode a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$?

- Redundancy is right out: $|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$ is not linear!
- Quantum theory cannot produce nonlinear maps like this. (No-cloning)
- Yet, one can “copy” information in a particular basis (e.g. CNOT).

A *quantum code* is a subspace $\mathfrak{C} \subset \mathfrak{H}$.

- Encoding will generally take the form $|\psi_{\text{enc}}\rangle = G_{\text{enc}}(|\psi\rangle \otimes |0 \ldots 0\rangle)$.
- This creates “redundancy” by entangling information with the ancilla.
- Error channels then operate as $\mathcal{E}(|\psi_{\text{enc}}\rangle\langle\psi_{\text{enc}}|)$.
- The decoding $\text{tr}_{\text{anc}}(G_{\text{dec}}\mathcal{E}(|\psi_{\text{enc}}\rangle\langle\psi_{\text{enc}}|)G_{\text{dec}}^{\dagger})$ is hopefully close to $|\psi\rangle$.

A common metric for quality is worst-case fidelity:

$$F(\mathfrak{C}, \mathcal{E}) = \min_{|\psi\rangle} F(|\psi\rangle\langle\psi|, \text{tr}_{\text{anc}}(G_{\text{dec}}\mathcal{E}(|\psi_{\text{enc}}\rangle\langle\psi_{\text{enc}}|)G_{\text{dec}}^{\dagger})).$$

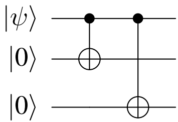
Three qubit code

Like the three bit code, we define the three qubit repetition code as

$$\mathfrak{C} = \text{span}\{|000\rangle, |111\rangle\}.$$

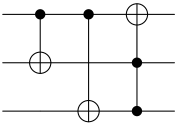
We encode $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$.

- Encoding is done by a unitary circuit, G_{enc}.
- We need two ancilla qubits set to $|0\rangle$.



Decoding uses majority vote.

- This is similar to encoding.
- The first two CNOTs decode codewords.
- The final Toffoli is part of error correction, in case the first qubit was flipped.



Three qubit code

Bit flip errors

Let us consider the "error model" where $\mathcal{B}_p$ is applied to each qubit:

$$\mathcal{B}_p^{\otimes 3}(\rho) = (1-p)^3\rho + p(1-p)^2(X_1\rho X_1 + X_2\rho X_2 + X_3\rho X_3) \\ + p^2(1-p)(X_1X_2\rho X_1X_2 + X_2X_3\rho X_2X_3 + X_1X_3\rho X_1X_3) + p^3 X_1X_2X_3\rho X_1X_2X_3.$$

E.g. for the error operator $\propto X_2$ on encoded $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$G_{\text{dec}}X_2(\alpha|000\rangle + \beta|111\rangle) = G_{\text{dec}}(\alpha|010\rangle + \beta|101\rangle) \\ = \alpha|010\rangle + \beta|110\rangle = |\psi\rangle \otimes |10\rangle.$$

The other errors are similar giving: writing $|\phi\rangle = \alpha|111\rangle + \beta|000\rangle$:

$$G_{\text{dec}}\mathcal{B}_p^{\otimes 3}(\rho)G_{\text{dec}}^\dagger \\ = |\psi\rangle\langle\psi| \otimes \Big((1-p)^3|00\rangle\langle 00| + p(1-p)^2|11\rangle\langle 11| + p(1-p)^2|10\rangle\langle 10| + p(1-p)^2|01\rangle\langle 01|\Big) \\ + |\phi\rangle\langle\phi| \otimes \Big(p^3|00\rangle\langle 00| + p^2(1-p)|11\rangle\langle 11| + p^2(1-p)|10\rangle\langle 10| + p^2(1-p)|01\rangle\langle 01|\Big).$$

We have $|\langle\psi|\phi\rangle|^2 = |\alpha^*\beta + \alpha\beta^*|^2 = 0$ when $\alpha^*\beta = -\alpha\beta^*$. Therefore:

$$F(\mathfrak{C}, \mathcal{B}_p^{\otimes 3}) = \min_{|\psi\rangle} \sqrt{(1-p)^2(1+2p) + O(p^2)|\alpha^*\beta + \alpha\beta^*|^2} = \sqrt{(1-p)^2(1+2p)}.$$

Syndrome measurements

Consider the two "check" operators $S_1 = Z_1 Z_2$ and $S_2 = Z_2 Z_3$.

- Each has eigenvalues ± 1, with four dimensional eigenspaces.
- For S_1 we have the eigenspaces
  - $V_{+1} = \text{span}\{|000\rangle, |001\rangle, |110\rangle, |111\rangle\}$
  - $V_{-1} = \text{span}\{|100\rangle, |101\rangle, |010\rangle, |011\rangle\}$.
- For S_2 we have the eigenspaces
  - $V_{+1} = \text{span}\{|000\rangle, |100\rangle, |011\rangle, |111\rangle\}$
  - $V_{-1} = \text{span}\{|001\rangle, |101\rangle, |010\rangle, |110\rangle\}$.
- Note the code, $\text{span}\{|000\rangle, |111\rangle\}$, is the *joint* $(+1, +1)$ eigenspace.

These are just like classical check equations.

- Measuring gives syndrome values.
- These syndrome values locate the error.
- We look up the correction in a table.
- We then correct the error appropriately.

Syndrome measurment	Correction operator
$(+1, +1)$	$\mathbb{1}$
$(-1, +1)$	X_1
$(+1, -1)$	X_3
$(-1, -1)$	X_2

Outline

Correction channels

We corrected single bit flip errors on the three qubit code:

- measure with respect to special syndrome operators, and
- adaptively applying a correction operation based on the result.

We combine these to a *recovery channel* $\mathcal{R}$. E.g. for 3 qubit repetition code

- the measurement operator $\Pi_{(+1,-1)}$ is the POVM operator for measuring syndome $(+1,-1)$,
- according the table the correction operator is X_3.

So $X_3\Pi_{(+1,-1)}$ is a Kraus operator in our recovery channel.

Definition

Let $\mathfrak{C} \subset \mathfrak{H}$ be a quantum code. An error channel $\mathcal{E}$ is *correctable* on $\mathfrak{C}$ (or $\mathfrak{C}$ *corrects* $\mathcal{E}$) if there exists a recovery channel $\mathcal{R}$ so $(\mathcal{R} \circ \mathcal{E})(\rho) \propto \rho$ for all densities ρ supported on $\mathfrak{C}$.

The quantum error correction condition

Just as often, one says the Kraus operators $\{E_j\}_{j=1}^r$ of $\mathcal{E}$ are correctable.

- Recall: Kraus operators for $\mathcal{E}$ are not unique.
- Any time we write $\mathcal{E}(\rho) = \sum_{j=1}^{\ell} A_j \rho A_j^\dagger$, all A_j will be correctable!
- See Assignment 5, #3 (a-b).

A checkable condition for the existence of a recovery channel is:

Theorem (Knill-Laflamme (1996))

Let $\mathfrak{C} \subset \mathfrak{H}$ be a quantum code, and $\Pi_{\mathfrak{C}}$ the orthogonal projection onto $\mathfrak{C}$. An error channel with Kraus operators $\{E_j\}_{j=1}^r$ is correctable on $\mathfrak{C}$ if and only if $\Pi_{\mathfrak{C}} E_j^\dagger E_k \Pi_{\mathfrak{C}} = \alpha_{jk} \Pi_{\mathfrak{C}}$ for some scalar matrix (α_{jk}).

- This is called the quantum error correction condition.
- Note: the matrix (α_{jk}) is Hermitian.
- If it is invertible (i.e. of maximal rank), we $\mathfrak{C}$ is *nondegenerate* for $\mathcal{E}$.
- Nondegeneracy means: each E_j has an orthogonal "syndrome space."

Next time...

- The Shor code.
- The Steane code.
- The CSS construction.