LECTURE 8
DISTANCE MEASURES FOR QUANTUM STATES AND QUANTUM CRYPTOGRAPHY

Quantum Information and Computing

Thomas Debris-Alazard

Inria, École Polytechnique

Introduction to quantum cryptography!

Security relies on:

- No-cloning theorem
- Measuring modifies quantum states
- Incapacity to distinguish non-orthogonal quantum states

Distance between quantum states: essential tool for ensuring the security of quantum cryptography (what is possible or not, what can be done at best to distinguish, etc. . .)

$\longrightarrow$ We need first (as usual) to understand where these concepts come from: classical world!

Classical Information theory modelizes an information source as a random variable

$\longrightarrow$ Our aim: meaning of *"two information sources are similar to one another, or not"*

similar $\approx$ undistinguishable ; not-similar $\approx$ distinguishable

English and French texts:

May be modelling as a sequence of random variables over the Roman alphabet:

- English: "th" most frequent pair of letters
- French: "es" most frequent pair of letters

$\longrightarrow$ To distinguish English and French: look the output distribution of letters

How to "quantify" that they are different? Are they as different as French and Hungarian?

$\longrightarrow$ Define a distance between sources of information/distributions

Distance between distributions/random variables:

- Quantifying the minimum amount of operations to distinguish them
- Difference of behaviours of an algorithm when changing some internal distribution

Extremely useful tool for cryptography, study of algorithms, etc. . .

Application case: f depends of some secret and g not but distance$(f, g) = \varepsilon$

$\longrightarrow$ Owning f does not help to recover the secret. . .

Distance between quantum states:

enough to look at the distance between measurement outputs?

$\longrightarrow$ No! But let us first see the classical case!

DISTANCES OVER DISTRIBUTIONS

$\mathcal{X}$ be a finite set

- $f : \mathcal{X} \to \mathbb{R}$ such that $\begin{cases} f \geq 0 \\ \sum_{x \in \mathcal{X}} f(x) = 1 \end{cases}$ is called **a distribution**

- A **random variable** X taking its values in $\mathcal{X}$ is defined via the distribution $\mathbb{P}(\mathsf{X} = x)$ for $x \in \mathcal{X}$

Distributions $\iff$ Random Variables

- From f: X be such that $\mathbb{P}(\mathsf{X} = x) \stackrel{\text{def}}{=} f(x)$

- From X: f be such that $f(x) \stackrel{\text{def}}{=} \mathbb{P}(\mathsf{X} = x)$

$\longrightarrow$ In what follows: we identify random variables and their associated distributions

Many "distances" $\left(\alpha\text{-divergences}\right)$ between distributions f and g:

- Statistical/Total-Variational/Trance distance:

$$\Delta(f,g) \stackrel{\text{def}}{=} \frac{1}{2}\sum_{x\in\mathcal{X}} |f(x) - g(x)|$$

- Hellinger distance:

$$H(f,g) \stackrel{\text{def}}{=} \sqrt{1 - \sum_{x\in\mathcal{X}} \sqrt{f(x)}\sqrt{g(x)}}$$

- Kullback–Leibler divergence:

$$D_{\mathrm{KL}}(f||g) \stackrel{\text{def}}{=} \sum_{x\in\mathcal{X}} f(x)\log_2\left(\frac{f(x)}{g(x)}\right)$$

- etc. . .

In what follows:

Focus on statistical distance

Statistical distance:

The statistical distance between two distributions f, g over a finite set $\mathcal{X}$:

$$\Delta(f, g) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{x \in \mathcal{X}} |f(x) - g(x)|$$

- The factor 1/2 ensures that $\Delta(f, g) \in [0, 1]$
- $\Delta(f, g) = 0 \iff f = g$
- $\Delta(\cdot, \cdot)$ defines a metric for distributions

Given $S \subseteq \mathcal{X}$

$\sum_{x\in S} f(x)$ is *the probability that an event S occurs when picking x according to f*

An important property:

$$\Delta(f,g) = \max_{S\text{ event}} \left| f(S) - g(S) \right| = \max_{S\text{ event}} \left| \sum_{x\in S} f(x) - \sum_{x\in S} g(x) \right|$$

Consequence:

Let S_0 be the event reaching the maximum. This event S_0 is optimal to distinguish f and g

$\longrightarrow \Delta(f,g)$ is quantifying **how well** it is possible $\left(\text{using } S_0\right)$ to distinguish f and g . . .

$\left(\text{in practice } S_0 \text{ is hard to compute}\right)$

Let f_0 and f_1 be two distributions

- Alice chooses a bit $b \in \{0, 1\}$ unknown to Bob
- Suppose that Alice gives to Bob one x picked according to f_b

What is the best probability for Bob to guess b?

Proposition (see Exercise Session):

$$\max_{\{\text{strategy}\}} \mathbb{P}\left(\text{Bob guesses } b\right) = \frac{1}{2} + \frac{\Delta(f_0, f_1)}{2}$$

$\longrightarrow$ The trace distance gives how well distributions can be distinguished

But do many samples could help Bob? Yes! But how much?

Let f_0 and f_1 be two distributions

- Alice chooses a bit $b \in \{0,1\}$ unknown to Bob
- Suppose that Alice gives to Bob n samples $x_1, \ldots, x_n$ each picked according to f_b

Proposition:

Given distributions $f_1, \ldots, f_n$ and $g_1, \ldots, g_n$ we have

$$\Delta\Big((f_1, \ldots, f_n), (g_1, \ldots, g_n)\Big) \le \sum_{i=1}^{n} \Delta(f_i, g_i)$$

$$\max_{\{\text{strategy}\}} \mathbb{P}\,(\text{Bob guesses } b) = \frac{1}{2} + \frac{\Delta\Big((\overbrace{f_0, \ldots, f_0}^{n \text{ times}}), (\overbrace{f_1, \ldots, f_1}^{n \text{ times}})\Big)}{2} \le \frac{1}{2} + \frac{n}{2}\Delta(f_0, f_1)$$

$\longrightarrow$ Bob needs at least $n = \frac{1}{\Delta(f_0, f_1)}$ samples to make the correct guess with probability 1

$$\Big(\text{for having } \tfrac{1}{2} + \tfrac{n}{2}\Delta(f_0, f_1) = 1\Big)$$

To take away:

Given f or g but you don't know which one:

at least $\frac{1}{\Delta(f,g)}$ calls to the given random variable to take the good decision with probability 1

One could imagine: applying a physical process/algorithm to the random variables X_f given by f and X_g given by g could help to distinguish them

One could imagine: applying a physical process/algorithm to the random variables X_f given by f and X_g given by g could help to distinguish them

$\longrightarrow$ No! Statistical distance can only decrease

An important property: data processing inequality

Given any function/algorithm F, then $F(X_f)$ and $F(X_g)$ are still random variables and

$$\Delta\Big(F(X_f), F(X_g)\Big) \leq \Delta(X_f, X_g)$$

F can be randomized, but its internal randomness has to be independent from X_f and X_g

Concrete consequence:

$\mathcal{A}$ be an algorithm such that

$$\varepsilon \stackrel{\text{def}}{=} \mathbb{P}\Big(\mathcal{A}(X) = \text{“success”}\Big)$$

where “success” could mean: find the secret key from a public key output by X, factorise a number output by X, etc. . .

Then,

$$\varepsilon - \Delta(X, Y) \leq \mathbb{P}\Big(\mathcal{A}(Y) = \text{“success”}\Big) \leq \varepsilon + \Delta(X, Y)$$

$\longrightarrow$ Extremely useful in cryptography!

The statistical distance between two distributions:

- Cannot increase after applying an algorithm, physical process $\big($data processing inequality$\big)$
- Minimum amount of resources to distinguish distributions: at least $\frac{1}{\Delta(f,g)}$ queries to distinguish f and g

In many scenarii this lower-bound is optimistic...

$\longrightarrow$ Sometimes necessarily: $\frac{1}{\Delta(f,g)^2} \gg \frac{1}{\Delta(f,g)}$ calls to be able to distinguish

$\big($statistical distance is a brutal tool$\big)$

Statistical distance: quantify how close are distributions

But how to quantify how close are quantum states?

DISTANCE BETWEEN QUANTUM STATES

Define a distance between quantum states why verifies:

- Cannot increase after "quantum" operations $\Big($data processing inequality$\Big)$
- Quantify the "minimum amount of resources" to distinguish

More about the distances can be found in $\Big($particularly proofs are omitted here$\Big)$:

Quantum computation and quantum information, Chapter 9, Nielsen and Chuang

Trace distance:

Let ρ, σ be two density operators, their trace distance is defined as

$$\Delta(\rho,\sigma) \stackrel{\text{def}}{=} \frac{1}{2}\ |\rho - \sigma|_{\text{tr}} \quad \text{where} \quad |\mathbf{M}|_{\text{tr}} \stackrel{\text{def}}{=} \mathbf{tr}\left(\sqrt{\mathbf{M}^\dagger \mathbf{M}}\right)$$

Be careful: $\Delta(\rho,\sigma) \neq \mathbf{tr}(\rho - \sigma)$

$\Delta(\cdot,\cdot)$ is a metric over density operators:

- $\Delta(\rho,\sigma) = 0 \iff \rho = \sigma$
- $\Delta(\rho,\sigma) \in [0,1]$
- $\Delta(\rho,\sigma) = \Delta(\sigma,\rho) \quad \left(\text{symmetry}\right)$
- $\Delta(\rho,\tau) \leq \Delta(\rho,\sigma) + \Delta(\sigma,\tau) \quad \left(\text{triangle inequality}\right)$

- If ρ and σ are co-diagonalizable $\Big(\iff \rho\sigma = \sigma\rho \Big)$, in an orthonormal basis $(|e_i\rangle)_i$:

$$\rho = \sum_i p_i \, |e_i\rangle\langle e_i| \quad \text{and} \quad \sigma = \sum_i q_i \, |e_i\rangle\langle e_i|$$

where $p \overset{\text{def}}{=} (p_i)_i$ and $q \overset{\text{def}}{=} (q_i)_i$ are distributions

$$\Delta(\rho, \sigma) = \tfrac{1}{2} \textstyle\sum_i |p_i - q_i| = \Delta(p, q)$$

$\longrightarrow$ We recover the classical statistical distance!

- If ρ and σ are pure states, $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\varphi\rangle\langle\varphi|$, then:

$$\Delta(\rho, \sigma) = \sqrt{1 - |\,\langle\psi|\varphi\rangle\,|^2}$$

$\longrightarrow$ If quantum states are orthogonal, their trace distance is maximal!

Is it intuitive?

- If ρ and σ are co-diagonalizable $\big(\iff \rho\sigma = \sigma\rho \big)$, in an orthonormal basis $(|e_i\rangle)_i$:

$$\rho = \sum_i p_i \, |e_i\rangle\langle e_i| \quad \text{and} \quad \sigma = \sum_i q_i \, |e_i\rangle\langle e_i|$$

where $p \stackrel{\text{def}}{=} (p_i)_i$ and $q \stackrel{\text{def}}{=} (q_i)_i$ are distributions

$$\Delta(\rho, \sigma) = \tfrac{1}{2} \textstyle\sum_i |p_i - q_i| = \Delta(p, q)$$

$\longrightarrow$ We recover the classical statistical distance!

- If ρ and σ are pure states, $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\varphi\rangle\langle\varphi|$, then:

$$\Delta(\rho, \sigma) = \sqrt{1 - |\langle\psi|\varphi\rangle|^2}$$

$\longrightarrow$ If quantum states are orthogonal, their trace distance is maximal!

Is it intuitive?

$\longrightarrow$ Yes! Orthogonal pure states are perfectly distinguishable...

(see Lecture 2)

Let ρ_0 and ρ_1 be two known density operators

- Alice has a bit $b \in \{0, 1\}$ unknown to Bob
- Suppose that Alice send ρ_b to Bob

What is the best probability for Bob to guess b?

Proposition (see Exercise Session):

$$\max_{\{\text{strategy}\}} \mathbb{P}\left(\text{Bob guesses } b\right) = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

$\longrightarrow$ The trace distance gives how well quantum states can be distinguished

Be careful: we know the strategy which reaches the maximum, but in most cases it is non-effective

One could imagine: applying a unitary evolution to quantum states help to distinguish?

i.e., increase $\Delta(\rho, \sigma)$

One could imagine: applying a unitary evolution to quantum states help to distinguish?

i.e., increase $\Delta(\rho, \sigma)$

$\longrightarrow$ No!

Invariance under unitary evolutions:

$$\Delta(\mathsf{U}\rho\mathsf{U}^\dagger, \mathsf{U}\sigma\mathsf{U}^\dagger) = \Delta(\rho, \sigma), \quad \textit{for any unitary } \mathsf{U}$$

Given ρ and σ: can we detect a difference when measuring? How to quantify it?

Given ρ and σ: can we detect a difference when measuring? How to quantify it?

$$\Delta(\rho,\sigma) = \max_{\mathsf{P}\ \text{projector}} \operatorname{tr}\left(\mathsf{P}(\rho-\sigma)\right)$$

Theorem:

Let $\{\mathsf{E}_m\}$ be a POVM with $p \stackrel{\text{def}}{=} (\operatorname{tr}(\mathsf{E}_m\rho))_m$ and $q \stackrel{\text{def}}{=} (\operatorname{tr}(\mathsf{E}_m\sigma))_m$ be the distributions of outcomes m. Then,

$$\Delta(\rho,\sigma) = \max_{\{\mathsf{E}_m\}} \Delta(p,q)$$

In particular, whatever is the measurement

$$\Delta(p,q) \leq \Delta(\rho,\sigma)$$

Concrete consequence:

One needs at least $\geq \frac{1}{\Delta(\rho,\sigma)}$ measures to distinguish ρ and σ with probability 1

And what about more general “quantum operations”?

Definition:

A quantum operation Φ is defined from a collection of matrices $A_1, \ldots, A_k$ such that

$$\sum_{i=1}^{k} A_i A_i^\dagger = I \quad \text{and} \quad \Phi(\rho) = \sum_{i=1}^{k} A_i \rho A_i^\dagger$$

$\longrightarrow$ Most general “quantum operation”

It captures: measurements, unitary, tracing out, noisy channel, etc...

Example: depolarizing channel

Quantum operation defined from $(1-p)I$, $\frac{p}{3}X$, $\frac{p}{3}Y$ and $\frac{p}{3}Z$.

Quantum data processing inequality:

For any quantum operation Φ,

$$\Delta(\Phi(\rho), \Phi(\sigma)) \leq \Delta(\rho, \sigma)$$

Another important "distance" in the quantum world:

Fidelity:

Let ρ, σ be two density operators, their fidelity is defined as

$$F(\rho, \sigma) \overset{\text{def}}{=} \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$$

Following properties:

- $F(\sigma, \rho) = 1 \iff \sigma = \rho$
- $F(\sigma, \rho) \in [0, 1]$
- $F(\sigma, \rho) = F(\rho, \sigma)$ $\left(\text{symmetry}\right)$

Be careful: fidelity not a metric $\left(\text{triangular inequality not verified}\right)$

- If ρ and σ are co-diagonalizable $\Big(\iff \rho\sigma = \sigma\rho \Big)$, in an orthonormal basis $(|e_i\rangle)_i$:

$$\rho = \sum_i p_i \, |e_i\rangle\langle e_i| \quad \text{and} \quad \sigma = \sum_i q_i \, |e_i\rangle\langle e_i|$$

where $p \overset{\text{def}}{=} (p_i)_i$ and $q \overset{\text{def}}{=} (q_i)_i$ are distributions

$$F(\rho, \sigma) = \textstyle\sum_i \sqrt{p_i}\sqrt{q_i} = 1 - H(p, q)^2 \quad \Big(H(\cdot, \cdot) \text{ Hellinger distance} \Big)$$

$\longrightarrow$ We recover $1 - H(p, q)^2$ known classically as the fidelity/Bhattacharyya coefficient!

- If ρ and σ are pure states, $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\varphi\rangle\langle\varphi|$, then:

$$F(\rho, \sigma) = |\, \langle\psi|\varphi\rangle \,|$$

In particular: $F(\rho, \sigma) = 0$ when ρ, σ are orthogonal pure states

Invariance under unitary evolutions:

$$F(\mathsf{U}\rho\mathsf{U}^\dagger, \mathsf{U}\sigma\mathsf{U}^\dagger) = F(\rho, \sigma), \quad \textit{for any unitary } \mathsf{U}$$

Recall: trace distance is "invariant" by projection

$$\Delta(\rho, \sigma) = \max_{P \text{ projector}} \operatorname{tr}(P(\rho - \sigma))$$

$\longrightarrow$ "Dual" operation for the fidelity: purification

Uhlmann's theorem:

For any two density operators ρ, σ,

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

where the maximum is taken over purifications $|\psi\rangle$ of ρ, and a fixed purification $|\varphi\rangle$ of σ

$\longrightarrow$ Useful characterization involved in many proofs concerning the fidelity

Example:

Let $\rho \stackrel{\text{def}}{=} \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ and $\sigma \stackrel{\text{def}}{=} \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$: diagonalizable in the same basis

$$F(\rho, \sigma) = \sqrt{\frac{1}{2}}\sqrt{\frac{3}{4}} + \sqrt{\frac{1}{2}}\sqrt{\frac{1}{4}} = \sqrt{\frac{3}{8}} + \sqrt{\frac{1}{8}}$$

$|\psi\rangle \stackrel{\text{def}}{=} \frac{|00\rangle}{\sqrt{2}} + \frac{|11\rangle}{\sqrt{2}}$ and $|\varphi\rangle \stackrel{\text{def}}{=} \sqrt{\frac{3}{4}}|00\rangle + \sqrt{\frac{1}{4}}|11\rangle$ are purifications which are optimal with regards to Uhlmann's theorem

Quantum trace distance could be related to the classical trace distance via measurements

$\longrightarrow$ The same holds for the fidelity

Theorem:

Let $\{\mathsf{E}_m\}$ be a POVM with $p \stackrel{\text{def}}{=} (\mathbf{tr}(\mathsf{E}_m\rho))_m$ and $q \stackrel{\text{def}}{=} (\mathbf{tr}(\mathsf{E}_m\sigma))_m$ be the distributions of outcomes m. Then,

$$F(\rho,\sigma) = \min_{\{\mathsf{E}_m\}} F(p,q) \quad \text{where} \quad F(p,q) = \sum_m \sqrt{p_m}\sqrt{q_m} \qquad \Big(\text{classical fidelity}\Big)$$

In particular, whatever is the measurement

$$F(\rho,\sigma) \leq F(p,q)$$

Trace distance: cannot increase after a quantum operation

$\longrightarrow$ Fidelity cannot decrease

Quantum data processing inequality:

For any quantum operation Φ,

$$F(\rho, \sigma) \leq F\left(\Phi(\rho), \Phi(\sigma)\right)$$

Uhlmann's theorem: fidelity is equal to the maximum inner product between two quantum states $\big($purification$\big)$

It suggests: angle between states (density operators) ρ and σ as

$$A(\rho, \sigma) \overset{\text{def}}{=} \arccos F(\rho, \sigma)$$

Proposition $\big($**proof uses Uhlmann's theorem**$\big)$:

$A(\cdot, \cdot)$ is a metric for density operators

A priori: only quantum trace distance matters, why did we introduce the quantum fidelity?

A priori: only quantum trace distance matters, why did we introduce the quantum fidelity?

$\longrightarrow$ We can relate them

Fuchs - Van de Graaf inequalities:

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

But is the fidelity useful?

A priori: only quantum trace distance matters, why did we introduce the quantum fidelity?

$\longrightarrow$ We can relate them

Fuchs - Van de Graaf inequalities:

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

But is the fidelity useful?

$\longrightarrow$ Yes!

Proposition:

$$\Delta(\rho^{\otimes k},\sigma^{\otimes k}) \leq k\,\Delta(\rho,\sigma) \quad \text{and} \quad F(\rho^{\otimes k},\sigma^{\otimes k}) = F(\rho,\sigma)^k$$

$\longrightarrow$ The strength of the fidelity comes from the above equality

Let's play the following game: if you ask, Alice gives to you

$$\rho_0 \stackrel{\text{def}}{=} \left(\frac{1}{2} - \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} + \varepsilon\right) |1\rangle\langle 1| \quad \text{or} \quad \rho_1 \stackrel{\text{def}}{=} \left(\frac{1}{2} + \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} - \varepsilon\right) |1\rangle\langle 1|$$

$\longrightarrow$ But once Alice made a first random choice, she will always make the same choice!

Your aim: find with probability 1 if Alice chose ρ_0 or ρ_1

Let's play the following game: if you ask, Alice gives to you

$$\rho_0 \stackrel{\text{def}}{=} \left(\frac{1}{2} - \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} + \varepsilon\right) |1\rangle\langle 1| \quad \text{or} \quad \rho_1 \stackrel{\text{def}}{=} \left(\frac{1}{2} + \varepsilon\right) |0\rangle\langle 0| + \left(\frac{1}{2} - \varepsilon\right) |1\rangle\langle 1|$$

$\longrightarrow$ But once Alice made a first random choice, she will always make the same choice!

Your aim: find with probability 1 if Alice chose ρ_0 or ρ_1

How to proceed:

Make k queries to Alice, measure each time in the $(|0\rangle, |1\rangle)$ basis

- With one query,

$$\max_{\{\text{strategy}\}} \mathbb{P}\,(\text{We guess the correct } b) = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

- With k queries,

$$\max_{\{\text{strategy}\}} \mathbb{P}\,(\text{We guess the correct } b) = \frac{1}{2} + \frac{\Delta(\rho_0^{\otimes k}, \rho_1^{\otimes k})}{2}$$

$$\max_{\{\text{strategy}\}} \mathbb{P}\,(\text{We guess the correct } b) = \frac{1}{2} + \frac{\Delta(\rho_0^{\otimes k}, \rho_1^{\otimes k})}{2}$$

But how many queries k are needed to make the good decision $\Big($with high probability$\Big)$?

$$\Delta(\rho_0, \rho_1) = \varepsilon$$

- Upper-bound on the trace distance:

$$\Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \leq k\varepsilon \implies \text{Necessarily: } k \geq \tfrac{1}{\varepsilon} \text{ to ensure } \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \text{ not too small}$$

Is it optimal?

$$\max_{\{\text{strategy}\}} \mathbb{P}\,(\text{We guess the correct } b) = \frac{1}{2} + \frac{\Delta(\rho_0^{\otimes k}, \rho_1^{\otimes k})}{2}$$

But how many queries k are needed to make the good decision $\left(\text{with high probability}\right)$?

$$\Delta(\rho_0, \rho_1) = \varepsilon$$

- Upper-bound on the trace distance:

$$\Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \leq k\varepsilon \implies \text{Necessarily: } k \geq \tfrac{1}{\varepsilon} \text{ to ensure } \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \text{ not too small}$$

Is it optimal? **No!** It turns out that $\Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \leq k\varepsilon$ is **not-tight**

- $F(\rho_0, \rho_1) = 2\sqrt{\frac{1}{4} - \frac{\varepsilon^2}{4}} \approx 1 - \varepsilon^2/2$ **and** $F(\rho_1^{\otimes k}, \rho_2^{\otimes k}) = F(\rho_1, \rho_2)^k \approx 1 - k\varepsilon^2/2$

$$k\frac{\varepsilon^2}{2} \approx 1 - F(\rho_0^{\otimes k}, \rho_1^{\otimes k}) \leq \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \implies \textbf{Choose: } k \geq \tfrac{2}{\varepsilon^2} \text{ to ensure } \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \text{ not small}$$

$\longrightarrow k \approx \frac{1}{\varepsilon^2}$ is the optimal number of queries to make the good decision $\left(\text{with high probability}\right)$

$$\Delta(\rho_0, \rho_1) = \varepsilon$$

- Upper-bound on the trace distance

$$\Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right) \leq k\varepsilon$$

- Lower-bound on the trace distance (by using Fidelity and Fuchs - Van de Graaf inequalities)

$$k\varepsilon^2/2 \leq \Delta\left(\rho_0^{\otimes k}, \rho_1^{\otimes k}\right)$$

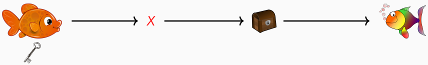
Compare to the trace distance, the fidelity turns out to be in many situations a finer tool to analyze the “distance” between quantum states

$\longrightarrow$ It gives in many scenarii the tight number of necessary samples to perform a correct distinguishing!

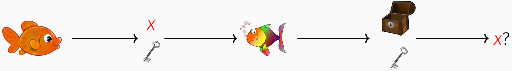
BIT COMMITMENT

COMMITMENT WITH A SAFE

- Commit phase:
  - Alice writes x on a piece of paper
  - Alice puts the paper in a safe. She is the only one to have the key of the safe
  - Alice sends the safe to Bob



- Reveal phase:
  - Alice reveals x and the key to unlock the safe
  - Bob opens the safe to check x



Our aim:

Use "quantum computation" to build a commitment scheme

$\longrightarrow$ Is the quantum world will offer to us an unconditionally secure commitment? $\Big($Spoil: no. . . $\Big)$

$$S_0 \stackrel{\text{def}}{=} \{|0\rangle, |1\rangle\} \quad \text{and} \quad S_1 \stackrel{\text{def}}{=} \{|+\rangle, |-\rangle\}$$

$\longrightarrow$ Alice wants to commit a bit $b \in \{0, 1\}$ to Bob!

Exercise:

Describe a commitment protocol using S_0 and S_1 enabling Alice to commit her bit

(**Hint:** we don't want Bob "to have any information about the commited bit")

$$S_0 \stackrel{\text{def}}{=} \{|0\rangle, |1\rangle\} \quad \text{and} \quad S_1 \stackrel{\text{def}}{=} \{|+\rangle, |-\rangle\}$$

Alice wants to commit b:

1. **Commit phase:** Alice chooses $|\psi\rangle \in S_b$ uniformly at random and send $|\psi\rangle$ to Bob
2. **Reveal phase:** Alice reveals $ab \in \{0,1\}^2$ to Bob where ab description of $|\psi\rangle$
$$00 \leftrightarrow |0\rangle, \quad 10 \leftrightarrow |1\rangle, \quad 01 \leftrightarrow |+\rangle \quad \text{and} \quad 11 \leftrightarrow |-\rangle$$
3. **Verification phase:** Bob measures $|\psi\rangle$ in the basis S_b $\left(b \text{ is known from } ab\right)$

Exercise:

Is Bob can guess the committed bit?

Bob can only guess the committed bit with probability 1/2 . . .

- If Alice committed 0, Bob has
$$\rho_0 = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1|$$
- If Alice committed 1, Bob has
$$\rho_1 = \frac{1}{2} |+\rangle\langle +| + \frac{1}{2} |-\rangle\langle -|$$

$\longrightarrow$ But: $\rho_0 = \rho_1 = \frac{I}{2}$: they are indistinguishable $\Big($in particular, $\Delta(\rho_0, \rho_1) = 0\Big)$

But, is the commitment scheme secure?

Exercise:

Give a cheating strategy for Alice: she chooses the committed bit after the commit phase. . .

CHEATING STRATEGY FOR ALICE

Alice chooses her committed value after the commit phase. . .

1. Alice starts with an EPR-pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
2. Alice gives the second qubit to Bob and pretends this is her commitment $\Big($up to now Alice did not make a choice$\Big)$
3. If ultimately Alice wants to reveal $b = 0$: Alice measures her qubit $|x\rangle$ and gives to Bob $x0$
4. If ultimately Alice wants to reveal $b = 1$: Alice first performs an Hadamard gate on her qubit, the state becomes
$$\frac{|{+}0\rangle + |{-}1\rangle}{\sqrt{2}} = \frac{|0{+}\rangle + |1{-}\rangle}{\sqrt{2}}$$
Alice measures her qubit and she reveals 01 if she measured $|0\rangle$, otherwise she reveals 11

When Bob measures, everything is fine for him while Alice has chosen her commit after the commit phase. . .

One may wonder: maybe our approach with S_0 and S_1 is flawed?

$\longrightarrow$ No! But to understand this let us being more “generic”...

Remark:

In what follows: a particular $\big($but general$\big)$ generic approach cannot work

$\longrightarrow$ It turns out that any “non-interactive” bit commitment scheme can be written in the ongoing formalism

- Impossibility to build an unconditionally secure bit commitment from quantum computation:

  https://arxiv.org/pdf/quant-ph/9712023.pdf

Definition: bit commitment scheme

Protocol between two parties Alice and Bob, denoted hereafter A and B. A bit commitment scheme consists of two phases: a commit phase $\big($Alice commits a bit $b\big)$ and a reveal phase $\big($Alice reveals to Bob her bit$\big)$

- Alice's aim: Bob cannot gain any information on her committed bit b
- Bob's aim: once Alice has made her commit, she cannot change her mind

Security requirements:

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

$$P_{\mathrm{B}}^{\star} \overset{\text{def}}{=} \max_{\text{strategy}} \mathbb{P}\Big(\text{Bob guesses } b \text{ before the reveal phase}\Big)$$

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

$$P_{\mathrm{A}}^{\star} = \max_{\text{strategy}} \frac{1}{2}\Big(\mathbb{P}\left(\text{Alice successfully reveals } b = 0\right) + \mathbb{P}\left(\text{Alice successfully reveals } b = 1\right)\Big)$$

$\longrightarrow$ Alice optimal possibility to reveal both $b = 0$ and $b = 1$ successfully random $\big($for a same commit$\big)$

$|\psi^0_{AB}\rangle$ and $|\psi^1_{AB}\rangle$ be two (publicly known) quantum bipartite states

- **Commit phase:** Alice wants to commit b. She creates $\left|\psi^b_{AB}\right\rangle$ and sends the B-part to Bob

  $\longrightarrow$ After the commit phase, Bob has $\mathrm{tr}_A\left(\left|\psi^b_{AB}\right\rangle\right)$

- **Reveal phase:** Alice sends the A part of the quantum state $\left|\psi^b_{AB}\right\rangle$ as well as b

  $\longrightarrow$ Bob checks that he has $\left|\psi^b_{AB}\right\rangle$ by projecting his (joint) state to $\left|\psi^b_{AB}\right\rangle$

Sadly, this generic quantum bit commitment scheme cannot be made secure-efficient. . .

There is a strategy for Alice and Bob such that

$$P_{\mathrm{A}}^{\star} + P_{\mathrm{B}}^{\star} \geq \frac{3}{2} \quad \text{in particular, } \max\left(P_{\mathrm{A}}^{\star}, P_{\mathrm{B}}^{\star}\right) \geq \frac{3}{4}$$

In our instantiation:

We have described a bit commitment scheme where $P_{\mathrm{A}}^{\star} = 1$ and $P_{\mathrm{B}}^{\star} = \frac{1}{2}$

Bob has before the commit phase:

$$\rho_0 = \mathrm{tr}_A\left(\left|\psi^0_{AB}\right\rangle\right) \text{ or } \rho_1 = \mathrm{tr}_A\left(\left|\psi^1_{AB}\right\rangle\right)$$

Bob's optimal cheating probability:

The optimal probability of Bob to guess b is

$$P^\star_B = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

$\longrightarrow$ Choose ρ_0 and ρ_1 such that $\Delta(\rho_0, \rho_1)$ is small

- Remark: the perfect secure situation is $P^\star_B = \frac{1}{2}$, Bob has nothing to do better than choosing b randomly

But how is the optimal Alice's strategy to cheat?

Alice's optimal cheating probability:

The optimal cheating probability of Alice $\big($revealing the commit of her choice after the commit phase$\big)$ is

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

Proof:

Fix a cheating strategy for Alice, σ be the state that Bob has after the commit phase.

During the reveal phase:

- $b = 0$: Alice sends qubits such that Bob has a pure state $|\varphi_0\rangle$
- $b = 1$: Alice sends qubits such that Bob has a pure state $|\varphi_1\rangle$

$$\mathbb{P}\left(\text{Bob accepts} \mid b = 0\right) = \left|\left\langle \varphi_0 \middle| \psi_{AB}^0 \right\rangle\right|^2 \quad \text{and} \quad \mathbb{P}\left(\text{Bob accepts} \mid b = 1\right) = \left|\left\langle \varphi_1 \middle| \psi_{AB}^1 \right\rangle\right|^2$$

By definition of the protocol: $\sigma = \mathrm{tr}_A\left(|\varphi_0\rangle\right) = \mathrm{tr}_A\left(|\varphi_1\rangle\right)$. Therefore, by Uhlmann's theorem

$$\max_{|\varphi_0\rangle} \left|\left\langle \varphi_0 \middle| \psi_{AB}^0 \right\rangle\right|^2 = F(\sigma, \rho_0)^2 \quad \text{and} \quad \max_{|\varphi_1\rangle} \left|\left\langle \varphi_1 \middle| \psi_{AB}^1 \right\rangle\right|^2 = F(\sigma, \rho_1)^2$$

Therefore, if Alice chooses correctly σ and its purifications $|\varphi_0\rangle$ and $|\varphi_1\rangle$, her probability of cheating becomes:

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

To conclude: see exercise session

Bob has before the commit phase:

$$\rho_0 = \mathrm{tr}_A\left(\left|\psi_{AB}^{0}\right\rangle\right) \text{ or } \rho_1 = \mathrm{tr}_A\left(\left|\psi_{AB}^{1}\right\rangle\right)$$

$$P_A^\star = \frac{1}{2} + \frac{F(\rho_0, \rho_1)}{2} \quad \text{and} \quad P_B^\star = \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

Fuchs-Van de Graaf inequalities: $F(\rho_0, \rho_1) \geq 1 - \Delta(\rho_0, \rho_1)$, therefore

$$P_A^\star + P_B^\star \geq \frac{3}{2} \quad \text{in particular,} \quad \max\left(P_A^\star, P_B^\star\right) \geq \frac{3}{4}$$

There is always a strategy for Bob or Alice to cheat with probability $\geq \frac{3}{4}$ ...

$\longrightarrow$ The presented bit commitment scheme cannot be unconditionally secure...

But can we build some secure cryptography by using quantum computation?

$\longrightarrow$ Yes! Quantum Key Distribution (QKD) but under some computational assumption

(classical cryptography)

Don't forget:

The QKD's also needs "classical cryptography" to be secure... It is false to say "QKD is secure because laws of physic"

$\longrightarrow$ For the QKD to be secure we need cryptography to authenticate the channel...

EXERCISE SESSION