UMD PHYS623 – QM II → Guest Lecture, QECC

5/10/16

Notes by Antony Speranza

- Classical Error Correcting Codes
- Quantum Error Correcting Codes
- 5-qubit code → stabilizer codes
- 3-qutrit code

Motivation: Q. computing
holography
math

1. Classical Error Correcting Codes

Issue: random interactions w/ environ. can flip a bit:

000 ⟶ 010

If all three bits were nec., this destroys the info.

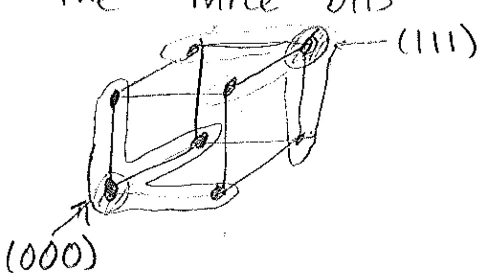
ECC → encode "logical" bits nonlocally across several "physical" bits.

Ex: 3 bit code: encodes one logical bit among 3 physical bits.

logical		codewords
0	⟶	000
1	⟶	111

← called a "repetition code"

Represent the three bits on a cube



This code protects against one error: single bit flip will keep the bit closest to its codeword, so can correct.

Error space: 000 → 100, 010, 001

111 → 011, 101, 110

Note: does not correct against arbitrary errors, only single bit flips. Generic property of ECC.

Some notation:

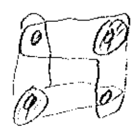
This code has distance $d = 3$, since every codeword is separated by at least 3 bit flips (Hamming distance).

Call this a $[3, 1, 3]$ code.

\# of physical bits — # of logical bits — distance.

Say we can correct $t = \frac{d-1}{2}$ errors → minimum radius of "Hamming" spheres to be non-overlapping.

[$d-1$ because consider $0 \to 00$, $1 \to 11$



← errors overlap]

$[3, 1, 3]$ code has no wasted space → codespace ⊕ errorspace = whole space.

Call this a perfect code.

Another example → 2 logical bits.

$[5, 2, 3]$ code

Logical		Codeword
00	⟶	00000
10	⟶	11100
01	⟶	00111
11	⟶	11011

Can check: all codewords seperated by distance 3 or 4. ⇒ corrects one error.

Not perfect: 10010 is distance 2 or 3 from all codewords.

Note: perfect codes for more than one logical bit that correct multiple errors are rare → essentially 2 of them:

Binary Golay code $[23, 12, 7]$ ← corrects 3 errors

Ternary Golay Code $[11, 6, 5]_3$

Binary Golay code has deep connections to other structures in mathematics → related to sphere packing in 24 dims. (Leech Lattice), as well as many sporadic finite simple groups. Culminating in 10^{53} elt. Monster group.

---

2. Quantum Error Correcting Codes

Same problem, (qubits interact w/ environment, producing errors), slightly more complicated → why?

Ans: more types of errors can occur on a qubit.

$|0\rangle \to |1\rangle$
$|1\rangle \to |0\rangle$ Bit flip → X (Pauli σ_x).

– Also have phase flip:

$|0\rangle \to |0\rangle$
$|1\rangle \to -|1\rangle$ Z

[Note → somewhat heuristic, environment states might overlap]

– Or both

$|0\rangle \to -|1\rangle$
$|1\rangle \to |0\rangle$ $Y \; (\equiv \overbrace{i\sigma_y}^{\text{anti-Hermitian}} = ZX)$.

(I, X, Y, Z) are a basis for 2×2 matrices
⇒ all unitaries can be expanded in terms of them.

Another complication → must be careful not to <u>measure</u> the logical qubit, which destroys superpositions that are necessary in quantum computing.

Need to be able to diagnose if an error occurred and correct it <u>without</u> disturbing the logical qubit.

This is possible b/c we are not correcting every type of error, but only a subset of errors (just like CECC).

Errors in a quantum system:

Initial state: $\underset{\text{qubits}}{|\psi\rangle} \otimes \underset{\text{environment.}}{|0\rangle_E}$

Error: some unitary evolution that acts on $|\psi\rangle$ and $|0\rangle_E$

$$U\left(|\psi\rangle \otimes |0\rangle_E\right)$$

$$= \sum_a \left(\underset{\substack{\text{unitary} \\ \text{error operators} \\ \text{on } |\psi\rangle.}}{E_a}|\psi\rangle\right) \otimes \underset{\text{not nec. orthonormal states}}{|e_a\rangle_E} + \underset{\text{no error occurs.}}{|\psi\rangle \otimes |e_I\rangle_E}$$

On one qubit, we saw that a basis for E_a was (X, Y, Z). For multiple qubits, just take tensor products:

E.g. 5 qubits

$E \to$ $XIIII$ ← weight 1 → analogous to one classical bit flip error.

$IYZII$ weight 2

Codes generally try to correct all errors up to a given weight w, then the quantum code <u>distance</u> is $d = 2w+1$, in analogy with classical codes.

Conditions for error correction:

$|\bar{i}\rangle \to$ orthonormal basis for code subspace $\mathcal{H}_{code} \subset \mathcal{H}$.

We want errors acting on codewords to not send one word to another:

$$\left.\begin{matrix} E_a|\bar{i}\rangle \\ E_b|\bar{j}\rangle \end{matrix}\right. \quad \text{need to remain orthogonal}$$

$$\Rightarrow \quad \langle \bar{j}| E_b^\dagger E_a |\bar{i}\rangle \propto \delta_{ij}$$

if we want to know which error occurred, need

$$\langle \bar{j}| E_b^\dagger E_a |\bar{i}\rangle = \delta_{ab}\delta_{ij}$$

i.e. each error E_a maps $\mathcal{H}_{code}$ to a distinct orthogonal subspace, so

$$\mathcal{H} = \mathcal{H}_{code} \oplus E_1\mathcal{H}_{code} \oplus E_2\mathcal{H}_{code} \oplus \cdots \oplus E_n\mathcal{H}_{code}$$

These codes are called <u>nondegenerate</u> $\to$ can identify which error occurred. <u>Degenerate</u> codes are more general, can't always tell which error occurred ($E_i\mathcal{H}_{code}$ and $E_j\mathcal{H}_{code}$ may overlap), but still can correct. Deg: $\langle \bar{j}|E_b^\dagger E_a|\bar{i}\rangle = C_{ab}\delta_{ij}$, C_{ab} indep. of $\underline{i}$.

<u>So</u>: when an error occurs, make a projective measurement to collapse state to a definite error subspace, then apply inverse error operator.

$$|\psi\rangle \otimes |0\rangle_E \xrightarrow{\text{error}} \sum_a E_a|\psi\rangle \otimes |e_a\rangle_E \xrightarrow{\text{measurement}} E_i|\psi\rangle \otimes |e_i\rangle_E$$

$$\xrightarrow{\text{Correct}} E_i^\dagger E_i|\psi\rangle \otimes |e_i\rangle_E = \underline{|\psi\rangle \otimes |e_i\rangle_E}$$

obtain original state w/o learning what it is.

Role of measurement: not really necessary, could instead use an ancilla qubit.

$$|\psi\rangle \otimes |0\rangle_E \otimes |0\rangle_A$$

$$\rightarrow \left(\sum_a E_a|\psi\rangle \otimes |e_a\rangle_E\right) \otimes |0\rangle_A$$

Can do a unitary that records error subspace in the ancilla

$$\rightarrow \left(\sum_a E_a|\psi\rangle \otimes |e_a\rangle_E \otimes |f_a\rangle_A\right)$$

Then correct the error conditioned on $|f_a\rangle_A$

$$\rightarrow |\psi\rangle \otimes \sum_a |e_a\rangle_E \otimes |f_a\rangle_A$$

Error introduces entanglement between $|\psi\rangle$ and environment $\rightarrow$ entropy increases.

Recovery operator transfers entanglement of environment with $|\psi\rangle$ to entanglement between E and ancilla.

Ancilla are a low entropy resource used to purify the quantum information.

---

3. 5-qubit code.

Classical code: needed 3 bits to protect one logical bit against 1 error.

What about quantum case?

For n physical qubits, Hilbert space has dimension 2^n.

Weight 1 errors: $3n$

(XIIII, YIIII, ...)

Code subspace $\mathcal{H}_{code}$ is 2-dim $(|0\rangle, |1\rangle)$.

So $$\mathcal{H} = \mathcal{H}_{code} \oplus \sum_{a=1}^{3n} E_a \mathcal{H}_{code}$$

dimension is $2(3n+1) = 6n+2$.

we need $6n+2 \leq 2^n$

$n=5$, get $32 = 32$

So $n \geq 5$ works, bound saturated when $\underline{n=5}$.

If 5 qubit code exists, it is <u>perfect</u> → code space plus error spaces is the whole space.

<u>Note</u>: same argument for qutrits:

8 error operators per qutrit.

$\mathcal{H}_{code}$ is 3 dimensional

$3(8n+1) \leq 3^n$

$n=3$ $\quad 27 = 27$ ← also exists a 3 qutrit code.

---

5 qubit code is an example of a <u>stabilizer code</u> → Code subspace is a simultaneous eigenspace of a stabilizer. → just a set of commuting operators.

<u>Stabilizer</u>:

$M_1 = XZZXI$
$M_2 = IXZZX$
$M_3 = XIXZZ$
$M_4 = ZXIXZ$

← check these commute: only collide at 2 and give -1 there, opposite order still gives overall -1.

These also commute w/ the logical operators

$$\left.\begin{aligned} \bar{X} &= XXXXX \\ \bar{Z} &= ZZZZZ. \end{aligned}\right\} \text{same reason these commute}$$

← These are in the <u>normalizer</u>

Code subspace has eigenvalue 1 for all the $M_{1,2,3,4}$ $\rightarrow$ 2 states, labelled by e.g. Z_5 eigenvalue.

When a single qubit error occurs, the eigenvalue of one of the M_i changes. Pauli groups: every two elements (in the basis) either commute or anticommute.

Can check that all weight 1 errors anticommute with some M_i, so they will flip the eigenvalue.
Syndrome of the error given by eigenvalues of M_i
$(s_1, s_2, s_3, s_4) \rightarrow 16$ possible values, in correspondence w/ the 15 possible errors (plus $I \rightarrow$ no error).

Hence, measuring the M_i determines if error occurred, and then can correct the error depending on the measured syndrome (s_1, s_2, s_3, s_4).

Ex: $X_1 \equiv XIIII$

$$X_1 M_1 = M_1 X_1$$
$$X_1 M_2 = M_2 X_1$$
$$X_1 M_3 = M_3 X_1$$
$$X_1 M_4 = -M_4 X_1$$

Syndrome is $\underline{(1, 1, 1, -1)} \rightarrow$ if this is measured, just apply $X_1^\dagger$ $(= X_1)$ to correct the error.

3 qutrit code:

qutrit: $|0\rangle, |1\rangle, |2\rangle$ ← 3-state system

Encoding:

$$|\bar{1}\rangle = \frac{1}{\sqrt{3}}\left(|000\rangle + |111\rangle + |222\rangle\right)$$

$$|\bar{2}\rangle = \frac{1}{\sqrt{3}}\left(|012\rangle + |120\rangle + |201\rangle\right)$$

$$|\bar{3}\rangle = \frac{1}{\sqrt{3}}\left(|120\rangle + |201\rangle + |102\rangle\right)$$

Stabilizers:

ZZZ (commute b/c $XZ = \omega ZX$)

XXX

X, Z generalized Pauli matrices

$$X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \qquad \omega = e^{2\pi i/3}$$

$$XZ = \omega ZX$$

Logical Gates

$\bar{X} = I\,X\,X^2$ OR $X\,X^2\,I$ OR $X^2\,I\,X$

$\bar{Z} = Z^2\,Z\,I$ OR $Z\,I\,Z^2$ OR $I\,Z^2\,Z$

Quantum secret sharing:

Can check that any single qutrit is in a totally mixed state, but any two qutrits are enough to construct the whole state.

E.g. on the first 2, 2 × first + second (mod 3) gives original logical state.

3-qubit codes

Try generalizing the $[3,1,3]$ classical code

$|\bar{0}\rangle = |000\rangle$

$|\bar{1}\rangle = |111\rangle$

X_i acting on any qubit is just like a classical bit flip → can detect + correct.

Z introduces phase error:

$ZII|111\rangle = -|111\rangle$

So can destroy superpositions, such as GHZ:

$Z_1(|000\rangle + |111\rangle) = |000\rangle - |111\rangle$.

Instead use X eigenbasis

$|\bar{0}\rangle \to |+++\rangle$ $\qquad |+\rangle = |0\rangle + |1\rangle$

$|\bar{1}\rangle \to |---\rangle$ $\qquad |-\rangle = |0\rangle - |1\rangle$

Z acts as bit flip in $|+\rangle, |-\rangle$ basis, so this code corrects Z errors.

But X now acts as phase error,

Solution: 9-qubit code:

$|\bar{0}\rangle \to (\overbrace{|000\rangle + |111\rangle}^{|\bar{+}\rangle})^{\otimes 3} \sim |+\rangle_3 |+\rangle_3 |+\rangle_3$

$|\bar{1}\rangle \to (|000\rangle - |111\rangle)^{\otimes 3}$

Z on any one is a bit flip on a group of 3

X on any one is a bit flip within the group → also correctible

+ Y also correctible