Quantum Information and quantum cryptography

André Chailloux

Contents

Chapter 1

General formalism of quantum computing

1.1 Mixed states

Consider the state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ shared between 2 parties *Alice* and *Bob*. How do we describe Alice and Bob's state locally? Assume Alice measures her state in the computational basis. From the laws of partial measurement she measures "0" wp. $\frac{1}{2}$ and Bob has the state $|0\rangle$; or she measures "1" wp. $\frac{1}{2}$ and Bob has the state $|1\rangle$. If we look only from Bob's perspective, and if we define ρ_B his state, we have $\rho_B = \begin{cases} |0\rangle \text{ wp. } \frac{1}{2} \\ |1\rangle \text{ wp. } \frac{1}{2} \end{cases}$.

A mixed state (or density matrix) is a clean way of describing probabilistic quantum states as the one described above. A state

$$\rho = \begin{cases} |e_1\rangle \text{ wp. } p_1 \\ \vdots \\ |e_k\rangle \text{ wp. } p_k \end{cases}$$

is written $\rho = \sum_i p_i |e_i\rangle\langle e_i|$. If these states are n qubit states, recall Dirac's notation: $|e_i\rangle$ is a column vector of and $\langle e_i|$ is a line vector and $|e_i\rangle\langle e_i|$ is the multiplication of the two which gives a matrix. For example: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \cdot \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} = \begin{pmatrix} \alpha\alpha^* & \alpha\beta^* \\ \beta\alpha^* & \beta\beta^* \end{pmatrix}.$$

A few notable examples on 1 qubit:

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \; ; \; |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \; ; \; |+\rangle\langle +| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \; ; \; |-\rangle\langle -| = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

Definition 1.1. *A mixed state on n qubits is a matrix $\rho = \sum_i p_i |e_i\rangle\langle e_i|$ where each $|e_i\rangle$ is an n-qubit state, each $p_i \geq 0$ and $\sum_i p_i = 1$.*

Notice that the states $|e_i\rangle$ in the decomposition of a mixed state needn't be orthogonal. For example:

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}.$$

is a valid 1-qubit mixed state.

Properties of quantum mixed states.

- A quantum mixed state ρ is a Hermitian matrix $\rho = \rho^* := \overline{\rho}^\intercal$. This is because each $|\phi\rangle\langle\phi|$ is Hermitian.
- $\mathrm{Tr}(\rho) = 1$ since $\mathrm{Tr}(|\phi\rangle\langle\phi|) = 1$ for each $|\phi\rangle$.
- Since ρ is Hermitian it is diagonalizable with real valued eigenvalues, and moreover, these eigenvalues are non-negative (since the $p_i \geq 0$ in the definition). This means we can write $\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$ $0 \leq \lambda_i \leq 1$, $\sum_i \lambda_i = 1$ and the $|e_i\rangle$ are pairwise orthogonal quantum states.

1.1.1 Applying quantum operations on mixed states

A mixed state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ is a complete description of the quantum state you have.

Unitaries. Applying a unitary U on a pure state $|\psi\rangle$ gives the state $U|\psi\rangle = |\phi\rangle$. If we from a density matrix $\rho = |\psi\rangle\langle\psi|$, then applying a unitary U on this state gives the state $|\phi\rangle\langle\phi| = U|\psi\rangle\langle\psi|U^\dagger$. More generally, applying U on a state ρ gives the state $U\rho U^\dagger$.

Projective measurements. Consider a state ρ of n qubits and a basis $B = |b_1\rangle, \ldots, |b_{2^n}\rangle$ of the Hilbert space of n qubits. If you measure ρ in the basis B, you have

$$\Pr[\text{ outcome } |b_k\rangle] = \sum_i p_i |\langle\psi_i|b_k\rangle|^2 = \langle b_k|\rho|b_k\rangle.$$

1.1.2 Different mixtures of quantum states can have the same density matrix

Let $\rho_1 = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$ and $\rho_2 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|$. We have

$$\rho_1 = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}$$

and

$$\rho_2 = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1/8 & 1/8 \\ 1/8 & 1/8 \end{pmatrix} + \begin{pmatrix} 1/8 & -1/8 \\ -1/8 & 1/8 \end{pmatrix} = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}.$$

Two different decompositions can lead to the same density matrix. This means that these two quantum states are the same, they can't be distinguished one from the other by using quantum operations.

1.2 Partial trace

Let's go back to our original motivation. Assume you have a state $|\psi\rangle_{AB} = \sum_{i,j} \alpha_i |e_i\rangle_A |i\rangle_B$ shared between 2 parties Alice and Bob. What is the state that Alice has? She has the mixed state

$$\rho_A = \sum_i |\alpha_i|^2 |e_i\rangle\langle e_i|.$$

To see this, assume Bob measures his state in the computational basis. He gets outcome "i" wp. $|\alpha_i|^2$ and Alice has the state $|e_i\rangle$ which means she has the state ρ_A. Notice also that Alice's state doesn't depend on whether Bob has measured or not, so we can always describe Alice's state as ρ_A.

The mathematical operation that describes Alice's reduced state is called the *partial trace*. For a (possibly mixed) state ρ_{AB} shared between Alice and Bob, we define

$$\mathrm{Tr}_B(\rho_{AB}) = \sum_j (I_A \otimes \langle j|)\rho_{AB}(I_A \otimes |j\rangle). \tag{1.1}$$

$\mathrm{Tr}_B(\rho_{AB})$ means that we "trace out" Bob's registers from ρ_{AB} (so we keep Alice's part). We will rarely use Equation 1.1 directly. Rather, we will use the following results:

- For $|\psi\rangle_{AB} = \sum_{i,j} \alpha_i |e_i\rangle_A |i\rangle_B$, $\mathrm{Tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|) = \sum_i |\alpha_i|^2 |e_i\rangle\langle e_i|$.
- For $\rho_{AB} = \sum_i p_i |f_i\rangle\langle f_i|$, $\mathrm{Tr}_B(\rho_{AB}) = \sum_i p_i \mathrm{Tr}_B |f_i\rangle\langle f_i|$.

With the partial, we are now able to characterize the reduced state of a quantum state share between different registers.

1.3 Generalized measurements

POVM, for Positive Operator Value Measurements, generalize projective measurements.

Definition 1.2. *A POVM is an ensemble of matrices $\{M_i\}_i$ st. $\sum_i M_i M_i^\dagger = I$. Measuring a state ρ with this POVM gives outcome i wp. $p_i = tr(\rho M_i M_i^\dagger)$ and conditioned on obtaining outcome i, the resulting state is*

$$\rho_i = \frac{M_i \rho M_i^\dagger}{tr(M_i \rho M_i^\dagger)}.$$

Remarks.

- A POVM is sometimes defined by the matrices $F_i = M_i M_i^\dagger$. Be careful however, the probabilities p_i depend only on F_i but the resulting states ρ_i actually depend on the M_i so using the F_i is fine if you are only interested in the outcome distribution but you need the M_i is you want to specify the resulting states.
- There is no restriction on the M_i but the $F_i = M_i M_i^\dagger$ are positive semi-definite (hence the name POVM).
- Projective measurements are a special case, where the M_i are projectors (which implies $M_i = M_i M_i^\dagger = F_i$).

- Physically, a POVM on a state ρ corresponds to the setting where we add some extra qubits $|0^m\rangle\langle 0^m|$ to ρ, perform a projective measurement and then trace-out some qubits. So POVM are not more powerful from a physical point of view but are an elegant and compact form for describing these operations.

1.4 Purifications

A purification $|\psi\rangle_{AB}$ of a state ρ_B satisfies $\mathrm{Tr}_A|\psi_{AB}\rangle\langle\psi_{AB}| = \rho_B$. For example, if $\rho_B = \sum_i p_i|f_i\rangle\langle f_i|$ then the state $|\phi\rangle_{AB} = \sum_i \sqrt{p_i}\,|i\rangle_A\,|f_i\rangle_B$ is a purification of ρ_B.

Proposition 1.3 (Schmidt Decomposition)**.** *Let $|\psi\rangle_{AB}$ be a state of $2n$ qubits, where each register A, B contains n qubits. There exists two basis $\{|e_1\rangle, \ldots, |e_{2^n}\rangle\}$ and $\{|f_1\rangle, \ldots, |f_{2^n}\rangle\}$ st. $|\psi\rangle_{AB} = \sum_{i=1}^{2^n} \alpha_i\,|e_i\rangle_A\,|f_i\rangle_B$. with $\sum_i |\alpha_i|^2 = 1$. This decomposition is unique. Moreover,*

$$\mathrm{Tr}_A|\psi_{AB}\rangle\langle\psi_{AB}| = \sum_i |\alpha_i|^2|f_i\rangle\langle f_i| \;;\; \mathrm{Tr}_B|\psi_{AB}\rangle\langle\psi_{AB}| = \sum_i |\alpha_i|^2|e_i\rangle\langle e_i|.$$

Proposition 1.4. *Assume we have two quantum pure states $|\phi_{AB}\rangle$ and $|\psi_{AB}\rangle$ st. $\mathrm{Tr}_A(|\phi_{AB}\rangle\langle\phi_{AB}|) = \mathrm{Tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|) = \rho_B$. There exists a unitary U acting on A st. $(U \otimes I)\,|\phi_{AB}\rangle = |\psi_{AB}\rangle$.*

Proof. We write $\rho_B = \sum_i p_i|f_i\rangle\langle f_i|$ the spectral decomposition of ρ_B (so all the $|f_i\rangle$ are pairwise orthogonal). This means we can write $|\phi_{AB}\rangle$ and $|\psi_{AB}\rangle$ as follows, using the Schmidt decomposition.

$$|\phi_{AB}\rangle = \sum_i \alpha_i\,|e_i\rangle\,|f_i\rangle$$
$$|\phi_{AB}\rangle = \sum_i \alpha'_i\,|e'_i\rangle\,|f_i\rangle$$

with $|\alpha_i| = |\alpha'_i| = \sqrt{p_i}$ and $\{|e_i\rangle\}$ as well as the $\{|e'_i\rangle\}$ each form a basis. This means there exists a unitary U st. for each i, $U\,|e_i\rangle = \frac{\alpha'_i}{\alpha_i}\,|e'_i\rangle$. We then immediately have

$$(U \otimes I)\,|\phi_{AB}\rangle = |\psi_{AB}\rangle\,.$$

□

Chapter 2

Distance measures for quantum states and first notion of quantum information theory

2.1 How close are two quantum states?

2.1.1 The trace distance

We introduce here the notion of trace distance, which is very useful in determining how close two mixed states are. We present here basic properties of this distance. More about the trace distance can be found in [**?**].

Definition and basic properties

Definition 2.1. *For any two quantum mixed states ρ and σ, the trace distance between ρ and σ is defined as $\Delta(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_{\text{tr}}$ where $\|M\|_{\text{tr}} = Tr(\sqrt{M^\dagger M})$.*

Since ρ and σ are hermitian, we have

$$\Delta(\rho,\sigma) = \frac{1}{2}Tr(\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}).$$

Be careful, this *doesn't necessarily imply* $\Delta(\rho,\sigma) = \frac{1}{2}Tr(\rho-\sigma)$!

$\rho-\sigma$ is Hermitian but not necessarily positive. This means we can write $\rho-\sigma = \sum_i \lambda_i |e_i\rangle\langle e_i|$ where $\{|e_i\rangle\}_i$ is a orthonormal basis and the $\lambda_i \in \mathbb{R}$. We have $\Delta(\rho,\sigma) = \frac{1}{2}\sum_i |\lambda_i|$.

Notice also that $\sum_i \lambda_i = Tr(\rho-\sigma) = Tr(\rho) - Tr(\sigma) = 1-1 = 0$.

The trace distance is a distance. Indeed, it satisfies the following properties:

- $\Delta(\rho,\sigma) = 0 \Leftrightarrow \rho = \sigma$.

- $0 \leq \Delta(\rho, \sigma) \leq 1$.
- $\Delta(\rho, \sigma) = \Delta(\sigma, \rho)$.
- $\forall \rho, \sigma, \tau,\ \Delta(\rho, \tau) \leq \Delta(\rho, \sigma) + \Delta(\sigma, \tau)$

Example of Trace distances

- ρ and σ are diagonalizable in the same basis : this means we can write $\rho = \sum_i p_i |e_i\rangle\langle e_i|$ and $\sigma = \sum_i q_i |e_i\rangle\langle e_i|$ where $\{|e_i\rangle\}_i$ is a orthonormal basis. In this case, we have $\Delta(\rho, \sigma) = \frac{1}{2}\sum_i |p_i - q_i|$.
- ρ and σ are two pure states : this means we can write $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$. In this case, we have $\Delta(\rho, \sigma) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$.
- Other example: $\rho = |0\rangle\langle 0|$, $\sigma = \frac{3}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|$. Let's calculate $\Delta(\rho, \sigma)$ using the definition. We have

$$\begin{aligned}\rho - \sigma &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \left[\frac{3}{4}\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\right] \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 1/2 & 1/4 \\ 1/4 & 1/2 \end{pmatrix} \\ &= \begin{pmatrix} 1/2 & -1/4 \\ -1/4 & -1/2 \end{pmatrix}\end{aligned}$$

  Calculation tip: at that point, make sure that $\rho - \sigma$ is Hermitian and that its trace is 0.

$$(\rho - \sigma)^\dagger(\rho - \sigma) = \begin{pmatrix} 1/2 & -1/4 \\ -1/4 & -1/2 \end{pmatrix} \cdot \begin{pmatrix} 1/2 & -1/4 \\ -1/4 & -1/2 \end{pmatrix} = \begin{pmatrix} 5/16 & 0 \\ 0 & 5/16 \end{pmatrix}$$

  From there, we have

$$\sqrt{(\rho - \sigma)^2} = \sqrt{\begin{pmatrix} 5/16 & 0 \\ 0 & 5/16 \end{pmatrix}} = \begin{pmatrix} \sqrt{5}/4 & 0 \\ 0 & \sqrt{5}/4 \end{pmatrix}$$

  which allows us to conclude that $\Delta(\rho, \sigma) = \frac{1}{2}Tr(\sqrt{(\rho - \sigma)(\rho - \sigma)^\dagger}) = \sqrt{5}/4$.

Invariance over unitary operations. The trace distance has the following property:

Proposition 2.2. *For any two quantum mixed states ρ, σ and any unitary operation U, we have $\Delta(\rho, \sigma) = \Delta(U\rho U^\dagger, U\sigma U^\dagger)$.*

Interpretation of the trace distance

Let's consider two people Alice and Bob. Alice has bit b unknown to Bob. Suppose now Alice sends a mixed state ρ_b that depends on b. With what probability can Bob guess b? This probability in fully characterized by the trace distance between ρ_0 and ρ_1. We have:

Proposition 2.3. $\max(\Pr[\textit{Bob guesses } b]) = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$

Proof. We will not go through the whole proof. However, we'll show that $\max(\Pr[\text{Bob guesses } b]) \geq \frac{1}{2} + \frac{\Delta(\rho_0,\rho_1)}{2}$. To do this, we present a measurement for Bob that allows him to guess b with probability $\frac{1}{2} + \frac{\Delta(\rho_0,\rho_1)}{2}$.

We write $\rho_0 - \rho_1 = \sum_i \lambda_i |e_i\rangle\langle e_i|$ where $\{|e_i\rangle\}_i$ is a orthonormal basis and $\sum_i \lambda_i = 0$. Bob's strategy is to measure in the $\{|e_1\rangle, \ldots, |e_n\rangle\}$ basis. Suppose Bob's outcome is $|e_i\rangle$:

- If $\lambda_i \geq 0$, Bob's guess is 0.
- If $\lambda_i < 0$, Bob's guess is 1.

Let

$$p_i = \langle e_i|\rho_0|e_i\rangle = \Pr[\text{Bob's outcome is } |e_i\rangle \mid \text{Bob receives } \rho_0]$$
$$q_i = \langle e_i|\rho_1|e_i\rangle = \Pr[\text{Bob's outcome is } |e_i\rangle \mid \text{Bob receives } \rho_1]$$

Notice that we have $\langle e_i|\rho_0 - \rho_1|e_i\rangle = \lambda_i = p_i - q_i$. We write

$$\Pr[\text{Bob guesses } b \text{ correctly } |b=0] = \sum_{i:\lambda_i \geq 0} p_i$$
$$\Pr[\text{Bob guesses } b \text{ correctly } |b=1] = \sum_{i:\lambda_i < 0} q_i$$

Since b is a random bit, we have

$$\Pr[\text{Bob guesses } b \text{ correctly}] = \frac{1}{2}\sum_{i:\lambda_i \geq 0} p_i + \frac{1}{2}\sum_{i:\lambda_i < 0} q_i$$

Moreover, we have

$$\begin{aligned}\sum_i |\lambda_i| = \sum_i |p_i - q_i| &= \sum_{i:\lambda_i \geq 0} p_i - q_i + \sum_{i:\lambda_i < 0} q_i - p_i \\ &= \sum_{i:\lambda_i \geq 0} p_i - (1 - \sum_{i:\lambda_i < 0} q_i) + \sum_{i:\lambda_i < 0} q_i - (1 - \sum_{i:\lambda_i \geq 0} p_i) \quad using \sum_i p_i = \sum_i q_i = 1 \\ &= 2(\sum_{i:\lambda_i \geq 0} p_i) + 2(\sum_{i:\lambda_i < 0} q_i) - 2\end{aligned}$$

From there, we conclude:

$$\Pr[\text{Bob guesses } b \text{ correctly}] = \frac{1}{2}\sum_{i:\lambda_i \geq 0} p_i + \frac{1}{2}\sum_{i:\lambda_i < 0} q_i = \frac{1}{4}\sum_i |\lambda_i| + \frac{1}{2} = \frac{\Delta(\rho,\sigma)}{2} + \frac{1}{2}$$

NB: This measurement is optimal for Bob □

2.1.2 Unambiguous state discrimination

Assume we have 2 qubits $|\phi_0\rangle = |0\rangle$ and $|\phi_1\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$. We just saw that there is a measurement that distinguishes between $|\phi_0\rangle$ and $|\phi_1\rangle$ wp. $\frac{1}{2} + \frac{1}{2}\sqrt{1 - \cos^2(\theta)} = \frac{1}{2} + \frac{\sin(\theta)}{2}$. The measurement is a projective measurement $\{E_0, E_1\}$ st. $tr(E_i|\phi_i\rangle\langle\phi_i|) =$

$\frac{1}{2}+\frac{\sin(\theta)}{2}$. We are ourselves another question, we want a measurement that maybe succeeds with a smaller probability but is always correct when it succeeds. More precisely, we want a measurement that has up to 3 outcomes: "0", "1" and "2" st. the measurement always succeeds when measuring "0" or "1". (the "2" outcome corresponds to unknown). If you only consider projective measurements, the best outcome is to consider the measurement $\{|1\rangle\langle 1|, \vec{0}, |0\rangle\langle 0|\}$, and this measurement succeeds wp. $\frac{1}{2}\sin^2(\theta)$.

With the use of POVM, we can do much better. Let $|f_1\rangle = \sin(\theta)|0\rangle - \cos(\theta)|1\rangle$. We consider the 3 outcome POVM $F = \{F_1, F_2, F_3\}$ with $F_i = M_i M_i^\dagger$. We take $F_1 = \frac{1}{1+\cos(\theta)} kbf_1,$, $F_2 = \frac{1}{1+\cos(\theta)}|1\rangle\langle 1|$, $F_3 = (I - kbf_1 - |1\rangle\langle 1|)\}$. One can check that F_1, F_2, F_3 are positive semi-definite. We have

$$tr(|i\rangle\langle i|F_i) = \frac{\sin^2(\theta)}{1+\cos(\theta)} = 1 - \cos(\theta)$$
$$tr(|i\rangle\langle i|F_{1-i}) = 0 \quad \text{for } iin\{0,1\}$$

This means the measurements always succeeds if you don't have a "2" outcome and it succeeds wp. $1 - \cos(\theta)$.

2.2 Fidelity for quantum states

We now present a second notion for quantifying how close two quantum states are, *the fidelity*. We will use this notion to analyze more formally cheating possibilities in quantum bit commitment protocols.

2.2.1 Definition and basis properties

Definition 2.4. *For any two quantum mixed states ρ and σ, the fidelity between ρ and σ is defined as $F(\rho,\sigma) = Tr(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$*

The fidelity has the following properties

- $0 \leq F(\rho,\sigma) \leq 1$.
- $F(\rho,\sigma) = 1 \Leftrightarrow \rho = \sigma$
- $F(\rho,\sigma)$

It seems that the quantity $(1 - F(\rho,\sigma)$ has similar properties than $\Delta(\rho,\sigma)$. However, the quantity $1 - F$ does not satisfy the triangle inequality, meaning we don't necessarily have

$$(1 - F(\rho,\tau)) \leq (1 - F(\rho,\sigma)) + (1 - F(\sigma,\tau))$$

. However, we have a 'weak' triangle inequality in the following form

Proposition 2.5. *For any states ρ, σ, τ, we have* $(1-F(\rho,\tau)) \leq 2(1-F(\rho,\sigma))+2(1-F(\sigma,\tau))$

Example of fidelities

- ρ and σ are diagonalizable in the same basis : this means we can write $\rho = \sum_i p_i |e_i\rangle\langle e_i|$ and $\sigma = \sum_i q_i |e_i\rangle\langle e_i|$ where $\{|e_i\rangle\}_i$ is a orthonormal basis. In this case, we have $F(\rho,\sigma) = \sum_i \sqrt{p_i q_i}$.
- ρ and σ are two pure states : this means we can write $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$. In this case, we have $F(\rho,\sigma) = |\langle\psi|\phi\rangle|$.

Invariance over unitary operations. The fidelity also has the following property:

Proposition 2.6. *For any two quantum mixed states ρ, σ and any unitary operation U, we have $F(\rho,\sigma) = F(U\rho U^\dagger, U\sigma U^\dagger)$.*

2.2.2 Purifications and Uhlmann's theorem

Our goal here is to introduce the notion of purifications. Then we give an interpretation of fidelity of two states using Uhlmann's theorem.

Purifications

Definition 2.7. *For any state ρ_B, we say that a bipartite state $|\psi_{AB}\rangle$ is a purification of ρ_B is $Tr_A(\psi_{AB}) = \rho$.*

Typically, if two players Alice and Bob share a state $|\psi_{AB}\rangle$ then $\rho_B = Tr_A(|\psi_{AB}\rangle)$ is Bob's reduced density matrix and $|\psi_{AB}\rangle$ is a purification of ρ_B.

For example, if $\rho_B = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$, then $|\psi_{AB}\rangle = \sqrt{\frac{3}{4}}\,|0\rangle\,|0\rangle + \sqrt{\frac{1}{4}}\,|1\rangle\,|1\rangle$ is a purification of ρ_B. We also have that $|\psi'_{AB}\rangle = \sqrt{\frac{3}{4}}\,|+\rangle\,|0\rangle + \sqrt{\frac{1}{4}}\,|-\rangle\,|1\rangle$. This means that a state ρ_B can have many purifications.

Fix $\rho_B = \sum_i p_i |e_i\rangle\langle e_i|$. We have that $|\psi_{AB}\rangle = \sum_i \sqrt{p_i}\,|i\rangle\,|e_i\rangle$ is a purification of ρ_B. In fact, for any orthonormal basis $\{|f_i\rangle\}_i$, $|\psi_{AB}\rangle = \sum_i \sqrt{p_i}\,|f_i\rangle\,|e_i\rangle$ is a purification of ρ_B. NB: the above holds even if $\{|e_i\rangle\}_i$ is not a basis.

Uhlmann's Theorems

We now present an interpretation of the fidelity of quantum states

Theorem 2.8 (Uhlmann's first theorem)**.** *For any two states ρ, σ,*

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\phi\rangle} |\langle\psi|\phi\rangle|$$

where the maximum is taken over purifications $|\psi\rangle$ of ρ and purifications $|\phi\rangle$ of σ.

Theorem 2.9 (Uhlmann's second theorem)**.** *For any two states ρ, σ and any purification $|\psi\rangle$ of ρ, we have*

$$F(\rho,\sigma) = \max_{|\phi\rangle} |\langle\psi|\phi\rangle|$$

where the maximum is taken over purifications $|\phi\rangle$ of σ.

For example, consider $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ and $\sigma = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$. Since ρ and σ are diagonalizable in the same basis, we know that $F(\rho,\sigma) = \sqrt{\frac{3}{8}} + \sqrt{\frac{1}{8}}$. Let $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and $|\phi\rangle = \sqrt{\frac{3}{4}}|00\rangle + \sqrt{\frac{1}{4}}|11\rangle$.

$|\psi\rangle$ (resp. $|\phi\rangle$) is a purification of ρ (resp. σ). Moreover, we have $\langle\psi|\phi\rangle = \sqrt{\frac{3}{8}} + \sqrt{\frac{1}{8}}$. These purifications are optimal with regards to Uhlmann's theorem.

2.2.3 Angle distance

As we said previously, the quantity $1 - F$ is not a distance since it doesn't satisfy the triangle inequality. Our goal here is to construct a distance out of the fidelity.

Definition 2.10. *For any two quantum states ρ, σ, we define their angle as $Angle(\rho,\sigma) = Arccos(F(\rho,\sigma))$*

Fix two pure states $|\psi\rangle$ and $|\phi\rangle$ with $|\langle\psi|\phi\rangle| = \cos(\alpha)$, then $Angle(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \alpha$. The notion of angle for mixed states somehow extends the notion of angle that exists for pure states.

The angle is a distance Indeed, it satisfies the following properties

- $Angle(\rho,\sigma) = 0 \Leftrightarrow \rho = \sigma$
- $0 \leq Angle(\rho,\sigma) \leq \pi/2$
- $Angle(\rho,\sigma) = Angle(\sigma,\rho)$
- $Angle(\rho,\tau) \leq Angle(\rho,\sigma) + Angle(\sigma,\tau)$

2.2.4 Fuchs - Van de Graaf inequalities

Finally, we present a relationship between the trace distance of two quantum states and the fidelity of those states.

Proposition 2.11 ([?])**.** *For any states ρ, σ, we have*

$$(1 - F(\rho,\sigma) \leq \Delta(\rho,\sigma) \leq \sqrt{1 - F^2(\rho,\sigma)}$$

or conversely

$$(1 - \Delta(\rho,\sigma) \leq F(\rho,\sigma) \leq \sqrt{1 - \Delta^2(\rho,\sigma)}$$

Chapter 3

First quantum cryptographic protocols

3.1 Bit commitment

A bit commitment scheme is a protocol between two parties Alice and Bob, denoted hereafter A and B. A bit commitment scheme consists of 2 phases; a *commit phase* and a *reveal phase*.

- At the commit phase, Alice commits to a bit $b \in \{0, 1\}$ and Bob should not be able to guess b at the end of the commit phase.
- At the reveal phase, Alice reveals b. She shouldn't be able to change her mind about the bit b she reveals.

Security requirements:

- *Completeness:* If both players are honest, the protocol should succeed wp. 1.
- *Hiding property:* If Alice is honest and Bob is dishonest, his cheating probability is

$$P_B^* = \Pr[\text{ Bob guesses } b \text{ after the commit phase }].$$

- *Binding property:* If Alice is dishonest and Bob is honest, her cheating probability is

$$P_A^* = \frac{1}{2}\left(\Pr[\text{ Alice successfully reveals } b = 0] + \Pr[\text{ Alice successfully reveals } b = 1]\right).$$

for the same commit phase. This means that after the commit phase, we want to bound Alice possibility to reveal both $b = 0$ and $b = 1$ successfully.

3.1.1 Generic example of commitment schemes

Let $\left|\psi_{AB}^0\right\rangle$ and $\left|\psi_{AB}^1\right\rangle$ two quantum bipartite states. Consider the following protocol

- **Commit phase:** Alice wants to commit to a bit b. She creates $\left|\psi_{AB}^{b}\right\rangle$ and sends the B part to Bob. After the commit phase, Bob has $\rho_b = Tr_A(\left|\psi_{AB}^{b}\right\rangle)$.
- **Reveal phase:** Alice sends the A part of the quantum state $\left|\psi_{AB}^{b}\right\rangle$ as well as b. Bob checks that he has $\left|\psi_{AB}^{b}\right\rangle$ by projecting the state he has onto $\left|\psi_{AB}^{b}\right\rangle$.

Cheating probabilities We define the cheating probabilties for the two players:

- $P_A^* = \max(\Pr[\text{Alice cheats}]) = \max\left(\frac{1}{2}\Pr[\text{Alice reveals } b=0] + \frac{1}{2}\Pr[\text{Alice reveals } b=1]\right)$ (for the same commit phase)
- $P_B^* = \max(\Pr[\text{Bob cheats}]) = \max(\Pr[\text{Bob can guess b after the commit phase}])$

3.1.2 Cheating strategies

Cheating Bob : He has ρ_b after the commit phas and tries to guess b. We have that

$$P_B^* = \Pr[\text{Bob can guess } b] = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

Cheating Alice: Fix a cheating strategy for Alice and let σ the state that Bob has after the commit phase. During the reveal phase, is she reveals $b = 0$ then she sends qubits such that Bob has a pure state $|\phi_0\rangle$. If she reveals $b = 1$, then she sends qubits such that Bob has a pure state $|\phi_1\rangle$.

We have $Tr_A(|\phi_0\rangle) = Tr_A(|\phi_1\rangle) = \sigma$. If Alice reveals $b = 0$, we have

$$\Pr[\text{Bob accepts } |b=0] = |\left\langle \phi_0 \middle| \psi_{AB}^{b} \right\rangle|^2$$

If Alice reveals $b = 1$, we have

$$\Pr[\text{Bob accepts } |b=1] = |\left\langle \phi_1 \middle| \psi_{AB}^{b} \right\rangle|^2$$

Using Uhlmann's theorem, we have

$$\max_{|\phi_0\rangle} |\left\langle \phi_0 \middle| \psi_{AB}^{0} \right\rangle|^2 = F^2(\sigma, \rho_0)$$

where the maximum is taken over purifications $|\phi_0\rangle$ of σ. We also have

$$\max_{|\phi_1\rangle} |\left\langle \phi_1 \middle| \psi_{AB}^{1} \right\rangle|^2 = F^2(\sigma, \rho_1)$$

where the maximum is taken over purifications $|\phi_1\rangle$ of σ.

This gives us

$$\frac{1}{2}\left(\Pr[\text{Bob accepts } |b=0] + \Pr[\text{Bob accepts } |b=1]\right) = \frac{1}{2}F^2(\sigma, \rho_0) + \frac{1}{2}F^2(\sigma, \rho_1)$$

Since Alice can choose any σ, we have

$$P_A^* = \max_{\sigma}\left(\frac{1}{2}F^2(\sigma, \rho_0) + \frac{1}{2}F^2(\sigma, \rho_1)\right)$$

Recall also that

$$P_B^* = \frac{1}{2} + \Delta(\rho_0, \rho_1)/2$$

We want to remove the maximization for Alice's cheating probability. We use the following Lemma

Lemma 1.

$$\forall \sigma, \frac{1}{2}F^2(\sigma, \rho_0) + \frac{1}{2}F^2(\sigma, \rho_1) \leq \frac{1}{2}\left(1 + F(\rho_0, \rho_1)\right)$$

Proof. Use the Angle distance (proof skipped here) □

Also, there exists a σ such that $\frac{1}{2}F^2(\sigma, \rho_0) + \frac{1}{2}F^2(\sigma, \rho_1) = \frac{1}{2}\left(1 + F(\rho_0, \rho_1)\right)$. From there, we conclude that

$$P_A^* = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2}$$
$$P_B^* = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

Best coin flipping protocols of this type By using the Fuchs - Van de Graaf inequalities, we have $F(\rho_0, \rho_1) \geq 1 - \Delta(\rho_0, \rho_1)$. This implies $P_A^* + P_B^* \geq 3/2$ or $\max\{P_A^*, P_B^*\} \geq 3/4$. Is this tight ? Yes

Consider the states $\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|2\rangle\langle 2|$ and $\rho_1 = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|$. We can calculate

$$\Delta(\rho_0, \rho_1) = \frac{1}{2}(|1/2 - 0| + |0 - 1/2| + |1/2 - 1/2|) = 1/2$$
$$F(\rho_0, \rho_1) = \sqrt{1/2 \cdot 0} + \sqrt{0 \cdot 1/2} + \sqrt{1/2 \cdot 1/2} = 1/2$$

NB: This analysis covers only quantum bit commitment protocols for specific commit/reveal phases. This is not the most general analysis. In fact, there exists interactive quantum BC protocols with cheating probabiltiies $< 3/4$.

3.2 Bit commtiment based coin flipping

Here, we show that any bit commitment protocols with cheating probabilities P_A^*, P_B^* can be transformed into a quantum bit commitment scheme with the same cheating probabilities.

Protocol for QCF using QBC

1. Alice picks a random $a \in \{0, 1\}$. Then, she commits to a using the QBC protocol.
2. Bob sends a random $b \in \{0, 1\}$ and sends b to Alice.
3. Alice reveals a, as described in the QBC protocol.
4. The output of the coin is $c = a \oplus b$.

We can see that

Pr[Bob cheats in the CF protocol] = Pr[Bob guesses a after step 1] = Pr[Bob cheats in the BC protocol].

and

$$\begin{aligned}\Pr[\text{Alice cheats in the CF protocol}] &= \frac{1}{2}\Pr[\text{Alice cheats in the CF protocol } | \text{Bob sends } b=0] + \\ &\qquad \frac{1}{2}\Pr[\text{Alice cheats in the CF protocol } | \text{Bob sends } b=1] \\ &= \frac{1}{2}\Pr[\text{Alice successfully reveals } a=0] + \frac{1}{2}\Pr[\text{Alice successfully reveals } a=1] \\ &= \Pr[\text{Alice can cheat in the BC protocol}]\end{aligned}$$

NB: On the other hand, we don't have $QCF \Rightarrow QBC$.

3.3 Quantum Random Access codes

A quantum encoding $x \in \{0,1\}^n \to |\psi_x\rangle$ on m qubits is called a $(n,m,p) - QRAC$, if one can recover any bit x_i with probability p when having access to $|\psi_x\rangle$. $(n,m,1) - QRACs$ are impossible for $m < n$.

Construction of a $(2,1,\cos^2(\pi/8))$-QRAC We consider the encoding $|\psi_{00}\rangle = |0\rangle$, $|\psi_{01}\rangle = |+\rangle$, $|\psi_{10}\rangle = |-\rangle$, $|\psi_{11}\rangle = |1\rangle$.

- If I want to learn x_1, I measure in the $\{|v\rangle, |v^\perp\rangle\}$ basis with $|v\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and $|v^\perp\rangle = \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle$.
- If I want to learn x_2, I measure in the $\{|w\rangle, |w^\perp\rangle\}$ basis with $|w\rangle = \cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle$ and $|w^\perp\rangle = \sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$.

We have

$$\begin{aligned}|\langle v|\psi_{00}|\rangle|^2 = |\langle v|\psi_{01}\rangle|^2 = \cos^2(\pi/8) \\ |\langle v^\perp|\psi_{10}\rangle|^2 = |\langle v^\perp|\psi_{11}\rangle|^2 = \cos^2(\pi/8) \\ |\langle w|\psi_{00}\rangle|^2 = |\langle v|\psi_{10}\rangle|^2 = \cos^2(\pi/8) \\ |\langle w^\perp|\psi_{01}\rangle|^2 = |\langle w^\perp|\psi_{11}\rangle|^2 = \cos^2(\pi/8)\end{aligned}$$

which shows that this construction is indeed a $(2,1,\cos^2(\pi/8))$-QRAC.

NB: These measurements are optimal.

Chapter 4

Quantum key distribution

Key distribution is an important cryptographic primitive, which is defined as follows.

Key distribution

- Alice and Bob communicate over a *public* and *authenticated* channel.
- At the end of the scheme, they should agree on a key $K \in \{0,1\}^k$.
- Any adversary eavesdropping and tampering the channel shouldn't be able to have any (or vanishingly little) information about K.

4.1 Encoding bits of key inside qubits

Alice has a string $K = k_1, \ldots, k_n$ which we call the initial key. Her goal is to transmit the bits of K to Bob in a way that can't be intercepted without being caught. For each i, She performs the following encoding:

The BB84 encoding of a bit k_i

- Pick a random $b_i \in \{0,1\}$.
- If $b_i = 0$, construct $|\psi_i\rangle = |k_i\rangle$. If $b_i = 1$, construct $|\psi_i\rangle = H|k_i\rangle$.
- Output $|\psi_i\rangle$.

This encoding is very simple. You pick a random $b_i \in \{0,1\}$, and you encode k_i in the computational basis if $b_i = 0$ and in the Hadamard basis if $b_i = 1$.

k_i	b_i	$\|\psi_i\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

The full protocol is then the following

The BB84 protocol

- Alice picks a random initial raw key $K = k_1, \ldots, k_n$ uniformly at random.
- For each $i \in \{1, \ldots, n\}$, Alice picks a random $b_i \in \{+, \times\}$, constructs $|\psi_i\rangle = |k_i\rangle^{b_i}$ and sends $|\psi_i\rangle$ to Bob.
- Bob picks some random basis $b'_1, \ldots, b'_n \in \{+, \times\}$ and measures each qubit $|\psi_i\rangle$ in the b'_i basis. Let c_i be the outcome of this measurement.
- Bob sends to Alice the basis $\mathbf{b}' = b'_1, \ldots, b'_n$ he used for his measurements using a public channel. Alice sends back the subset $I = \{i \in [n] : b_i = b'_i\}$ to Bob.
- Alice then picks a random subset $J \subseteq I$ of size $\frac{|I|}{2}$ which is the subset of indices for which Alice and Bob check that there wasn't any interception and sends J to Bob. For $j \in J$, Alice also sends k_j to Bob.
- For each $j \in J$, Bob checks that $k_j = c_j$. If one of these checks fail, he aborts.
- Let $L = I \backslash J = l_1, \ldots, l_{|L|}$ be the subset of indices used for the final raw key. We write $K_A = \{k_l\}_{l \in L}$ and $K_B = \{c_l\}_{l \in L}$.
- Alice and Bob perform key reconciliation to agree on a key K_{raw}.
- They perform privacy amplification to ensure that Alice has no information about the key.

4.1.1 Key reconciliation

The idea of key reconciliation is that $K_A \in \{0,1\}^m$ is usually different from K_B. How does that happen? There are two possible scenarios:

- An eavesdropper only intercepted a small number of qubits (so he wasn't caught with some constant probability), but disturbed the signal enough st. there is i st. $k_i \neq c_i$ for $i \in I \backslash J$.
- Hardware imperfection in the signal transmission and in the measurement create some inconsistency.

In order to perform key reconciliation the idea is to use a binary error-correcting code. For our purposes, an error correcting code is a set $\mathcal{C} \subseteq \{0,1\}^m$ st. $\min_{x,y \neq x \in \mathcal{C}} |x - y|_H = d$ for a parameter d of the code called the minimal distance. Alice chooses a code $\mathcal{C}$ st. $K_A \in \mathcal{C}$. This means that if $|K_B - K_A| \leq \frac{d}{2}$ then Bob can recover K_A from K_B since it is the unique element of $\mathcal{C}$ at distance at most $\frac{d}{2}$. Here are the challenges of this method.

- We must choose a code $\mathcal{C}$ with a large enough minimal distance d such that $|K_B - K_A| < \frac{d}{2}$.
- However, the adversary now knows that $K_A \in \mathcal{C}$ so the size of $\mathcal{C}$ must remain very large. There is a trade-off between the size of $\mathcal{C}$ and the minimal distance d.
- Even if the decoding is unique, it has to be computationally efficient. Even if it is unique, recovering K_A from K_B can be a very difficult task. For example, if we take a random code $\mathcal{C}$, this task is NP-hard.

Basic BB84 protocol

Alice		**Bob**
$k_1, \ldots, k_n \leftarrow\!\!\$\ \{0,1\}$		
$b_1, \ldots, b_n \leftarrow\!\!\$\ \{+,\times\}$		
	$\xrightarrow{\quad \lvert k_1\rangle^{b_1}, \ldots, \lvert k_n\rangle^{b_n} \quad}$	
		$b'_1, \ldots, b'_n \leftarrow\!\!\$\ \{+,\times\}$
		$\forall i,\ c_i \leftarrow$ measure $\lvert k_i\rangle^{b_i}$ in basis b'_i
	$\xleftarrow{\quad b'_1, \ldots, b'_n \quad}$	
$I = \{i : b_i = b'_i\}$		
$J \leftarrow\!\!\$\ \{S \subseteq I : \lvert S\rvert = \frac{\lvert I\rvert}{2}\}$		
	$\xrightarrow{\quad I, J, \{k_j\}_{j\in J} \quad}$	
		Check that $\forall j \in J, k_j = c_j$
	$\xleftarrow{\quad \text{“Check passed”} \quad}$	
$K_A = \{k_l\}_{l \in I \setminus J}$		$K_B = \{c_l\}_{l \in I \setminus J}$
	$\xrightarrow{\quad \text{Key reconciliation} \quad}$	
	$\xleftarrow{\quad\quad\quad\quad}$	
Agree on $K \in \{0,1\}^{k'}$		Agree on $K \in \{0,1\}^{k'}$
	$\xrightarrow{\quad \text{Agree on } h \quad}$	
	$\xleftarrow{\quad\quad\quad\quad}$	
$K_{\text{final}} = h(K)$		$K_{\text{final}} = h(K)$

Figure 4.1: Description of a basic BB84 quantum key distribution protocol

There are varieties of choices for this task, for example using LDPC codes.

4.1.2 Privacy amplification

At the end of the reconciliation phase, the eavesdropper Eve could still have a little bit of information about K. In order to construct K_{final}, we apply a hash function to ensure that this information is destroyed.

Chapter 5

Quantum information theory

5.1 Classical entropy

5.2 Classical entropy

Entropy is arguably one of the most important concepts in information theory.

Definition 5.1. *Let $p = (p_1, \ldots, p_n)$ be a discrete probability function, so $p_i \geq 0$ and $\sum_i p_i = 1$. The entropy $H(p)$ of p is defined as*

$$H(p) = \sum_{i=1}^{n} -p_i \log_2(p_i).$$

The entropy $H(p)$ measures the amount of uncertainty in p. For example, for $p = (1, 0, \ldots, 0)$, we have $H(p) = 0$. For $p = (\frac{1}{2}, \frac{1}{2}, 0, \ldots, 0)$ then $H(p) = 1$. If $p = (\frac{1}{n}, \ldots, \frac{1}{n})$ then $H(p) = \log_2(n)$ (maximal). The entropy can be informally seen as the amount of coins required to mimic p.

Other example: $p(0) = \frac{3}{4}, p(1) = \frac{1}{4}$ so $H(p) = \frac{3}{4}\log(4/3) + \frac{1}{4}\log(1/4) \approx 0.811$. It doesn't seem we can send i with strictly less than 1 bit. How do we interpret $H(p) < 1$ as a noiseless compression bound? Consider $p^2(xy) = p(x)p(y)$ for $x, y \in \{0, 1\}$. We have $H(p^2) = 2H(p)$. Now, if Alice has i, j wp. $p^2(i, j)$ and wants to send these 2 bits, she can do the following:

1. If $(x, y) = (0, 0)$: send "0".
2. If $(x, y) = (0, 1)$: send "01".
3. If $(x, y) = (1, 0)$: send "011".
4. If $(x, y) = (1, 1)$: send "111".

We have

$$\text{Average amount of bits sent } = \frac{9}{16} + 2 * \frac{3}{16} + 3 * (\frac{3}{16} + \frac{1}{16}) = \frac{27}{16} = 1.6875.$$

and we have $H(p^2) \leq \frac{27}{16} < 2$. If we take p^n, we can find an encoding st. the average number of bits sent will be closer and closer to $H(p)$. This is Shannon's noiseless source coding theorem.

Hoeffding's inequality. Suppose $X_1, ..., X_n$ are independent random variables taking values in [a,b]. Let X denote their sum and let $\mu = \mathrm{E}[X]$ denote the sum's expected value. Then for any $t > 0$,

$$\mathrm{Pr}(X \leq \mu - t) < e^{-2t^2/(n(b-a)^2)},$$
$$\mathrm{Pr}(X \geq \mu + t) < e^{-2t^2/(n(b-a)^2)}.$$

Proposition 1. *[CT91] Let $\delta(\epsilon, n) \triangleq 1 - \mathbf{P}(\mathcal{A}_\epsilon^{(n)})$. For $\epsilon > 0$, we have the following assertions:*

1. *If $(x_1, ..., x_n) \in \mathcal{A}_\epsilon^{(n)}$, then $H_q(X) - \epsilon \leqslant \frac{1}{n} \log_q p(x_1, ..., x_n) \leqslant H_q(X) + \epsilon$*
2. *$\delta(\epsilon, n) = \mathrm{negl}(n)$.*
3. *$(1 - \mathrm{negl}(n))q^{n(H_q(X)-\epsilon)} \leqslant |\mathcal{A}_\epsilon^{(n)}| \leqslant q^{n(H_q(X)+\epsilon)}$*

proof of proposition 1.2. For $\epsilon > 0$, for $n \in \mathbb{N}$,

$$\begin{aligned}\delta(\epsilon, n) &= \mathrm{Pr}\left(p(x_1, ..., x_n) \geqslant q^{-n(H_q(X)-\epsilon)}\right) + \mathrm{Pr}\left(p(x_1, ..., x_n) \geqslant q^{-n(H_q(X)+\epsilon)}\right) \\ &= \mathrm{Pr}\left(\log(p(x_1, ..., x_n)) - nH_q(X) \geqslant n\epsilon\right) + \mathrm{Pr}\left(nH_q(X) - \log(p(x_1, ..., x_n)) \geqslant n\epsilon\right) \\ &= \mathrm{Pr}\left(|\sum_{i=1}^{n} \log(p(x_i)) - nH_q(X)| \geqslant n\epsilon\right)\end{aligned}$$

Then, using Hoeffding's inequality (1), we get

$$\delta(\epsilon, n) \leqslant e^{-\frac{2n^2\epsilon^2}{M}}$$

5.2.1 Properties of the quantum entropy

- Let $\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$ a quantum mixed state with it's spectral decomposition.
- Let U a quantum unitary and let $|f_i\rangle = U(|e_i\rangle)$. Recall that applying U to ρ gives the state $U\rho U^\dagger = \sum_i \lambda_i |f_i\rangle\langle f_i|$.
- We immediately have $H(U\rho U^\dagger) = S(\rho)$.
- $S(\rho) \geq 0$.
- $S(A)_{\rho_{AB}} - S(B)_{\rho_{AB}} \leq S(AB)_{\rho_{AB}} \leq S(A)_{\rho_{AB}} + S(B)_{\rho_{AB}}$.
- $S(\rho_A \otimes \rho_B) = S(\rho_A) + S(\rho_B)$.

5.2.2 Conditional quantum entropy and conditional mutual information

Definition 5.2. *The conditional entropy $S(A|B)$ is defined as*

$$S(A|B)_{\rho_{AB}} := S(AB)_{\rho_{AB}} - S(B)_{\rho_{AB}}.$$

- Unlike classical conditional entropy, the quantum one can be negative! Take for example $\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$. We have $S(AB)_{\rho_{AB}} = 0$ and $S(A)_{\rho_{AB}} = S(B)_{\rho_{AB}} = 1$.
- Chain rule:
$$S(A|C)_{\rho_{ABC}} + S(B|AC)_{\rho_{ABC}} = S(AB|C)_{\rho_{ABC}}.$$
- We also have $S(A|B)_{\rho_{ABC}} \leq S(A)_{\rho_{ABC}}$ and $S(A|BC)_{\rho_{ABC}} \leq S(A|B)_{\rho_{ABC}}$. This implies
$$S(A|C)_{\rho_{ABC}} + S(B|C)_{\rho_{ABC}} \geq S(A|C)_{\rho_{ABC}} + S(B|AC)_{\rho_{ABC}} = S(AB|C)_{\rho_{ABC}}. \tag{5.1}$$

Definition 5.3. *The mutual information $I(A:B)$ is defined as*
$$I(A:B)_{\rho_{AB}} = S(A)_{\rho_{AB}} + S(B)_{\rho_{AB}} - S(AB)_{\rho_{AB}}.$$

Definition 5.4. *The conditional mutual information $I(A:B|C)$ is defined as*
$$I(A:B|C)_{\rho_{ABC}} = S(A|C)_{\rho_{ABC}} + S(B|C)_{\rho_{ABC}} - S(AB|C)_{\rho_{ABC}}.$$

We have that $I(A:B)_{\rho_{AB}} \geq 0$ and $I(A:B|C)_{\rho_{ABC}} \geq 0$ from Equation 5.1. One can check that
$$I(A:BC) = I(A:B) + I(A:C|B) \geq I(A:B).$$

Proposition 5.5 (Pinsker's inequality)**.** *For a quantum state ρ_{AB}, we have*
$$I(A:B) \geq \frac{1}{2}\Delta^2(\rho_{AB}, \rho_A \otimes \rho_B).$$

5.2.3 The index problem

The index problem; Alice has a uniformly random string $x \in \{0,1\}^n$. Bob is given a uniformly random index i. Alice and Bob cooperate and the goal of the index game is for Bob to output x_i. Without any communication, Bob can't do better than randomly guess x_i so he will succeed wp. $\frac{1}{2}$.

Now, assume Alice sends a quantum pure state $|\psi_x\rangle$ of $m < n$ qubits to Bob. An m-qubit state consists of 2^m complex numbers so it shouldn't be hard to encode the information of each x in a different state $|\psi_x\rangle$. However, when Bob receives $|\psi_x\rangle$, he can't recover all the amplitudes of $|\psi_x\rangle$ and he is limited by the laws of quantum measurements in order to recover x.

We can actually show that for $m < n$, Bob cannot recover perfectly x_i. We will also give quantitative versions of this result.

Bounding the probability of winning $Index_n$ with m bits of communication Let p_i the probability of winning when Bob has input i. After Alice sends her message, Alice and Bob share the state
$$\rho = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} |x\rangle\langle x|_A |\psi_x\rangle\langle\psi_x|_B.$$

We have

$$I(A:B)_\rho = S(A)_\rho + S(B)_\rho - S(AB)_\rho = n + S(B)_\rho - n = S(B)_\rho \leq m.$$

We write $A = X_1, \ldots, X_n$, and

$$I(A:B) = S(A) - S(A|B) = S(A) - S(X_1, \ldots, X_n|B) \geq n - \sum_{i=1}^{n} S(X_i|B)$$
$$= \sum_{i=1}^{n} 1 - S(X_i|B) = \sum_{i=1}^{n} S(X_i) - S(X_i|B) = \sum_{i=1}^{n} I(X_i:B)$$

which gives

$$\frac{1}{n}\sum_{i=1}^{n} I(X_i:B) \leq \frac{m}{n}.$$

Bob can perform a measurement on his part that guesses x_i wp. p_i on input i. So after his guess, the state is

$$\xi = \frac{1}{n2^n} \sum_{\substack{x\in\{0,1\}^n \\ i\in[n]}} |x\rangle\langle x|_A \otimes \left(|i\rangle\langle i|_I \otimes \left(p_i |x_i\rangle\langle x_i|_G \otimes \zeta_E^{x,i} + (1-p_i)|\overline{x_i}\rangle\langle\overline{x_i}|_G \otimes \widetilde{\zeta}_E^{x,i} \right) \right).$$

where there registers I, G, E are on Bob's side. We have

$$I(X_i:B)_\xi \geq I(X_i:G)_\xi = 1 + 1 - (1 + H_2(p)) = 1 - H_2(p_i)$$

with $H_2(p) = -p\log(p) - (1-p)\log(1-p)$. Here, we use

- $\xi_{X_i} = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$.
- $\xi_G = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$.
- $\xi_{X_iG} = \frac{1-p_i}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right) + \frac{p_i}{2}\left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)$. So $H(X_iG)_\xi = 1 + H_2(p_i)$.

Putting everything together, we have

$$m \geq \sum_{i=1}^{n} (1 - H(p_i)).$$

This gives interesting information. For example, if we want Bob to win wp. 1, we have necessarily $m \geq n$ meaning that we cannot perform better than sending the whole string x. Moreover, if the players want that Bob always succeeds wp. p for each i, we have necessarily $m \geq n - nH(p)$. These bounds are not necessarily tight.

Bibliography