Alguns problemas em teoria de informação quântica.

Daniel Cariello

Julho 2020 - Uberlândia


Andrés Cassinello e
José Luis Sánchez Gómez
O MISTÉRIO
QUÂNTICO
Uma expedição às
fronteiras da física
CRÍTICA

Table of Contents

1. Problema da Separabilidade
2. Quantificação de Emaranhamento
3. Bases mutuamente imparciais
4. Bibliografia

Notação: $M_k = \{\text{matrizes complexas de ordem } k\}, P_k = \{\text{matrizes Hermitianas positivas semidefinidas de ordem } k\}$.

As matrizes Hermitianas positivas semidefinidas de ordem k são aquelas que podem ser escritas como $\sum_{i=1}^{r} w_i w_i^*$, onde $w_i \in \mathbb{C}^k$ e $w_i^* = \overline{w_i}^t$.

Além disso, considere o produto de Kronecker das matrizes $A_{k\times k}, B_{m\times m}$: $A \otimes B = (a_{ij}B)_{km\times km}$.

Note que $A \otimes B$ é uma matriz de ordem km.

Exemplo:

$$A \otimes B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} =$$

$$\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

Os elementos do produto tensorial $M_k \otimes M_m$ podem ser interpretados como matrizes em M_{km} e vice e versa, utilizando o produto de Kronecker.

Se $A \in M_k \otimes M_m$ então $A = \sum_{i=1}^{n} A_i \otimes B_i$, onde $A_i \in M_k$ e $B_i \in M_m$. Agora utilizando o produto de Kronecker, $A_i \otimes B_i$ se transforma numa matrix de ordem km.

Agora considere uma matriz de ordem 4, $A = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}$, onde B_i é uma matriz de ordem 2. Podemos escrevê-la:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes B_1 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes B_2 + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes B_3 + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes B_4.$$

Assim identificamos $M_k \otimes M_m \simeq M_{km}$.

Definition

Dizemos que uma matriz $B \in M_k \otimes M_m \simeq M_{km}$ é separável se $B = \sum_{i=1}^{n} C_i \otimes D_i$, onde $C_i \in P_k$ e $D_i \in P_m$ para todo i. Se B não é separável então B está emaranhada.

Problem (Problema da Separabilidade dos Estados Quânticos)

Encontrar um critério determinístico para distinguir as matrizes separáveis das matrizes emaranhadas.

Distinguir as matrizes emaranhadas das separáveis em $M_k \otimes M_m$ é o caso bipartido do problema da separabilidade. Esse caso já é NP-difícil.

Assim identificamos $M_k \otimes M_m \simeq M_{km}$.

Definition

Dizemos que uma matriz $B \in M_k \otimes M_m \simeq M_{km}$ é separável se $B = \sum_{i=1}^{n} C_i \otimes D_i$, onde $C_i \in P_k$ e $D_i \in P_m$ para todo i. Se B não é separável então B está emaranhada.

Problem (Problema da Separabilidade dos Estados Quânticos)

Encontrar um critério determinístico para distinguir as matrizes separáveis das matrizes emaranhadas.

Distinguir as matrizes emaranhadas das separáveis em $M_k \otimes M_m$ é o caso bipartido do problema da separabilidade. Esse caso já é NP-difícil.

O caso $km \leq 6$ foi resolvido pelo critério PPT.

Definition (Condição Necessária para Separabilidade)

Seja $A = \sum_{i=1}^{n} A_i \otimes B_i \in M_k \otimes M_m \simeq M_{km}$. Dizemos que A é positiva sob transposição parcial (ou simplesmente PPT) se A e $A^{\Gamma} = \sum_{i=1}^{n} A_i \otimes B_i^t$ são matrizes Hermitianas positivas semidefinidas.

Solução do problema da Separabilidade quando $km \leq 6$:
$A \in M_k \otimes M_m \simeq M_{km}$, $km \leq 6$, é separável se e só se A é PPT.

Exemplo: Seja $u = \sum_{i=1}^{k} e_i \otimes e_i$, onde $e_1, \ldots, e_k$ é a base canônica do $\mathbb{C}^k$.

A matriz $uu^* = \sum_{i,j=1}^{k} (e_i \otimes e_i)(e_j^t \otimes e_j^t) = \sum_{i,j=1}^{k} e_i e_j^t \otimes e_i e_j^t$ é positiva semidefinida, mas

$$(uu^*)^\Gamma = \sum_{i,j=1}^{k} e_i e_j^t \otimes e_j e_i^t = \sum_{i,j=1}^{k} (e_i \otimes e_j)(e_j \otimes e_i)^t.$$

Agora $(uu^*)^\Gamma (e_j \otimes e_i) = e_i \otimes e_j$. Portanto

$$(uu^*)^\Gamma (e_i \otimes e_j - e_j \otimes e_i) = -(e_i \otimes e_j - e_j \otimes e_i).$$

A matriz $(uu^*)^\Gamma$ tem autovalores negativos e uu^* não é positiva sob transposição parcial. Portanto não é separável.

Problema 1: Encontrar critérios que ajudem a detectar as matrizes emaranhadas em $M_k \otimes M_m$ ou em dimensões específicas (e.g., $M_2 \otimes M_4$) ou para conjuntos particulares de matrizes.

Outra maneira de estudar emaranhamento é quantificando-o, ou seja, dizer quão emaranhada uma matriz está. Isso é feito através de medidas de emaranhamento. Uma delas se chama número de Schmidt da matriz.

Definition

O posto de um tensor $v \in \mathbb{C}^k \otimes \mathbb{C}^m$ é 1 se $v = a \otimes b$, onde $a \in \mathbb{C}^k \setminus \{\vec{0}\}$, $b \in \mathbb{C}^m \setminus \{\vec{0}\}$. Dizemos que o posto de um tensor $w \in \mathbb{C}^k \otimes \mathbb{C}^m$ é n, se o menor número de tensores de posto 1 que somados dão w é n.

Exemplo: Se $r = c \otimes d + e \otimes f$, mas não puder ser escrito como $a \otimes b$. Então o posto de r é 2.

Agora toda matriz $A \in M_k \otimes M_m$ positiva semidefinida Hermitiana pode ser escrita como $A = \sum_{i=1}^{r} w_i w_i^*$, onde $w_i \in \mathbb{C}^k \otimes \mathbb{C}^m$.

Definition

Definimos o número de Schmidt de uma matriz $A \in M_k \otimes M_m$ positiva semidefinida Hermitiana por

$$NS(A) = \min \left\{ \max_i \{\text{posto}(w_i)\}, \; A = \sum_{i=1}^{r} w_i w_i^* \right\}.$$

Esse mínimo é calculado sobre todas as possíveis maneiras de se escrever A como $\sum_{i=1}^{r} w_i w_i^*$.

Exemplo: Se uma matriz positiva semidefinida Hermitiana $A \in M_k \otimes M_m$ tem número de Schmidt 1. Então existe uma maneira de escrevê-la como $A = \sum_{i=1}^{r} w_i w_i^*$, onde posto$(w_i) \leq 1$ para todo i. Portanto $w_i = a_i \otimes b_i$ para todo i.

Assim $A = \sum_{i=1}^{r} (a_i \otimes b_i)(a_i \otimes b_i)^* = \sum_{i=1}^{r} a_i a_i^* \otimes b_i b_i^*$.

Agoras as matrizes $a_i a_i^*, b_i b_i^*$ são positivas semidefinidas Hermitianas, ou seja, A é separável. Portanto $NS(A) = 1$ implica que A é separável. A volta também vale.

Isto é, A é separável se e só se $NS(A) = 1$.
Portanto A está emaranhada se e só se $NS(A) > 1$.

Uma matriz com número de Schmidt alto está associada a uma ideia de emaranhamento alta.
Uma matriz PPT emaranhada é considerada fracamente emaranhada. A pergunta natural é a seguinte:

Problema 2: Qual é o maior número de Schmidt para uma matriz PPT em $M_k \otimes M_m$?

• Por exemplo, sabemos que o maior número de Schmidt de uma matriz PPT em $M_3 \otimes M_3$ é 2.

• Para k arbitrário, até o momento o maior número de Schmidt conhecido para uma matriz PPT em $M_k \otimes M_k$ é $\left\lfloor \frac{k}{2} \right\rfloor$.

Um pouquinho mais de física:

Os níveis de energia de uma partícula estão associados a uma base ortonormal do $\mathbb{C}^k$, $\{v_1, \ldots, v_k\}$, e as suas posições também estão associadas a outra base ortonormal, $\{w_1, \ldots, w_k\}$.

Se obtermos em um experimento que a energia da partícula está associada ao vetor v_i, um postulado da mecânica quântica diz que se você fizer o experimento para obter o vetor associado a posição da partícula então a probabilidade de obter o vetor w_j é

$$|\langle v_i, w_j \rangle|^2.$$

Definition (Bases Mutuamente Imparciais)

Sejam $\{v_1, \ldots, v_k\}$ e $\{w_1, \ldots, w_k\}$ bases ortonormais do $\mathbb{C}^k$. Dizemos que elas são mutuamente imparciais se $|\langle v_i, w_j \rangle|^2 = \frac{1}{k}$ para quaisquer i, j.

OBS: As bases associadas aos níveis de energia e as posições de uma partícula são mutuamente imparciais. Portanto se você obter o vetor v_i associado a energia então a probabilidade de obter qualquer w_j é igual a $\frac{1}{k}$. Esse é o caso mais incerto possível. Se você souber exatamente qual o nível de energia, você não sabe nada da posição.

Além disso, essas bases tem aplicações em tomografia quântica, criptografia quântica, etc.

Problem (Outro problema Importante em TIQ)

Encontre o número máximo de bases ortonormais de $\mathbb{C}^k$ que são duas a duas mutuamente imparciais.

Sabemos que $k+1$ é uma cota superior para a solução. Além disso, quando k é uma potência de primos sabemos encontrar essas $k+1$ bases. Não sabemos a resposta quando k não é uma potência de primo (e.g. $k=6$).

A solução desse problema na dimensão 6 vale 2020 euros nesse ano, ano que vem valerá 2021 e assim por diante.

Um dos melhores teoremas que temos sobre bases mutuamente imparciais em dimensão arbitrária é o teorema de Weiner.

Theorem (Weiner)

Se $\mathbb{C}^k$ contém k bases mutuamente imparciais então existe outra base ortonormal que é mutuamente imparcial com essas k (Se $\mathbb{C}^k$ contém k então $\mathbb{C}^k$ contém $k+1$).

Problema 3: Encontrar o número máximo de bases mutuamente imparciais em $\mathbb{C}^k$ com alguma propriedade extra.

Por exemplo, sabemos o seguinte teorema.

Theorem

O número máximo de bases mutuamente imparciais de $\mathbb{C}^m \otimes \mathbb{C}^n$ *formada por tensores de posto menor ou igual a d* $(d < m \leq n)$ *não excede* $\dfrac{d(m^2-1)}{m-d}$.

O. Gühne and G. Tóth
Entanglement detection
Physics Reports **474** (2009), no. 1-6, p. 1-75.

L. Gurvits
Classical complexity and quantum entanglement
Journal of Computer and System Sciences **69** (2004), no. 3, p. 448-484.

Y. Yang, D. H. Leung, W. S.Tang
All 2-positive linear maps from M3 (C) to M3 (C) are decomposable
Linear Algebra and its Applicationss **503** (2016), p. 233-247.

D. Cariello
Inequalities for the Schmidt number of bipartite states.
Lett. Math. Phys. **110** (2020), p. 827-833.

P. Horodecki, L. Rudnicki, K. Zyczkowski
Five open problems in quantum information
arXiv:2002.03233

M. Weiner
A gap for the maximum number of mutually unbiased bases
Proceedings of the American Mathematical Society **141** (2013), no. 6, p. 1963-1969.

D. Cariello
Conservation Laws in mutually unbiased bases
arXiv:2004.04226.

Obrigado!!!