Quantum Information theory

Ashwin Nayak

MSRI, Waterloo

Summary

- measure of quantum information

  von Neumann entropy

- accessible information

  Holevo bound

- vN entropy as incompressible information content

Review of quantum error correction

- Errors in quantum memory caused by interaction with environment

  faulty gates / measurement in a computation

  ...

— Reasonable assumptions :

errors are local, limited

e.g. t out of n get corrupted

example : Bit flip $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$\alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|1\rangle + \beta|0\rangle$

Phase flip $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$\alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|0\rangle - \beta|1\rangle$

Handling bit errors

Use a classical code

$\alpha|0\rangle + \beta|1\rangle$

$\Downarrow$ encoding : repetion code

$\alpha|000\rangle + \beta|111\rangle$

$\searrow$ bit flip error

$\alpha|001\rangle + \beta|110\rangle$

$\Downarrow$ decoding : compare bits, undo error

$(\alpha|001\rangle + \beta|110\rangle) \otimes |\text{"3rd bit flipped"}\rangle$

$\Downarrow$

$\alpha|000\rangle + \beta|111\rangle$

Handling phase errors

$$|0_H\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |1_H\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Phase flip

If in the Hadamard basis, a state is a superposition over classical codewords, we can correct Phase flips:

$$(|0\rangle + |1\rangle)^{\otimes 3} = |0_H\rangle|0_H\rangle|0_H\rangle$$

Phase flip

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)$$

Hadamard transform $H^{\otimes 3}$

$$|0\rangle|1\rangle|0\rangle$$

⋮

General errors

- effect of arbitrary error

$$|\psi\rangle \longmapsto \{ A_i|\psi\rangle \}$$

$$\rho \qquad\qquad \sum_i A_i \rho A_i^\dagger$$

- each A_i (1 qubit case) is a linear combination of bit, phase flips :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Pauli operators

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

On more qubits A_i : linear combination of tensors of Pauli operators

CSS codes : main idea

$\mathcal{C}$ subgroup of $\mathbb{Z}_2^n$

$$\sum_{u \in \mathcal{C}} |u\rangle \xrightarrow[H^{\otimes n}]{F.T.} \sum_{v \in \mathcal{C}^\perp} |v\rangle$$

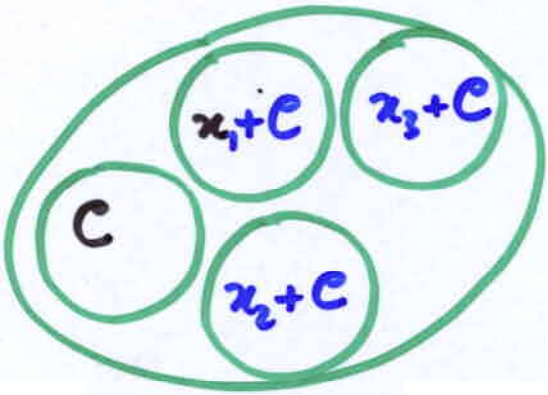
dual $\mathcal{C}^\perp = \{x : x \cdot u = 0 \ \forall u \in \mathcal{C}\}$

- if $\mathcal{C}, \mathcal{C}^\perp$ are both $[n, k, d]$ classical codes, can correct $t = \frac{d-1}{2}$ bit & phase flip errors

Encoding more states

- suffices that $\exists$ linear code C_2 :

$$C \subset C_2$$



$$|\psi_x\rangle = \sum_{u \in C} |x+u\rangle$$ valid codeword

$$\Downarrow \text{ Hadamard}$$

$$\sum_{v \in C^\perp} \alpha_{x,v} |v\rangle$$

$|\psi_x\rangle$, $x \in C_2/C$: orthonormal set of codewords

Encoding of superpositions & error correction follows from linearity

Code parameters

- Constructions use weakly self-dual classical codes: $C \subsetneq C_2 = C^{\perp}$

C : $[n, k, d]$ code

$\Downarrow$

quantum $[\![n, k', d]\!]$ code

$k' = 2k - n$, $t = \frac{d-1}{2}$ errors

- Gilbert-Varshamov type bound shows:

any $\frac{k}{n} \leq 1 - 2H\left(\frac{2t}{n}\right)$ possible

"Good" quantum codes exist

How good can the codes be?

Non-degenerate codes:

each correctable error maps code subspace to an orthogonal subspace

[9 qubit Shor code is degenerate:

$|000\rangle + |111\rangle \longmapsto |000\rangle - |111\rangle$]

σ_z on any qubit

Hamming bound

- $[[n, k, d=2t+1]]$ code $\Rightarrow$

2^k basis codewords

$\forall i \leq t$ $\binom{n}{i}$ error locations

3^i possible errors

$$\Rightarrow \sum_{i=0}^{t} \binom{n}{i} 3^i \cdot 2^k \leq 2^n$$

orthogonal vectors

Properties of bi-partite states

Alice Bob

$$|\psi\rangle = \sum_{i,j} \alpha_{ij} |i\rangle \otimes |j\rangle$$

$|i\rangle \in \mathcal{H}$ $|j\rangle \in \mathcal{K}$

- State of Bob : as if Alice had measured her qubits

$$\rho_{Bob} \equiv \{ \sum_j \alpha_{ij} |j\rangle \}$$

e.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Hadamard on Bob's qubit + measurement

⇓

random bit

(on $|0\rangle+|1\rangle$, outcome $= |0\rangle$)

- ρ_{Bob} : independent of measurement basis

$$= Tr_A |\psi\rangle\langle\psi|$$

No-cloning bound (any code)

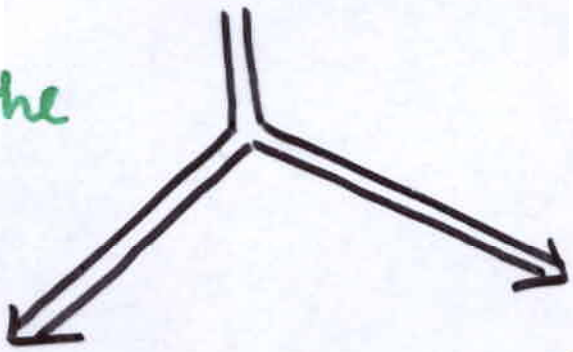
Fact: $[\![n, k, d]\!]$ code can correct $d-1$ located errors

For $k \geq 1$, if $n \leq 2(d-1)$, we can clone quantum states

$|\varphi\rangle \in \mathcal{H}_2^{\otimes k}$

encode ⇓

$|\psi\rangle \in \mathcal{H}_2^{\otimes n}$



first $n-(d-1)$ ⇓ can recover $|\psi\rangle$

last $(d-1)$ if $n-(d-1) \leq (d-1)$ can recover $|\psi\rangle$

×

$\therefore$ $n > 2(d-1)$

Bipartite states:

- Any $|\psi\rangle \in \mathcal{H} \otimes K$ can be represented

$$\| \quad \sum_{ij} a_{ij} |i\rangle \otimes |j\rangle$$

as:

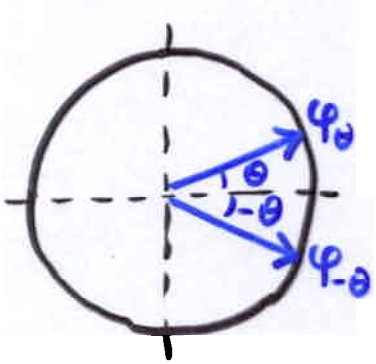
$$|\psi\rangle = \sum_k \sqrt{\lambda_k}\, |e_k\rangle \otimes |f_k\rangle$$

$\lambda_k \geq 0$, $\sum \lambda_k = 1$

$\{e_k\}$, $\{f_k\}$ orthonormal bases

[Schmidt decomposition]

example: $|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle|\varphi_\theta\rangle + |1\rangle|\varphi_{-\theta}\rangle \right)$



$$= \cos\theta \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \otimes |0\rangle$$

$$+ \sin\theta \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \otimes |1\rangle$$

Corollary:

$$\rho_{Bob} = \sum_\ell \lambda_\ell \, |f_\ell\rangle\langle f_\ell|$$

$$\rho_{Alice} = \sum_\ell \lambda_\ell \, |e_\ell\rangle\langle e_\ell|$$

$$S(\rho_{Bob}) = H(\{\lambda_\ell\}) = S(\rho_{Alice})$$

von Neumann entropy

Quantum singleton bound

$$n - k \geq 2(d-1) = 4t$$

- Consider

$$\frac{1}{2^{k/2}} \sum_{x \in \{0,1\}^k} \underbrace{|x\rangle}_{A} \underbrace{|\psi_x\rangle}_{Q_1 Q_2 Q_3}$$

encoding of x

Q_1, Q_2 : $d-1$ qubits

Q_3 : $n - 2(d-1)$

- Note that von Neumann entropy

$$S(A) = k$$

$$S(Q_3) \leq n - 2(d-1)$$

suffices to show $S(A) \leq S(Q_3)$

Singleton bound ...

- Since $|Q_1|, |Q_2| \leq d-1$,

  & $\{|\psi_x\rangle\}$ can correct $d-1$ located errors

Q_1 & Q_2 contain no information about x

$\therefore \quad AQ_1 = A \otimes Q_1$,

& $AQ_2 = A \otimes Q_2$

$$\Rightarrow \quad S(AQ_1) = S(A) + S(Q_1) = S(Q_2Q_3)$$
$$\leq S(Q_2) + S(Q_3)$$

& $$S(A) + S(Q_2) \leq S(Q_1) + S(Q_3)$$

$$\Rightarrow \quad k = S(A) \leq S(Q_3)$$
$$\leq n - 2(d-1)$$

$$n - k \geq 2(d-1) = 4t$$

classical : $n - k \geq d-1$

Other bounds

- Rains: $t \leq \left\lfloor \frac{n+1}{6} \right\rfloor$

- From channel capacity considerations

  (for block encoding, correcting 'typical' errors)

III Entanglement

Alice $\otimes$ Bob

$\frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle$

$+ \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$

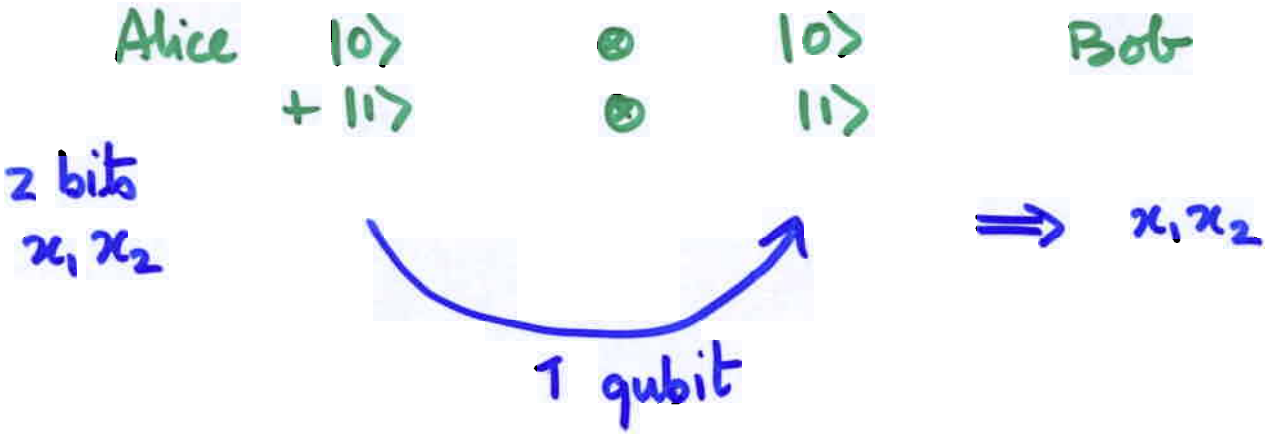
Bell state
EPR pair

- resource in addition to a (quantum) communication channel

quantum teleportation, superdense coding

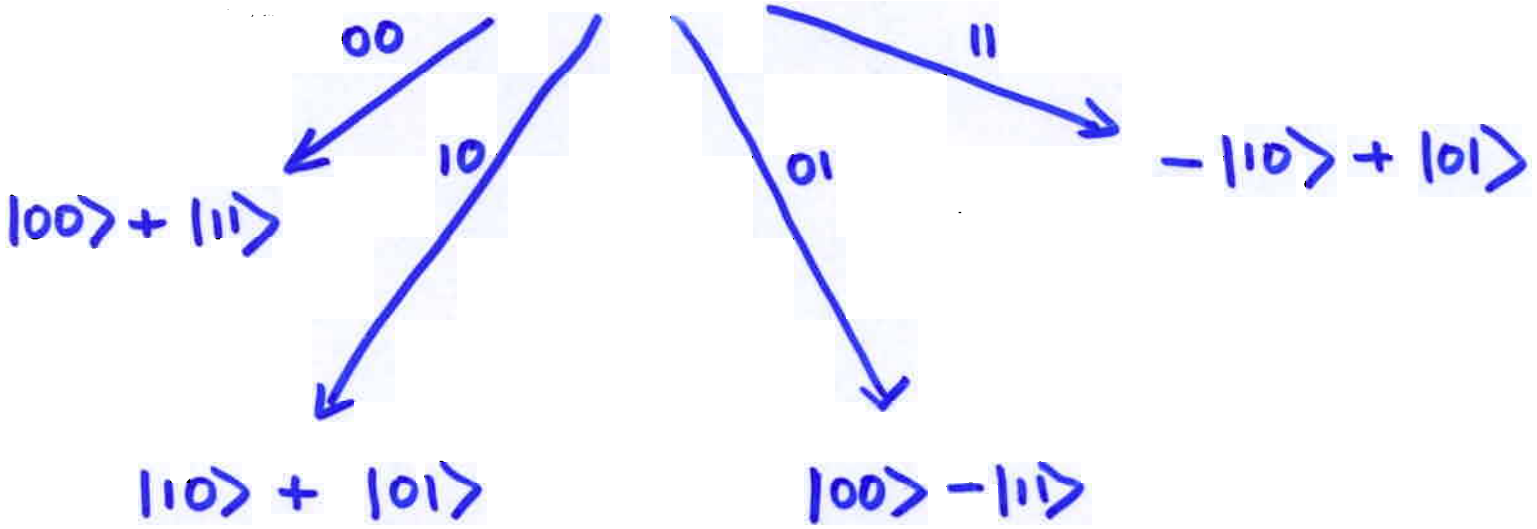
Superdense coding

(Bennett, Wiesner '92)



encoding : Alice

- apply NOT to qubit if $x_1 = 1$
- apply Phase-flip to qubit if $x_2 = 1$



4 orthogonal states : measurement distinguishes perfectly

Quantifying entanglement : Pure states

yardstick : EPR pairs

1 bit of entanglement

general shared state

Alice Bob

$$|\psi\rangle = \sum_{ij} \alpha_{ij} \; |i\rangle \otimes |j\rangle$$

Asymptotic measure :

- How many EPR pairs is this "equivalent" to ?

formation # EPR pairs required to construct $|\psi\rangle$

distillation # EPR pairs that can be extracted from $|\psi\rangle$

Another measure : $S(\rho_{Bob}) = S(\rho_{Alice})$

Separable states (unentangled states)

pure state $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

is separable

e.g. $|00\rangle + |01\rangle + |10\rangle + |11\rangle$

$= (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$

mixed state

$\rho = \rho \otimes \sigma$ is separable

more generally $\sum_i p_i \rho_i \otimes \sigma_i$

e.g. equal mixture of

$|00\rangle \pm |11\rangle$, $|01\rangle \pm |10\rangle$ - entangled

$\rho \equiv$ equal mixture of $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$\therefore$ separable

Note: Local operations & classical communication preserve separability.

Distillation entanglement (from known state)

example : $|\psi\rangle = \sqrt{\lambda_0}\,|0\rangle \otimes |0\rangle + \sqrt{\lambda_1}\,|1\rangle \otimes |1\rangle$

$S(\rho) = H(\lambda_0)$

The procedure: given $|\psi\rangle^{\otimes n}$ shared

- Alice measures # 1's in her string of qubits

output $= m$ $\Rightarrow$ state = uniform over

$x \in \{0,1\}^n$, $\omega(x) = m$

$$= \sum_{\text{such } x} \lambda_1^{m/2}\, \lambda_0^{\frac{n-m}{2}}\, |x\rangle|x\rangle$$

$\#$ such x $= \binom{n}{m}$

if $\binom{n}{m} \cong 2^k$, we have k EPR pairs

Distillation procedure

- If $\binom{n}{m}$ is not close to 2^k

sample again from blocks of length n

with high probability, for large l,

$$\binom{n}{m_1}\binom{n}{m_2}\cdots\binom{n}{m_l} \sim 2^{k'}$$

Note: m is typically $H(\lambda_i)\cdot n$

$\therefore k' \sim H(\lambda_i)\cdot n\cdot l$

The tensor product of the l samples is uniform over $\sim 2^{H(\lambda_i)\cdot n\cdot l}$ states

Measure to discard extra states.

EPR pairs generated per copy of $|\psi\rangle$

$\equiv H(\lambda_i) = S(\rho)$

Higher dimensional state $\in \mathbb{C}^d \otimes \mathbb{C}^d$

$$|\psi\rangle \overset{\text{Schmidt decomposition}}{=\!=\!=} \sum_i \sqrt{\lambda_i}\, \underbrace{|e_i\rangle}_{\text{Alice}} \otimes \underbrace{|f_i\rangle}_{\text{Bob}}$$

$$\equiv \sum_i \sqrt{\lambda_i}\, |i\rangle |i\rangle$$

via local unitary operations

- Similar procedure: $|\psi\rangle^{\otimes n}$
  - measure the #occurrences of each $i \in [d]$
  - state collapses to uniform superposition of $\frac{n!}{m_1!\, m_2! \cdots m_d!} = N$ basis states

$$m_i \sim \lambda_i \cdot n$$

$$\therefore \quad N \sim n \cdot H(\{\lambda_i\}) = n \cdot S(\rho)$$

- As before, $S(\rho)$ EPR pairs can be distilled on average with high probability

Applications of distillation

unknown shared state / possibly mixed.

Error correction

$$\rho \Longrightarrow \mathcal{E}(\rho)$$

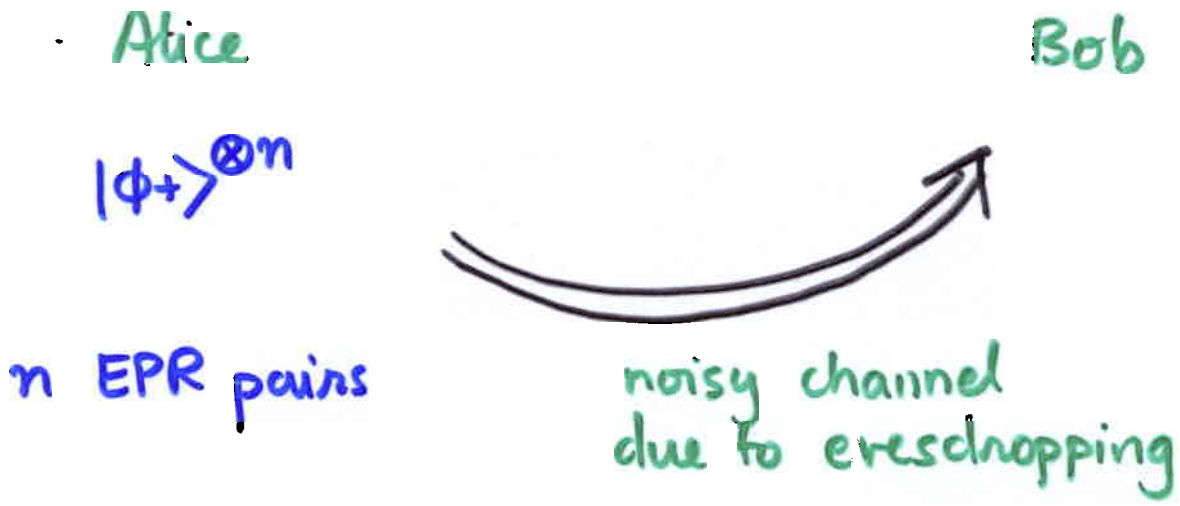
noisy channel

- create n EPR pairs, send half the qubits through channel
- distil $m = n \cdot D$ EPR pairs

distillation entanglement of $(I \otimes \mathcal{E})(|\Phi^+\rangle^{\otimes n})$

- teleport desired quantum state using EPR pairs

Application: Key distribution



- Alice sends n EPR halves to Bob
- Eavesdropping introduces arbitrary noise in EPR pairs
- IF Alice & Bob can distil m near perfect EPR pairs, Eve has little information:

$$I(E:AB) = S(E) + S(AB) - S(EAB)$$

$$= 2S(AB)$$

Further:

if $\left| \langle \phi^+|^{\otimes m} \; AB \; |\phi^+\rangle^{\otimes m} \right| \geq 1-\varepsilon = 1-2^{-cm}$

$\Rightarrow$ Largest eigenvalue of $AB \geq 1-\varepsilon = 1-2^{-cm}$

$\Rightarrow$ $S(AB) \leq \frac{c'm}{2^{cm}}$

$\Rightarrow$ $I(E:AB) \leq \frac{2c'm}{2^{cm}} \ll 1$ (*)

Alice & Bob now measure to get a random string: K, the key

(*) $\Rightarrow$ $I(E:K) \leq 2^{-c''m}$

Final remarks

Many topics not covered; riddled with open problems:

- Mixed state data compression
- Accessible information
- Optimal parameters for error correcting codes
- Channel capacities
- Measure for mixed state entanglement
  or even a test
- ...

Applications to

- communication complexity
- cryptography
- ...