Classical and Quantum Information Theory (Preskill ch. 4)

Key Elements of Information Theory.

Classical Information Theory is mostly about two things.

(1) How much redundancy is present in a typical message?
Shannon showed that an n-letter message composed of letters a_x drawn from an alphabet ($a_1, a_2, a_3, \ldots a_k$), with a priori probability of occurrence $p(a_x)$. can be compressed to $n\mathrm{H}(p)$, where $\mathrm{H}(p)$ is the Shannon Entropy.

(2) How much redundancy must be added to a message in order to communicate reliably over a noisy channel. Shannon's Noisy Channel Coding Theorem tells us that the code rate R must be less than or equal to the Channel Capacity

$$R \leq 1 - H(\mathrm{p}) = C(p)$$

(3) There are other entropic measures such as Joint Entropy, Conditional Entropy (p8), Mutual Information (p9), etc. All of these ideas and concepts translate to Quantum Information.

Quantum Information Theory is largely based on further developments of the ideas and concepts above.

Key Elements of Quantum Information Theory.

(1) A quantum message consists of letters drawn from a quantum alphabet, $\{\rho_x, p(\mathrm{x})\}$. The message is thus of the form $\rho = \Sigma_x\, p(\mathrm{x})\rho_x$.Note that the message is a tensor product $\rho = \rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \ldots \otimes \rho_k$, where the individual letters can be pure or mixed states.

We define the Von Neumann Entropy $S(\rho) = -Tr(\rho \,\mathrm{Log}(\rho))$. It can be shown that $S(\rho)$ is the number of incompressible quantum bits per letter in the message.

In the eigenbasis of ρ, the letters can be expressed as $\rho = \Sigma_\lambda\, \lambda|\lambda\rangle\langle\lambda|$. Also,

$$S(\rho) = \mathrm{Tr}\,(\, \Sigma_\lambda\, \lambda \log(\lambda)\, |\lambda\rangle\langle\lambda|) = \mathrm{H}(\Lambda) \qquad \text{(page 11).}$$

Thus, if the alphabet consists of mutually orthogonal pure states, then the quantum source reduces to a classical source, i.e, $S(\rho) = \mathrm{H}(\Lambda)$, and most everything we have learned about Shannon Information carries over.

(2) The Von Neuman entropy has a number of information theoretical properties, the first 3 of which are straightforward, while the remaining 9 listed by Preskill are increasingly obtuse when working one's way down the list. (page 13).

Quantum Data Compression

(1) This is the quantum analogy to Shannons Noiseless Coding Theorem. Preskill offers an example of quantum data compression, but needs to do an awfull lot of work to achieve a very modest gain. Thus, we should probably conclude that this is a proof of principle, but not necessarily something that we might do to improve quantum data storage or tyhroughput. To summarize:

(2) Preskills first step is to use an alphabet of non-orthogonal letters, $|\uparrow_Z\rangle$, $|\uparrow_X\rangle$, each occurring with probability $p = 1/2$. The letters are then of the form

$$\rho = 1/2\, |\uparrow_z\rangle\langle\uparrow_z| + 1/2\, |\uparrow_x\rangle\langle\uparrow_x|$$

(3) Looking at the message in the diagonal basis, $|0'\rangle$ and $|1'\rangle$ (page 17), it is clear that both letters overlap strongly with $|0'\rangle$ and weakly with $|1'\rangle$. In this situation it is possible for Alice to significantly compress her message by projecting onto Likely and Unlikely Subspaces (page 20). The non-obvious choices of letters, $|\uparrow_Z\rangle$, $|\uparrow_X\rangle$, and thus the diagonal representation $|0'\rangle$, $|1'\rangle$ for the compressed state, is chosen to ensure that "compression" onto the likely and unlikely subspaces is likely to succeed (21/22). Preskill adds a few more bells and whistles to recover as much as possible of the information that was projected onto the unlikely subspace, page (185/186). When all is said and done, the fidelity of the transmitted state is only improved by ~2% relative to the simple strategy of sending two bits and having Bob guess the third.

Uses of Entanglement (Preskill ch. 4)

Information in entangled Qubit pairs

2 spins ⇨ $\mathcal{D}im(\mathcal{E} = \mathcal{E}_A \otimes \mathcal{E}_B)$ 2 bits of information

* We can store this info in product states

  ⇨ the info is locally available to Alice & Bob

* Alternatively, we can store this info in EPR basis

$$\left.\begin{array}{l} |\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle) \\ |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle) \end{array}\right\} \text{maximally entangled states}$$

$$\left.\begin{array}{l} \text{Parity bit } (|\varphi\rangle \text{ or } |\psi\rangle) \\ \text{Phase bit } (\text{"}+\text{" or "}-\text{"}) \end{array}\right\} \text{not locally accessible to Alice \& Bob}$$

* Perhaps surprisingly, info stored in the EPR basis can be manipulated locally:

Alice applies σ_x to spin A ⇨ flips $|\uparrow_A\rangle \leftrightarrow |\downarrow_A\rangle$

$$\Rightarrow \left\{\begin{array}{l} |\varphi^+\rangle \leftrightarrow |\psi^+\rangle \\ |\varphi^-\rangle \leftrightarrow -|\psi^-\rangle \end{array}\right.$$

* Local Unitary U can change any max entangled Bell state to any other!

* Global Unitary U (e. g., $CNOT$) needed to change entangled states to product states and vice versa

Uses of Entanglement (Preskill ch. 4)

Information in entangled Qubit pairs

2 spins ⇒ $\mathcal{D}im(\mathcal{E} = \mathcal{E}_A \otimes \mathcal{E}_B)$ 2 bits of information

* We can store this info in product states
  ⇒ the info is locally available to Alice & Bob

* Alternatively, we can store this info in EPR basis

$$\left.\begin{array}{l} |\varphi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle\right) \\ |\psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle\right) \end{array}\right\} \text{maximally entangled states}$$

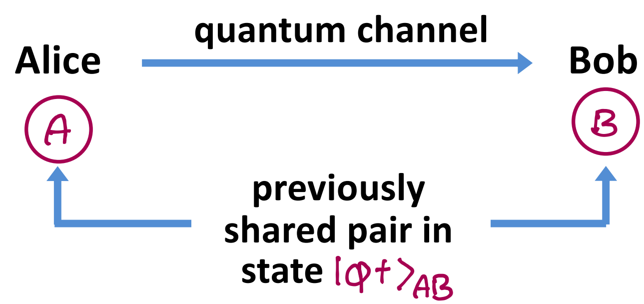
$$\left.\begin{array}{l} \text{Parity bit } (|\varphi\rangle \text{ or } |\psi\rangle) \\ \text{Phase bit } (\text{"+" or "−"}) \end{array}\right\} \text{not locally accessible to Alice \& Bob}$$

* Perhaps surprisingly, info stored in the EPR basis can be manipulated locally:

Alice applies σ_x to spin A ⇒ flips $|\uparrow_A\rangle \leftrightarrow |\downarrow_A\rangle$

$$\Rightarrow \begin{cases} |\varphi^+\rangle \leftrightarrow |\psi^+\rangle \\ |\varphi^-\rangle \leftrightarrow -|\psi^-\rangle \end{cases}$$

Quantum Dense Coding



Basic resource - shared Bell states

$$\boxed{\begin{array}{l} |\varphi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle\right) \\ |\psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right) \end{array}}$$

Protocol:

(1) Alice applies one of 4 local unitaries

$U = \mathbb{1}$: $|\varphi^+\rangle_{AB} \rightarrow |\varphi^+\rangle_{AB}$ $\quad$ $U = \sigma_y$: $|\varphi^+\rangle_{AB} \rightarrow |\psi^-\rangle_{AB}$

$U = \sigma_x$: $|\varphi^+\rangle_{AB} \rightarrow |\psi^+\rangle_{AB}$ $\quad$ $U = \sigma_z$: $|\varphi^+\rangle_{AB} \rightarrow |\varphi^-\rangle_{AB}$

(2) Alice sends A to Bob over the quantum channel

(3) Bob does measurement on AB that distinguishes the 4 Bell states → Bob receives 2 classical bits of information.

* Proof of principle: entanglement is a resource for communication

Uses of Entanglement (Preskill ch. 4)

Quantum Dense Coding

Alice $\xrightarrow{\text{quantum channel}}$ Bob

A B

previously shared pair in state $|\phi^+\rangle_{AB}$

Basic resource - shared Bell states

$$\boxed{\begin{aligned} |\phi^\pm\rangle &= \tfrac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle\right) \\ |\psi^\pm\rangle &= \tfrac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right) \end{aligned}}$$

Protocol:

(1) Alice applies one of 4 local unitaries

$U = \mathbb{1}: \ |\phi^+\rangle_{AB} \rightarrow |\phi^+\rangle_{AB}$ $U = \sigma_y: \ |\phi^+\rangle_{AB} \rightarrow |\psi^-\rangle_{AB}$

$U = \sigma_x: \ |\phi^+\rangle_{AB} \rightarrow |\psi^+\rangle_{AB}$ $U = \sigma_z: \ |\phi^+\rangle_{AB} \rightarrow |\phi^-\rangle_{AB}$

(2) Alice sends A to Bob over the quantum channel

(3) Bob does measurement on AB that distinguishes the 4 Bell states → Bob receives 2 classical bits of information.

* Proof of principle: entanglement is a resource for communication

Note: It is really hard to store entangled qubits

Alice & Bob must probably use channel immediately beforehand ⇨ no obvious gain

But: The message is unconditionally secure, an eavesdropper learns nothing from intercepting Alice's qubit in transmission

Quantum Key Distribution

Alice $\xrightarrow{\text{secure message}}$ Bob

Provably secure coding scheme: Private key (shared random bit string)

Example:

message →	⊕ key →	encrypted →	⊕ key
10100110	11010111	01110001	10100110

info entirely in message/key correlations

Uses of Entanglement (Preskill ch. 4)

Quantum Key Distribution

Alice $\xrightarrow{\text{secure message}}$ Bob

Provably secure coding scheme: Private key (shared random bit string)

Example:

message	$\rightarrow$	$\oplus$ key	$\rightarrow$	encrypted	$\rightarrow$	$\oplus$ key
10100110		11010111		01110001		10100110

info entirely in message/key correlations

Key Challenge of cryptography: Secure key distribution

Conventional methods

* Exchange by courier ← inconvenient, 3rd party not secure
* Public Key (RSA) ← not provably secure

Idea: Rely on QM for security

Alice (A) $\xrightarrow{\text{quantum channel}}$ (B) Bob

shared pairs in $|\psi^-\rangle_{AB}$

Singlet
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right)$$
Bell state

Protocol:

(1) Alice & Bob each measure σ_x or σ_y at random

(2) Alice & Bob exchange classical info on measurement bases, discard pairs when bases where different

⇨ Remaining qubits are perfectly correlated (private key)

What about eavesdropping?

Can Eve gain access to key? – not by intercepting individual qubits

npj | Quantum Information

ARTICLE OPEN

Check for updates

Finite key effects in satellite quantum key distribution

Jasminder S. Sidhu[1,2]✉, Thomas Brougham[1,2], Duncan McArthur[1], Roberto G. Pousa[1] and Daniel K. L. Oi[1]✉

Global quantum communications will enable long-distance secure data transfer, networked distributed quantum information processing, and other entanglement-enabled technologies. Satellite quantum communication overcomes optical fibre range limitations, with the first realisations of satellite quantum key distribution (SatQKD) being rapidly developed. However, limited transmission times between satellite and ground station severely constrains the amount of secret key due to finite-block size effects. Here, we analyse these effects and the implications for system design and operation, utilising published results from the Micius satellite to construct an empirically-derived channel and system model for a trusted-node downlink employing efficient Bennett-Brassard 1984 (BB84) weak coherent pulse decoy states with optimised parameters. We quantify practical SatQKD performance limits and examine the effects of link efficiency, background light, source quality, and overpass geometries to estimate long-term key generation capacity. Our results may guide design and analysis of future missions, and establish performance benchmarks for both sources and detectors.

npj Quantum Information (2022)8:18 ; https://doi.org/10.1038/s41534-022-00525-3

INTRODUCTION

Quantum technologies have the potential to enhance the capability of many applications[1] such as sensing[2–4], communications[5–8], and computation[9]. Ultimately, a worldwide networked infrastructure of dedicated quantum technologies, i.e. a quantum internet[10], could enable distributed quantum sensors[11–14], precise timing and navigation[15–17], and faster data processing through distributed quantum computing[18]. This will require the establishment of long distance quantum links at global scale. A fundamental difficulty is exponential loss in optical fibres, which limits direct transmission of quantum photonic signals to < 1000 km[19–22]. Quantum repeaters may overcome the direct transmission limit but stringent performance requirements render them impractical by themselves for scaling to the intercontinental ranges needed for global scale-up[23]. Alternatively, satellite-based free-space transmission significantly reduces the number of ground quantum repeaters required[24].

the secret key rate[37,38]. Analyses based on smooth entropies[32] improve finite-key bounds[39] and have been applied to free-space quantum communication experiments[40]. Recently, tight bounds[36] and small block analyses[41] further improve key lengths for finite signals. Here, we provide a detailed analysis of SatQKD secret key generation, which utilises tight finite block statistics in conjunction with system design and operational considerations.

As part of our modelling, we implement tight statistical analyses for parameter estimation and error correction to determine the optimised, finite-block, single-pass secret key length (SKL) for weak coherent pulse (WCP) efficient BB84 protocols using three signal intensities (two-decoy states). We base our nominal system model on recent experimental results reported by the Micius satellite[42] and use a simple scaling method to extrapolate performance to other SatQKD configurations. The effects of different system parameters are explored, such as varying system link efficiencies, protocol choice, background counts, source quality, and overpass geometries.

Uses of Entanglement (Preskill ch. 4)

What about <u>errors</u> in the channel ?

* Alice & Bob can do classical error correction on their key bit string
* Errors make it harder to detect an eavesdropper
* Privacy amplification: 1 key bit = parity of *n* bits

<u>Note</u>: Entangled pairs are not required for QKD
Alice can prepare qubits in one of the 4 states $|\uparrow_x\rangle, |\downarrow_x\rangle, |\uparrow_z\rangle, |\downarrow_z\rangle$ at random, send to Bob who measures σ_x, σ_z at random. They compare preparation/measurement choices, keep the bits where they made the same choices ⇨ private key

This is the Bennet & Brassard (BB-84 Protocol)

<u>Note</u>: QKD systems based on photon polarization and running in fibers or free space have been available for many years. QKD has also been implemented with satellite relays.

<u>Aside</u> – <u>No Cloning</u>: Insures against obvious attacks

Let $|\varphi\rangle, |\psi\rangle$ be non-orthogonal states in $\mathcal{E}$
Consider a unitary U that implements the map

$$U: |\varphi\rangle \otimes |0\rangle_E \rightarrow |\varphi\rangle \otimes |e\rangle_E$$
$$U: |\psi\rangle \otimes |0\rangle_E \rightarrow |\psi\rangle \otimes |f\rangle_E$$

Unitarity implies conservation of scalar products

$$\langle\psi|\varphi\rangle = \left({}_E\langle 0| \otimes \langle\psi|\right)\left(|\varphi\rangle \otimes |0\rangle_E\right)$$
$$= \left({}_E\langle f| \otimes \langle\psi|\right)\left(|\varphi\rangle \otimes |e\rangle_E\right)$$
$$= \langle\psi|\varphi\rangle_E\langle f|e\rangle_E$$

Then $\langle\psi|\varphi\rangle \neq 0 \rightarrow {}_E\langle e|f\rangle_E = 1 \rightarrow |e\rangle_E = |f\rangle_E$

⇩

Orthogonal states can be copied since $\langle\psi|\varphi\rangle = 0$

Non-Orthogonal states cannot be copied !

Uses of Entanglement (Preskill ch. 4)

Teleportation Setup

Alice —— classical channel ——→ Bob

A ←—— $|\varphi^+\rangle_{AB}$ ——→ B

C ←—— unknown $|\chi\rangle_C$

Reminder: $|\varphi^+\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle\right)$

Protocol:

Alice combines C A and does a 2-qubit measurement in the Bell state basis

⇨ she projects out a state $|\cdot\rangle_{CA}$ which is one of the Bell states $|\phi^{\pm}\rangle_{CA}, |\psi^{\pm}\rangle_{CA}$

Alice sends classical info to Bob that her actual outcome was the state $|\cdot\rangle_{CA}$

Bob applies a unitary transformation to B according to

$$\left.\begin{array}{llll} \text{if } |\cdot\rangle_{CA} = |\varphi^+\rangle_{CA} & \text{apply} & \mathbb{1}_B \\ \phantom{\text{if } |\cdot\rangle_{CA} =} |\psi^+\rangle_{CA} & \text{"} & \sigma_x^{(B)} \\ \phantom{\text{if } |\cdot\rangle_{CA} =} |\psi^-\rangle_{CA} & \text{"} & \sigma_y^{(B)} \\ \phantom{\text{if } |\cdot\rangle_{CA} =} |\varphi^-\rangle_{CA} & \text{"} & \sigma_z^{(B)} \end{array}\right\}$$

3-qubit state transforms as

$$|\chi\rangle_C \otimes |\varphi^+\rangle_{AB} \;\Big\downarrow\; |\chi\rangle_B \otimes |\cdot\rangle_{CA}$$

Note: At the end Bob's qubit is in the unknown state $|\chi\rangle$, while Alice's qubit C is maximally entangled with A, i. e., the original state has been completely erased.

Proof: Initial state $|\Phi\rangle_{ABC} = |\varphi^+\rangle_{AB} \otimes \left(\alpha|\uparrow\rangle_C + \beta|\downarrow\rangle_C\right)$

Alice's measurement yields, e. g., $|\psi^+\rangle_{AC}$. This projects out the $|\psi^+\rangle_{AC}$ part of $|\Phi\rangle_{ABC}$:

$$P_{AC}|\Phi\rangle_{ABC} = |\psi^+\rangle_{AC}\left(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B\right)$$

where $P_{AC} = |\psi^+\rangle_{AC\,AC}\langle\psi^+| \otimes \mathbb{1}_B$

Bob applies $\sigma_x^{(B)}\left(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B\right) = \left(\alpha|\uparrow\rangle_B + \beta|\downarrow\rangle_B\right) = |\chi\rangle_B$

Repeat for other Bell state outcomes ⇨ QED

Uses of Entanglement (Preskill ch. 4)

Bob applies a unitary transformation to B according to

if $\|\cdot\rangle_{CA} =$	$\|\varphi^+\rangle_{CA}$	apply	$\mathbb{1}_B$
	$\|\psi^+\rangle_{CA}$	"	$\sigma_x^{(B)}$
	$\|\psi^-\rangle_{CA}$	"	$\sigma_y^{(B)}$
	$\|\varphi^-\rangle_{CA}$	"	$\sigma_z^{(B)}$

3-qubit state transforms as

$$|\chi\rangle_C \otimes |\varphi^+\rangle_{AB} \;\downarrow\; |\chi\rangle_B \otimes |\cdot\rangle_{CA}$$

Note: At the end Bob's qubit is in the unknown state $|\chi\rangle$, while Alice's qubit C is maximally entangled with A, i. e., the original state has been completely erased.

Proof: Initial state $|\Phi\rangle_{ABC} = |\varphi^+\rangle_{AB} \otimes (\alpha|\uparrow\rangle_C + \beta|\downarrow\rangle_C)$

Alice's measurement yields, e. g., $|\psi^+\rangle_{AC}$. This projects out the $|\psi^+\rangle_{AC}$ part of $|\Phi\rangle_{ABC}$:

$$P_{AC}|\Phi\rangle_{ABC} = |\psi^+\rangle_{AC}(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B)$$

where $P_{AC} = |\psi^+\rangle_{AC\,AC}\langle\psi^+| \otimes \mathbb{1}_B$

Bob applies $\sigma_x^{(B)}(\alpha|\downarrow\rangle_B + \beta|\uparrow\rangle_B) = (\alpha|\uparrow\rangle_B + \beta|\downarrow\rangle_B) = |\chi\rangle_B$

Repeat for other Bell state outcomes ⇨ QED

Preskill: Show that for any $|\Phi\rangle_{ABC}$ we have

$$|\Phi\rangle_{ABC} = \frac{1}{2}|\varphi^+\rangle_{CA}|\chi\rangle_B + \frac{1}{2}|\psi^+\rangle_{CA}\sigma_x^{(B)}|\chi\rangle_B + \frac{1}{2}|\psi^-\rangle_{CA}(-i\sigma_y^{(B)})|\chi\rangle_B + \frac{1}{2}|\varphi^-\rangle_{CA}\sigma_z^{(B)}|\chi\rangle_B$$

QED !

Discussion:

* Initially the unknown $|\chi\rangle_C$ is separate from $|\varphi^+\rangle_{AB}$, qubit C is not entangled with qubits A & B.
* Alice's measurement creates correlation between A,C
* Alice's outcome is random ⇨ no info about $|\chi\rangle_C$
* Info allows Bob to manipulate B to create $|\chi\rangle_B$
* Consistent w/no cloning: $|\chi\rangle_C$ is erased in the measurement that allows Bob to create $|\chi\rangle_B$

What might this be good for ?

Uses of Entanglement (Preskill ch. 4)