### **Shannon's Noisy Channel Coding Theorem**

Alice noisy channel

Alice Bob  $X = \{x, y(x)\}$  errors specified by y(y(x))  $y = \{y, y(y)\}$ 

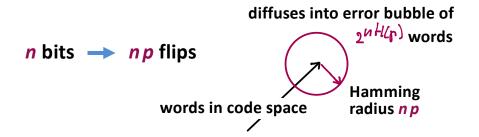
Alice & Bob need redundancy to communicate reliably over a noisy channel. How much?

Key Question: Can we always find a reliable code when the message length n→∞?

Binary alphabet:  $\{o_{i}\}$  p(no flip) = 1 - p p(flip) = n p(old) = p(1|1) = 1 - p p(old) = p(1|0) = p

Basic Idea: Encode k bits of info in block of size nWe define the Code Rate  $R = \frac{k}{n}$ 

Optimal Code: max # of bits must flip to interchange code words



Reliable Decoding: Error bubbles must not overlap

Setting  $k = \eta R$  and solving for the Code Rate we get

$$R \le 1 - H(\eta) = C(\eta)$$
 Channel Capacity

### **Quantum Information Theory:**

#### **Key Results** from Classical Information Theory

\* Message of letters drawn from ensemble  $\{x, \eta(x)\}$ 

Shannon Info H(X) =# of incompressible bits per letter in limit  $N \rightarrow \infty$ 

\* Correlation between sent (X) and received (Y) messages

Mutual Info 
$$\mathbb{D}(X,Y) = H(X) - H(X|Y)$$
$$= H(Y) - H(Y|X)$$

# of bits of info about (X) learned from (Y)

#### **Quantum Information Theory**

Need to generalize these concepts

#### **Basic Scenario:**

Alice sends letters drawn from the ensemble

**Bob reads** message by measuring the POVM

We define the von Neumann Entropy

$$S(g) = -Tr(glogg)$$

In the eigenbasis of  ${f e}$  we have

$$g = \sum_{\lambda} \lambda |\lambda \times \lambda| \Rightarrow$$

$$S(g) = -\sum_{\lambda} \lambda |\log_{\lambda} |\lambda \times \lambda| = H(\Lambda)$$

Shannon Entropy of the ensemble  $\Lambda = \{ |\lambda \rangle, \lambda \}$ 

#### **Basic Scenario:**

Alice sends letters drawn from the ensemble

**Bob reads** message by measuring the POVM

We define the von Neumann Entropy

In the eigenbasis of  $\mathcal{G}$  we have

$$g = \sum_{\lambda} \lambda |\lambda \times \lambda| \Rightarrow$$

$$S(g) = -\sum_{\lambda} \lambda |\log \lambda |\lambda \times \lambda| = H(\Lambda)$$

Shannon Entropy of the ensemble  $\Lambda = \{\lambda > \lambda\}$ 

#### **Conclusion:**

- \* If the alphabet consists of mutually orthogonal pure states then the quantum source reduces to a classical source
- \* In that case all signal states are perfectly distinguishable

$$*S(g) = H(\Lambda)$$

We can show the Von Neumann entropy quantifies

- \* The incompressible information content of a quantum source
- \* The quantum information content per quantum letter
- \* The classical information content per quantum letter (extractable by POVM)
- \* Entanglement of a bipartite pure state

#### **Conclusion:**

- \* If the alphabet consists of mutually orthogonal pure states then the quantum source reduces to a classical source
- \* In that case all signal states are perfectly distinguishable
- $*S(g) = H(\Lambda)$

#### We can show the Von Neumann entropy quantifies

- The incompressible information content of a quantum source
- \* The quantum information content per quantum letter
- \* The classical information content per quantum letter (extractable by POVM)
- \* Entanglement of a bipartite pure state

# Mathematical properties of S(g) (No proofs, see Preskill)

- (1) Purity  $g = |4 \times 4| \rightarrow S(g) = 0$
- (2) Invariance  $S(UgU^+) = S(g)$
- (3) Maximum g has d eigenvalues  $\neq 0 \Rightarrow S(g) \leq log d$
- (4) Concavity For  $\lambda_1, \lambda_2, \dots, \lambda_n \ge 0$ ,  $\sum_i \lambda_i = 1$   $\longrightarrow$   $S(\lambda_1 g_1 + \dots + \lambda_n g_n) \ge \lambda_1 S(g_1) + \dots + \lambda_n S(g_n)$

 $\Big(egin{array}{c} extsf{vNE} & extsf{grows} & extsf{when} & extsf{ignorant} & extsf{of} \ extsf{how} & extsf{the state} & extsf{was} & extsf{prepared} \ extsf{of} \ extsf{of}$ 

(6) Entropy of Measurement (Q Meas adds randomness)

Measure 
$$A = \sum_{y} a_{y} |a_{y} \times a_{y}|$$
 outcomes  $Y = \{a_{y}, \gamma(a_{y})\}$ 

- S. E. of outcomes  $H(Y) \geq S(g), W/"="for [A,g] = 0$
- (7) Entropy of Preparation (Mix N. O. states cannot recover full info

Draw from 
$$\{|\varphi_{\kappa}\rangle, \eta_{\kappa}\}, g = \sum_{x} \eta_{x} |\varphi_{x} \chi \varphi_{x}| \rightarrow H(\chi) \geq S(g)$$

# Mathematical properties of S(g) (No proofs, see Preskill)

(1) Purity 
$$Q = |4 \times 4| \longrightarrow S(Q) = 0$$

(2) Invariance 
$$S(UgU^+) = S(g)$$

(3) Maximum 
$$g$$
 has  $d$  eigenvalues  $\neq 0 \rightarrow S(g) \leq log d$ 

(4) Concavity

For 
$$\lambda_1, \lambda_2, \dots, \lambda_n \ge 0$$
,  $\sum_i \lambda_i = 1$ 
 $S(\lambda_1 g_1 + \dots + \lambda_n g_n) \ge \lambda_1 S(g_1) + \dots \lambda_n S(g_n)$ 

(vNE grows when ignorant of how the state was prepared)

(6) Entropy of Measurement (Q Meas adds randomness)

Measure 
$$A = \sum_{\eta} a_{\eta} |a_{\eta} \times a_{\eta}|$$
 outcomes  $Y = \{a_{\eta}, \gamma(a_{\eta})\}$ 

S. E. of outcomes 
$$H(Y) \geq S(g)$$
,  $W/"="for [A,g] = 0$ 

(7) Entropy of Preparation (Mix N. O. states cannot recover full info

Draw from 
$$\{ |\varphi_{\kappa}\rangle, \eta_{\kappa} \}, g = \sum \eta_{\kappa} |\varphi_{\kappa} \times \varphi_{\kappa}| \rightarrow H(X) \geq S(g)$$

# Mathematical properties of S(g) (No proofs, see Preskill)

(8) <u>Subadditivity</u> (info in whole ≤ sum of info in parts)

$$S(Q_{AB}) \leq S(Q_{A}) + S(Q_{B})$$
 (classical  $H(X,Y) \leq H(X) + H(Y)$  with)

"=" when  $X, Y$  uncorrelated)

(9) <u>Triangle inequality</u> (uncertainty about whole can be less than uncertainty about parts)

$$S(Q_{AB}) \ge |S(Q_A) - S(Q_B)|$$
 (classical  $H(X,Y) \ge H(X), H(Y)$ )

### **Quantum Data Compression**

(Quantum analog of Shannons Noiseless Coding Theorem)

Starting Point: n-letter message drawn from  $\{ \iota \varphi_k \geq_{n} \gamma_{k} \}$ 



Each letter described by 
$$g = \sum_{x} \eta_{x} 1 Q_{x} \times Q_{x}$$

Message described by 
$$g^n = g \otimes g \otimes \dots \otimes g$$

**Basic Question:** How redundant is this information?

- is there a "quantum code" which can compress to a smaller Hilbert space while retaining the fidelity of the encoded quantum information?

**Answer**: Optimal Compression requires

$$Log(dim \mathcal{X}) = n S(g)$$
 qubits

(Schumacher's Theorem)

Corrollary: The von Neumann entropy is the # of qubits carried per letter in a message. We can always compress unless  $\mathcal{C} = \frac{1}{2} \mathbf{1}$ 

**Example** of how we might do this:

Alice sends a message using the alphabet  $\frac{|f_2\rangle}{|f_2\rangle}, \quad |f|=\frac{1}{2}$ 

Symmetry  $\longrightarrow$  eigenvectors are  $\uparrow$ ,  $\downarrow$  along  $\vec{n} = \frac{1}{\sqrt{9}} (\vec{x} + \vec{2})$ 

eigenvectors
$$\begin{cases}
|0'\rangle = |\widehat{\eta}\rangle = \begin{pmatrix} \cos \overline{u}/g \\ \sin \overline{u}/g \end{pmatrix} \\
|t'\rangle = |\widehat{J}_{\vec{N}}\rangle = \begin{pmatrix} \sin \overline{u}/g \\ -\cos \overline{u}/g \end{pmatrix}$$

eigenvalues
$$\begin{cases}
\lambda(0^{1}) = \frac{1}{2} + \frac{1}{2\sqrt{2}} = \cos^{2} \frac{1}{2} \\
\lambda(1^{1}) = \frac{1}{2} - \frac{1}{2\sqrt{2}} = \sin^{2} \frac{1}{2}
\end{cases}$$

Corrollary: The von Neumann entropy is the # of qubits carried per letter in a message. We can always compress unless  $\mathcal{Q} = \frac{1}{2} \mathbf{1}$ 

#### **Example** of how we might do this:

Alice sends a message using the alphabet  $\frac{|\mathcal{T}_{2}\rangle}{|\mathcal{T}_{k}\rangle}, \quad |\mathcal{T}|^{-1/2}$ 

Symmetry  $\longrightarrow$  eigenvectors are  $\uparrow$ ,  $\downarrow$  along  $\vec{n} = \frac{1}{\sqrt{9}} (\vec{x} + \vec{2})$ 

eigenvectors
$$\begin{cases}
|0'\rangle = |\widehat{1}_{N}\rangle = \begin{pmatrix} \cos \overline{u}/g \\ \sin \overline{u}/g \end{pmatrix} \\
|t'\rangle = |J_{N}\rangle = \begin{pmatrix} \sin \overline{u}/g \\ -\cos \overline{u}/g \end{pmatrix} \\
\frac{\lambda(0')}{1} = \frac{1}{2} + \frac{1}{2\sqrt{2}} = \cos^{2}\overline{u}/g \\
\lambda(1') = \frac{1}{1} - \frac{1}{2\sqrt{1}} = \sin^{2}\overline{u}/g
\end{cases}$$

Overlap 
$$\begin{cases} \langle 0'| T_2 \rangle^2 = \langle 0'| T_x \rangle^2 = \cos^2 T /_3 = 0.9535 \\ \langle 1'| T_2 \rangle^2 = \langle 1'| T_x \rangle^2 = \sin^2 T /_3 = 0.1465 \end{cases}$$

If Bob does not know what was sent, best guess is 14>= 10'>

$$\Rightarrow \quad f = \langle 4|g|4\rangle = \frac{1}{2}|\langle 1_{2}|4\rangle|^{2} + \frac{1}{2}|\langle 1_{x}|4\rangle|^{2} = 0.8535$$

#### Scenario:

Alice wants to send a 3-qubit message, but can transmit only 2 qubits. Could send Bob those qubits (4:1) and have Bob guess (6) for the third

#### How to improve:

Diagonalize 
$$g$$

Likely subspace  $|0'\rangle$ 

for 1 bit

Unlikely subspace  $|1'\rangle$ 

either  $|1\rangle$  or  $|1\rangle$ 

Note: all possible  $|1\rangle$  have the same overlap with states of the type  $|1\rangle$ 

where  $i,j,k \in \{o',1'\}$ 

Corrollary: The von Neumann entropy is the # of qubits carried per letter in a message. We can always compress unless  $\mathcal{Q} = \frac{1}{2} \mathbf{1}$ 

#### **Example** of how we might do this:

Alice sends a message using the alphabet

Symmetry  $\longrightarrow$  eigenvectors are  $\uparrow$ ,  $\downarrow$  along  $\vec{n} = \frac{1}{\sqrt{2}} (\vec{x} + \vec{2})$ 

eigenvectors
$$\begin{cases}
|0'\rangle = |\Upsilon_{\vec{N}}\rangle = \begin{pmatrix} \cos \pi/g \\ \sin \pi/g \end{pmatrix} \\
|t'\rangle = |J_{\vec{N}}\rangle = \begin{pmatrix} \sin \pi/g \\ -\cos \pi/g \end{pmatrix}
\end{cases}$$
eigenvalues
$$\begin{cases}
\lambda(0!) = \frac{1}{2} + \frac{1}{2\sqrt{2}} = \cos^2 \pi/g \\
\lambda(1!) = \frac{1}{1} - \frac{1}{2\sqrt{1}} = \sin^2 \pi/g
\end{cases}$$

Overlap  $\begin{cases} \langle 0'| T_2 \rangle^2 = \langle 0'| T_x \rangle^2 = \cos^2 T T_8 = 0.9535 \\ \langle 1'| T_2 \rangle^2 = \langle 1'| T_x \rangle^2 = \sin^2 T T_8 = 0.1465 \end{cases}$ 

#### How to improve:

Diagonalize 
$$\mathcal{G}$$

Likely subspace  $0^{\circ}$  for 1 bit

Unlikely subspace  $1^{\circ}$ 

either 
$$| \hat{\eta}_{2} \rangle$$
 or  $| \hat{\eta}_{x} \rangle$ 

Let  $| \psi_{1} \rangle = | \psi_{1} \rangle | \psi_{2} \rangle$ 

Note: all possible  $| \psi_{2} \rangle$  have the same overlap with states of the type  $| i \rangle | i \rangle | \psi_{2} \rangle$ 

where  $| i \rangle | k \in \{ \mathcal{O}'_{1}, 1' \}$ 

Note: for any (♦>) drawn from Alice and Bobs alphabet, we have

#### Likely subspace $\Lambda$

$$|\langle 0'0'0'| \psi \rangle|^2 = \cos^6 \frac{\pi}{3} = 0.6219$$

$$|\langle 0'0'0'| \psi \rangle|^2 = |\langle 0'1'0'| \psi \rangle|^2 = |\langle 1'0'0'| \psi \rangle|^2 = \cos^4 \frac{\pi}{3} \sin^2 \frac{\pi}{3} = 0.1067$$

### Unlikely subspace $\Lambda^{\perp}$

Overlap 
$$\begin{cases} \langle 0'| \Upsilon_{2} \rangle^{2} = \langle 0'| \Upsilon_{x} \rangle^{2} = \cos^{2} \pi \gamma_{3} = 0.9535 \\ \langle 1'| \Upsilon_{2} \rangle^{2} = \langle 1'| \Upsilon_{x} \rangle^{2} = \sin^{2} \pi \gamma_{3} = 0.1465 \end{cases}$$

#### How to improve:

either 
$$\{\hat{\tau}_{2}\}$$
 or  $\{\hat{\tau}_{x}\}$ 

Let  $\{\hat{\tau}_{2}\} = \{\hat{\tau}_{1}\} \{\hat{\tau}_{2}\} \{\hat{\tau}_{3}\}$ 

Note: all possible  $\{\hat{\tau}_{1}\}$  have the same overlap with states of the type  $\{\hat{\tau}_{1}\}\{\hat{\tau}_{2}\}$ 

where  $\{\hat{\tau}_{1}\}\{\hat{\tau}_{2}\}\{\hat{\tau}_{3}\}$ 

Note: for any | transport | drawn from Alice and Bobs alphabet, we have

#### Likely subspace $\Lambda$

$$|\langle 0'0'0'| \mathcal{T} \rangle|^{2} = \cos^{6} \sqrt[4]{g} = 0.6219$$

$$|\langle 0'0'0'| \mathcal{T} \rangle|^{2} = |\langle 0'0'0'| \mathcal{T} \rangle|^{2} = |\langle 1'0'0'| \mathcal{T} \rangle|^{2} = \cos^{4} \frac{11}{g} \sin^{2} \frac{17}{g} = 0.1067$$

### Unlikely subspace $\Lambda$

$$|\langle 0'1'1'| \psi \rangle|^2 = |\langle 1'0'1'| \psi \rangle|^2 = |\langle 1'1'0'| \psi \rangle|^2 = \cos^2 \frac{\pi}{3} \sin^4 \frac{\pi}{3} = 0.0183$$

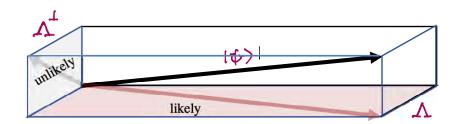
$$|\langle 1'1'1'| \psi \rangle|^2 = \sin^6 \frac{\pi}{3} = 0.0031$$

This structure of message space suggests Alice should send only the part  $\in \Lambda$ , which fits in 2 qubits ( $\emptyset$  in  $\Lambda = \gamma$ ). She can do this by performing a measurement that projects her 3-qubit state onto either  $\Lambda$  or  $\Lambda^{\perp}$ 

$$P_{likely} = 0.6219 + 3 \times 0.1067 = 0.9419$$

$$P_{unlikely} = 3 \times 0.0183 + 0.0031 = 0.0531$$

Geometric illustration of a space with likely and unlikely subspaces.



The state vector (black) has a large projection on the "likely subspace" (pink), and a much smaller projection on the "unlikely subspace" (grey). Accordingly, when we project onto the likely subspace and ignore the unlikely subspace, we don't loose much information.

Overlap 
$$\begin{cases} \langle 0'| \Upsilon_2 \rangle^2 = \langle 0'| \Upsilon_K \rangle^2 = \cos^2 \pi \gamma_3 = 0.9535 \\ \langle 1'| \Upsilon_2 \rangle^2 = \langle 1'| \Upsilon_K \rangle^2 = \sin^2 \pi \gamma_3 = 0.1465 \end{cases}$$

#### How to improve:

either 
$$\{\hat{\eta}_2\}$$
 or  $|\hat{\eta}_2\rangle$   
Let  $|\psi\rangle = |\psi_1\rangle |\psi_2\rangle |\psi_3\rangle$ 

where  $i_{i,j}, k \in \{0, 1'\}$ 

Note: for any | drawn from Alice and Bobs alphabet, we have

#### Likely subspace $\Lambda$

$$|\langle 0'0'0'| \psi \rangle|^2 = \cos^6 \pi /_g = 0.6219$$

$$|\langle 0'0'0'| \psi \rangle|^2 = |\langle 0'0'0'| \psi \rangle|^2 = \cos^4 \frac{\pi}{3} \sin^2 \frac{\pi}{3} = 0.1067$$

### Unlikely subspace $\Lambda^{\perp}$

$$|\langle 0'1'1'| \psi \rangle|^{2} = |\langle 1'0'1'| \psi \rangle|^{2} = |\langle 1'0'1'| \psi \rangle|^{2} = |\langle 1'0'| \psi \rangle|^{2}$$

This structure of message space suggests Alice should send only the part  $\in \Lambda$ , which fits in 2 qubits ( $\emptyset$  in  $\Lambda = \gamma$ ). She can do this by performing a measurement that projects her 3-qubit state onto either  $\Lambda$  or  $\Lambda^{\perp}$ 

$$\begin{cases}
P_{\text{likely}} = 0.6219 + 3 \times 0.1067 = 0.9419 \\
P_{\text{unlikely}} = 3 \times 0.0183 + 0.0031 = 0.0531
\end{cases}$$

To do this Alice can apply the Unitary Transformation **U** that maps

She measures the 3<sup>rd</sup> qubit

$$\begin{cases} \text{lo} \Rightarrow \text{ projects onto } \Lambda \\ \text{li} \Rightarrow \text{ projects onto } \Lambda^{\perp} \end{cases}$$

If Alice's outcome is to she sends | \$\psi\_{comp} > = |\cdot > |\cdot > \cdot > |\cdot > |\cd

Bob decompresses by appending [6'> and undoing U

This structure of message space suggests Alice should send only the part  $\in \Lambda$ , which fits in 2 qubits ( $\lim_{n \to \infty} \Lambda = q$ ). She can do this by performing a measurement that projects her 3-qubit state onto either  $\Lambda$  or  $\Lambda^{\perp}$ 

$$\begin{cases}
P_{\text{likely}} = 0.6219 + 3 \times 0.1067 = 0.9419 \\
P_{\text{unlikely}} = 3 \times 0.0183 + 0.0031 = 0.0581
\end{cases}$$

To do this Alice can apply the <u>Unitary Transformation</u>
U that maps

She measures the 3<sup>rd</sup> qubit

$$\begin{cases} |0^i\rangle \rightarrow \text{ projects onto } \Lambda \\ |1^i\rangle \rightarrow \text{ projects onto } \Lambda^{\perp} \end{cases}$$

If Alice's outcome is  $|0\rangle$  she sends  $|\sqrt[4]{comp}\rangle = |\bullet\rangle|\bullet\rangle$ Bob decompresses by appending  $|0\rangle$  and undoing U

If Alice's outcome is 11') she sends Ulo'o'>

This leaves Bob with the state

$$S_{Bob} = E|\Phi \times \psi|E + \langle \psi|1 - E|\psi \rangle |O'O'O'XO'O'O'|$$
(E= projection on  $\Lambda$ )

which has Fidelity

$$\mathcal{G} = \langle \psi | g_{600} | \psi \rangle$$

$$= \langle \psi | E | \psi \rangle + \langle \psi | 1 - E | \psi \rangle | \langle \psi | 0'0'0' \rangle |^{2}$$

$$= 0.9419^{2} + 0.0521 \times 0.6219 = 0.9224 > 0.8525$$

As with classical data compression, longer messages allow for more compression or compression without loss.

In Quantum Communication one has the option of choosing an alphabet where the individual letters are mixed states. This makes it much more challenging to find bounds for compressibility and code rates. See Preskill Chapter 5 for more information.