Quantum Information theory

Ashwin Nayak

MSRI, Waterloo

Information theory

How "information" may be conveyed reliably between communicating parties

Information is physical in nature

Quantum information theory

- novel aspects e.g. entanglement
- conveying classical/quantum information with quantum resources

Quantifying information

Shannon entropy

information content of a classical source

X r.v. over $\{0,1\}^n$

$\{p_x, x\}$

$$H(X) = \sum_x p_x \log \frac{1}{p_x}$$

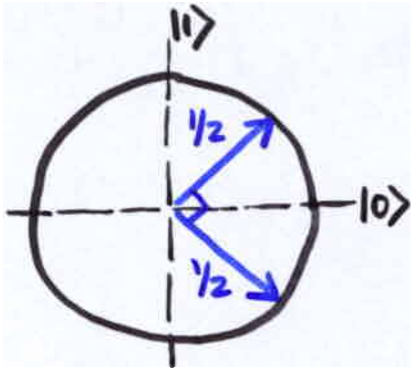
Quantum source

X n qubits

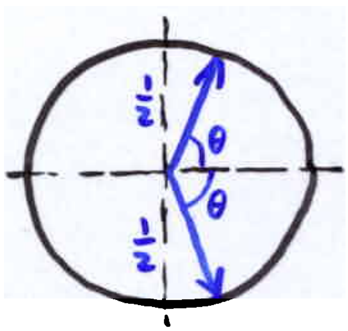
probability p_i state $\psi_i \in H_2^{\otimes n}$

entropy of X = ?

Example



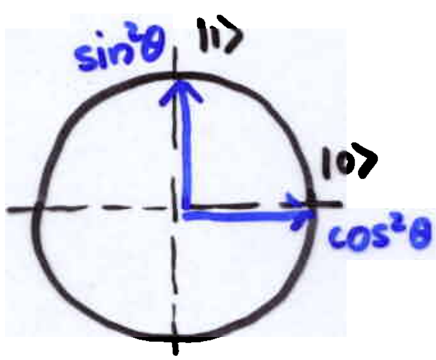
1 bit



< 1 bit

> 0 bits

$\equiv$



entropy $= H(\cos^2\theta)$

von Neumann entropy

$X = \{ p_i , \psi_i \}$

if $X \equiv \{ \lambda_j , e_j \} = Y$ $\quad$ e_j orthonormal

then

$$S(X) \triangleq H(Y)$$

$$= \sum_j \lambda_j \log \frac{1}{\lambda_j}$$

Every quantum ensemble is physically equivalent to a classical ensemble

Y is obtained from the density matrix of X

Density matrix

superposition $|\psi\rangle \in H_2^{\otimes n}$

$$\Downarrow$$

density matrix $\rho = |\psi\rangle\langle\psi|$

example : $|\psi\rangle = \cos\theta\, |0\rangle + \sin\theta\, |1\rangle$

$$\rho = \begin{pmatrix} c \\ s \end{pmatrix} \cdot \begin{pmatrix} c & s \end{pmatrix} = \begin{pmatrix} c^2 & cs \\ cs & s^2 \end{pmatrix}$$

Evolution : $|\psi\rangle \longmapsto U|\psi\rangle$

$$\Downarrow$$

$$\rho = |\psi\rangle\langle\psi| \longmapsto U\rho U^{\dagger} = U|\psi\rangle\langle\psi|U^{\dagger}$$

Measurement : $\{P_j\}$

observe j with prob $\| P_j |\psi\rangle \|^2$

$$= \langle\psi| P_j |\psi\rangle$$

$$= \mathrm{Tr}\left(P_j \, |\psi\rangle\langle\psi| \right)$$

$$= \mathrm{Tr}\left(P_j \rho \right)$$

Mixed states

$$X = \{ p_i , \psi_i \}$$

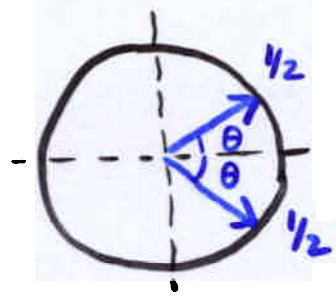
$$\Downarrow$$

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i|$$

example:

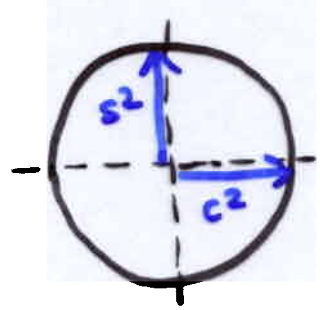
$\left(\tfrac{1}{2},\ c|0\rangle + s|1\rangle\right)$,

$\left(\tfrac{1}{2},\ c|0\rangle - s|1\rangle\right)$



$$\rho = \frac{1}{2}\begin{pmatrix} c^2 & cs \\ cs & s^2 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} c^2 & -cs \\ -cs & s^2 \end{pmatrix}$$

$$= \begin{pmatrix} c^2 & 0 \\ 0 & s^2 \end{pmatrix}$$



All physically accessible information in an ensemble $X = \{p_i, \psi_i\}$ is contained in its density matrix $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

U evolution: $\rho \xmapsto{U} U\rho U^\dagger$

$\{P_j\}$ measurement: observe j with prob. $\mathrm{Tr}(P_j \rho)$

Von Neumann entropy

For $X = \{p_i, \psi_i\}$ determine physically equivalent "classical" distribution:

ρ_X is positive semi-definite, has trace $= 1$.

$$\rho_X = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

$\therefore$ ρ_X has spectrum $\{\lambda_j\}$ $\lambda_j \geq 0$, $\sum_j \lambda_j = 1$

corresponding to orthonormal eigenvectors $|e_j\rangle$

$$\rho_X = \sum_j \lambda_j |e_j\rangle\langle e_j|$$

$$S(X) = H(\{\lambda_j\}) = \sum_j \lambda_j \log \frac{1}{\lambda_j}$$

vN entropy

Rest of the talk

interpretation & applications of von Neumann entropy

- Quantum encoding of classical messages
- Quantum data compression
- Pure state entanglement

Encoding classical data

exponentially many degrees of freedom
in n qubit superposition (2^n amplitudes)

$$\Downarrow$$

encode $\approx 2^n$ classical bits in n qubits ?

No! Measurements limit access to information

Holevo Theorem (1973)

$X = x_1 \cdots x_m$

$\{p_x, x\}$

$\left.\begin{array}{l} \rightarrow \\ \rightarrow \\ \rightarrow \end{array}\right\}$ measure $\Rightarrow Y$

n qubits

Then, $I(X:Y) \leq n$

$H(X) + H(Y) - H(XY)$

Holevo Bound

if

$$X = \{ p_x, x \}$$

$$x \mapsto \rho_x \quad (n \text{ qubits})$$

measurement of ρ_X gives Y

Then
$$I(X:Y) \leqslant \underbrace{S(\rho) - \sum_x p_x S(\rho_x)}_{\text{accessible information}}$$

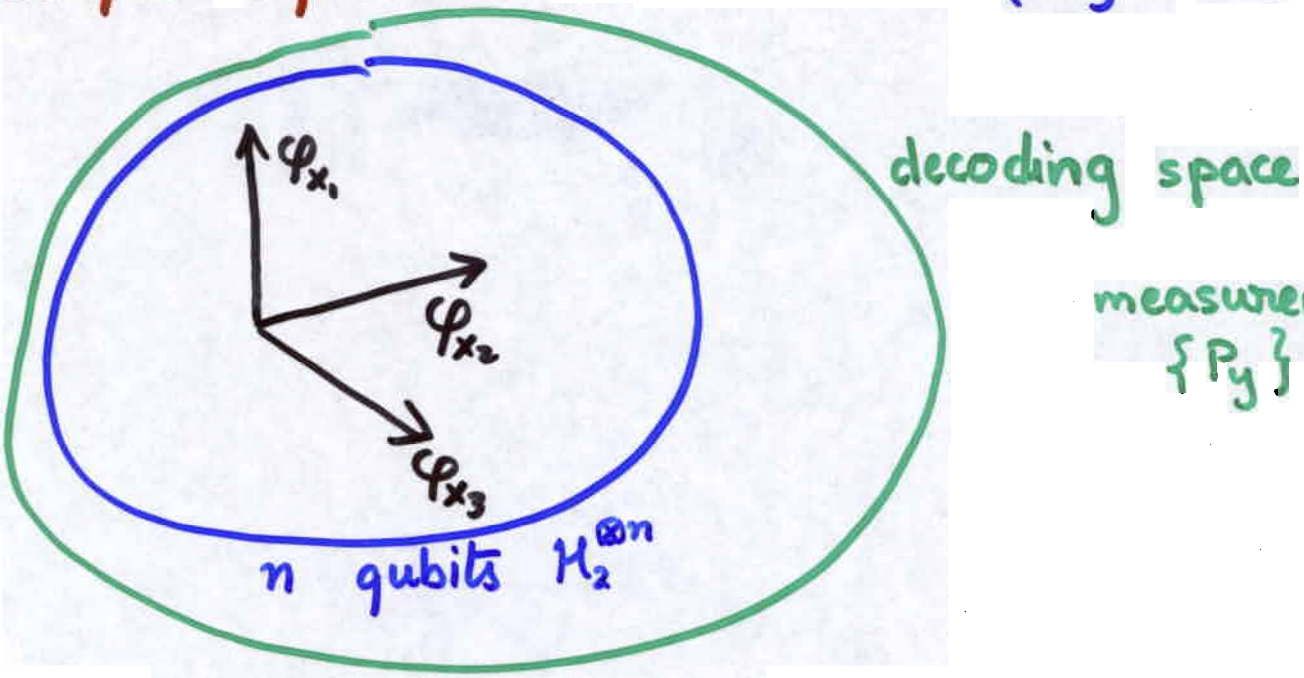
where
$$\rho = \sum_x p_x \rho_x$$

Corollary :

- $I(X:Y) \leqslant S(\rho) \leqslant n$

- if X uniform over $\{0,1\}^m$ & $Y = X$, then $m \leqslant n$

Simpler explanation (Nayak '99)



X – uniformly distributed over $\{0,1\}^m$

Pr[correct decoding]

$$= \frac{1}{2^m} \sum_x \| P_x |\varphi_x\rangle \|^2$$

$$= \frac{1}{2^m} \sum_{x,j} |\langle \varphi_x | e_{x,j}\rangle|^2$$

$$\leq \frac{1}{2^m} \sum_{x,j} \| Q |e_{x,j}\rangle \|^2$$

projection onto $\mathcal{H}_2^{\otimes n}$

$$= \frac{1}{2^m} \mathrm{Tr}(Q) \leq \frac{2^n}{2^m}$$

Quantum Data Compression

Source produces "text" $|\psi_x\rangle$ with prob. p_x

$\{p_x,\ \psi_x\}$ encode $\longrightarrow$ $\}$ decode $\Longrightarrow$ $\tilde{\psi}_x$

m qubits n qubits

Can tolerate

1) error in reconstruction

would like $\sum_x p_x \left|\langle \psi_x | \tilde{\psi}_x \rangle\right|^2 \geq 1-\delta$

2) probability of failure

would like (1) to hold with prob. $\geq 1-\varepsilon$

Schumacher '95

asymptotically $S(\rho)$ qubits are necessary & sufficient

The compression procedure

source $\quad X = \{p_x, \psi_x\}$

$$\rho \triangleq \rho_X = \sum_x p_x |\psi_x\rangle\langle\psi_x|$$

$$= \sum_y \lambda_y \, |e_y\rangle\langle e_y| \quad \text{in diagonal form}$$

$$S \triangleq S(X) = \mathop{\mathbb{E}}_{Y} \log \frac{1}{\lambda_Y}$$

Consider $k \gg 1$ copies of X $\qquad X^{\otimes k}$

and the equivalent sources $Y_1 \cdots Y_k$

Law of large numbers: with prob $\geq 1-\varepsilon$

$$\left| \frac{1}{k} \sum_i \log \frac{1}{\lambda_{Y_i}} - S \right| \leq \nu$$

$$\Updownarrow$$

$$2^{-k(S+\nu)} \leq \text{prob}(Y_1 \cdots Y_k) \leq 2^{-k(S-\nu)}$$

Typical sequence

Typical sequence

$y_1 \cdots y_k$ s.t. $2^{-k(S+\nu)} \leq \Pr(\vec{Y} = \vec{y}) \leq 2^{-k(S-\nu)}$

By definition

$\Pr(\vec{Y} \text{ is typical}) \geq 1-\varepsilon$

$\#(\text{typical sequences}) \leq 2^{k(S+\nu)}$

Typical subspace T

spanned by $|e_{y_1}\rangle |e_{y_2}\rangle \cdots |e_{y_k}\rangle$

where $\vec{y}$ is typical.

Let Π = orthogonal projection onto T

Since $\dim T \leq 2^{k(S+\nu)}$ $\exists$ unitary U that maps basis state $|e_{y_1}\rangle \cdots |e_{y_k}\rangle$ to state $|j\rangle$ over $k(S+\nu)$ qubits

Encoding procedure   source $X^{\otimes k}$

measure according to $(\Pi, I-\Pi)$:

if the sequence is typical,

compress state into $k\cdot(S+\nu)$ qubits

using unitary U.

if not, send $|junk\rangle$

Decoding procedure

if state received $= |junk\rangle$, fail.

else, apply $U^\dagger$ to get a state in T.

Analysis of the procedure

- \# qubits transmitted $= k \cdot (s+\nu)$

  $s+\nu$ per signal

- Fidelity (when procedure succeeds)

$$\sum_{\vec{x}} p_{\vec{x}} \left|\langle \psi_{\vec{x}} | \Pi | \psi_{\vec{x}} \rangle\right|^2$$

$$= \sum_{\vec{x}} p_{\vec{x}} \left\| \Pi |\psi_{\vec{x}}\rangle \right\|^4$$

$$\geq \sum p_{\vec{x}} \left(2 \left\| \Pi |\psi_{\vec{x}}\rangle \right\|^2 - 1 \right)$$

$$\geq 2 \sum p_{\vec{x}} \, \mathrm{Tr}\left(\Pi |\psi_{\vec{x}}\rangle\langle \psi_{\vec{x}}| \right) - 1$$

$$\geq 2(1-\varepsilon) - 1 \geq 1 - 2\varepsilon$$

- Probability of failure $\leq \varepsilon$

Data compression

- source $X = \{p_x, \psi_x\}$ entropy S can be compressed to $\lesssim S$ qubits

- similar arguments show $\gtrsim S$ qubits are necessary.

Summary

- measure of quantum information

  von Neumann entropy

- accessible information

  Holevo bound

- vN entropy as incompressible information content