A Gentle Introduction to Quantum Communication and Networking

Samuel Oslovich[1] Sounak Kar[1]
[1]Wehner Group, QuTech, TU Delft

Tutorial at IFIP Performance: Part I

November 13, 2025

Acknowledgement

Much of the material presented here is adapted from the following:

- Vidick, T. and Wehner, S., 2023. Introduction to quantum cryptography. Cambridge University Press.
- Preskill, J., 1998. Lecture notes for physics 229: Quantum information and computation. California Institute of Technology, 16(1), pp.1-8.

Contents

The Advantage of Quantum Communication

Why use Quantum Communication?

- Efficient transfer of classical data.
  - Superdense coding.
- Information-theoretically secure transfer of classical data over a public channel.
  - Quantum key distribution (QKD).
- Transfer quantum data.
  - Quantum teleportation.
  - Application in Chemistry, Material Science, etc.
  - To encode one (pure) quantum bit, we need two reals.

What is Already Possible?

For communication, quantum information is usually encoded via light signals (photon polarisation, time-bin encoding, etc.) and can be transmitted over amenable physical media such as fibre or free space.

- Point-to-point QKD over distances of ~ 100km already commercially available.
  - Most require dark (dedicated) fibre.
  - Rate depends on fibre type and distance but ~ 100kb/s key rate achievable at < 50km.
- Toshiba labs claimed to have achieved 40bit/s and 1bits/s key rates over 500km and 600km distances, respectively.
- How about longer distances?

Long Distance Quantum Communication

- Cannot take the classical approach of ‘copy and resend’, because copying arbitrary quantum bits is not allowed. There are mainly two approaches depending on the distance:
  - On top of telecom fibre infrastructure, place quantum repeaters at regular intervals. (Only proof-of-principle experiments have been performed so far)
  - For very long distances, use of quantum satellites has been proposed: short-lived quantum entanglement was established over 1200km distance [1].
    - With entanglement, we can do more than QKD, such as sending quantum data.

Formalism of Closed Quantum Systems

Notations

- **Dirac's bra-ket notation**: Helps write down vectors and their tensor (Kronecker) products in a succinct way.

$$\underbrace{|v\rangle}_{\text{'ket' } v} = \begin{bmatrix} v_1 \\ v_2 \\ \dots \\ v_d \end{bmatrix} \quad \underbrace{|v\rangle^*}_{\text{instead of } |\bar{v}\rangle} = \begin{bmatrix} v_1^* \\ v_2^* \\ \dots \\ v_d^* \end{bmatrix} \quad \underbrace{|v\rangle^\dagger}_{\text{instead of } |v\rangle^*} = \begin{bmatrix} v_1^* & v_2^* & \dots & v_d^* \end{bmatrix} \quad \underbrace{\langle v|}_{\text{'bra' } v} := |v\rangle^\dagger$$

$$|w\rangle = \begin{bmatrix} w_1 \\ w_2 \\ \dots \\ w_{d'} \end{bmatrix} \quad |vw\rangle := |v\rangle \otimes |w\rangle = \begin{bmatrix} v_1\,|w\rangle \\ v_2\,|w\rangle \\ \dots \\ v_d\,|w\rangle \end{bmatrix} \quad v_i, w_j \in \mathbb{C}.$$

Inner Product: Convention

- **Inner product**: For $|u\rangle, |v\rangle \in \mathbb{C}^d$, their inner product is given by

$$\langle u|v\rangle := \sum_{i=1}^{d} u_i^* v_i \,. \qquad (\text{Not } \sum_{i=1}^{d} v_i^* u_i)$$

(Linear in the second argument)

- **Norm**: For $|u\rangle \in \mathbb{C}^d$, $\| |u\rangle \|_2 = \sqrt{\langle u|u\rangle}\,.$

Axioms of Closed Quantum Systems

Closed systems are considered to be *isolated* from the environment, i.e., no impact of the environment on their evolution. Axioms describe the following aspects of the system.

- **States**: how to adequately describe the state of a closed system?
- **Measurements**: in quantum mechanics, information about a system can be obtained only through measurements. In general, measurement outcomes are probabilistic, and the act of measurement changes the state of the system in a way that also depends on the outcome.
- **Observables**: properties of the system that can be measured.
- **Evolution**: how does the state evolve over time?
- **Composite systems**: formalism for describing multiple closed systems together.

Quantum States

- A system is completely described by its state, which is a *non-zero ray* in $\mathbb{C}^d$. (We focus only on finite-dimensional state spaces.)
  - Define an equivalence relation $\sim$ on $\mathbb{C}^d$ where $|u\rangle \sim |v\rangle$ if

$$|v\rangle = \alpha |u\rangle , \; \alpha \in \mathbb{C}, \; \alpha \neq 0 \, .$$

  - A non-zero ray is an element of $\mathbb{C}^d / \sim$, represented by a unit vector in $\mathbb{C}^d$. That is, for a valid quantum state $|\psi\rangle$,

$$\langle \psi | \psi \rangle = 1 \, .$$

  - For $a \in \mathbb{R}$, $|\psi\rangle$ and $e^{ia} |\psi\rangle$ are the same state by definition. e^{ia} is called global phase, which has no bearing on the state description.

Quantum States: Examples

- Smallest non-trivial example is $\mathbb{C}^2$.
- An orthonormal basis of $\mathbb{C}^2$ is $\{|0\rangle, |1\rangle\}$, where

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

- **Qubit**[1]: a unit-norm vector in $\mathbb{C}^2$, i.e., a qubit $|\psi\rangle$ can be represented as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \text{ where } \alpha, \beta \in \mathbb{C}, \ |\alpha|^2 + |\beta|^2 = 1.$$

  - α and β are called amplitudes.

[1]Here we are only talking about qubits in a closed system, later we also consider open systems.

Bit vs. Qubit

- A (classical) bit can be in one of the two states: 0 or 1, which we will denote as

$$0 \to |0\rangle \ , \quad 1 \to |1\rangle \ .$$

- A qubit can be in any state with the form $\alpha |0\rangle + \beta |1\rangle$, called a superposition between $|0\rangle$ and $|1\rangle$.

Bit vs. Qubit

- A (classical) bit can be in one of the two states: 0 or 1, which we will denote as

$$0 \to |0\rangle \ , \quad 1 \to |1\rangle \ .$$

- A qubit can be in any state with the form $\alpha |0\rangle + \beta |1\rangle$, called a superposition between $|0\rangle$ and $|1\rangle$.
  - A superposition is not a probabilistic mixture (with weights $|\alpha|^2$ and $|\beta|^2$), we will see concrete examples of this later!
  - Informally, probabilistic mixture implies that the state is in one or the other, whereas superposition implies it is in both.
  - We can create superposition physically, for example, between presence ($|1\rangle$) and absence ($|0\rangle$) of a photon.

Quiz: Valid Qubits

Which of the following is/are valid qubits? (select all that apply)

(A) ~~$\frac{1}{3}|0\rangle + \frac{2}{3}|1\rangle$~~

(B) $\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$

(C) $\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$

(D) $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$|\alpha|^2 + |\beta|^2 = 1$ for B, C, D.

Orthonormal Bases

We have so far only looked at the standard/computational/Z basis for qubits: $\{|0\rangle, |1\rangle\}$. But one can adopt any basis, given by a suitable unitary transformation of the standard basis. Special bases:

- Hadamard/X basis: $\{|+\rangle, |-\rangle\}$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}.$$

- Y basis: $\{|+i\rangle, |-i\rangle\}$

$$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}, \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}.$$

Orthonormal Bases

- The names X, Y, Z bases are derived from Pauli[2] X, Y, Z matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

  - The basis vectors are eigenvectors of the corresponding Pauli matrix.

[2] Wolfgang Pauli

Global vs. Relative Phase

For $a \in \mathbb{R}$,

- $\alpha |0\rangle + \beta |1\rangle$ and $e^{ia}(\alpha |0\rangle + \beta |1\rangle)$ are the same qubit. (Global/overall phase)
- $\alpha |0\rangle + \beta |1\rangle$ and $\alpha |0\rangle + e^{ia}\beta |1\rangle$ are different. (Relative phase)

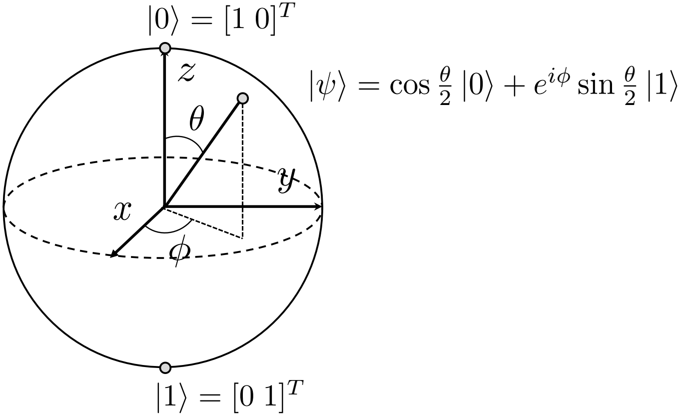
Bloch Sphere

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) \rightarrow \left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

- Ignore global phase.

- This shows a qubit (in a closed system) can be represented using two reals.

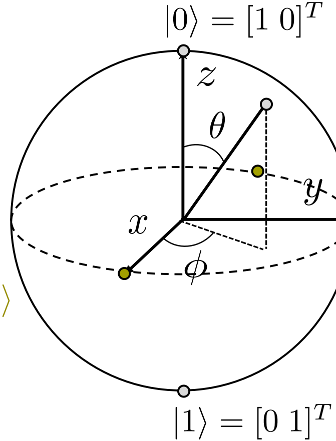
Bloch Sphere



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \mapsto (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

$$\theta \in [0, \pi],\ \phi \in [0, 2\pi)$$

Bloch Sphere



$$|-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

$$(\theta = \frac{\pi}{2},\ \phi = \pi)$$

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

$$(\theta = \frac{\pi}{2},\ \phi = 0)$$

Observables and Measurements

- Physically, information about a quantum state can be obtained only by performing measurements.
- In general, measurements change the state of the system.

Observables and Measurements

- Physically, information about a quantum state can be obtained only by performing measurements.
- In general, measurements change the state of the system.
- An observable is a property of the considered quantum state that can be measured.
  - Formally, an observable is a Hermitian matrix (of appropriate order).
  - By spectral decomposition, a Hermitian matrix M can be written as:

$$M = \sum_i \lambda_i P_i \quad \lambda_i : \text{real eigenvalues}, \; P_i : \text{orthogonal projector onto corresp. eigenspace}$$

$$(P_i^2 = P_i, \; P_i^\dagger = P_i, \; P_i P_j = \delta_{ij} P_i, \; \sum_i P_i = I)$$

  - What happens when an observable is measured on a quantum state $|\psi\rangle$?

Measurement Outcomes

- When we measure an observable $M = \sum_i \lambda_i P_i$ on state $|\psi\rangle$
  - We observe λ_i with probability $\mathsf{P}(\lambda_i) = \| P_i |\psi\rangle \|^2 = \langle\psi| P_i |\psi\rangle$. $\left(\sum_i P_i = I\right)$
  - Right after measurement, the state becomes $\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$. (states must have unit norm)
  - *Expectation value* of measurement M:

$$\langle M\rangle := \sum_i \lambda_i \mathsf{P}(\lambda_i) = \sum_i \lambda_i \langle\psi| P_i |\psi\rangle = \langle\psi| \left(\sum_i \lambda_i P_i\right) |\psi\rangle = \langle\psi| M |\psi\rangle .$$

Measurement Outcomes

- Let us look at some examples to understand measurements better.
  - Consider measuring $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = 1 \underbrace{|0\rangle\langle 0|}_{P_0} - 1 \underbrace{|1\rangle\langle 1|}_{P_1}$
  - For $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we observe

Meas. outcome	Probability	Post-measurement state
1	$\| \|0\rangle\langle 0\|\psi\rangle \|^2 = \|\alpha\|0\rangle\|^2 = \|\alpha\|^2$	$\frac{\|0\rangle\langle 0\|\psi\rangle}{\|\alpha\|} = \frac{\alpha}{\|\alpha\|}\|0\rangle$
-1	$\| \|1\rangle\langle 1\|\psi\rangle \|^2 = \|\beta\|1\rangle\|^2 = \|\beta\|^2$	$\frac{\|1\rangle\langle 1\|\psi\rangle}{\|\beta\|} = \frac{\beta}{\|\beta\|}\|1\rangle$

  - This is called measurement in the standard (Z) basis.

Measurement Outcomes

- Measuring $Z = 1\,|0\rangle\langle 0| - 1\,|1\rangle\langle 1|$ on $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

Meas. outcome	Probability	Post-measurement state
1	$\| \|0\rangle\langle 0\|\psi\rangle \|^2 = \|\alpha\,\|0\rangle\|^2 = \|\alpha\|^2$	$\frac{\|0\rangle\langle 0\|\psi\rangle}{\|\alpha\|} = \frac{\alpha}{\|\alpha\|}\,\|0\rangle = \|0\rangle$
-1	$\| \|1\rangle\langle 1\|\psi\rangle \|^2 = \|\beta\,\|1\rangle\|^2 = \|\beta\|^2$	$\frac{\|1\rangle\langle 1\|\psi\rangle}{\|\beta\|} = \frac{\beta}{\|\beta\|}\,\|1\rangle = \|1\rangle$

(States are non-zero rays/global phase)

Measurement Outcomes

- For measurement in X basis on $|\psi\rangle$, the observable is:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \end{bmatrix} = 1 \underbrace{|+\rangle \langle +|}_{P_0} - 1 \underbrace{|-\rangle \langle -|}_{P_1}$$

- Rewrite the qubit state in X basis: $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \frac{\alpha+\beta}{\sqrt{2}} |+\rangle + \frac{\alpha-\beta}{\sqrt{2}} |-\rangle$.

Meas. outcome	Probability	Post-measurement state
1	$\||+\rangle \langle +\|\psi\rangle\|^2 = \frac{\|\alpha+\beta\|^2}{2}$	$\|+\rangle$
-1	$\||-\rangle \langle -\|\psi\rangle\|^2 = \frac{\|\alpha-\beta\|^2}{2}$	$\|-\rangle$

Measurement Outcomes

Sometimes authors refer to post-measurement states as outcomes. Using the convention outcomes = post-measurement states, it is easy to see the following result.

- When a qubit $|\psi\rangle \in \mathbb{C}^2$ is measured in the orthonormal basis $\{|b_i\rangle\}_i$, the probability of observing the outcome $|b_i\rangle$ is $|\langle b_i|\psi\rangle|^2$.

Quiz: Measurements

When $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is measured in Y basis: $\{|+i\rangle, |-i\rangle\}$ where $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ and $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$, what are the possible outcome(s) and respective probabilities?

(A) $|+\rangle$ w.p. 1

(B) $|+\rangle$ w.p. $\frac{1}{2}$, $|-\rangle$ w.p. $\frac{1}{2}$

(C) $|+i\rangle$ w.p. $\frac{1}{2}$, $|-i\rangle$ w.p. $\frac{1}{2}$

(D) $|+i\rangle$ w.p. $\frac{|1+i|}{2}$, $|-i\rangle$ w.p. $\frac{|1-i|}{2}$

$|+\rangle = \frac{1-i}{2}\,|+i\rangle + \frac{1+i}{2}\,|-i\rangle$, $|\langle +|+i\rangle|^2 = \frac{|1-i|^2}{4} = \frac{1}{2}$, $|\langle +|-i\rangle|^2 = \frac{|1+i|^2}{4} = \frac{1}{2}$. (C)

Operations on Closed Quantum Systems

Arbitrary operations are not allowed. Specifically,

- Operations must be linear.
- Operations must preserve length, as states must have unit norm.

Such operations are given by unitary matrices.

Example Operations

- Hadamard transform/gate: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

  $\rightarrow \; H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle, \; H|1\rangle = |-\rangle.$

- X/NOT/bit-flip gate[3]: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

  $\rightarrow \; X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle, \; X|1\rangle = |0\rangle.$ (qubits are flipped)

- Z/phase-flip gate: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

  $\rightarrow \; Z|0\rangle = |0\rangle, \; Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle.$ ($|1\rangle$ acquired a phase)

- For any gate G, $G(\alpha|0\rangle + \beta|1\rangle) = \alpha G|0\rangle + \beta G|1\rangle$.

[3]Recall Pauli X, Y, Z matrices.

Example Operations

- Z/phase-flip gate: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - $\rightarrow$ $Z\left|0\right\rangle = \left|0\right\rangle, \; Z\left|1\right\rangle = -\left|1\right\rangle$. (global phase)
  - $\rightarrow$ $Z\left|+\right\rangle = Z(\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle) = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) = \left|-\right\rangle$. (relative phase)

Composite Systems

- **State space**: If the state of the ith system is given by $\mathbb{C}^{d_i}, i \in [n]$, then the state space of the composite system is $\otimes_{i=1}^{n}\mathbb{C}^{d_i} := \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_n}$, where $\otimes$ denotes the tensor product.
- **State description**: If the state of the ith system is individually prepared in state $|\psi_i\rangle, i \in [n]$, then the state of the composite system is $|\psi_1\psi_2 \ldots \psi_n\rangle := |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$. Observe that Dirac notation lets us write states in higher dimensions, such as $|0010\rangle$ in a succinct way.
- For vectors and matrices, $\otimes$ denotes the Kronecker product.
- **Measurements**: As before, measurements will be given by observables (Hermitian matrices) on $\otimes_{i=1}^{n}\mathbb{C}^{d_i}$. We will generalise this further while studying open systems.
- **Unitary operations**: If the unitary U_i acts individually on the ith qubit $|\psi_i\rangle$, the overall unitary for the composite state $|\psi_1\psi_2 \ldots \psi_n\rangle$ is given by $U := U_1 \otimes U_2 \otimes \cdots \otimes U_n$. It is easy to check that U is unitary.

Quiz: Partial Measurements

We measure the first qubit of $|+0\rangle$ in Z-basis, what is the distribution of the post-measurement state?

(A) $|+0\rangle$ w.p. $\frac{1}{2}$, $|-0\rangle$ w.p. $\frac{1}{2}$

(B) $|00\rangle$ w.p. $\frac{1}{2}$, $|10\rangle$ w.p. $\frac{1}{2}$

(C) $|00\rangle$ w.p. $\frac{1}{4}$, $|01\rangle$ w.p. $\frac{1}{4}$, $|10\rangle$ w.p. $\frac{1}{4}$, $|11\rangle$ w.p. $\frac{1}{4}$

Probability	**Resulting state**
$\lVert (P_0 \otimes I)\,|+0\rangle \rVert^2 = \lVert (P_0\,|+\rangle) \otimes (I\,|0\rangle) \rVert^2 = \lVert P_0\,|+\rangle \rVert^2 \lVert |0\rangle \rVert^2 = \frac{1}{2}$	$\frac{(P_0|+\rangle)\otimes|0\rangle}{1/\sqrt{2}} = |00\rangle$
$\lVert (P_1 \otimes I)\,|+0\rangle \rVert^2 = \frac{1}{2}$	$\frac{(P_1|+\rangle)\otimes|0\rangle}{1/\sqrt{2}} = |10\rangle$

We use $(A \otimes B)(C \otimes D) = AC \otimes BD$ when dimensions permit. Correct answer is (B).

Measurements on Multiple Qubits

- Consider the projection matrix

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

- It cannot be written as $P_1 \otimes P_2$ for $P_1, P_2 \in \mathbb{C}^2$.

Example Unitary Operation on Two Qubits: CNOT Gate

- In the single qubit case, we saw the quantum equivalent of the NOT gate, called X gate: $X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$.
- For 2-qubit states, we define CNOT (conditional NOT), where the X gate is applied on the second qubit if the first is $|1\rangle$.

$$\text{CNOT: } |x, y\rangle \mapsto |x, y \oplus x\rangle,$$

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

$$\text{CNOT}(|\psi\rangle) = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|11\rangle + \alpha_{11}|10\rangle.$$

No Cloning Theorem

- Suppose a universal cloning unitary U exists such that for any state $|\psi\rangle$,

$$U\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle,$$

  where $|0\rangle$ denotes the register where we copy the data qubit $|\psi\rangle$.
- Then, we also have

$$U\left(|\phi\rangle \otimes |0\rangle\right) = |\phi\rangle \otimes |\phi\rangle.$$

- Therefore,

$$\begin{aligned}\langle\phi|\psi\rangle = \langle\phi|\psi\rangle \otimes \underbrace{\langle 0|0\rangle}_{=1} = \Big(\langle\phi| \otimes \langle 0|\Big)\Big(|\psi\rangle \otimes |0\rangle\Big) &= \Big(\langle\phi| \otimes \langle 0|\Big)U^\dagger U\Big(|\psi\rangle \otimes |0\rangle\Big) \\ &= \left(\langle\phi| \otimes \langle\phi|\right)\left(|\psi\rangle \otimes |\psi\rangle\right) = \langle\phi|\psi\rangle^2\end{aligned}$$

- This implies $\langle\phi|\psi\rangle = 0$ or 1. Therefore, cloning is possible only if the set of possible states contains two states that are orthogonal (e.g., the classical states $|0\rangle$ and $|1\rangle$).

Why Superposition $\neq$ Probabilistic Mixture

We consider successive application of the Hadamard gate H on $|0\rangle$.

- Recall that for the Hadamard gate H, $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$.
- Had superposition and probability mixture been the same, we would have had

$$|+\rangle = \begin{cases} |0\rangle & \text{w.p. } \frac{1}{2} \\ |1\rangle & \text{w.p. } \frac{1}{2} \end{cases} \qquad |-\rangle = \begin{cases} |0\rangle & \text{w.p. } \frac{1}{2} \\ |1\rangle & \text{w.p. } \frac{1}{2} \end{cases}$$

- Applying H once on $|0\rangle$, we would have $|0\rangle$ w.p. $\frac{1}{2}$ or $|1\rangle$ w.p. $\frac{1}{2}$. From each possible outcome, another application of H would again produce $|0\rangle$ w.p. $\frac{1}{2}$ or $|1\rangle$ w.p. $\frac{1}{2}$.
- Combining, we would have had $|0\rangle$ w.p. $\frac{1}{2}$ or $|1\rangle$ w.p. $\frac{1}{2}$.
- What actually happens:

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = |0\rangle$$

  - This is called quantum interference, observed for example in the Mach-Zehnder interferometer.

The EPR[4] pair

- Consider the EPR pair:

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$$

- Assume we can write the joint state as a tensor product $|\psi_1\rangle \otimes |\psi_2\rangle$ with

$$|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle, \quad |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle.$$

- Then

$$|\psi_1\rangle \otimes |\psi_2\rangle = \underbrace{\alpha_1\alpha_2}_{1/\sqrt{2}}|00\rangle + \underbrace{\alpha_1\beta_2}_{0}|01\rangle + \underbrace{\beta_1\alpha_2}_{0}|10\rangle + \underbrace{\beta_1\beta_2}_{1/\sqrt{2}}|11\rangle$$

Impossible!

- The state is entangled.

[4] Einstein, Podolsky, Rosen.

Bell[5] Pairs

- The following four states are called Bell pairs or Bell states.

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

[5] John Bell.

Quiz: Bell Pairs

- We consider the following local unitary operations $\{X \otimes I, Z \otimes I, XZ \otimes I\}$ on $|\Phi^+\rangle$. What do we get?

(A) $|\Phi^-\rangle, |\Psi^+\rangle$, no Bell pair.

(B) $|\Psi^+\rangle, |\Phi^-\rangle$, no Bell pair.

(C) $|\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle$.

$$
\begin{aligned}
(XZ \otimes I)\left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}((XZ|0\rangle)\otimes|0\rangle + (XZ|1\rangle)\otimes|1\rangle) \\
&= \frac{1}{\sqrt{2}}(X|0\rangle\otimes|0\rangle - X|1\rangle\otimes|1\rangle) \\
&= \frac{1}{\sqrt{2}}(|1\rangle\otimes|0\rangle - |0\rangle\otimes|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle) = |\Psi^-\rangle. \quad \text{(C)}
\end{aligned}
$$

Quiz: Bell Pairs

- The Bell pairs are:

$$\left|\Phi^+\right\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \left|\Phi^-\right\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$\left|\Psi^+\right\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad \left|\Psi^-\right\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Which of the other three is $\left|\Phi^+\right\rangle$ orthogonal to?

(A) Only $\left|\Phi^-\right\rangle$.

(B) Only $\left|\Phi^-\right\rangle$ and $\left|\Psi^+\right\rangle$.

(C) All three.

$$\left\langle \Phi^+ \middle| \Psi^- \right\rangle = \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$
$$= \frac{1}{2}\big(\langle 00|10\rangle - \langle 00|01\rangle + \langle 11|10\rangle - \langle 11|01\rangle\big) = 0. \quad \text{(C)}$$

- Thus the Bell pairs form an orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$.

Examples of Quantum Communication Protocols

▷ Superdense Coding

- A wants to send 2 bits of information to B. Can she do that just by sending 1 qubit?
- Yes, if A and B preshare the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (each one qubit of the pair). This state can be viewed as a quantum communication resource.
- A applies unitary to her qubit as follows:

Bit pair to be sent (a, b)	**Unitary operation** $X_A^a Z_A^b (\otimes I_B)$	**Final state**
00	$I_A(\otimes I_B)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
01	$Z_A(\otimes I_B)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
10	$X_A(\otimes I_B)$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
11	$X_A Z_A(\otimes I_B)$	$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle)$

▷ Superdense Coding

- Joint state after A applies unitary to her qubit:

Bit pair to be sent (a, b)	**Unitary operation** $X_A^a Z_A^b$	**Final state**
00	I_A	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
01	Z_A	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
10	X_A	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$
11	$X_A Z_A$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$

- The four states on the right are orthogonal, i.e., perfectly distinguishable.
- Now, A sends her qubit to B. B measures the two qubits in Bell-basis and interprets the result accordingly[6].

[6] It can be shown that one qubit cannot encode more than one bit of information w/o entanglement.

The BB84[7] QKD Protocol

- We only present the main idea behind the protocol, no formal security proof. The setup is as follows.
- **Goal**: A and B want to share a key (classical bit string). They are connected by:
  - A quantum channel.
  - A classical public channel (messages are authenticated).
- The security of the protocol hinges on the following properties of quantum states:
  - Perfect copying of qubits is not possible (no-cloning).
  - Quantum measurements disturb the state, which is detectable by A and B.

[7] Proposed by Bennett and Brassard in 1984.

BB84 in a Noiseless Channel: Main Idea

- A encodes the bits in a random binary base. A (bit, base) combination is encoded as qubits according to the following rule:

Bit	**Base** $= 0$ (Z Basis)	**Base** $= 1$ (X Basis)
0	$\vert 0\rangle$	$\vert +\rangle = \frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$
1	$\vert 1\rangle$	$\vert -\rangle = \frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$

- A sends the encoded qubits via the quantum channel. Once received, B measures each qubit in a random base.
- Once measured, A and B exchange base information via the classical public channel.
  - They keep only the bits for which bases match.
  - On a fraction of this set, they check if the following holds: Qubit sent by A $=$ Qubit measured by B.
  - If true, they use the rest of the string as key. Else, restart.
- Copying is not possible, and measuring in a base other than the one used by A alters the state, which will be detected. But the base info is not available to the eavesdropper.

BB84 Example[8]

A's bits	0	1	1	0	1	0	0	1
A's random bases	1	0	0	0	1	0	1	1
Qubits A sends	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$
B's random bases	1	1	0	1	0	0	0	1
B's measurements	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$
Bases match	✓		✓			✓		✓
Check bits	✓					✓		
Shared key			1					1

[8] Credit: Chekhova Research Group, MPI

Quantum Teleportation

- Now we focus on transferring quantum information, encoded via an arbitrary qubit. In reality, sending qubits is an error-prone process.
- This is more problematic while sending an arbitrary qubit because of the following:
  - Fixed qubits, (e.g., $|0\rangle, |-\rangle$ or half of the pair $|\Psi^+\rangle$) are easier to prepare. Arbitrary qubits may be the result of a long experiment.
  - In classical networks, we would have made copies and resent them, which is not possible in quantum networks due to no cloning!

Quantum Teleportation

- Setup: A wants to send the data qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to B. A and B preshare the EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, i.e., each holds one half. We can write the initial state as
$$(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).$$
where the first two qubits are held by A and the third by B.

Quantum Teleportation

- Setup: A wants to send the data qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to B. A and B preshare the EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, i.e., each holds one half. We can write the initial state as
$$(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).$$
where the first two qubits are held by A and the third by B.
- A applies $\mathrm{CNOT}_{1\to2}$: $\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$
- A applies H_1 $(H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$:
$$\frac{1}{2}\Big(\alpha(|0\rangle + |1\rangle)|00\rangle + \alpha(|0\rangle + |1\rangle)|11\rangle + \beta(|0\rangle - |1\rangle)|10\rangle + \beta(|0\rangle - |1\rangle)|01\rangle\Big)$$
$$= \frac{1}{2}\Big(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big).$$

Quantum Teleportation

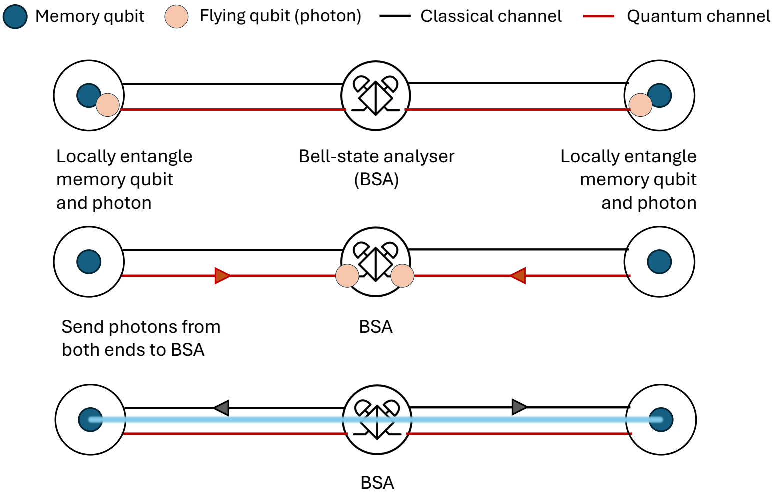
- Now, A measures her 2 qubits in the computational basis. The state was: $\frac{1}{2}\Big(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)\Big)$. The set of projection matrices corresponding to the measurement: $\{(|00\rangle\langle 00|)\otimes I, (|01\rangle\langle 01|)\otimes I, (|10\rangle\langle 10|)\otimes I, (|11\rangle\langle 11|)\otimes I\}$.
- A sends the measurement outcome ab $(a, b \in \{0, 1\})$ to B classically and B applies unitary $X^a Z^b$ to his qubit to retrieve the original data qubit.

Probability	**Resulting 3-qubit state**	**Correction $X^a Z^b$**	**B's final state**
1/4	$\|00\rangle(\alpha\|0\rangle+\beta\|1\rangle)$	I	$\alpha\|0\rangle+\beta\|1\rangle$
1/4	$\|01\rangle(\alpha\|1\rangle+\beta\|0\rangle)$	X	$\alpha\|0\rangle+\beta\|1\rangle$
1/4	$\|10\rangle(\alpha\|0\rangle-\beta\|1\rangle)$	Z	$\alpha\|0\rangle+\beta\|1\rangle$
1/4	$\|11\rangle(\alpha\|1\rangle-\beta\|0\rangle)$	XZ	$\alpha\|0\rangle+\beta\|1\rangle$

Resource Requirements: From QKD to Teleportation

- For superdense coding and quantum teleportation, A and B needed to preshare the state $\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- For the QKD example, we only need a sender that can prepare quantum states and a receiver that can measure quantum states.
- The other two however need a mechanism to distribute entanglement between the parties. That is, each party must hold one half of the pair $\left|\Psi^+\right\rangle$, which requires quantum memory. Also, how do we entangle two quantum memories separated by distance?

The Single Click Protocol



If **one of the detectors** clicks, it successfully entangles memory qubits. Success message is sent **classically** to end nodes (**heralding**), with click pattern.

- Succeeds probabilistically.
- Heralding ensures memory qubits are successfully entangled, so we are safe to start our protocol (e.g., teleportation) rather than discovering it at the end.
- Alternative protocols exist.

The Challenge of Distance in Entanglement Distribution

- **Photon loss in fibre**: Input (P_{in}) and output (P_{out}) optical power follow the following relation:

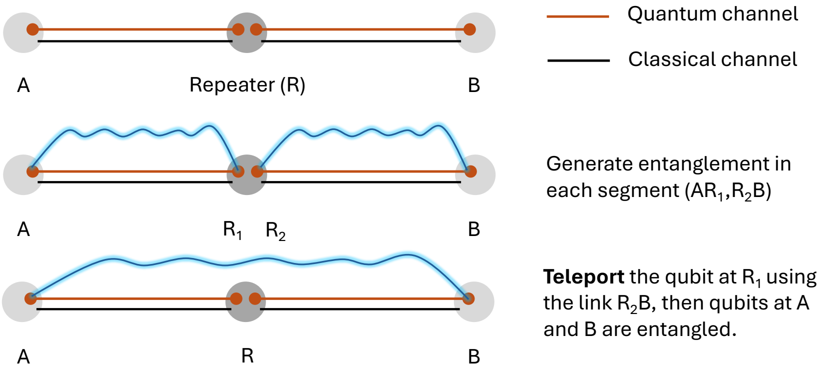
$$P_{\text{out}} = P_{\text{in}} 10^{-\frac{\alpha}{10}L}, \quad \alpha : \text{attenuation coeff. (dB/km)}, \; L : \text{distance (km)}$$

  At telecom wavelength, $\alpha = 0.2$ dB/km.

- Of course, we cannot adopt the classical approach where we make multiple copies and send them.
- It is possible to introduce redundancy to solve this problem, but then we need many memory registers. (Infeasible at the current stage)
- How do we solve this?

Entanglement Swapping

- **Solution**: Split the distance into shorter segments and use entanglement swapping via quantum repeaters.



Generate entanglement in each segment (AR_1,R_2B)

Teleport the qubit at R_1 using the link R_2B, then qubits at A and B are entangled.

Entanglement Distribution: Practical Considerations

- We have now seen entanglement distribution:
  - at a shorter distance, which we will call elementary link.
  - and further scaling to long distance, which we will call end-to-end link.
- A link represents two entangled memory qubits that can be used as a quantum communication resource. Their joint state in our examples was described by the EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- In reality, quantum states are fragile. They interact with the environment and degrade to some other state. This phenomenon is called decoherence.
- Decoherence is particularly relevant for entanglement swapping, where elementary links are rarely produced simultaneously, meaning that one of them has been interacting with the environment while the other was still being generated.

Formalism of Open Quantum Systems

Reasons for Studying Open Systems

- As said, the system of interest is never perfectly isolated. In reality, we observe a subsystem that is part of a larger system.
- We have also seen examples (EPR pair) where the individual states cannot be described by the closed system formalism even if the joint state can be.
- Sometimes quantum operations produce states probabilistically, i.e., instead of a single state we have a probability distribution over states. How do we describe such states?

Density Matrices

We want a formalism that is capable of expressing states of subsystems or when the system is prepared probabilistically. It turns out that the following formalism adequately does this.

- **Density matrix**: A density matrix ρ on $\mathbb{C}^d$ is a $d \times d$ matrix such that
  - → ρ is positive semi-definite (psd).
  - → $\mathrm{tr}(\rho) = 1$.

Relating back to Closed Systems and More

- **Closed system**: The density matrix representation of a closed system state $|\psi\rangle$ is given by $\rho = |\psi\rangle\langle\psi|$. Note that for such states $\text{rank}(\rho) = 1$, we call them pure states.
- States with $\text{rank}(\rho) > 1$ are called mixed states.
- **Probabilistic mixture**: A state prepared in state ρ_i with probability p_i ($\sum_i p_i = 1$) is given by $\sum_i p_i \rho_i$. $\{p_i, \rho_i\}_i$ is called ensemble representation of ρ.
  - Ensemble representations are not unique, i.e., the same state can be prepared in different ways. For example,

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{I}{2}.$$

Quiz: Mixed States

Which of the following represent(s) *valid* mixed state(s)?

(A) $\frac{1}{\sqrt{2}} |+\rangle \langle +| + \frac{1}{\sqrt{2}} |-\rangle \langle -|$

(B) $\frac{1}{4} |+\rangle \langle +| + \frac{3}{4} |-\rangle \langle -|$

(C) $\frac{1}{4} |0\rangle \langle 0| + \frac{3}{4} |0\rangle \langle 0|$

(D) $\frac{1}{4} |0\rangle \langle 0| + \frac{3}{4} |1\rangle \langle 1|$

(A) is *not* a valid density matrix ($\text{tr}(\rho) > 1$), (C) is a pure state ($\text{rank}(\rho) = 1$). (B,D)

Other Aspects

- **Composite systems**: If system $i \in [n]$ is individually prepared in the state ρ_i, the state of the composite system is given by $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$.
- **Measurements**: Recall that for closed system, we defined measurements by an observable $M = \sum_i \lambda_i P_i$, P_i being orthogonal projector onto the eigenspace of λ_i:

$$P_i^2 = P_i,\ P_i^\dagger = P_i,\ P_i P_j = \delta_{ij} P_i,\ \sum_i P_i = I$$

- Now we generalise this notion to so-called Positive Operator Valued Measures (POVM), where we do not care about post-measurement states. A POVM (on a density matrix ρ) is given by set of psd matrices $\{M_i\}_i$ such that

$$\sum_i M_i = I, \quad i : \text{index of the measurement outcome}$$

$$\mathsf{P}(\text{outcome}\, i) = \text{tr}(M_i \rho).$$

Measurements

- To know the post-measurement states, we need a Kraus operator representation of the POVM: $M_i = A_i^\dagger A_i$. Given measurement outcome i, the post-measurement state is then given by
$$\rho_{|i} = \frac{A_i \rho A_i^\dagger}{\mathrm{tr}(A_i^\dagger A_i \rho)}.$$
- Note that for any $M = A^\dagger A$, we also have $M = B^\dagger B$ where $B = UA$ for some unitary matrix U. So the Kraus decomposition must be specified.
- This is consistent with the closed system formalism where $P_i = P_i^\dagger P_i$.

▷ Measurements: Lookback at Closed Systems

- For orthogonal projectors, the default Kraus operator decompostion is $P_i = P_i^\dagger P_i$. Recall that the density matrix representation of a pure state $|\psi\rangle$ is $|\psi\rangle\langle\psi|$. Now, we previously had

$$\text{P(outcome}\, i) = \| P_i |\psi\rangle \|^2 = \langle\psi| P_i^\dagger P_i |\psi\rangle = \text{tr}(P_i^\dagger P_i |\psi\rangle\langle\psi|) = \text{tr}(P_i^\dagger P_i \rho)$$

$$\text{post-measurement state} : \frac{P_i |\psi\rangle}{\| P_i |\psi\rangle \|} \to \frac{P_i |\psi\rangle}{\| P_i |\psi\rangle \|} \frac{\langle\psi| P_i^\dagger}{\| P_i |\psi\rangle \|} = \frac{P_i \rho P_i^\dagger}{\text{tr}(P_i^\dagger P_i \rho)}$$

Expressing State of a Subsystem: Partial Trace

- In general, joint state of system AB can be written as $\rho_{AB} = \sum_{ijkl} \alpha_{ijkl} \left|i\right\rangle\left\langle j\right|_A \otimes \left|k\right\rangle\left\langle l\right|_B$. We define the state of A ρ_A via the partial trace operation defined as

$$\rho_A = \text{tr}_B(\rho_{AB}) = \sum_{ijkl} \alpha_{ijkl} \left|i\right\rangle\left\langle j\right|_A \otimes \text{tr}(\left|k\right\rangle\left\langle l\right|_B) = \sum_{ijkl} \alpha_{ijkl} \left|i\right\rangle\left\langle j\right|_A \otimes \delta_{kl}$$

$$= \sum_{ij} \left(\sum_k \alpha_{ijkk} \right) \left|i\right\rangle\left\langle j\right|_A$$

- Similarly, the state of B ρ_B is given by

$$\rho_B = \text{tr}_A(\rho_{AB}) = \sum_{ijkl} \alpha_{ijkl} \text{tr}(\left|i\right\rangle\left\langle j\right|_A) \otimes \left|k\right\rangle\left\langle l\right|_B = \sum_{kl} \left(\sum_i \alpha_{iikl} \right) \left|k\right\rangle\left\langle l\right|_B$$

Getting Back to the EPR Pair Question

- The density matrix representation of $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is given by

$$
\begin{aligned}
\rho =& \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)\frac{1}{\sqrt{2}}\left(\langle 00| + \langle 11|\right) \\
=& \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right) \\
=& \frac{1}{2}\left(|0\rangle\langle 0|\otimes|0\rangle\langle 0| + |0\rangle\langle 1|\otimes|0\rangle\langle 1| + |1\rangle\langle 0|\otimes|1\rangle\langle 0| + |1\rangle\langle 1|\otimes|1\rangle\langle 1|\right) = \frac{1}{2}\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 1\end{bmatrix}
\end{aligned}
$$

- The state of the first qubit is given by

$$
\begin{aligned}
\rho_1 = \mathrm{tr}_2(\rho) =& \frac{1}{2}\Big(|0\rangle\langle 0|\underbrace{\mathrm{tr}(|0\rangle\langle 0|)}_{1} + |0\rangle\langle 1|\underbrace{\mathrm{tr}(|0\rangle\langle 1|)}_{0} + |1\rangle\langle 0|\underbrace{\mathrm{tr}(|1\rangle\langle 0|)}_{0} + |1\rangle\langle 1|\underbrace{\mathrm{tr}(|1\rangle\langle 1|)}_{1}\Big) \\
=& \frac{1}{2}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix} = \frac{I_2}{2}
\end{aligned}
$$

Quiz: Partial Trace

Suppose A and B are in an unknown joint state ρ_{AB} and we are only given their individual states ρ_A and ρ_B. What can we say about ρ_{AB}?

(A) It is $\rho_A \otimes \rho_B$.

(B) Can't say in general.

The previous example shows that (A) is not necessarily true. (B)

Entanglement

- We have already seen that the EPR pair does not admit a product state description (in the closed system formalism) and is entangled. Here we define entanglement.
- **Entanglement**: For quantum systems A and B, the joint state ρ_{AB} is separable if there exists a pmf $\{p_i\}_i$ and density matrices $\{\rho_A^{(i)}\}_i$, $\{\rho_B^{(i)}\}_i$ such that $\rho_{AB} = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}$.
  The state ρ_{AB} is entangled w.r.t the bipartiion A-B if no such decomposition exists.
  - A pure state $|\psi\rangle_{AB}$ is separable iff it can be written as $|\psi\rangle_{AB} = |\psi_1\rangle_A \otimes |\psi_2\rangle_B$.
- Determining entanglement for mixed states for a given bipartition is a non-trivial task in general.

Allowed Quantum Operations in Open Systems: Quantum Channels

- For closed systems, the set of allowed operations was given by unitaries.
- For open systems, maps must be
  - linear,
  - *completely positive*: A map $\mathcal{M}$ is completely positive if $\mathcal{I}_d \otimes \mathcal{M}$ is positive for any d, where $\mathcal{I}_d$ is the identity map on density matrices of dimension d. A map is positive if it takes psd matrices to psd matrices.
  - *trace-preserving*: density matrices must have unit trace.

  Such maps are called quantum channels.
- It can be shown that such a map $\mathcal{N}$ admits the following Kraus decomposition

$$\mathcal{N}(\rho) = \sum_i N_i \rho N_i^\dagger, \quad \text{where } \sum_i N_i^\dagger N_i = I.$$

- Quantum operations, including noise, can be described as a quantum channel.

The Depolarising Channel

- The depolarising channel is a noise model that drives a quantum state towards the maximally noisy state $\frac{I}{2}$. For a single qubit state, it is given by

$$\mathcal{D}(\rho) = (1-p)\rho + p\frac{I}{2}.$$

- The time-dependence of noise is often characterised by $p = 1 - e^{-t/T}$, where T is called coherence time, a parameter that reflects the quality of the memory storing the qubit. Effectively,

$$\mathcal{D}_t(\rho) = e^{-t/T}\rho + \left(1 - e^{-t/T}\right)\frac{I_2}{2}.$$

- For a two-qubit system σ where both memories have the same coherence time T,

$$\mathcal{D}_t(\sigma) = e^{-2t/T}\sigma + \left(1 - e^{-2t/T}\right)\frac{I_4}{4}.$$

Werner[9] States

- Recall that we described states of quantum links using the EPR pair $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in the absence of noise.
- Now we assume that the effect of decoherence (interaction with the environment) is given by the depolarising noise. This acts on the corresponding density matrix $|\Phi^+\rangle\langle\Phi^+|$ as:

$$\mathcal{D}_t\left(|\Phi^+\rangle\langle\Phi^+|\right) = e^{-2t/T}\,|\Phi^+\rangle\langle\Phi^+| + \left(1 - e^{-2t/T}\right)\frac{I_4}{4},$$

  where T denotes the (same) coherence time of each of the two memory qubits holding the EPR pair.
- This state is in Werner form.

[9] Reinhard Werner.

Werner States

- **Werner state:** A 2-qubit state with Werner parameter w is given by
$$\rho_w = w\,|\Phi^+\rangle\langle\Phi^+| + (1-w)\frac{I_4}{4}, \quad 0 \leq w \leq 1$$
- For $w = 1$, we recover the EPR pair $|\Phi^+\rangle\langle\Phi^+|$, while for $w = 0$, we have the maximally mixed state $I_4/4$.

Werner States: Other Properties

- Depolarising noise on Werner states produces Werner states:

$$\mathcal{D}_t(\rho_w) = e^{-\frac{2t}{T}}\rho_w + \left(1 - e^{-\frac{2t}{T}}\right)\frac{I_4}{4} = we^{-\frac{2t}{T}}\,|\Phi^+\rangle\langle\Phi^+| + (1 - we^{-\frac{2t}{T}})\frac{I_4}{4} = \rho_{we^{-2t/T}}.$$

- When we swap two Werner states ρ_{w_1} and ρ_{w_2}, we get a Werner state $\rho_{w_1 w_2}$. (Recall entanglement swapping for creating end-to-end links.)
- Thus, using Werner states to describe quantum communication links simplifies further analysis, as we can parametrise a 4×4 matrix by a scalar.

Similarity Between Quantum States: Fidelity

- Suppose we want to prepare a state $|\psi\rangle\langle\psi|$ but the preparation mechanism succeeds probabilistically, with the outcome state denoted as ρ. To check success, we can use the following two-outcome measurement [2, Chap. 5]:

$$\{M_1, M_0\}, \quad M_1 = |\psi\rangle\langle\psi|\,,\ M_0 = I - |\psi\rangle\langle\psi|\,.$$

- The success probability of the mechanism is then given by $\mathrm{tr}(M_1\rho) = \langle\psi|\,\rho\,|\psi\rangle$.

Fidelity

- **Fidelity**: The fidelity between a density matrix ρ and a pure state $|\psi\rangle\langle\psi|$ is given by $F(\rho, |\psi\rangle) = \langle\psi| \rho |\psi\rangle$.
- When $\rho = |\phi\rangle\langle\phi|$, we have $F(\rho, |\psi\rangle) = | \langle\psi|\phi\rangle |^2$.

Fidelity of Werner States

We can write the identity matrix in terms of the Bell states as follows:

$$I_4 = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|.$$

Also,

$$\rho_w = w|\Phi^+\rangle\langle\Phi^+| + \frac{1-w}{4}|\Phi^+\rangle\langle\Phi^+| + \frac{1-w}{4}|\Phi^-\rangle\langle\Phi^-| + \frac{1-w}{4}|\Psi^+\rangle\langle\Psi^+| + \frac{1-w}{4}|\Psi^-\rangle\langle\Psi^-|.$$

Then the fidelity of ρ_w (defined as the fidelity between ρ_w and $|\Phi^+\rangle$),

$$F(\rho_w, |\Phi^+\rangle) = \frac{1+3w}{4}.$$

Fidelity of Werner States

- **Fact**: Any 2-qubit state can be transformed into a Werner state of the same fidelity via a process called twirling [3].
  - Apart from tractability[10], this fact also provides justification for using Werner states to describe a quantum communication link.

[10] See slide 72.

Key Performance Metrics in Quantum Networks

Resources for Quantum Communication

- In classical networks, the primary communication resource is the transmission rate (or capacity). In quantum networks, in addition to rate, the quality (fidelity) of the links is also a fundamental resource.
- But fidelity alone does not tell the whole story when it comes to running applications. We briefly illustrate this using two communication protocols we have already seen — quantum teleportation and QKD.

Fidelity of Teleportation

- We run teleportation with an imperfect resource state and we denote this teleportation channel as $\mathcal{E}$.
- When we teleport $|\psi\rangle$, we recover $\mathcal{E}(|\psi\rangle\langle\psi|)$.
- The fidelity of this channel is defined as[11]

$$F(\mathcal{E}) = \int \mathrm{d}\psi \, \langle\psi| \, \mathcal{E}(|\psi\rangle\langle\psi|) \, |\psi\rangle \, .$$

- **Fact**: Denote a teleportation channel with resource state ρ_w (Werner state) by $\mathcal{E}_w$. Then $F(\mathcal{E}_w) = \frac{1+w}{2}$.

[11] Fidelity between the actual and desired outputs, averaged over possible inputs.

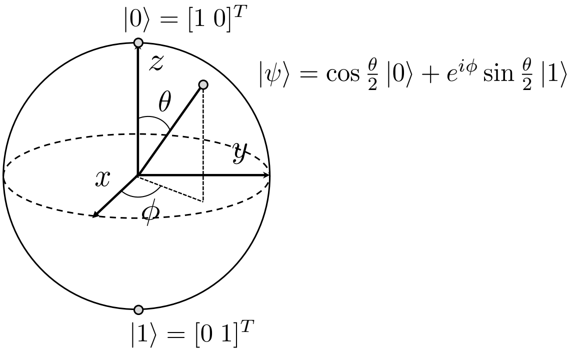
How Good can we do Classically?

- A measures the qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and sends the measurement outcome (0 w.p. $|\alpha|^2$, 1 w.p $|\beta|^2$, i.e.[12], $\rho = |\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$) classically.
- Corresponding fidelity: $\langle\psi|\rho|\psi\rangle = |\alpha|^4 + |\beta|^4 =: f(|\psi\rangle)$.
- Fidelity of the protocol: $\int d\psi f(|\psi\rangle)$.

[12] Recall how we represent probability mixtures using density matrices.

How to Evaluate Fidelity of the Classical Protocol?

- To evaluate the integral (fidelity of the protocol), we use Bloch sphere parametrisation of a pure qubit.



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \mapsto (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

$\theta \in [0, \pi]$, $\phi \in [0, 2\pi)$

How to Evaluate Fidelity of the Classical Protocol?

- $f(|\psi\rangle) = |\alpha|^4 + |\beta|^4 = \cos^4\frac{\theta}{2} + \sin^4\frac{\theta}{2}$.
- Fidelity of the protocol:

$$
\begin{aligned}
\int \mathrm{d}\psi f(|\psi\rangle) &= \int_0^{2\pi}\int_0^{\pi}\left(\cos^4\frac{\theta}{2} + \sin^4\frac{\theta}{2}\right)\frac{1}{4\pi}\sin\theta\, d\phi\, d\theta \\
&= \frac{1}{4\pi}\int_0^{2\pi} d\phi \int_0^{\pi}\left(\cos^4\frac{\theta}{2} + \sin^4\frac{\theta}{2}\right)\sin\theta\, d\theta \\
&= \frac{1}{2}\int_0^{\pi}\left(1 - \frac{1}{2}\sin^2\theta\right)\sin\theta\, d\theta = \frac{2}{3}.
\end{aligned}
$$

- Unless we generate a quantum link with sufficient fidelity (i.e., Werner state satisfying $\frac{1+w}{2} \geq \frac{2}{3}$), quantum teleportation has no advantage.

Usefulness for QKD: Secret Key Fraction

- It is possible to have an entanglement-based implementation of BB84.

$$\frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) = \frac{1}{\sqrt{2}}\Big(|{+}{+}\rangle + |{-}{-}\rangle \Big).$$

  - A and B's measurement outcomes are perfectly correlated if they choose the same base, irrespective of the choice.

- Under the influence of noise, instead of the EPR pair, A and B share a Werner state.
- In a noisy channel, B's measurement outcome may not match the qubit sent by A even if B uses the same base[13]. If the noise level is below a threshold, A and B can produce a secure key by removing information leakage via classical post-processing. Otherwise they abort the protocol.

[13] See slide 46.

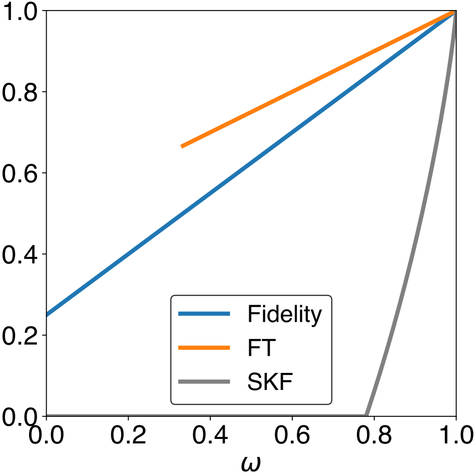
Secret Key Fraction

- What is the amount of secret key A and B can generate when the entangled link is given by a noisy state (Werner state ρ_w) instead of a perfect link ($|\Phi^+\rangle$)? It is given by the secret key fraction:

$$f_{\text{sk}}(w) = \max\left(1 - 2h\left(\frac{1-w}{2}\right), 0\right),$$

where h is the binary-entropy function $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

Usefulness of Link Quality



- FT: fidelity of teleportation, only shown beyond the classical threshold.
- SKF: secret key fraction.

Gate Fidelity

- Recall that the fidelity of teleportation was defined as the average fidelity between the output of an imperfect teleportation channel and the desired output (the input state itself).
- Similarly, we can define fidelity of quantum gates, given by suitable unitaries. As before, we find the fidelity between the actual and the desired outputs and average over all possible input states.

Gate Fidelity

- Suppose we want to implement a quantum gate given by a unitary G. We assume that the real-world implementation of this gate is given by an ideal implementation, followed by a time-dependent noise. That is, we model the implementation as $\mathcal{N}_t \circ G$, where $\mathcal{N}_t$ denotes the noise (e.g., depolarising noise).
- The fidelity of this implementation is defined as [4]:

$$F(\mathcal{N}_t, G) = \int \mathrm{d}\Psi \, \langle\Psi|G^\dagger \mathcal{N}_t \circ G(|\Psi\rangle\langle\Psi|)G|\Psi\rangle, \quad \text{(recall fidelity: } \langle\psi|\,\rho\,|\psi\rangle\text{)}$$

where the averaging is uniform over all pure states $|\Psi\rangle$.

- Since for any unitary G, $G\,|\Psi\rangle$ is uniformly distributed over pure states when $|\Psi\rangle$ is,

$$F(\mathcal{N}_t, G) = \int \mathrm{d}\Psi \, \langle\Psi|G^\dagger \mathcal{N}_t(G|\Psi\rangle\langle\Psi|G^\dagger)G|\Psi\rangle = \int \mathrm{d}\Psi \, \langle\Psi|\mathcal{N}_t(|\Psi\rangle\langle\Psi|)|\Psi\rangle$$

Depolarising Noise and Average Gate Fidelity

- For popular noise models, $F(\mathcal{N}_t, G)$ is often an affine function of $e^{-\theta t}$ for some parameter θ of the noise model [4].
- If we know that the gate implementation time or total waiting time is given by a random variable W, then computing the average gate fidelity due to waiting $\mathsf{E}_W(F(\mathcal{N}_W, G))$ boils down to finding MGF of W. For further applications under different noise models, see [4].

Summary of Performance Metrics

- We have so far considered the aspect of quality for quantum communication links, which is given by fidelity. We further considered application-specific quality measures such as fidelity of teleportation and secret key fraction (SKF).
- But in general, the rate of link generation also influences the performance of an application.
- A metric that combines both rate and fidelity is secret key rate, given by the product of link generation rate and SKF. This metric has particular operational significance for QKD.
- Of course, depending on the setup and objective, there could be other performance metrics. See, for example, [5] for a dynamic setup where quantum communication links are generated and consumed by an application probabilistically over time.

Performance Analysis in Quantum Networks: Examples

Towards Fair Resource Distribution in Quantum Networks

- We have seen two metrics for usefulness of link quality from an application point of view, namely fidelity of teleportation and secret key fraction.
- In general, the usefulness can be described by an entanglement measure f, which takes link fidelity (alternatively, the Werner parameter w) as input.
- Along with high-fidelity links, we also need reasonable generation rate. In general, there is a tradeoff in entanglement generation rate and quality.
  - When we generate links using the single-click protocol, the tradeoff between rate (x) and fidelity (w actually) is given by

$$x = d(1-w), \qquad d: \text{a link-specific constant.}$$

Network Utility Maximisation [6]

- **Goal**: Distribute rate among routes fairly and efficiently.
- **Setup**: Usefulness of allocations is given by route and network utility.
  - Route utility: route i has a measure of usefulness corresponding to rate allocation x_i, given by $g_i(x_i)$.
  - Network utility: route utilities are aggregated via a function G (such as product) to get network utility: $G(g_1(x_1), \ldots, g_n(x_n))$.
- Objective is to maximise $G(g_1(x_1), \ldots, g_n(x_n))$ over feasible rate allocations $\vec{x}$.
  - For example, for proportional fairness, we have $g_i(x) = x$ and G is the product function. The optimisation problem is given by

$$\begin{aligned} \max_{\vec{x}} \ & \prod_i x_i \\ \text{s.t. } & \vec{0} \preceq \vec{x} \\ & \text{capacity constraints} \end{aligned} \iff \begin{aligned} \max_{\vec{x}} \ & \sum_i \ln(x_i) \quad \left(\sum_i U_i(x_i),\ U_i \text{ concave}\right) \\ \text{s.t. } & \vec{0} \preceq \vec{x} \quad \text{(canonical form)} \\ & \text{capacity constraints} \end{aligned}$$

Quantum Network Utility Maximisation [7]

How does QNUM differ from classical NUM?

- *Resources*: We have two resources, namely entanglement generation rate x_i for route i and quality of link j: w_j.
- *End-to-end link quality*: Quality of route i is given by the Werner parameter of the end-to-end link, produced by swapping all links along route i. Since swapping Werner states produces another Werner state with parameter (u_i) given by the product of individual parameters (w_js), we have

$$u_i = \prod_{j \in \text{route } i} w_j. \quad \text{(Werner parameter} \leftrightarrow \text{fidelity)}$$

- *Route utility*: Usually, route utility is defined as $x_i f_i(u_i)$, f_i being the entanglement measure for route i. (product form adopted to emphasise importance of both rate and quality)
- *Network utility*: The network utility is given as product of route utilities: $\prod_i x_i f_i(u_i)$.

Quantum Network Utility Maximisation

How does QNUM differ from classical NUM?

- *Capacity constraint*: For single-click protocol, max generation rate μ_j of link j is given by $\mu_j = d_j(1 - w_j)$. Of course, total rate allocation on link j cannot exceed μ_j

$$\sum_{i:j \in \text{route } i} x_i \leq \mu_j .$$

- Using a link-route incidence matrix A, the QNUM problem can be written as

$$\begin{aligned} \max_{\vec{x},\vec{w}} \quad & \prod_{i=1}^{r} x_i f_i\left(\prod_{j=1}^{l} w_j^{a_{ji}} \right) \\ \text{s.t.} \quad & \vec{0} \prec \vec{x} \ , \\ & \vec{0} \prec \vec{w} \preceq \vec{1} \ , \ \text{(Fidelity bounds)} \\ & \langle A_j, \vec{x} \rangle \leq \mu_j = d_j(1 - w_j) \ \ \forall j \in [l]. \ \text{(Rate constraints)} \end{aligned}$$

Convexifying QNUM [8]

- Monotonicity of f_is implies $w_j = 1 - \langle A_j, \vec{x} \rangle / d_j$, letting us eliminate $\vec{w}$. Taking log, we have

$$\max_{\vec{x}} \sum_{i=1}^{r} \left(\ln x_i + \ln \left(f_i \left(\prod_{j=1}^{l} \left(1 - \frac{\langle A_j, \vec{x} \rangle}{d_j} \right)^{a_{ji}} \right) \right) \right)$$

$$\text{s.t.} \quad \vec{0} \prec \vec{x} \; ,$$

$$0 < \frac{\langle A_j, \vec{x} \rangle}{d_j} < 1 \; , \; j \in [l] \; ,$$

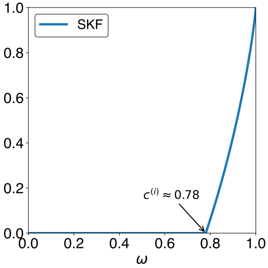
$$c^{(i)} < \prod_{j=1}^{l} \left(1 - \frac{\langle A_j, \vec{x} \rangle}{d_j} \right)^{a_{ji}} , \; i \in [r] \; ,$$

where $c^{(i)} := \sup\{z : f_i(z) = 0\}$. (Otherwise, zero network utility.)

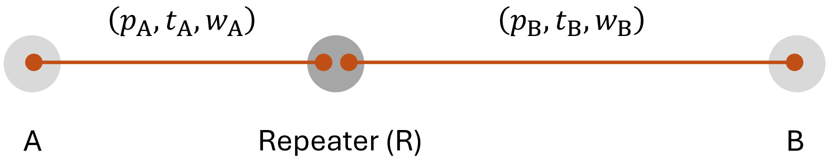
- In classical NUM, the utility function is usually concave. What about QNUM?

Convexifying QNUM

- For certain entanglement measures f_i, we can transform the problem into one with a concave objective function.
- The main idea is to transform the allocations $\vec{x} = e^{\vec{y}}$ (like geometric programming) and see the behaviour of the transformed objective function and feasible set.
  - The feasible set turns out to be convex as long as the entanglement measures are positive only if the end-to-end links have high enough fidelity. ($c^{(i)} \geq 1/2$ to be precise)
  - Popular entanglement measures behave nicely on this feasible set [8].



Hardware Requirements for Quantum Applications



- Every t_i time, an elementary link is successfully generated with probability p_i and if successful, the state of a freshly generated link is given by a Werner state with parameter w_i, $i \in \{A, B\}$.

Hardware Requirements for Quantum Applications

- In reality, the cycle times t_i are largely determined by propagation delay.
- We assume a depolarising noise model on the links.
- Thus, the controllable hardware configuration of the network is given by $\vec{\theta} := (p_\mathsf{A}, w_\mathsf{A}, p_\mathsf{B}, w_\mathsf{B}, T)$, where T is the coherence time of memories at A, R and B.
- Want to know if the current state of hardware $\vec{\theta}_0$ can achieve a fidelity threshold[14] F_0, and if not, which level of hardware improvement is necessary?
  - The difficulty in hardware improvement is given by $h(\vec{\theta}), \vec{\theta} \succeq \vec{\theta}_0$.
- Suppose the expected fidelity for a given hardware parameter $\vec{\theta}$ can be calculated as $\mathsf{E}(F(\vec{\theta}))$. Then the problem is given by

$$\min_{\vec{\theta} \succeq \vec{\theta}_0} h(\vec{\theta})$$
$$\text{s.t. } \mathsf{E}(F(\vec{\theta})) \geq F_0$$

[14] See slide 82 for a motivating example.

Hardware Requirements for Quantum Applications

- In general, the optimisation problem is not convex and is handled by a global optimisation heuristic.

$$\min_{\vec{\theta} \succeq \vec{\theta}_0} h(\vec{\theta})$$
$$\text{s.t. } \mathsf{E}(F(\vec{\theta})) \geq F_0$$

- How do we compute $\mathsf{E}(F(\vec{\theta}))$?
  - Link i is generated as Werner states with parameter w_i.
  - Swapping of Werner states produces a Werner state with parameter given by the product of the input parameters.
  - Action of depolarising noise on an elementary link (2-qubit Werner states): $w \to we^{-2t/T}$.

Computing $\mathsf{E}(F(\vec{\theta}))$

- Successful generation time of link i is given by $X_i \sim t_i\mathsf{Geo}(p_i)$. Thus, the amount of time the earlier link interacts with the environment is $|X_\mathsf{A} - X_\mathsf{B}|$.
- Under the depolarising noise model, the Werner parameter of the end-to-end link (after entanglement swap) is then $w_\mathsf{A} w_\mathsf{B} e^{-|X_\mathsf{A}-X_\mathsf{B}|/2T}$, T being the coherence time of each memory. In this simple setting, we have $\mathsf{E}(F(\vec{\theta})) = 1 + 3w_\mathsf{A} w_\mathsf{B}\mathsf{E}(e^{-|X_\mathsf{A}-X_\mathsf{B}|/2T})/4$. (fidelity of Werner states: $(1+3w)/4$)

Computing $\mathsf{E}(F(\vec{\theta}))$

- In reality, however, we can improve the expected fidelity by employing a cutoff strategy: (i) if the latter link is not generated by t_c time from the generation of the earlier link, restart generation of both links, (ii) repeat until success.
- The expected fidelity is then $\mathsf{E}(F(\vec{\theta}, t_c)) = 1 + 3w_{\mathsf{A}}w_{\mathsf{B}}\mathsf{E}(e^{-|X_{\mathsf{A}} - X_{\mathsf{B}}|/2T} \mid |X_{\mathsf{A}} - X_{\mathsf{B}}| \leq t_c)/4$, and we can optimise over the feasible range of the non-hardware parameter t_c.
- How does optimising the fidelity w.r.t. the cutoff parameter (t_c) impact the end-to-end link generation rate?
- How do we determine the hardware requirement in a dumbbell network?

Questions?

s.kar-1@tudelft.nl

www.sounakkar.com

References

[1] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al.
Satellite-based entanglement distribution over 1200 kilometers.
Science, 356(6343):1140–1144, 2017.

[2] Thomas Vidick and Stephanie Wehner.
Introduction to quantum cryptography.
Cambridge University Press, 2023.

[3] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters.
Mixed-state entanglement and quantum error correction.
Physical Review A, 54(5):3824, 1996.

[4] Gayane Vardoyan, Matthew Skrzypczyk, and Stephanie Wehner.
On the quantum performance evaluation of two distributed quantum architectures.
ACM SIGMETRICS Performance Evaluation Review, 49(3):30–31, 2022.

[5] Álvaro G Iñesta, Bethany Davies, Sounak Kar, and Stephanie Wehner.
Entanglement buffering with multiple quantum memories.
arXiv preprint arXiv:2502.20240, 2025.

[6] Frank Kelly.
Charging and rate control for elastic traffic.
European transactions on Telecommunications, 8(1):33–37, 1997.

[7] Gayane Vardoyan and Stephanie Wehner.
Quantum network utility maximization.
In *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, volume 1, pages 1238–1248. IEEE, 2023.

[8] Sounak Kar and Stephanie Wehner.
Convexification of the quantum network utility maximisation problem.
IEEE Transactions on Quantum Engineering, 2024.