Master 2 Systèmes Dynamiques et Signaux

Soutenance de master

Conception de détecteurs quantiques optimaux via le calcul par intervalles

6 juillet 2021

Pierre Engelstein

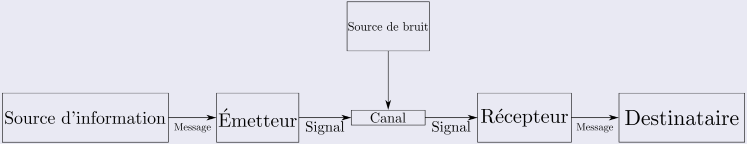
Membres du jury

Président : Pr. Laurent Hardouin

Examinateurs : Dr. Nicolas Delanoue
Pr. François Chapeau-Blondeau
Pr. Sébastien Lahaye
Dr. Mehdi Lhommeau
Pr. David Rousseau

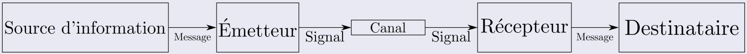
Encadrants : Dr. Nicolas Delanoue
Pr. François Chapeau-Blondeau

Présentation du problème



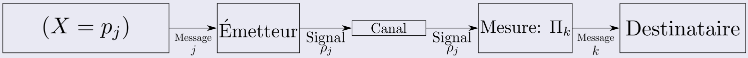
Problème classique du traitement de l'information : détection optimale.

Présentation du problème



Problème classique du traitement de l'information : détection optimale.

Présentation du problème



Cas quantique : ensemble d'états quantiques ρ_j, ayant une probabilité p_j, mesurés avec un opérateur de mesure Π_k.

1.1 : État d'un système quantique

Définition : état d'un système quantique

Système quantique **pur** : vecteur d'état $|\psi\rangle$

- dans un espace de Hilbert complexe $\mathcal{H}$,
- de norme unité : $||\psi||^2 = \langle\psi|\psi\rangle = 1$,
- avec des coordonnées :

$$|\psi\rangle = \sum_i c_i \, |k_i\rangle \, , \tag{1}$$

- où $\{|k_i\rangle\}_i$ une base orthonormée de $\mathcal{H}$,
- et les coefficients $c_i \in \mathbb{C}$.

1.1 : État d'un système quantique

Définition : opérateur densité

Opérateur densité : matrice Hermitienne ρ, telle que $\rho = \rho^\dagger$, $\mathrm{tr}(\rho) = 1$ et $\rho \succeq 0$.

1.1 : État d'un système quantique

Définition : opérateur densité

Opérateur densité : matrice Hermitienne ρ, telle que $\rho = \rho^\dagger$, $\mathrm{tr}(\rho) = 1$ et $\rho \succeq 0$.

État **pur** : opérateur densité $\rho_j = |\psi_j\rangle \langle\psi_j|$.

État **mélangé** : opérateur densité ρ_j non représentable en vecteur d'état.

1.1 : État d'un système quantique

Définition : opérateur densité

Opérateur densité : matrice Hermitienne ρ, telle que $\rho = \rho^\dagger$, $\mathrm{tr}(\rho) = 1$ et $\rho \succeq 0$.

État **pur** : opérateur densité $\rho_j = |\psi_j\rangle \langle\psi_j|$.

État **mélangé** : opérateur densité ρ_j non représentable en vecteur d'état.

Exemple

Soit un état quantique $|\psi_j\rangle = |+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$.

L'opérateur densité correspondant est :

$$\rho_j = |\psi_j\rangle \langle\psi_j| = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix}.$$

1.2 : Mesure quantique

Définition : Mesure projective

Mesure projective : N projecteurs orthogonaux $|n\rangle\langle n| = \Pi_n$, tels que $\sum_n |n\rangle\langle n| = \sum_n \Pi_n = I_N$ et $Pr\{|n\rangle\} = \mathrm{tr}(\rho\Pi_n)$.

1.2 : Mesure quantique

Définition : Mesure projective

Mesure projective : N projecteurs orthogonaux $|n\rangle\langle n| = \Pi_n$, tels que $\sum_n |n\rangle\langle n| = \sum_n \Pi_n = I_N$ et $Pr\{|n\rangle\} = \mathrm{tr}(\rho\Pi_n)$.

Définition : Mesure généralisée (POVM)

POVM : *Positive Operator-Valued Measurement*, K opérateurs de mesure non nécessairement projecteurs orthogonaux $\{\Pi_k\}$, tels que $\sum_k \Pi_k = I_k$ et $Pr\{\Pi_k\} = \mathrm{tr}(\rho\Pi_k)$.

1.3 : Problème de la mesure optimale

Problème à résoudre

Obtenir les $\{\Pi_k\}$ opérateurs de mesure permettant d'identifier le mieux possible les états d'entrée $\{\rho_j\}$.

1.3 : Problème de la mesure optimale

Problème à résoudre

Obtenir les $\{\Pi_k\}$ opérateurs de mesure permettant d'identifier le mieux possible les états d'entrée $\{\rho_j\}$.

Critères d'optimisation

1. Maximiser la probabilité de détection correcte (linéaire), [a]
2. Minimiser l'erreur quadratique de mesure, [b]
3. Maximiser information mutuelle (non linéaire) [c].

a. Eldar, Y., "Designing Optimal Quantum Detectors Via Semidefinite Programming", IEEE Transaction on Information Theory 49 (2003), 1012-1017

b. Eldar, Y., "On Quantum Detection and the Square-Root Measurement", IEEE Transaction on Information Theory 47 (2001), 858-872

c. Davies, E., "Information and quantum measurement", IEEE Transaction on Information Theory 24 (1978), 596-599

1.3 : Problème de la mesure optimale

Définition : information mutuelle

L'*information mutuelle* est définie pour deux variables aléatoires X et Y par :

$$
\begin{aligned}
I(X;Y) &= H(X) + H(Y) - H(X,Y) && (2)\\
&= H(Y) - H(Y|X) && (3)\\
&= H(X) - H(X|Y) && (4)
\end{aligned}
$$

1. $H(X)$ et $H(Y)$ entropies marginales de X et Y ;
2. $H(X,Y)$ entropie conjointe de X et Y ;
3. $H(X|Y)$ entropie de X sachant Y.

$X = \{\rho_j = |\phi_j\rangle\langle\phi_j|, 1 \leq j \leq m\}$,

$Y = \{\Pi_k = |\mu_k\rangle\langle\mu_k|, 1 \leq k \leq m\}$

Avec $\{p_j\}$ distribution marginale de X.

1.3 : Problème de la mesure optimale

Problème

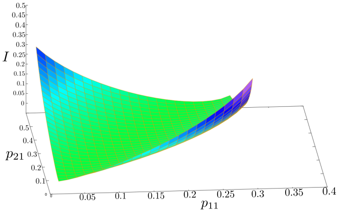
On cherche à résoudre le problème de maximisation :

$$\max_{\{\Pi\}} I(\rho, \Pi) \tag{2}$$

tel que :

$$\Pi_j \succeq 0, \quad 1 \leq j \leq m \tag{3}$$

$$\sum_{j=1}^{m} \Pi_j = I \tag{4}$$



- Problème de maximisation de fonction non linéaire, convexe : difficile en pratique à résoudre.
- Utilisation du calcul par intervalle pour fournir une solution optimale garantie.

2.1 : Intervalle et fonction d'inclusion

Notion d'intervalle

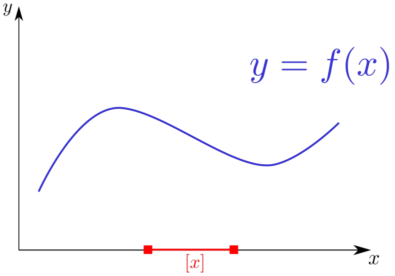
Un intervalle $\mathbf{x} = [\underline{x}, \overline{x}]$ est défini comme l'ensemble des nombres réels x t.q. $\underline{x} \leq x \leq \overline{x}$.

2.1 : Intervalle et fonction d'inclusion

Définition : fonction d'inclusion

Soit $f : \mathbb{R}^n \to \mathbb{R}^m$ une fonction, la fonction $[f] : \mathbb{R}^n \to \mathbb{R}^m$ est une *fonction d'inclusion* pour f si

$$\forall [\underline{x}, \overline{x}] \in \mathbb{R}^n, f([\underline{x}, \overline{x}]) \subset [f]([\underline{x}, \overline{x}]) \tag{5}$$

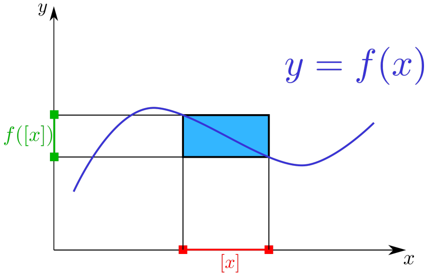


2.1 : Intervalle et fonction d'inclusion

Définition : fonction d'inclusion

Soit $f : \mathbb{R}^n \to \mathbb{R}^m$ une fonction, la fonction $[f] : \mathbb{R}^n \to \mathbb{R}^m$ est une *fonction d'inclusion* pour f si

$$\forall [\underline{x}, \overline{x}] \in \mathbb{R}^n, f([\underline{x}, \overline{x}]) \subset [f]([\underline{x}, \overline{x}]) \tag{5}$$

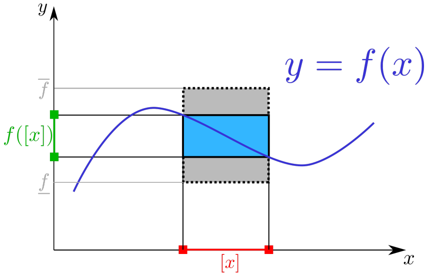


2.1 : Intervalle et fonction d'inclusion

Définition : fonction d'inclusion

Soit $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ une fonction, la fonction $[f] : \mathbb{R}^n \rightarrow \mathbb{R}^m$ est une *fonction d'inclusion* pour f si

$$\forall [\underline{x}, \overline{x}] \in \mathbb{R}^n, f([\underline{x}, \overline{x}]) \subset [f]([\underline{x}, \overline{x}]) \tag{5}$$



2.1 : Intervalle et fonction d'inclusion

On définit un ensemble d'opérateurs comme extension des opérateurs arithmétiques sur les nombres réels :

- $[x_1] + [x_2] = [\underline{x_1} + \underline{x_2}, \overline{x_1} + \overline{x_2}]$
- $[x_1] - [x_2] = [\underline{x_1} - \overline{x_2}, \overline{x_1} - \underline{x_2}]$
- $[x_1] \times [x_2] = [\min(\underline{x_1 x_2}, \underline{x_1}\overline{x_2}, \overline{x_1}\underline{x_2}, \overline{x_1 x_2}), \max(\underline{x_1 x_2}, \underline{x_1}\overline{x_2}, \overline{x_1}\underline{x_2}, \overline{x_1 x_2})]$
- $\log([x]) = [\log(\underline{x_1}), \log(\overline{x_2})]$
- ...

Exemple

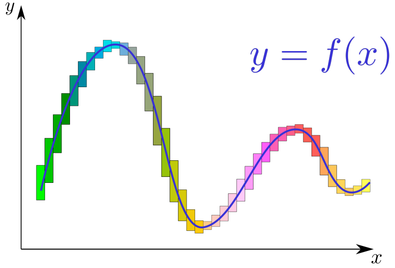
$$\begin{aligned}[z] &= ([2,3] - [-4,5])^2 + [-3,2] \\ &= [-3,7]^2 + [-3,2] \\ &= [0,49] + [-3,2] \\ &= [-3,51]\end{aligned}$$

2.2 : Algorithmes d'optimisation par intervalles

Théorème

Soit un a une solution admissible du problème $\max_x f(x)$ tel que $g(x) \leq 0$ et x^* la solution optimale, on a :

$$sup([f]([x])) \leq f(a) \Rightarrow x^* \notin [x] \quad (6)$$



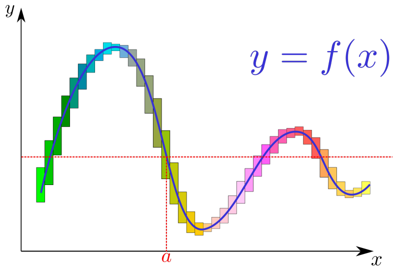
$y = f(x)$

2.2 : Algorithmes d'optimisation par intervalles

Théorème

Soit un a une solution admissible du problème $\max_x f(x)$ tel que $g(x) \leq 0$ et x^* la solution optimale, on a :

$$sup([f]([x])) \leq f(a) \Rightarrow x^* \notin [x] \qquad (6)$$



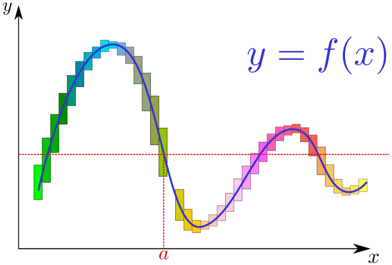
$y = f(x)$

2.2 : Algorithmes d'optimisation par intervalles

Théorème

Soit un a une solution admissible du problème $\max_x f(x)$ tel que $g(x) \leq 0$ et x^* la solution optimale, on a :

$$sup([f]([x])) \leq f(a) \Rightarrow x^* \notin [x] \quad (6)$$



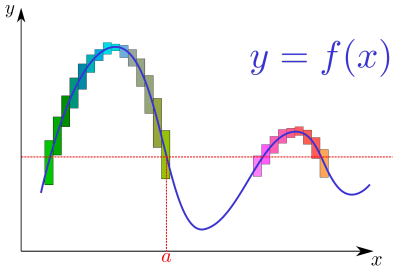
$y = f(x)$

2.2 : Algorithmes d'optimisation par intervalles

Théorème

Soit un a une solution admissible du problème $\max_x f(x)$ tel que $g(x) \leq 0$ et x^* la solution optimale, on a :

$$sup([f]([x])) \leq f(a) \Rightarrow x^* \notin [x] \tag{6}$$



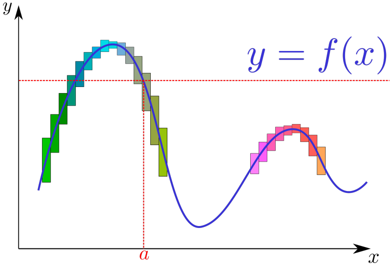
$y = f(x)$

2.2 : Algorithmes d'optimisation par intervalles

Théorème

Soit un a une solution admissible du problème $\max_x f(x)$ tel que $g(x) \leq 0$ et x^* la solution optimale, on a :

$$sup([f]([x])) \leq f(a) \Rightarrow x^* \notin [x] \qquad (6)$$



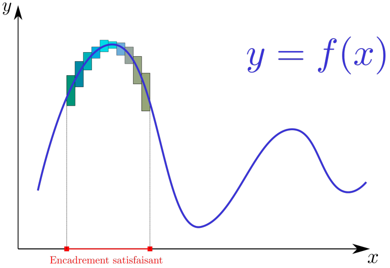
$y = f(x)$

2.2 : Algorithmes d'optimisation par intervalles

Théorème

Soit un a une solution admissible du problème $\max_x f(x)$ tel que $g(x) \leq 0$ et x^* la solution optimale, on a :

$$sup([f]([x])) \leq f(a) \Rightarrow x^* \notin [x] \tag{6}$$



$y = f(x)$

3.1 : Optimiseur générique

$$\max_{\Pi=\{\Pi_j\}} I(\rho, \Pi) \tag{7}$$

$$\Pi_j \succeq 0, \quad 1 \leq j \leq m \tag{8}$$

$$\sum_{j=1}^{m} \Pi_j = I \tag{9}$$

Faisabilité

- Fonction d'inclusion spécifique pour $x \mapsto x \log(x)$
- Critère de Sylvester pour la semi-définie positivité

3.1 : Optimiseur générique

$$\max_{\Pi=\{\Pi_j\}} I(\rho, \Pi) \tag{7}$$

$$\Pi_j \succeq 0, \quad 1 \leq j \leq m \tag{8}$$

$$\sum_{j=1}^{m} \Pi_j = I \tag{9}$$

Faisabilité

- Fonction d'inclusion spécifique pour $x \mapsto x\log(x)$
- Critère de Sylvester pour la semi-définie positivité

Temps de calcul

- Utilisation du gradient de $I(\rho, \Pi)$: forme centrée et convexité
- Parallélisation de l'algorithme : gain de performance

3.2 : Exemple

Entrées du problème

Deux états purs $|\psi_1\rangle = \begin{pmatrix} \frac{1}{3} \\ \frac{2\sqrt{2}}{3} \end{pmatrix}$ et $|\psi_2\rangle = |+\rangle$, avec $p_1 = 0.1$ et $p_2 = 0.9$. Opérateurs densité correspondant :

$$\rho_1 = \begin{pmatrix} \frac{1}{9} & \frac{2\sqrt{2}}{9} \\ \frac{2\sqrt{2}}{9} & \frac{8}{9} \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix}$$

Deux opérateurs de mesure inconnus

$$\Pi_1 = \begin{pmatrix} a_1 & b_1 + ic_1 \\ b_1 - ic_1 & d_1 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} a_2 & b_2 + ic_2 \\ b_2 - ic_2 & d_2 \end{pmatrix}$$

Information mutuelle maximum : $-0.1 \log_2(0.1) - 0.9 \log_2(0.9) = 0.47$ Shannon.

3.2 : Exemple

On veut résoudre le problème

$$\max_{\Pi_1,\Pi_2} I(\rho_1, \rho_2, \Pi_1, \Pi_2) \tag{10}$$

tel que :

$$\Pi_1 \succeq 0, \Pi_2 \succeq 0 \tag{11}$$

$$\Pi_1 + \Pi_2 = I \tag{12}$$

3.2 : Exemple

On sait que $\Pi_1 + \Pi_2 = I$, on réduit à 4 variables inconnues :

$$\Pi_2 = \begin{pmatrix} (1-a_1) & (-b_1) + i(-c_1) \\ (-b_1) - i(-c_1) & (1-d_1) \end{pmatrix}$$

ρ_j non complexes : on enlève c_1.

Semi-définie positivité des Π_k : critère de Sylvester.

$$\begin{cases} \Pi_1 \succeq 0 \\ \Pi_2 \succeq 0 \end{cases} \Leftrightarrow \begin{cases} a_1 \geq 0 \\ d_1 \geq 0 \\ a_1 \times d_1 - b_1^2 \geq 0 \\ (1-a_1) \times (1-d_1) - (-b_1)^2 \geq 0 \end{cases}$$

3.3 : Résultats

Ibex

- Information mutuelle optimale : 0.0681 Shannon
- Temps de calcul : 87 secondes, précision relative : 10^{-3}.
- Solutions optimales :

$$\Pi_1 = \begin{pmatrix} 0.454 & -0.498 \\ -0.498 & 0.546 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 0.546 & 0.498 \\ 0.498 & 0.454 \end{pmatrix}.$$

Notre solveur

- Information mutuelle optimale : 0.0681 Shannon
- Temps de calcul : 13 secondes, précision relative : 10^{-8}.
- Solutions optimales :

$$\Pi_1 = \begin{pmatrix} 0.454 & -0.498 \\ -0.498 & 0.546 \end{pmatrix}, \quad \Pi_2 = \begin{pmatrix} 0.546 & 0.498 \\ 0.498 & 0.454 \end{pmatrix}.$$

Conclusion

Contribution :
Réalisation d'un solveur générique pour le problème de la détection optimale quantique, via le calcul par intervalle, avec pour critère l'information mutuelle.

Perspectives :

1. Utilisations d'autres formes de fonction d'inclusion pour contrer des temps de calcul qui deviennent grands : forme centrée, arithmétique des pentes.
2. Étendre le problème en ajoutant du bruit sur le canal de communication ;

Merci pour votre attention !