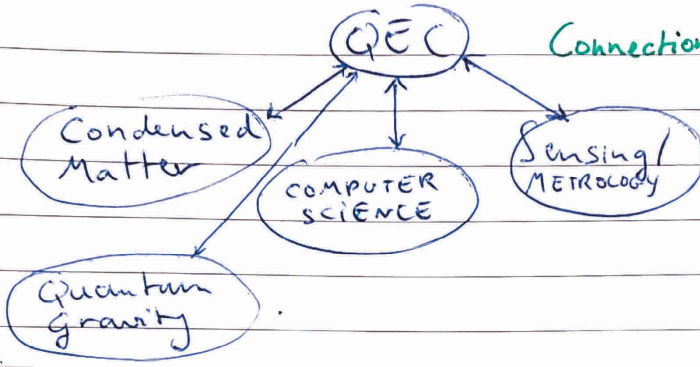
Connections to other fields?



Schedule:

Lecture 1: preliminaries
basics of QEC
small codes

Lecture 2: stabilizer codes
surface code
threshold theorem

Lecture 3: future of QEC
QLDPC codes

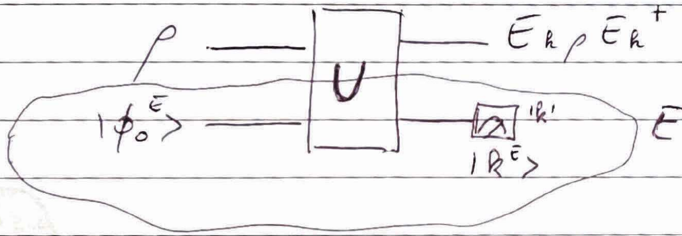
Lecture 4: comparing platforms
Grover's algorithm
Final remarks

NOT INCLUDED:
* Decoding algorithms
* FT COMPUTING
* Detailed proofs

LECTURE 1

preliminaries : understanding errors

What is decoherence ?



$E_k = \langle k^E | U | \phi_0^E \rangle$: error / Kraus operator / operation elements

Most general completely positive trace-preserving (CPTP) map can be written in operator-sum representation

$$\mathcal{E}(\rho) = \mathrm{Tr}_E\left[U \rho_{SOE} U^\dagger\right] = \sum_k E_k \rho E_k^\dagger$$

INTUITION : APPLY E_k with prob. $\mathrm{Tr}(E_k \rho E_k^\dagger)$
$(\rightarrow \sum E_k^\dagger E_k = I)$

We can always write (for qubit)

$$E_k = e_k^I I + e_k^x X + e_k^z Z + e_k^y Y$$

Why is this important ? Error Digitization

Pauli group:

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad |0\rangle \longleftrightarrow |1\rangle$$

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad |1\rangle \longleftrightarrow -|1\rangle$$

$$Y = ZX = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad |0\rangle \longleftrightarrow |1\rangle \ \& \ |1\rangle \longleftrightarrow -|1\rangle$$

n-qubit Pauli group:

$$P_n = \pm \{ I, X, Y, Z \}^{\otimes n}$$

Very useful fact: Paulis either commute or anticommute.

$X \otimes I$ and $Z \otimes X$? anticommute

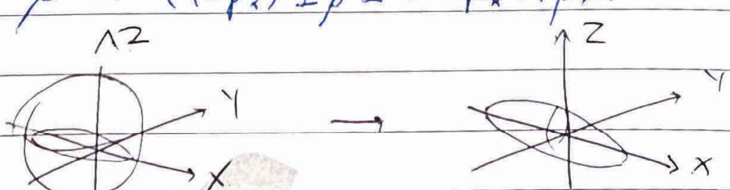
XYZ and YZZ ? commute

$XIIXIX$ and $IIXXXX$? commute

Know thy enemy: Notorious error channels

Bit-flip channel (only classical channel)

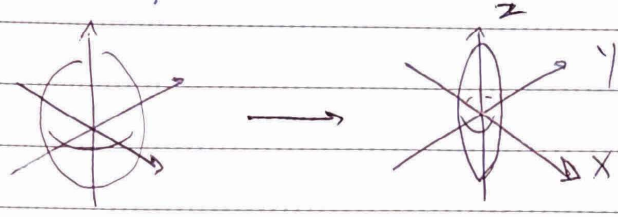
$$\rho \rightarrow (1-p_x) I \rho I + p_x X \rho X$$



Unleash ingenuity

Phase-flip / Dephasing channel

$$\rho \rightarrow (1-p_z)\, I \rho I + p_z\, Z \rho Z$$



purely quantum channel - removes coherences

$$\frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(\langle 0| + \langle 1|\right) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 1-2p_z \\ 1-2p_z & 1 \end{pmatrix}$$

Which-way measurement channel

$$E_0 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$E_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$E_2 = \sqrt{p}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

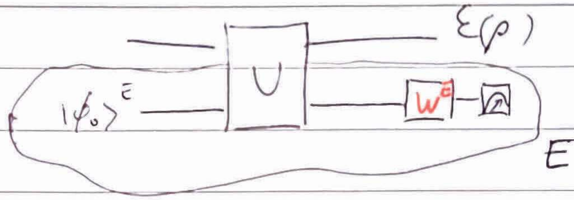
$$\rho \rightarrow (1-p)\, I \rho I + p\left(\underbrace{|0\rangle\langle 0|}_{\frac{I+Z}{2}}\rho\, |0\rangle\langle 0| + \underbrace{|1\rangle\langle 1|}_{\frac{I-Z}{2}}\rho\, |1\rangle\langle 1|\right)$$

$$= \left(1-\frac{p}{2}\right) I \rho I + \frac{p}{2}\, Z \rho Z$$

Unleash ingenuity

→ measuring ~ phase-flip!
What's the intuition?

freedom in operator-sum representation

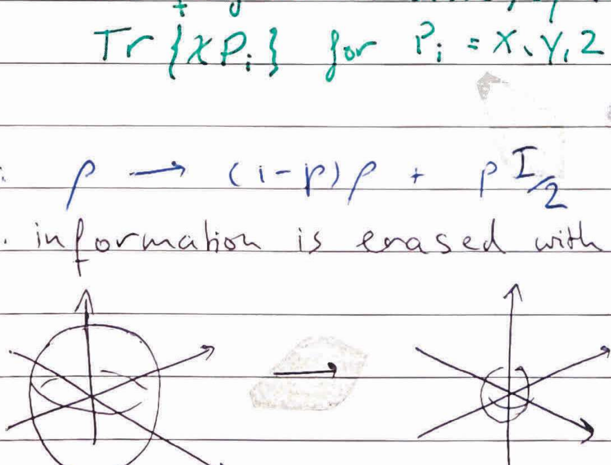


Depolarizing channel

$$\rho \to (1-p)\, I\rho I + \frac{p}{4}\left(I\rho I + X\rho X + Y\rho Y + Z\rho Z\right)$$

HW: prove $\chi = \frac{1}{4}\left(I\rho I + X\rho X - Y\rho Y + Z\rho Z\right) = \frac{I}{2}$
i.e. fully mixed state, by looking at
$Tr\{\chi P_i\}$ for $P_i = X, Y, Z$. Note $Y^2 = -I$

so: $\rho \to (1-p)\rho + p\frac{I}{2}$
i.e. information is erased with probability p.



Basics of QEC

use redundancy to protect quantum information.

$$(\mathbb{C}^2)^{\otimes k} \to \underset{(n>k)}{(\mathbb{C}^2)^{\otimes n}} \to (\mathbb{C}^2)^{\otimes k}$$

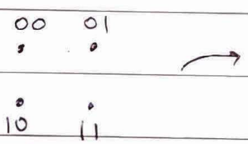
$\rho \to$ | Encoder | Noise | Decoder |

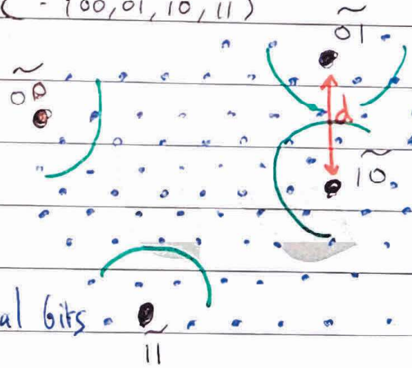
$\underbrace{\text{Noise}}$ spatial channel (communication) / temporal channel (storage)

We want $\mathcal{D}\mathcal{N}\mathcal{E}(\rho) \approx \rho$

code space $C = \{\tilde{00}, \tilde{01}, \tilde{10}, \tilde{11}\}$ → logical code words

classical picture





k logical bits, n physical bits

rate : k/n

distance d : Hamming weight of smallest operation from x to y, $x \neq y \in C$

Unleash ingenuity

example: $C = \{0000, 1111, 1100, 0011\}$

How many logical bits? $k = 2$

distance? $\|1100 - 0000\|_1 = 2$

$[n, k, d] = [4, 2, 2]$

An $[n, k, d]$ code can detect $d-1$ errors and correct $\lfloor \frac{d-1}{2} \rfloor$ errors, (by finding closest codeword)

<u>quantum case</u>

<u>single qubit</u>: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$C = \text{span}\{|0\rangle, |1\rangle\}$

problem: errors keep you within C

$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \in C$

$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle \in C$

$\rightarrow X, Z$ non-detectable and act non-trivially on C

Let's focus on the bit-flip channel

two qubits

$$C = \text{span}\{|00\rangle, |11\rangle\}$$

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$$

This does not contradict no-cloning

$$|\psi\rangle \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

error spaces:

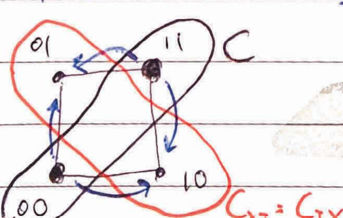
$$C_{XI} = XI|\psi\rangle = \alpha|10\rangle + \beta|01\rangle \notin C$$
$$C_{IX} = IX|\psi\rangle = \alpha|01\rangle + \beta|10\rangle \notin C$$

$\rightarrow$ 1 X-error detectable

but $C_{XI} = C_{IX}$ so cannot distinguish.
Is it a problem? Only if applying wrong correction causes logical error.

$$XI(IX)|\psi\rangle = \alpha|11\rangle + \beta|00\rangle \begin{cases} \in C \\ \neq |\psi\rangle \end{cases}$$

$\rightarrow$ 1 X-error not correctable



We write that C is a $[[n=2, k=1, d_X=2]]$ code.

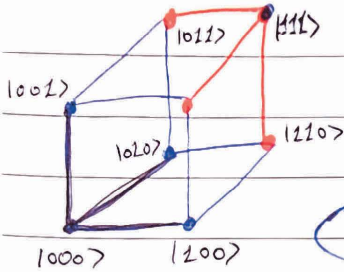
How can we detect if we're in C or in $C_{XI} = C_{IX}$?

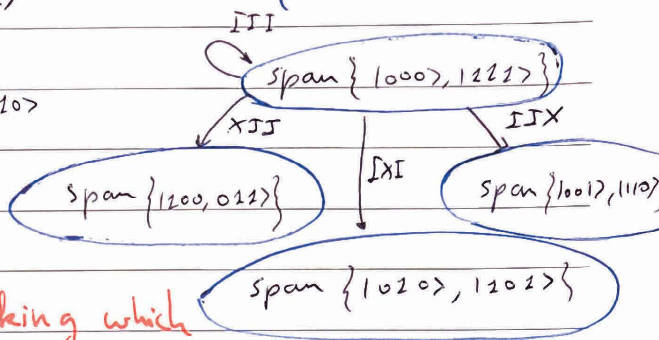
Unleash ingenuity

$\rightarrow$ parity measurement

3 qubits

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





QEC = checking which 2D subspace we're in w/o collapsing to specific state.

The information is mapped between orthogonal 2D subspaces w/o distortion

$\rightarrow \{III, XII, IXI, IIX\}$ is a correctable set of errors

Does C correct Z-errors? $[[3, 1, d_x = 3]]$

Quantum Hamming bound

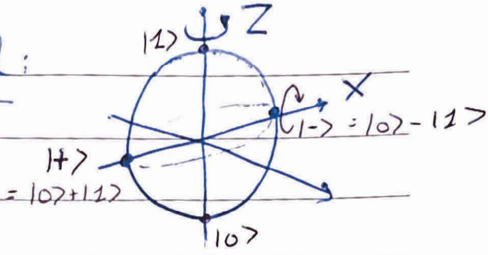
What's the smallest n allowing correction of all single-qubit errors?

Counting argument: $(\overset{I}{1} + \overset{X\,Y\,Z}{3}n)$ events $\times$ 2 states $\leq 2^n$

$\Rightarrow n \geq 5$

(good 5-qubit code exists) Unleash ingenuity

phase-flip channel:



$X|0\rangle = |1\rangle$	$Z|+\rangle = |-\rangle$
$X|1\rangle = |0\rangle$	$Z|-\rangle = |+\rangle$

phase-flip QEC = bit-flip QEC in the X / dual / Hadamard basis

$|+\rangle_L = |+++\rangle$

$|-\rangle_L = |---\rangle$

general single-qubit errors:

start with bit-flip code $|0\rangle \to |000\rangle$, $|1\rangle \to |111\rangle$

then concatenate

with phase-flip code

$|+\rangle_L = |(000+111)(000+111)(000+111)\rangle$

$|-\rangle_L = |(000-111)(000-111)(000-111)\rangle$

Z_1, Z_2 map C to same error space, but applying wrong correction $Z_1 Z_2 |\psi\rangle = |\psi\rangle$ gives trivial operation on C, so it's ok.

$\longrightarrow$ degenerate code

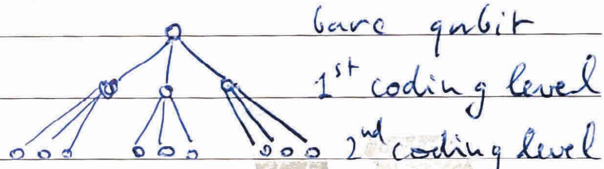
For detecting bit and phase-flips

$$|+\rangle_L = |(00+11)(00+11)\rangle$$
$$|-\rangle_L = |(00-11)(00-11)\rangle$$

$$\Rightarrow \quad |0\rangle_L = \left|\begin{matrix}0&0\\0&0\end{matrix}\right\rangle + \left|\begin{matrix}1&1\\1&1\end{matrix}\right\rangle$$
$$|1\rangle_L = \left|\begin{matrix}1&0\\1&0\end{matrix}\right\rangle + \left|\begin{matrix}0&1\\0&1\end{matrix}\right\rangle$$

HW: The distance in Z basis is 2. Prove that the distance in the dual basis is also 2 (for 2 errors)

Concatenation can be used to define a code family



$$[[n, k, d]] \rightarrow [[n^L, k, d^L]]$$

Error-correction conditions (Knill-Laflamme)

Let C be a quantum code, and $|0\rangle\langle 0|_L + |1\rangle\langle 1|_L = \hat{\Pi}_L$ the projector onto C. A set of errors $\{E_i\}$ can be corrected by C iff

$$\hat{\Pi}_L \hat{E}_i^\dagger \hat{E}_j \hat{\Pi}_L = \alpha_{ij} \hat{\Pi}_L \qquad \forall i,j$$

for some Hermitian matrix α.

Intuition:

* E_i, E_j mapping to orthogonal error spaces can be detected and corrected ($\alpha_{ij} =$
* E_i, E_j mapping to the same error space cannot be distinguished and must correct each other (degenerate code)
* An error that leaves you inside C must act trivially since it is undetectable.