FUNDAMENTOS MATEMÁTICOS DA SEPARABILIDADE QUÂNTICA

Autor: Mateus Araújo Santos
Orientador: Marcelo O. Terra Cunha

Setembro, 2010

Sumário

Resumo

Estados emaranhados são a chave da revolução que está acontecendo nos fundamentos da mecânica quântica: a descoberta da não-localidade como traço essencial do mundo quântico, através das desigualdades de Bell, o advento da computação quântica, com o famoso algoritmo de Shor, e a distribuição quântica de chaves criptográficas, com sua promessa de possibilitar comunicação perfeitamente segura.

Porém, emaranhamento é uma característica bastante complicada matematicamente, e ainda não sabemos caracterizá-lo completamente. Para tal, precisamos desenvolver critérios que decidem se um estado quântico é ou não emaranhado. Este trabalho faz uma revisão dos conceitos matemáticos fundamentais por trás do famoso critério da transposição parcial positiva: o teorema da hiperplano separador, o isomorfismo de Jamiołkowski e a decomponibilidade dos mapas positivos. A conexão entre esses conceitos aparentemente díspares é o teorema de Woronowicz: todo mapa positivo de dimensão baixa[1] pode ser escrito como uma soma de mapas completamente positivos e completamente copositivos. O principal foco deste trabalho é a sua demonstração, apresentada numa linguagem moderna e com notação adequada para a física.

O trabalho se encerra com uma exploração geométrica do espaço de estados, a partir do produto interno de Hilbert-Schmidt. Analisamos as propriedades básicas de simetria e a representação do simplexo de autovalores, culminando com uma representação do espaço de estados emaranhados e o cálculo numérico dos volumes relevantes para várias dimensões.

[1] Realmente baixa.

Abstract

Entangled states are the key for the revolution that is happening in the foundations of quantum mechanics: the discovery of nonlocality as the essential trait of the quantum world, through the Bell inequalities, the advent of quantum computation, with the famous Shor's algorithm, and the quantum key distribution, with its promise of a perfectly secure communication.

However, entanglement is a quite complicated characteristic, and we still don't know its complete mathematical characterisation. For this, we need to develop criteria that can decided if a given quantum state is entangled or not. This work makes a revision of the fundamental mathematical concepts behind the famous positive partial transpose (PPT) criterion: the separating hyperplane theorem, the Jamiołkowski isomorphism, and the decomposability of the positive maps. The connection between this apparently disjoint concepts is the Woronowicz theorem: every low-dimensional[2] positive map can be written as the convex combination of completely positive and completely copositive maps. The main focus of this work is its demonstration, presented with a modern language and notation adequate for physics.

The work finishes with an geometrical exploration of the state space, by the means of the Hilbert-Schmidt inner product. We analyse the basic symmetry properties and the eigenvalue simplex representation, culminating with a representation of the entangled states and the numerical calculation of the relevant volumes in various dimensions.

[2]Really low.

Introdução

O "problema do emaranhamento" pode ser resumido em duas perguntas: dado um estado quântico, ele está emaranhado? Quão emaranhado ele está?

Ainda não temos uma resposta satisfatória para ambas as perguntas. Sabemos que a primeira é uma pergunta NP-HARD, e possuímos apenas um algoritmo probabilístico [1] para respondê-la no caso mais geral. A segunda é mais delicada; não sabemos nem se o problema é bem posto. Vamos tratar apenas da primeira nesta monografia.

Sabemos algoritmos determinísticos e eficientes para respondê-la em vários casos particulares: o problema já foi completamente solucionado para estados puros bipartites, com a decomposição de Schmidt [2, 3], e é razoavelmente bem compreendido para as dimensões mais baixas. Para uma visão geral dos algoritmos mais difundidos, ver o cap. 7 da excelente revisão da família Horodecki [4], ou o cap. 15 do livro fundamental de Bengtsson e Życzkowski [5]. Nesta monografia meu foco será apenas o mais famoso: o critério da transposta parcial positiva.

No capítulo 1, vou definir os termos com os quais estou trabalhando e desenvolver as ferramentas básicas que utilizarei no restante da monografia. Procurei não incluir nenhum resultado mais esotérico nele, de forma que um leitor mais experiente pode pulá-lo com segurança. Ao mesmo tempo, procurei ser bastante didático e completo, de forma que esse capítulo possa ser útil para um leitor inexperiente que queira se adentrar do assunto.

No capítulo 2, faço o trabalho técnico mais pesado da monografia: a demonstração do teorema de Woronowicz, com o objetivo de tirar como corolário o critério da transposta parcial positiva. Considero isso importante por não conhecer nenhuma demonstração explícita desse critério na literatura. Com isso, espero ter facilitado o acesso à informação para quem se interessa pelos fundamentos matemáticos da teoria quântica da informação.

No capítulo 3, exploro uma consequência imediata das dualidades desenvolvidas no capítulo anterior: a existência das testemunhas de emaranhamento. Elas são importantes do ponto de vista teórico e prático, por conta dos algoritmos poderosos que podemos desenvolver com elas.

Já o capítulo 4, o considero como a cereja no topo do bolo: é um capítulo bem suave, que utiliza os resultados do restante da monografia para fazer uma exploração geométrica do espaço de estados. Ele é independente do capítulo 3 e utiliza apenas os resultados do 2, podendo ser lido logo após o 1.

Capítulo 1

Estados, mapas e cones

Neste capítulo irei preparar as ferramentas que utilizarei no restante do texto: definir os termos com os quais estou trabalhando, bem como provar alguns teoremas básicos sobre cada área.

Assumirei familiaridade do leitor com a notação de Dirac e com o produto tensorial, que usarei extensivamente. Creio que minha primeira assumpção é verdadeira e a segunda é falsa, mas uma exposição de suas propriedades fugiria muito do foco deste texto. O leitor interessado encontrará uma introdução amigável sobre ambos em [6, 7].

1.1 Estados quânticos

Definição 1.1. *Um estado quântico ρ é um operador positivo*[1] *de traço unitário. O conjunto dos estados de dimensão n é conhecido como espaço de estados, que pode ser visto como um subconjunto da álgebra (C^*) de matrizes complexas de ordem n denotada por $\mathcal{M}_n$.*

Definição 1.2. *Podemos definir um produto interno nesta álgebra, dotando-a assim da estrutura de um espaço de Hilbert. O produto interno canônico é o produto interno de Hilbert-Schmidt:*

$$\langle A, B\rangle := \mathrm{tr}(A^* B)$$

que facilmente verificamos possuir todas as propriedades necessárias[2,3]*.*

A condição de traço unitário é exigida porque gostamos de interpretar os elementos da diagonal (em uma dada base) como uma distribuição de probabilidade. Mas a normalização é irrelevante para uma discussão mais abstrata; só devemos exigir que o estado seja normalizável[4]. Como trataremos apenas de estados de dimensão finita, esta restrição só exclui o operador nulo como estado válido.

[1] Um operador positivo ρ é um operador cujos autovalores são todos maiores ou iguais a zero. Escrevemos $\rho \geq 0$.

[2] Note que ele é linear no segundo argumento, e não no primeiro. Isso é somente a convenção utilizada na mecânica quântica.

[3] Nesta monografia estaremos interessados apenas em operadores auto-adjuntos. Isso restringe o produto interno a retornar números reais; temos assim um espaço de Hilbert real.

[4] Lembrando que estados linearmente dependentes são equivalentes.

Existe um caso particular importante, quando o estado apresenta apenas um autovalor não-nulo: neste caso ele corresponde a um projetor, e é conhecido como estado puro. Esta nomenclatura coincide com a de ponto puro de um conjunto convexo, *i.e.*, todos os estados podem ser gerados a partir de uma combinação convexa de estados puros, e eles próprios não podem ser escritos como combinação convexa de outros estados.

Estamos interessados em estados que são compostos por dois subsistemas. Quando é este o caso, o espaço de estados do sistema composto é o produto tensorial[5] dos espaços individuais:

$$\mathcal{M}_{mn}^{AB} = \mathcal{M}_m^A \otimes \mathcal{M}_n^B$$

onde estamos seguindo a convenção de nomear as duas partes (A)lice e (B)ob. Um tema encantador, mas que não será abordado, é o estudo do emaranhamento em sistemas multipartites.

Uma tentação comum é dizer que os estados do sistema composto serão o produto tensorial dos estados individuais

$$\rho^{AB} = \rho^A \otimes \rho^B$$

mas isso é falso: existem estados em $\mathcal{M}_m^A \otimes \mathcal{M}_n^B$ que não podem ser escritos nesta forma. No caso mais interessante, eles representam estados que apresentam algum tipo de correlação quântica: são os famosos estados emaranhados.

Definição 1.3. *Um estado emaranhado é um estado que não é separável. Um estado separável (bipartite) é um estado que pode ser escrito na forma*

$$\rho = \sum_i \lambda_i \rho_i^A \otimes \rho_i^B$$

onde $\lambda_i > 0$ *e* $\sum_i \lambda_i = 1$.

Ou seja, um estado separável é uma combinação convexa de estados produto. Podemos interpretar isso da seguinte maneira: Alice possui um gerador de números aleatórios, que sorteia i com probabilidade λ_i. Feito o sorteio, Alice comunica a Bob a alternativa obtida (comunicação clássica), e eles geram (localmente) os estados ρ_i^A e ρ_i^B, respectivamente. Portanto, estados emaranhados são aqueles estados que não podem ser gerados fazendo-se apenas operações locais e comunicação clássica[6].

Agora já podemos ter uma visão básica[7] sobre a geometria do espaço de estados. Segue direto da definição 1.1 que o espaço de estados D é um conjunto convexo: se ρ e σ são estados, $\lambda\rho + (1-\lambda)\sigma$ é obviamente um estado válido. Também é trivial a demonstração de que ele é um conjunto fechado; além disso, a positividade junto com a condição $\mathrm{tr}(\rho) = 1$ implica que o maior autovalor possível é 1, e portanto o conjunto é limitado. Como estamos tratando de um espaço de Hilbert de dimensão finita, isso é suficiente para afirmar que ele é compacto.

[5] Cuidado para não confundi-lo com o produto cartesiano $\times$ ou a soma direta $\oplus$

[6] Comunicação clássica é exatamente o que você está imaginando — transmissão de bits.

[7] Detalhar essa visão é o objetivo do capítulo 4.

Analogamente, a definição 1.3 implica que o espaço de estados separáveis S é convexo e fechado, e um subconjunto fechado de um compacto é compacto.

Em vista desses resultados, é útil reescrever a definição do conjunto de estados emaranhados: $E := D \setminus S$; e a diferença de dois conjuntos convexos em geral não é convexa[8]. Este é um dos motivos pelos quais sua caracterização é bem mais complexa que nos casos anteriores.

1.2 Mapas positivos

Mapas positivos foram estudados muito tempo atrás e muito recentemente, por conta de suas aplicações à teoria quântica e ao problema da separabilidade, respectivamente. Em particular, a evolução mais geral[9] que um estado quântico pode sofrer é um mapa completamente positivo, e portanto este conjunto é identificado com as operações que podem ser implementadas fisicamente. Para sermos mais claros, precisamos de algumas definições.

Definição 1.4. *Um mapa positivo $\Lambda^P : \mathcal{M}_m \to \mathcal{M}_n$ é um mapa linear entre álgebras de operadores tal que $\rho \geq 0 \Rightarrow \Lambda^P(\rho) \geq 0$*

À primeira vista, esta parece ser uma condição suficiente para que o mapa seja físico, afinal seu domínio e contradomínio são estados quânticos válidos. Mas problemas aparecem quando se considera extensões triviais de mapas positivos. Podemos definir esta extensão num estado produto:

$$\Lambda \otimes \mathbb{1}\left(\rho^A \otimes \rho^B\right) := \Lambda\left(\rho^A\right) \otimes \rho^B$$

e estender esta definição para qualquer estado por linearidade.

Teorema 1.5. *Se $\Lambda^P : \mathcal{M}_m \to \mathcal{M}_n$ é um mapa positivo e $\rho \in \mathcal{M}_m \otimes \mathcal{M}_r$ um operador positivo, então $\Lambda^P \otimes \mathbb{1}(\rho) \in \mathcal{M}_{nr}$ é um operador auto-adjunto.*

Demonstração. Se ρ é positivo, ele é em particular auto-adjunto, e podemos representá-lo com coeficientes reais numa base auto-adjunta[10]:

$$\rho = \sum_{ij} p_{ij} \sigma_i \otimes \sigma_j$$

Então

$$\begin{aligned} \Lambda^P \otimes \mathbb{1}(\rho) &= \sum_{ij} p_{ij} \Lambda^P(\sigma_i) \otimes \sigma_j \\ &= \left(\sum_{ij} p_{ij} \Lambda^P(\sigma_i) \otimes \sigma_j \right)^* \end{aligned}$$

□

[8] Imagine D como um ovo, e S como sua gema.
[9] Ignorando-se sistemas de partículas indistinguíveis, cuja representação é mais delicada.
[10] Detalharemos essa representação na secção 4.2.

Mas a afirmação mais forte de que a extensão $\Lambda^P \otimes \mathbb{1}$ preserva positividade é falsa. Por exemplo, o mapa transposição $T : \mathcal{M}_m \to \mathcal{M}_m$ é um mapa positivo (ele preserva todo o espectro, na verdade), mas a extensão trivial[11] $T \otimes \mathbb{1}$ não. Aplique $T \otimes \mathbb{1} : \mathcal{M}_2 \otimes \mathcal{M}_2 \to \mathcal{M}_2 \otimes \mathcal{M}_2$ a um estado emaranhado, como o singleto

$$\psi_- = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

para se familiarizar com o efeito.

Certamente não é aceitável uma operação física que é válida apenas localmente[12]. Isso motiva a definição de mapa completamente positivo:

Definição 1.6. *Um mapa completamente positivo $\Lambda^{CP} : \mathcal{M}_m \to \mathcal{M}_n$ é um mapa positivo tal que a k-extensão trivial*

$$\mathbb{1} \otimes \Lambda^{CP} : \mathcal{M}_k \otimes \mathcal{M}_m \to \mathcal{M}_k \otimes \mathcal{M}_n$$

é um mapa positivo, para todo k natural.

Que agora garante que minhas operações terão sentido físico. Mas isso não torna inúteis os mapas positivos; de fato eles têm uma estrutura muito mais rica que os mapas completamente positivos, e uma aplicação muito interessante no problema de separabilidade, como veremos no capítulo 2. O próprio mapa transposição será bem estudado, pois ele é um mapa extremamente simples que já deixa de ser completamente positivo. Isso motiva uma definição que é num certo sentido complementar à 1.6.

Definição 1.7. *Um mapa completamente copositivo $\Lambda^{CcP} : \mathcal{M}_m \to \mathcal{M}_n$ é um mapa positivo tal que a k-extensão pela transposição*

$$T \otimes \Lambda^{CcP} : \mathcal{M}_k \otimes \mathcal{M}_m \to \mathcal{M}_k \otimes \mathcal{M}_n$$

é um mapa positivo, para todo k natural.

A complementaridade é expressa da seguinte maneira:

Teorema 1.8. *Se Λ^{CP} é completamente positivo então os mapas $\Lambda^{CP} \circ T$ e $T \circ \Lambda^{CP}$ são completamente copositivos.*

Demonstração. Pela definição, $\forall \rho \geq 0$,

$$\mathbb{1} \otimes \Lambda^{CP}(\rho) \geq 0$$

Mas como a transposição não altera o espectro,

$$0 \leq \mathbb{1} \otimes \Lambda^{CP}(\rho^T) = \mathbb{1} \otimes \Lambda^{CP} \circ T \otimes T(\rho) = T \otimes \Lambda^{CP} \circ T(\rho)$$

[11] Essa importante operação, conhecida como transposição parcial, será explorada com mais detalhes na definição 1.9.

[12] Localmente, em informação quântica, significa em uma das partes de um sistema quântico composto.

que é a definição de mapa completamente copositivo. Também podemos transpor após aplicar o mapa:

$$0 \leq \Big(\mathbb{1} \otimes \Lambda^{CP}(\rho)\Big)^T = T \otimes T\Big(\mathbb{1} \otimes \Lambda^{CP}(\rho)\Big) = T \otimes T \circ \Lambda^{CP}(\rho)$$

□

Esta definição de mapa completamente copositivo implora pela transposição parcial. Na verdade, essa operação já foi definida implicitamente, mas é útil explicitá-la e estabelecer a notação.

Definição 1.9. *Seja $Q \in \mathcal{M}_m^A \otimes \mathcal{M}_n^B$ um operador bipartite. Se escrevemos*

$$Q = \sum_{\substack{ijkl \\ kl}} q_{ij} |i\rangle\langle j| \otimes |k\rangle\langle l|$$

a transposição parcial em relação à parte A e em relação à base $|i\rangle\langle j|$ é dada por

$$Q^{T_A} := T \otimes \mathbb{1}(Q) = \sum_{\substack{ijkl \\ kl}} q_{ij} T(|i\rangle\langle j|) \otimes |k\rangle\langle l| = \sum_{\substack{ijkl \\ kl}} q_{ij} |j\rangle\langle i| \otimes |k\rangle\langle l|$$

Para ajudar a visualização, faremos a transposição parcial numa matriz arbitrária. Escrevemos Q como uma matriz por blocos:

$$Q = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1m} \\ B_{21} & B_{22} & & \\ \vdots & & \ddots & \\ B_{m1} & & & B_{mm} \end{pmatrix}$$

lembrando que cada bloco B_{ij} tem dimensão n. Sua transposição parcial fica

$$Q^{T_A} = \begin{pmatrix} B_{11} & B_{21} & \cdots & B_{m1} \\ B_{12} & B_{22} & & \\ \vdots & & \ddots & \\ B_{1m} & & & B_{mm} \end{pmatrix}$$

É fácil de perceber que não existe nada de especial com a parte em relação à qual a transposição está sendo feita. De fato

$$Q^{T_B} = \mathbb{1} \otimes T(Q) = T \otimes T(T \otimes \mathbb{1}(Q)) = \Big(Q^{T_A}\Big)^T$$

O leitor também não deve levar muito a sério o nome transposição para este mapa; a razão fica clara se tentarmos estender essa operação para agir em vetores também:

$$T(|\alpha\rangle\langle\alpha|) = |\alpha^*\rangle\langle\alpha^*| \to T|\alpha\rangle := |\alpha^*\rangle$$

o que deixa claro que o que está ocorrendo de fundamental é a conjugação complexa, e não a transposição. Esse ponto de vista permite a interpretação

física dessa operação como reversão temporal, com consequências particularmente interessantes para a transposição parcial [8]. Contudo, vamos continuar utilizando o nome de transposição, para não nos afastarmos da nomenclatura padrão da literatura.

O estudo dessa operação dominará boa parte da monografia. Vamos explicitar suas aplicações no corolário 2.7 e interpretá-la geometricamente com o teorema 4.1. Não faremos um estudo histórico; este pode ser encontrado em [9].

1.3 Análise convexa

Os três tipos de mapas apresentados na secção anterior serão largamente utilizados no restante da monografia. Uma propriedade interessante deles, e que utilizaremos para provar o principal teorema (no capítulo 2), é que seus conjuntos formam cones convexos. Portanto, precisamos fazer uma pequena recordação de conceitos de análise convexa.

Nesta secção irei demonstrar apenas um teorema. Farei isso pois a análise convexa em si não é de meu interesse (com desculpas para os especialistas), e vou necessitar apenas dos teoremas e definições mais básicos. O leitor interessado pode encontrar uma exploração bem prática desses conceitos na ref. [10], ou uma exposição matemática mais sóbria na ref. [11].

O principal objeto de estudo da análise convexa são os conjuntos convexos. Intuitivamente, eles são conjuntos nos quais podemos "misturar" seus pontos sem sair do conjunto. Esta é uma propriedade interessante do ponto de vista físico, pois vários sistemas podem ser realmente misturados.

Definição 1.10. *Um conjunto convexo é um conjunto C tal que*

$$x, y \in C \Rightarrow \lambda x + (1-\lambda)y \in C$$

para $\lambda \in [0,1]$.

Com apenas esta definição já é possível enunciar e demonstrar um teorema importante de análise convexa: o teorema do hiperplano separador. Ele afirma que dado um conjunto convexo e um ponto fora dele, sempre existe um hiperplano que os separa. Isso parece óbvio no caso de dimensão finita, e de fato o é; tanto que quase nenhum autor o demonstra. Não obstante, é útil ter seu enunciado preciso, e uma demonstração feita numa linguagem consistente com o resto do texto.

Além disso, existem vários teoremas de separação, dependendo da força das hipóteses e do tipo de separação desejada. Vou demonstrar apenas o caso mais particular que é útil para a informação quântica.

Teorema 1.11. *(Hiperplano separador)*
Seja $\mathcal{H}$ um espaço de Hilbert real[13] *de dimensão finita, $\rho \in \mathcal{H}$, e $C \subset \mathcal{H}$ convexo e compacto tal que $\rho \notin C$. Então existem $W \in \mathcal{H}, \beta \in \mathbb{R}$ tais que $\langle W, \rho \rangle < \beta$ e*

[13] A extensão para um espaço de Hilbert complexo é trivial, porém deixa de ter uma interpretação geométrica simples.

$\sigma \in C \Rightarrow \langle W, \sigma \rangle \geq \beta$. *Dizemos que o hiperplano* $\{x \in \mathcal{H} \mid \langle W, x \rangle = \beta\}$ separa ρ *do conjunto* C.

Demonstração. Seja $f : C \to \mathbb{R}, f(\sigma) = \|\sigma - \rho\|_2^2$. Então f é uma função real definida num domínio compacto, e pelo teorema de Weierstrass existe $\bar{\sigma}$ tal que $f(\bar{\sigma}) = \min f(\sigma)$.

Seja $W := \bar{\sigma} - \rho$.

1. $\langle W, \rho \rangle < \beta$. Como $\bar{\sigma} \neq \rho$, $W \neq 0$. Ou seja,

$$0 < \langle W, W \rangle = \langle W, \bar{\sigma} \rangle - \langle W, \rho \rangle$$

$$\Rightarrow \langle W, \rho \rangle < \langle W, \bar{\sigma} \rangle := \beta$$

2. $\sigma \in C \Rightarrow \langle W, \sigma \rangle \geq \beta$. Como C é um conjunto convexo, podemos construir uma família de pontos $\sigma_\lambda \in C$ fazendo uma combinação convexa de dois de seus elementos:

$$\sigma_\lambda = \lambda\sigma + (1 - \lambda)\bar{\sigma}$$

Como minimizamos f, segue que

$$f(\sigma_\lambda) \geq f(\bar{\sigma})$$

Lembrando que $\|\cdot\|_2^2 = \langle \cdot, \cdot \rangle$, expandimos:

$$\langle \lambda(\sigma - \bar{\sigma}) + \bar{\sigma} - \rho, \lambda(\sigma - \bar{\sigma}) + \bar{\sigma} - \rho \rangle \geq \langle \bar{\sigma} - \rho, \bar{\sigma} - \rho \rangle$$

e simplificamos:

$$\langle W, \sigma - \bar{\sigma} \rangle \geq -\frac{1}{2}\lambda \|\sigma - \bar{\sigma}\|_2^2$$

Podemos tomar $\lambda = 0$, chegando em

$$\langle W, \sigma \rangle \geq \langle W, \bar{\sigma} \rangle = \beta$$

□

Um tipo de conjunto convexo extremamente interessante são os cones convexos. Uma forma de construí-los é tomar um conjunto convexo D de n dimensões, mergulhado num espaço com $k > n$ dimensões. Escolha um ponto x fora do conjunto, e forme a união entre todos os raios que partem de x e passam por S. O resultado é um cone convexo (que corresponde à nossa visão intuitiva de cone), com vértice x e base D. Note que se tomarmos D como o conjunto dos estados quânticos, o cone convexo formado é equivalente a retirarmos a restrição de normalização; este conjunto é simplesmente o dos operadores positivos.

Um cone convexo fechado $\mathcal{V}$ pode ser usado para definir uma desigualdade generalizada, que é simplesmente um ordenamento parcial em $\mathcal{H}$; dizemos que

$$\mathcal{A} \succeq_{\mathcal{V}} \mathcal{B} \Leftrightarrow \mathcal{A} - \mathcal{B} \in \mathcal{V}$$

Quando o cone em questão é o cone dos operadores positivos, costuma-se usar simplesmente o símbolo $\geq$, pois de fato é a generalização natural do ordenamento padrão de $\mathbb{R}$; isso justifica a notação $\rho \geq 0$, para indicar que ρ é um operador positivo.

Conjuntos convexos compactos sempre possuem pontos especiais, que podem ser encarados como uma generalização dos vértices de um politopo:

Definição 1.12. *Um ponto puro de um conjunto convexo é um ponto que não pode ser escrito como combinação convexa de outros pontos que pertençam ao conjunto.*

Note que a definição de ponto puro não é muito interessante quando nosso conjunto convexo é um cone; o seu único ponto puro é o vértice. Para ele, utilizamos o conceito de raio extremo:

Definição 1.13. *Um raio extremo de um cone convexo é um raio que passa por um ponto puro da base.*

Definição 1.14. *Seja P um conjunto. O menor conjunto convexo C que contém todos os pontos de P é conhecido como casco convexo de P, denotado $C = \text{conv}\, P$.*

Essas definições são motivadas pela existência do teorema de Minkowski:

Teorema 1.15. *(Minkowski)*
Qualquer conjunto convexo compacto é igual ao casco convexo de seus pontos puros. Qualquer cone convexo é igual ao casco convexo de seus raios extremos.

Outro conceito muito importante em análise convexa (ou em toda a matemática) é o de cone dual. Relações de dualidade podem simplificar muitas contas, e trazer à tona relações obscuras entre áreas diferentes da matemática.

Definição 1.16. *Seja $\mathcal{V}$ um cone convexo pertencente a um espaço de Hilbert real de dimensão finita $\mathcal{H}$. Então o conjunto*

$$\mathcal{V}^* = \{A \in \mathcal{H} : \langle A, B\rangle \geq 0 \ \forall B \in \mathcal{V}\}$$

é o cone dual de $\mathcal{V}$.

Existem várias propriedades úteis dos cones duais, que são fáceis de provar porém tediosas. Irei simplesmente listá-las.

- $\mathcal{V}^*$ é sempre fechado e convexo.
- Se $\mathcal{V}$ é fechado, então $\mathcal{V}^{**} = \mathcal{V}$.
- $\mathcal{V}_1 \subseteq \mathcal{V}_2 \Rightarrow \mathcal{V}_1^* \supseteq \mathcal{V}_2^*$.
- Se $\mathcal{A}$ e $\mathcal{B}$ são cones convexos, então $\mathcal{V} = \text{conv}\, \mathcal{A} \cup \mathcal{B} \Rightarrow \mathcal{V}^* = \mathcal{A}^* \cap \mathcal{B}^*$.

Agora temos todas as nossas armas em punho. Podemos partir para a demonstração do principal teorema da monografia, e detalhar a estrutura do espaço de estados.

Capítulo 2

Teorema de Woronowicz

"Good mathematicians see analogies. Great mathematicians see analogies between analogies."

Stefan Banach

O objetivo principal deste capítulo é demonstrar o seguinte teorema:

Teorema 2.1. *(Woronowicz)*
Todo mapa positivo $\Lambda : \mathcal{M}_m \to \mathcal{M}_n$ pode ser escrito como

$$\Lambda = \Lambda_1^{CP} + \Lambda_2^{CP} \circ T \tag{2.1}$$

onde Λ_i^{CP} são completamente positivos e T é o mapa transposição, sse $mn \leq 6$

Ele foi demonstrado pela primeira vez por S.L. Woronowicz em 1976 [12], muito antes dele ter qualquer relevância para o problema da separabilidade, que nem era popular na época. Sua demonstração original está numa linguagem obscura que não permite muitas interpretações; mas se a modernizamos um pouco conseguimos ver várias idéias e teoremas que influenciaram muito a informação quântica. É este o meu objetivo ao escrever esta monografia: clarificar os fundamentos matemáticos por trás das ferramentas que utilizamos no dia-a-dia e mostrar suas interconexões fundamentais, o que sempre é um campo fértil para novas idéias.

2.1 Dualidades

É interessante e necessário, para prosseguir a demonstração, enunciar o teorema em sua forma dual:

Lema 2.2. *(Woronowicz — dual)*
O teorema 2.1 é equivalente à afirmação

$$\mathcal{P}^* = \mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$$

Demonstração. Pelo teorema 1.8 a equação (2.1) é equivalente a

$$\Lambda = \theta_1 \Lambda_1^{CP} + \theta_2 \Lambda_2^{CcP}$$

onde também estou utilizando o fato de que $\mathcal{CP}$ e $\mathcal{C}c\mathcal{P}$ são cones convexos, e $\theta_i \in R_+$. Ora, isso é simplesmente uma combinação cônica, e portanto

$$\mathcal{P} = \text{conv}(\mathcal{CP} \cup \mathcal{C}c\mathcal{P})$$

Passando para o espaço dual

$$\mathcal{P}^* = \mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$$

□

Precisamos agora detalhar quem são os cones duais $\mathcal{P}^*, \mathcal{CP}^*, \mathcal{C}c\mathcal{P}^*$. Para isso, definirei um isomorfismo[1] entre os mapas $\Lambda : \mathcal{M}_m \to \mathcal{M}_n$ e os operadores $D_\Lambda \in \mathcal{M}_{mn}$, através da fórmula

$$D_\Lambda := I \otimes \Lambda(|\phi_+\rangle\langle\phi_+|) = \sum_{i,j=0}^{m-1} |i\rangle\langle j| \otimes \Lambda(|i\rangle\langle j|)$$

onde

$$|\phi_+\rangle\langle\phi_+| := \sum_{i,j=0}^{m-1} |ii\rangle\langle jj| = \sum_{i,j=0}^{m-1} |i\rangle\langle j| \otimes |i\rangle\langle j|$$

é apenas uma base na qual é fácil trabalhar. Por exemplo, se $m = 2$, o operador D_Λ fica desta forma:

$$D_\Lambda = \begin{pmatrix} \Lambda\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \Lambda\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \Lambda\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & \Lambda\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{pmatrix}$$

Como $|i\rangle\langle j|$ forma uma base para $\mathcal{M}_m$, é evidente que D_Λ determina completamente o mapa e vice-versa. Além disso, vamos nos restringir a apenas mapas positivos, de forma que o teorema 1.5 nos garante que D_Λ será sempre auto-adjunto. Assim podemos nos restringir a um espaço de Hilbert real, e utilizar a definição 1.16 para construir o espaço dual[2]. Para os mapas completamente positivos, ela fica

$$\mathcal{CP}^* = \left\{ Q \in \mathcal{M}_{mn} : \langle Q, D_{\Lambda^{CP}} \rangle \geq 0 \ \forall \Lambda^{CP} \in \mathcal{CP} \right\}$$

ou seja, queremos os Q tais que

$$\left\langle Q, I \otimes \Lambda^{CP}(|\phi_+\rangle\langle\phi_+|) \right\rangle \geq 0$$

Como Λ^{CP} é completamente positivo, o lado direito do produto interno também o é, e $Q \geq 0$ implica que o produto interno é positivo. Para a parte somente se, suponha que Q tem um autovalor negativo. O produto interno tem de ser positivo para todo Λ^{CP}; em particular para o mapa com

[1] Este é o famoso isomorfismo de Choi-Jamiołkowski.
[2] Que vamos representar sem pejo no mesmo espaço.

o qual $I \otimes \Lambda^{CP}(|\phi_+\rangle\langle\phi_+|)$ é um projetor no autovetor associado ao autovalor negativo de Q, absurdo. Então temos o cone dual

$$\mathcal{CP}^* = \{Q \in \mathcal{M}_{mn} : Q \geq 0\} \tag{2.2}$$

que é simplesmente o cone dos estados quânticos não-normalizados.

Analogamente, para encontrar $\mathcal{CcP}^*$, analisamos a condição

$$\left\langle Q, I \otimes \Lambda^{CcP}(|\phi_+\rangle\langle\phi_+|) \right\rangle \geq 0$$

Como[3]

$$\langle T \otimes I(A), T \otimes I(B)\rangle = \langle A, T \otimes I(T \otimes I(B))\rangle = \langle A, B\rangle \tag{2.3}$$

a condição é equivalente a

$$\left\langle T \otimes I(Q), T \otimes \Lambda^{CcP}(|\phi_+\rangle\langle\phi_+|) \right\rangle \geq 0$$

Novamente, como Λ^{CcP} é completamente copositivo, o lado direito é positivo, e nossa condição se torna $Q^{T_A} \geq 0$. Assim, temos o cone

$$\mathcal{CcP}^* = \{Q \in \mathcal{M}_{mn} : Q^{T_A} \geq 0\} \tag{2.4}$$

Nos resta apenas encontrar o cone dual ao cone dos mapas positivos. Este caso é o mais delicado, e que tem implicações mais interessantes. Vou enunciá-lo como um teorema[4]:

Teorema 2.3. *(Jamiołkowski)*

$$\left\langle Q, \mathbb{1} \otimes \Lambda^{P}(|\phi_+\rangle\langle\phi_+|) \right\rangle \geq 0$$

para todo mapa positivo $\Lambda^P : \mathcal{M}_m \to \mathcal{M}_n$ *sse*

$$Q = \sum_k p_k |\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|$$

onde $|\alpha_k\rangle\langle\alpha_k| \in \mathcal{M}_m$ *e* $|\beta_k\rangle\langle\beta_k| \in \mathcal{M}_n$.

Demonstração. Se Q é dessa forma, podemos utilizar o mesmo argumento que usamos para encontrar $\mathcal{CcP}^*$, e o teorema segue. Para provar a direção conversa, sejam $\mathcal{M}_m \ni A \geq 0$ e $\mathcal{M}_n \ni B \geq 0$. Então

$$\begin{aligned} 0 &\leq \left\langle A, \Lambda^P(B)^T \right\rangle \\ &= \sum_j \langle j| A\, \Lambda^P(B)^T |j\rangle \\ &= \sum_{ij} \langle j|A|i\rangle\langle i|\Lambda^P(B)^T|j\rangle \end{aligned}$$

[3] Lembre-se que a $T^* = T$ e $T^2 = \mathbb{1}$.

[4] Este teorema foi demonstrado pela primeira vez em [13], num contexto diferente. A prova apresentada aqui é baseada na versão simplificada de [14]. A demonstração original de Woronowicz [12] prova apenas um caso particular.

$$
\begin{aligned}
&= \sum_{ij} \langle j|A|i\rangle \langle j|\Lambda^P(B)|i\rangle \\
&= \sum_{ij} \mathrm{tr}\left(A|i\rangle\langle j|\right) \mathrm{tr}\Big(\Lambda^P(B)|i\rangle\langle j|\Big) \\
&= \sum_{ij} \mathrm{tr}\Big(A|i\rangle\langle j| \otimes \Lambda^P(B)|i\rangle\langle j|\Big) \\
&= \sum_{ij} \mathrm{tr}\Big(A \otimes \Lambda^P(B)|ii\rangle\langle jj|\Big) \\
&= \mathrm{tr}\Big(A \otimes \Lambda^P(B)|\phi_+\rangle\langle\phi_+|\Big) \\
&= \Big\langle A \otimes \Lambda^P(B), |\phi_+\rangle\langle\phi_+|\Big\rangle \\
&= \Big\langle A \otimes B, \mathbb{1} \otimes \Lambda^P(|\phi_+\rangle\langle\phi_+|)\Big\rangle
\end{aligned}
$$

Como esse cálculo ainda é válido se considerarmos combinações convexas de $A \otimes B$ o teorema segue. □

Portanto, o cone dual é o cone dos estados separáveis[5]

$$\mathcal{P}^* = \left\{Q \in \mathcal{M}_{mn} : Q = \textstyle\sum_k p_k |\alpha_k\rangle\langle\alpha_k| \otimes |\beta_k\rangle\langle\beta_k|\right\} \tag{2.5}$$

É difícil subestimar a importância deste teorema. Foi reinterpretando-o que a família Horodecki conseguiu fazer um avanço crucial no problema da separabilidade [15]. Cabe enunciar sua versão:

Teorema 2.4. *(Horodecki$^{\otimes 3}$)*
Um estado $Q \in \mathcal{M}_m^A \otimes \mathcal{M}_n^B$ é separável sse

$$\mathbb{1} \otimes \Lambda^P(Q) \geq 0$$

para todo mapa positivo $\Lambda^P : \mathcal{M}_n \to \mathcal{M}_m$.

Demonstração. Se $\mathbb{1} \otimes \Lambda^P(Q) \geq 0$, $\langle \mathbb{1} \otimes \Lambda^P(Q), P\rangle \geq 0$ para qualquer projetor P, e em particular para $P = |\phi_+\rangle\langle\phi_+|$. Ou seja,

$$0 \leq \Big\langle \mathbb{1} \otimes \Lambda^P(Q), |\phi_+\rangle\langle\phi_+|\Big\rangle = \Big\langle Q, \mathbb{1} \otimes \Lambda^{P*}(|\phi_+\rangle\langle\phi_+|)\Big\rangle$$

que é a hipótese do teorema 2.3. □

[5] Esses p_k são apenas coeficientes de uma combinação convexa, como aparece na definição 1.3, e não autovalores.

2.2 Preparação

De posse dos cones duais $\mathcal{CP}^*$ (2.2), $\mathcal{C}c\mathcal{P}^*$ (2.4) e $\mathcal{P}^*$ (2.5), agora podemos transformar o lema 2.2 em uma afirmação mais concreta que saberemos demonstrar. Farei isso através do

Lema 2.5. *As seguintes afirmações são equivalentes:*

I $\mathcal{P}^* = \mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$

II *Para todo* $Q \in \mathcal{M}_m^A \otimes \mathcal{M}_n^B$ *tal que* $Q \geq 0$, $Q^{T_A} \geq 0$ *existe um vetor produto* $|\alpha\rangle|\beta\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n$ *tal que* $|\alpha\rangle|\beta\rangle \in \operatorname{Im} Q$ *e* $|\alpha^*\rangle|\beta\rangle \in \operatorname{Im} Q^{T_A}$.

Demonstração.

I $\Rightarrow$ **II** Se $Q \in \mathcal{P}^*$,

$$Q = \sum p_n |\alpha_n\rangle\langle\alpha_n| \otimes |\beta_n\rangle\langle\beta_n|$$
$$Q^{T_A} = \sum p_n |\alpha_n^*\rangle\langle\alpha_n^*| \otimes |\alpha_n\rangle\langle\beta_n|$$

Portanto, para cada n,

$$|\alpha_n\rangle|\beta_n\rangle \in \operatorname{Im} Q$$
$$|\alpha_n^*\rangle|\beta_n\rangle \in \operatorname{Im} Q^{T_A}$$

II $\Rightarrow$ **I** Se $|\alpha\rangle|\beta\rangle \in \operatorname{Im} Q$ e $|\alpha^*\rangle|\beta\rangle \in \operatorname{Im} Q^{T_A}$ é verdade que existe um $\varepsilon > 0$ tal que $Q - \varepsilon|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|$ é um operador positivo, e sua transposta parcial $Q^{T_A} - \varepsilon|\alpha^*\rangle\langle\alpha^*| \otimes |\beta\rangle\langle\beta|$ também; assim pertence a $\mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$. Pois para satisfazer a condição de positividade

$$0 \leq \langle\phi|Q - \varepsilon|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta||\phi\rangle = \langle\phi|Q|\phi\rangle - \varepsilon|\langle\phi|\alpha\beta\rangle|^2$$

e a análoga para a Q_A^T é suficiente tomar

$$\varepsilon \leq \min \frac{\lambda_\phi}{|\langle\phi|\alpha\beta\rangle|^2}$$

onde a minimização é feita nos autovetores da imagem de ambos os operadores. Agora podemos exigir que Q seja um raio extremo de $\mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$. Mas acabamos de escrever uma decomposição dele. Para não entrar em contradição, é necessário que

$$Q = \lambda|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|$$

um elemento de $\mathcal{P}^*$. Como um cone é simplesmente a combinação cônica de seus raios extremos, $\mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^* \subset \mathcal{P}^*$. Como trivialmente $\mathcal{P}^* \subset \mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$, o lema segue. □

2.3 Demonstração

Agora vamos demonstrar a afirmação **II**. Até agora, os teoremas que provei eram válidos para qualquer dimensão finita, mas o lema a seguir só é verdadeiro para $\dim \mathcal{M}_m^A \otimes \mathcal{M}_n^B \leq 6$. Ademais, precisaremos escolher uma dimensão específica para trabalhar. Os casos não-triviais[6] são $Q \in \mathcal{M}_2^A \otimes \mathcal{M}_2^B$ e $Q \in \mathcal{M}_2^A \otimes \mathcal{M}_3^B$. Provarei apenas o primeiro caso, pois até onde sei sua demonstração explícita não consta da literatura. Para o segundo caso a prova é bastante semelhante, porém muito maior; o leitor interessado pode estender a prova por conta própria ou seguir a demonstração apresentada em [12].

Um aviso. Aqui terminam as provas elegantes e interessantes. A prova do próxima lema será por exaustão.

Lema 2.6. *Para todo $Q \in \mathcal{M}_2^A \otimes \mathcal{M}_2^B$ tal que $Q \geq 0$, $Q^{T_A} \geq 0$ existe um vetor produto $|\alpha\rangle|\beta\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ tal que $|\alpha\rangle|\beta\rangle \in \operatorname{Im} Q$ e $|\alpha^*\rangle|\beta\rangle \in \operatorname{Im} Q^{T_A}$.*

Demonstração. Primeiro note que se Q é positivo,

$$Q = \begin{pmatrix} A & B \\ B^* & C \end{pmatrix}$$

onde $A, C \geq 0$, pois

$$\begin{pmatrix} \langle\psi| & 0 \end{pmatrix} \begin{pmatrix} A & B \\ B^* & C \end{pmatrix} \begin{pmatrix} |\psi\rangle \\ 0 \end{pmatrix} = \langle\psi|A|\psi\rangle \geq 0$$

e o mesmo argumento se aplica a C.

Esse é o formato geral do Q com o qual trabalharemos. A estratégia da prova será primeiro considerar os casos mais simples: A e C não-inversíveis ou B normal. A partir disso utilizarei a hipótese de inversibilidade de A para simplificar a forma de Q, o que nos permitirá encontrar uma condição algébrica para determinar a existência dos vetores produto. Validando essa condição para todos os casos possíveis provamos o lema.

2.3.1 A e C não-inversíveis

Se pelo menos um deles não for inversível, *e.g.*, $A|x\rangle = 0$, segue que

$$\langle 0|\langle x|Q|0\rangle|x\rangle = \begin{pmatrix} \langle x| & 0 \end{pmatrix} \begin{pmatrix} A & B \\ B^* & C \end{pmatrix} \begin{pmatrix} |x\rangle \\ 0 \end{pmatrix} = \begin{pmatrix} \langle x| & 0 \end{pmatrix} \begin{pmatrix} B^*|x\rangle \\ 0 \end{pmatrix} = 0$$

Como $Q \geq 0$, isso implica que $Q|0\rangle|x\rangle = 0$ e $B^*|x\rangle = 0$. Aplicando o mesmo raciocínio em Q^{T_A}, descobrimos que $B|x\rangle = 0$. Como o espaço é bidimensional, existe um único[7] $|\beta\rangle$ tal que $\langle\beta|x\rangle = 0$. Ou seja, $B = \lambda|y\rangle\langle\beta|$, para um $|y\rangle$ qualquer. Mas $B^* = \lambda^*|\beta\rangle\langle y| \Rightarrow |y\rangle = |\beta\rangle$. Também segue que $A = \gamma|\beta\rangle\langle\beta|$, $\gamma \geq 0$.

[6] O caso $\mathcal{M}_3^A \otimes \mathcal{M}_2^B$ pode ser obtido a partir do caso $\mathcal{M}_2^A \otimes \mathcal{M}_3^B$ passando-se para o mapa adjunto.

[7] A menos de uma fase global.

Se aplicarmos Q ao vetor $|0\rangle|\beta\rangle$, nosso problema está resolvido:

$$Q|0\rangle|\beta\rangle = \begin{pmatrix} \gamma|\beta\rangle\langle\beta| & \lambda|\beta\rangle\langle\beta| \\ \lambda^*|\beta\rangle\langle\beta| & C \end{pmatrix}\begin{pmatrix} |\beta\rangle \\ 0 \end{pmatrix} = \begin{pmatrix} \gamma|\beta\rangle \\ \lambda^*|\beta\rangle \end{pmatrix} = \begin{pmatrix} \gamma \\ \lambda^* \end{pmatrix} \otimes |\beta\rangle := |\alpha\rangle|\beta\rangle$$

$$Q^{T_A}|0\rangle|\beta\rangle = \begin{pmatrix} \gamma|\beta\rangle\langle\beta| & \lambda^*|\beta\rangle\langle\beta| \\ \lambda|\beta\rangle\langle\beta| & C \end{pmatrix}\begin{pmatrix} |\beta\rangle \\ 0 \end{pmatrix} = \begin{pmatrix} \gamma|\beta\rangle \\ \lambda|\beta\rangle \end{pmatrix} = \begin{pmatrix} \gamma \\ \lambda \end{pmatrix} \otimes |\beta\rangle = |\alpha^*\rangle|\beta\rangle$$

Note que esta prova é falsa se $\gamma = \lambda = 0$, mas este caso é trivial.

2.3.2 Mudança de base

Agora podemos fazer uma mudança de base no espaço de Bob:

$$Q' = \mathbb{1} \otimes A^{-1/2}\, Q\, \mathbb{1} \otimes A^{-1/2} = \begin{pmatrix} \mathbb{1} & B' \\ B'^* & C' \end{pmatrix}$$

Onde

$$B' := A^{-1/2}BA^{-1/2} \quad \text{e} \quad C' := A^{-1/2}CA^{-1/2}$$

Como C' mantém as propriedades de C de ser positivo e inversível, e B continua auto-adjunto, vou ignorar os $'$ para não carregar a notação.

Veja que podemos trabalhar somente com Q', pois se $|\alpha\rangle|\beta'\rangle \in \operatorname{Im} Q'$ tal que $|\alpha^*\rangle|\beta'\rangle \in \operatorname{Im} Q'^{T_A}$ segue que

$$|\alpha\rangle|\beta\rangle = \mathbb{1} \otimes A^{1/2}|\alpha\rangle|\beta'\rangle$$

é um vetor produto na imagem de Q com as propriedades desejadas.

2.3.3 B normal

Se B é um operador normal, $\exists|\beta\rangle;\ B|\beta\rangle = t|\beta\rangle$ e $B^*|\beta\rangle = t^*|\beta\rangle$, e assim nosso problema está resolvido:

$$Q'|0\rangle|\beta\rangle = \begin{pmatrix} |\beta\rangle \\ t^*|\beta\rangle \end{pmatrix}$$

$$Q'^{T_A}|0\rangle|\beta\rangle = \begin{pmatrix} |\beta\rangle \\ t|\beta\rangle \end{pmatrix}$$

2.3.4 Condição algébrica

Vamos agora encarar o caso não-trivial. Aplicamos Q' ao seguinte *ansatz*:

$$\begin{pmatrix} \mathbb{1} & B \\ B^* & C \end{pmatrix}\begin{pmatrix} |\beta\rangle + B|y\rangle \\ -|y\rangle \end{pmatrix} = \begin{pmatrix} |\beta\rangle \\ B^*|\beta\rangle - (C - B^*B)|y\rangle \end{pmatrix}$$

Para que o vetor resultante seja um vetor produto é necessário e suficiente que

$$B^*|\beta\rangle - (C - B^*B)|y\rangle = t|\beta\rangle$$

para algum $t \in \mathbb{C}$. Um *ansatz* análogo serve para Q'^{T_A}:

$$\begin{pmatrix} \mathbb{1} & B^* \\ B & C \end{pmatrix}\begin{pmatrix} |\beta\rangle + B^*|y\rangle \\ -|y\rangle \end{pmatrix} = \begin{pmatrix} |\beta\rangle \\ B^*|\beta\rangle - (C - BB^*)|y\rangle \end{pmatrix}$$

e queremos que o resultante, além de produto, obedeça à condição do teorema:

$$B^*|\beta\rangle - (C - BB^*)|y\rangle = t^*|\beta\rangle$$

Para decidir sobre a existência do t, vale estudar os operadores $C - B^*B$ e $C - BB^*$. É fácil perceber que ambos são auto-adjuntos, e portanto o complemento ortogonal de seu núcleo é a imagem. Assim reformulamos a questão:

$$(B^* - t\mathbb{1})|\beta\rangle = (C - B^*B)|y\rangle \Leftrightarrow (B^* - t\mathbb{1})|\beta\rangle \perp \ker(C - B^*B)$$

ou equivalentemente

$$|\beta\rangle \perp (B - t^*\mathbb{1}) \ker(C - B^*B)$$

e

$$|\beta\rangle \perp (B^* - t\mathbb{1}) \ker(C - BB^*)$$

onde devemos entender o lado direito como o operador $B - t^*\mathbb{1}$ aplicado a cada elemento do núcleo.

Ora, isso é simplesmente uma questão sobre a dimensionalidade do espaço H_t gerado por $(B - t^*\mathbb{1}) \ker(C - B^*B)$ e $(B^* - t\mathbb{1}) \ker(C - BB^*)$. Como estamos tratando de um espaço de dimensão 2, só pode existir um vetor no complemento ortogonal se

$$\dim H_t < 2$$

Vamos separar esta questão em casos. Seja $n = \dim \ker(C - B^*B)$ e $n^\star = \dim \ker(C - BB^*)$:

Caso 1. $n + n^\star \leq 1$

Este caso é trivial.

Caso 2. $n = 2$ **ou** $n^\star = 2$

Lembrando que $Q' \geq 0$, note que

$$0 \leq \begin{pmatrix} \langle x| & \langle y| \end{pmatrix} \begin{pmatrix} \mathbb{1} & B \\ B^* & C \end{pmatrix} \begin{pmatrix} |x\rangle \\ |y\rangle \end{pmatrix} = \big\| |x\rangle + B|y\rangle \big\|_2^2 + \langle y|C - B^*B|y\rangle$$

e portanto $C - B^*B \geq 0$. Equivalentemente, $C - BB^* \geq 0$.

Por concreteza, tome $n = 2$. Neste caso, $C - B^*B = 0$, e seu traço é nulo. Mas pela propriedade cíclica $0 = \mathrm{tr}(C - B^*B) = \mathrm{tr}(C - BB^*)$. Como $C - BB^*$ é positivo, o traço nulo implica que $C - BB^* = 0$. Ora, temos então que $B^*B = C = BB^*$, e portanto B é um operador normal, caso que já foi examinado. Note que $C - BB^* = 0$ também implica que $n^\star = 2$, ou seja, $n = 2 \Leftrightarrow n^\star = 2$, e portanto o único caso restante é $n = n^\star = 1$.

Caso 3. $n = n^\star = 1$

Este caso é o mais difícil. Primeiramente, note que $C - B^*B$ e $C - BB^*$ são operadores positivos de posto 1, ou seja

$$C - B^*B = \lambda|x\rangle\langle x|$$
$$C - BB^* = \gamma|y\rangle\langle y|$$

Além disso, $\lambda - \gamma = \mathrm{tr}(C - B^*B) - \mathrm{tr}(C - BB^*) = 0$, portanto $\lambda = \gamma$. Disso vem

$$BB^* - B^*B = \lambda(|x\rangle\langle x| - |y\rangle\langle y|) \tag{2.6}$$

Queremos que $\dim H_t < 2$, e para isso necessitamos que

$$(B - t^*\mathbb{1})|\hat{x}\rangle \text{ e } (B^* - t\mathbb{1})|\hat{y}\rangle \tag{2.7}$$

sejam linearmente dependentes, para algum t. Onde $|\hat{x}\rangle$ ($|\hat{y}\rangle$) é um vetor ortogonal a $|x\rangle$ ($|y\rangle$), que portanto gera o núcleo de $C - B^*B$ ($C - BB^*$).

Para tal, vamos simplificar a representação de B fazendo mais uma mudança de base em Q, desta vez no espaço de Alice[8]:

$$Q'' = \begin{pmatrix} 1 & -\alpha^* \\ \alpha & 1 \end{pmatrix} \otimes \mathbb{1}\, Q' \begin{pmatrix} 1 & \alpha^* \\ -\alpha & 1 \end{pmatrix} \otimes \mathbb{1}$$

Estamos interessados no efeito em B:

$$B'' = -{\alpha^*}^2 B^* - \alpha^*(\mathbb{1} - C) + B$$

Cada componente de B'' vai ser determinada por um polinômio de segundo grau em α^*, e $\det B''$ por um polinômio de quarto grau, que possui raízes em $\mathbb{C}$. Assim, posso escolher α de forma que B'' seja de posto um, podendo ser escrito como $B'' = \gamma|f\rangle\langle g|$. Ignorando novamente o $'$ e substituindo na equação (2.6), encontramos

$$B = \gamma|x\rangle\langle y|$$
$$B^* = \gamma^*|y\rangle\langle x|$$

e, substituindo isso na equação (2.7), necessitamos que os vetores

$$\gamma\langle y|\hat{x}\rangle|x\rangle - t^*|\hat{x}\rangle \text{ e } \gamma^*\langle x|\hat{y}\rangle|y\rangle - t|\hat{y}\rangle$$

sejam linearmente dependentes. Para decidir sobre a existência de t, vamos assumir $\{|x\rangle, |\hat{x}\rangle\}$ como a base computacional $\{|0\rangle, |1\rangle\}$, e deixar $\{|y\rangle, |\hat{y}\rangle\}$ arbitrário[9]:

$$|y\rangle = a|0\rangle + be^{i\beta}|1\rangle$$
$$|\hat{y}\rangle = b|0\rangle - ae^{-i\beta}|1\rangle$$

[8] Novamente, os vetores que encontrarmos para Q'' podem ser facilmente transformados em vetores que servem para Q'.

[9] Estou deixando livres a normalização e a fase global, que são irrelevantes para decidir dependência linear

Fazendo a matriz dos vetores e calculando a condição para que o determinante se anule, chegamos na seguinte equação:

$$|\gamma|^2 b^3 + t\gamma abe^{-2i\beta} + t^*\gamma^* ab - |t|^2 b = 0$$

que se separa naturalmente numa condição que depende somente do módulo de t e noutra que depende somente da fase:

$$|t|^2 = |\gamma|^2 b$$

$$t\gamma e^{-2i\beta} + t^*\gamma^* = 0$$

E portanto para todo $|x\rangle$, $|y\rangle$ existe um t tal que

$$(B - t^*\mathbb{1})\ker(C - B^*B) \text{ e } (B^* - t\mathbb{1})\ker(C - BB^*)$$

são linearmente dependentes, e assim $\dim H_t < 2$.

Como consideramos todos os casos possíveis, o lema está provado. □

2.4 Dimensões mais altas

Por enquanto, provamos apenas que a decomposição $\Lambda = \Lambda^{CP} + \Lambda^{CcP}$ é válida para $\mathcal{M}_2^A \otimes \mathcal{M}_2^B$, e afirmamos que ela é válida $\mathcal{M}_2^A \otimes \mathcal{M}_3^B$; mas o que nos garante que ela não é válida em dimensões mais altas? Nestes casos, conhecemos contra-exemplos. Note que necessitamos de apenas dois para demonstrar que em todas as dimensões mais altas existem mapas não-decomponíveis: um para $\mathcal{M}_3^A \otimes \mathcal{M}_3^B$ e outro para $\mathcal{M}_2^A \otimes \mathcal{M}_4^B$. Qualquer mapa de dimensão mais alta incluirá um mapa dessas dimensões como caso particular, herdando assim a não-decomponibilidade.

Para o caso $\mathcal{M}_3^A \otimes \mathcal{M}_3^B$ o exemplo canônico é o mapa de Choi [16], que foi inclusive o primeiro mapa não-decomponível a ser descoberto. Este mapa foi estudado e estendido por vários autores. De particular importância é o trabalho de Kossakowski [17], que criou uma classe grande de mapas com elegante interpretação geométrica. Para $\mathcal{M}_2^A \otimes \mathcal{M}_4^B$ a existência de um contra-exemplo foi provada pelo próprio Woronowicz [12], e uma construção explícita dada por Tang [18].

A busca por mapas não-decomponíveis continua ativa, por conta de sua capacidade de detectar estados emaranhados que escapam ao critério da transposta parcial positiva (PPT).

2.5 Transposta parcial positiva[10]

Este é de longe o critério de separabilidade mais famoso e mais utilizado. Embora ele seja um simples corolário do teorema de Woronowicz, historicamente sua demonstração apareceu de forma diferente [9, 15, 19].

Corolário 2.7. *(Transposta parcial positiva)*
Um estado $\sigma \in \mathcal{M}_m^A \otimes \mathcal{M}_n^B, mn \leq 6$, é separável sse $\sigma^{T_A} \geq 0$. Equivalentemente, se ρ^{T_A} não é positivo, então ρ é emaranhado.

[10] Este critério de separabilidade também é conhecido como critério de Peres-Horodecki.

Demonstração. O lema 2.2 nos garante que o teorema de Woronowicz é equivalente à afirmação

$$\mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^* = \mathcal{P}^*$$

Ora, como $\mathcal{CP}^*$ é simplesmente o cone dos estados quânticos, $\mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$ é o cone dos estados quânticos com transposta parcial positiva. $\mathcal{P}^*$ é o cone dos estados separáveis. Então, a afirmação $\mathcal{P}^* = \mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$ é simplesmente a afirmação de que um estado é separável sse sua transposta parcial é positiva. □

Corolário 2.8. *(Emaranhamento preso)*
Se $mn > 6$, existe $\rho \in \mathcal{M}_m^A \otimes \mathcal{M}_n^B$ tal que ρ é emaranhado e $\rho^{T_A} \geq 0$.

Demonstração. A existência de mapas não-decomponíveis nessas dimensões implica $\mathcal{P}^* \neq \mathcal{CP}^* \cap \mathcal{C}c\mathcal{P}^*$; portanto existem estados emaranhados com transposição parcial positiva. □

O curioso nome "emaranhamento preso" é devido ao fato de que estados emaranhados com transposição parcial positiva (PPTE) não podem ser utilizados facilmente como recurso para os protocolos quânticos de comunicação[11], por motivos que fogem ao escopo deste texto. O leitor interessado pode encontrar uma boa discussão do assunto na ref. [21], assim como no artigo original [22].

Podemos deixar mais clara a relação entre estados PPTE e decomponibilidade com mais um pequeno teorema:

Teorema 2.9. *Seja Λ^P um mapa positivo Woronowicz-decomponível e ρ um estado PPTE. Então $\mathbb{1} \otimes \Lambda^P(\rho) \geq 0$.*

Demonstração. Se Λ^P é decomponível, então $\Lambda^P = \Lambda_1^{CP} + \Lambda_2^{CP} \circ T$, e

$$\mathbb{1} \otimes \Lambda^P(\rho) = \mathbb{1} \otimes \Lambda_1^{CP}(\rho) + \mathbb{1} \otimes \Lambda_2^{CP}(\rho^{T_B})$$

Como Λ_1^{CP} é completamente positivo, o primeiro termo é positivo, e como ρ é PPTE, $\rho^{T_B} \geq 0$. Assim o segundo termo também é positivo, e o teorema segue por convexidade. □

Portanto, precisamos de mapas não-decomponíveis para sermos capazes de detectar o emaranhamento de estados PPTE. Porém, eles são notoriamente difíceis de ser obtidos; uma área de pesquisa que tem se mostrado muito mais frutífera em sua detecção é o estudo de testemunhas de emaranhamento.

[11] Existe uma vasta literatura sobre as aplicações do emaranhamento. Uma introdução moderna pode ser encontrada na ref. [20].

Capítulo 3

Testemunhas de emaranhamento

"O que importa é o clique no detector."
Reinaldo O. Vianna

Definição 3.1. *Uma testemunha de emaranhamento W é um operador auto-adjunto tal que* $\mathrm{tr}(W\sigma) \geq 0$ *para todo* $\sigma \in S$*, onde* S *é o conjunto dos estados separáveis. Dizemos que* W testemunha *o emaranhamento de* ρ *se* $\mathrm{tr}(W\rho) < 0$*.*

Alguns autores gostam de exigir também que as testemunhas tenham ao menos um autovalor negativo, para que elas sempre sejam capazes de detectar algum estado emaranhado. Mas isso atrapalharia a dualidade que faremos com os mapas positivos, sem nenhum ganho teórico.

3.1 Existência

O que torna as testemunhas de emaranhamento interessantes é que elas de fato existem; e, ao contrário dos mapas positivos, elas podem ser implementadas em laboratório. Lembre-se que operações físicas são associadas a mapas completamente positivos: o caso interessante de um mapa positivo que não é completamente positivo por definição deixa de ser físico. Já a testemunha é apenas um operador auto-adjunto, e portanto um observável quântico perfeitamente válido. Elas também possuem uma interpretação geométrica simples, que espero deixar clara com uma prova de sua existência:

Teorema 3.2. *Para todo estado emaranhado* ρ *existe uma testemunha de emaranhamento* W *tal que* $\mathrm{tr}(W\rho) < 0$*.*

Demonstração. De acordo com a secção 1.1, o conjunto S dos estados separáveis é compacto, convexo e disjunto do conjunto E dos estados emaranhados. Logo, se considerarmos um estado emaranhado $\rho \in E$, podemos aplicar o teorema 1.11: existe um operador W tal que $\langle W, \rho\rangle < \beta$ e $\sigma \in S \Rightarrow \langle W, \sigma\rangle \geq \beta$. Ademais, pela construção exibida em 1.11, W é a diferença entre dois operadores positivos, e portanto auto-adjunto. Finalmente, utilizamos a condição de traço unitário dos estados quânticos: se $\mathrm{tr}(W\rho) < \beta$ podemos

definir um novo operador $W' = W - \mathbb{1}\beta$, tal que

$$\mathrm{tr}(W'\rho) = \mathrm{tr}(W\rho) - \beta\,\mathrm{tr}(\rho) < 0$$

e o mesmo argumento vale para σ. Portanto, W' é a nossa testemunha de emaranhamento. □

Essa prova peca pelo fato de utilizar uma hipótese desnecessária: a condição do traço unitário. A mostrei primeiro por conta de sua elementaridade, e por ser bastante geométrica. Vou demonstrar esse teorema mais duas vezes: a segunda prova[1] enfatiza mais a fisicalidade das testemunhas, e faz uma curiosa conexão com o teorema minimax[2]. A terceira prova é completamente abstrata, mas retira a hipótese desnecessária.

Para fazer a segunda, precisamos antes da generalização de um teorema da teoria clássica da informação, presente no cap. 9 da ref. [7]:

Teorema 3.3. *Sejam $\rho, \sigma, A \in \mathcal{M}_n$, tais que ρ e σ são estados quânticos e A um operador positivo tal que $A \leq \mathbb{1}$. Então*

$$\max_A \mathrm{tr}(A(\sigma - \rho)) = \frac{1}{2}\|\sigma - \rho\|_1$$

onde $\|\sigma - \rho\|_1$ é a norma do traço, definida por

$$\|B\|_1 := \mathrm{tr}|B| := \mathrm{tr}\sqrt{B^*B}$$

Demonstração. Como ρ e σ são positivos, sua diferença é um operador autoadjunto, que possui decomposição espectral. Então autovalores diferentes dão origem a vetores ortogonais; em particular o autoespaço associado aos autovalores positivos é ortogonal ao autoespaço dos autovalores negativos. Então é claro que podemos escrever $\sigma - \rho = Q - S$, onde Q e S são operadores positivos com suporte ortogonal. Isso implica que $|\sigma - \rho| = Q + S$, e portanto $\|\sigma - \rho\|_1 = \mathrm{tr}(Q) + \mathrm{tr}(S)$. Mas $0 = \mathrm{tr}(\sigma - \rho) = \mathrm{tr}(Q - S) \Rightarrow \mathrm{tr}(Q) = \mathrm{tr}(S)$, e assim $\|\sigma - \rho\|_1 = 2\,\mathrm{tr}(Q)$.

Seja P o projetor no suporte de Q. Lembre-se qualquer projetor obedece à condição $0 \leq P \leq \mathbb{1}$. Então

$$\mathrm{tr}(P(\sigma - \rho)) = \mathrm{tr}(P(Q - S)) = \mathrm{tr}(Q) = \frac{1}{2}\|\sigma - \rho\|_1$$

Para completar, seja $0 \leq A \leq \mathbb{1}$. Então

$$\mathrm{tr}(A(Q - S)) \leq \mathrm{tr}(AQ) = \mathrm{tr}((\mathbb{1} - (\mathbb{1} - A))Q) \leq \mathrm{tr}(Q) = \frac{1}{2}\|\sigma - \rho\|_1$$

□

Para conveniência do leitor, darei também um enunciado preciso do minimax.

[1] Agradeço ao Fernando Brandão por ela.

[2] A demonstração de uma de suas formas, bem como uma discussão histórica, pode ser encontrada na ref. [23].

Teorema 3.4. *(minimax)*
Sejam M, N conjuntos convexos e compactos, pertencentes a um espaço de Hilbert de dimensão finita. Seja $f : M \times N \to \mathbb{R}$ uma função bilinear. Então

$$\max_{\mu\in M}\min_{\nu\in N} f(\mu,\nu) = \min_{\nu\in N}\max_{\mu\in M} f(\mu,\nu)$$

Agora podemos refazer a demonstração do teorema 3.2.

Teorema 3.2. *Para todo estado emaranhado ρ existe uma testemunha de emaranhamento W tal que* $\operatorname{tr}(W\rho) < 0$.

Demonstração. Seja M o conjunto dos $0 \leq A \leq \mathbb{1}$. M é convexo e compacto, tendo os projetores de posto 1 como pontos puros. Seja S o conjunto dos estados separáveis, $\sigma \in S$, $\rho \notin S$. Quero achar um A tal que para todo $\sigma \in S$, $\operatorname{tr}(A(\sigma-\rho)) \geq \beta$. Ou seja, quero achar uma cota inferior para

$$\begin{aligned}\max_{A\in M}\min_{\sigma\in S}\operatorname{tr}(A(\sigma-\rho)) &= \min_{\sigma\in S}\max_{A\in M}\operatorname{tr}(A(\sigma-\rho))\\ &= \min_{\sigma\in S}\frac{1}{2}\|\sigma-\rho\|_1\\ &:= \beta > 0\end{aligned}$$

onde usei os teoremas 3.4, 3.3 e o de Weierstrass, respectivamente.

Seja $\mu := \operatorname{tr} A\rho$. Então $\operatorname{tr}(A(\sigma-\rho)) \geq \beta \Rightarrow \operatorname{tr}((A-\mathbb{1}\mu-\mathbb{1}\beta)\sigma) \geq 0$, e $\operatorname{tr}((A-\mathbb{1}\mu-\mathbb{1}\beta)\rho) = -\beta < 0$. Portanto $W := A-\mathbb{1}\mu-\mathbb{1}\beta$ é nossa testemunha de emaranhamento. □

A fisicalidade mencionada anteriormente deve-se ao fato de que qualquer $0 \leq A \leq \mathbb{1}$ é um operador de medição válido, e $\operatorname{tr}(A\rho)$ a fórmula quintessencial da medição quântica; a demonstração constrói-se em torno da distinguibilidade de σ e ρ através de uma medição.

Agora vamos começar a terceira demonstração. Ela é simplesmente uma reinterpretação do teorema 2.3: note que ele encontrou uma certa classe de operadores auto-adjuntos que são positivos nos estados separáveis. Ora, isso é equivalente à definição que acabamos de dar para as testemunhas de emaranhamento!

Teorema 3.2. *Para todo estado emaranhado ρ existe uma testemunha de emaranhamento W tal que* $\operatorname{tr}(W\rho) < 0$.

Demonstração. Como o cone dual ao cone dos estados separáveis é formado pelos operadores da forma

$$W = \mathbb{1} \otimes \Lambda^P(|\phi_+\rangle\langle\phi_+|) \tag{3.1}$$

isso significa que $\langle\sigma, W\rangle \geq 0$ para todo W e todo σ separável, e que para todo estado ρ que não pertence ao cone dos separáveis existe pelo menos um operador W para o qual $\langle\rho, W\rangle < 0$. □

Da mesma forma, podemos reescrever o teorema 2.4 em termos das testemunhas de emaranhamento:

Teorema 3.5. *Um estado é separável sse* $\operatorname{tr}(W\sigma) \geq 0$ *para toda testemunha de emaranhamento W.*

3.2 Comparação

Com a existência das testemunhas bem estabelecida, podemos começar a explorar suas propriedades. Ora, temos duas ferramentas similares de detecção de emaranhamento: as testemunhas e os mapas positivos; é natural, então fazer essa exploração por contraste.

Primeiramente, note que nem a definição 3.1 nem nenhuma das provas do teorema 3.2 fizeram referência às partições do espaço de estados; então podemos concluir que as testemunhas são capazes de detectar emaranhamento multipartite. Isso também é verdade para os mapas positivos, mas o teste e a demonstração são mais delicados [24].

Outra coisa que nos vem à mente é: sabemos que o mapa transposição é capaz de detectar todos os estados emaranhados $\rho \in \mathcal{M}_2^A \otimes \mathcal{M}_2^B$. O mesmo pode ser verdade para alguma testemunha? A resposta é não.

Teorema 3.6. *Nenhuma testemunha de emaranhamento é capaz de detectar todos os estados emaranhados de uma dada dimensão.*

Demonstração. Na secção 1.1 descobrimos que o conjunto dos estados emaranhados E não é convexo. Logo, existem $\rho, \varrho \in E$ tais que $\lambda\rho + (1-\lambda)\varrho \notin E$ para algum $\lambda \in [0,1]$. Suponha que exista uma testemunha W capaz de detectar esses dois estados. Então

$$\operatorname{tr}(W\rho) < 0 \text{ e } \operatorname{tr}(W\varrho) < 0$$

e

$$\operatorname{tr}(W(\lambda\rho + (1-\lambda)\varrho)) = \lambda \operatorname{tr}(W\rho) + (1-\lambda)\operatorname{tr}(W\varrho) < 0$$

absurdo. □

Neste sentido os mapas são muito mais poderosos que as testemunhas.

Sabemos da limitação dos mapas decomponíveis em relação ao emaranhamento preso. Será que existe uma limitação análoga para as testemunhas?

Teorema 3.7. *Uma testemunha é da forma*

$$W = P + Q^{T_B}$$

onde $P, Q \geq 0$ sse seu mapa correspondente é decomponível. Testemunhas desta forma são chamadas decomponíveis.

Demonstração. Usando a equação (3.1),

$$\begin{aligned} W &= \mathbb{1} \otimes \Lambda^P(|\phi_+\rangle\langle\phi_+|) \\ &= \mathbb{1} \otimes \Lambda_1^{CP}(|\phi_+\rangle\langle\phi_+|) + \mathbb{1} \otimes T\Big(\mathbb{1} \otimes \Lambda_2^{CP}(|\phi_+\rangle\langle\phi_+|)\Big) \\ &= P + \mathbb{1} \otimes T(Q) \\ &= P + Q^{T_B} \end{aligned}$$

□

Disso segue diretamente que uma testemunha é não-decomponível sse seu mapa correspondente é não-decomponível.

Teorema 3.8. *Testemunhas decomponíveis não são capazes de detectar estados com emaranhamento preso.*

Demonstração.

$$\begin{aligned}\mathrm{tr}(W\rho) &= \mathrm{tr}(P\rho) + \mathrm{tr}(Q^{T_B}\rho) \\ &\geq \mathrm{tr}(Q^{T_B}\rho) \\ &= \langle \mathbb{1} \otimes T(Q), \rho \rangle \\ &= \langle Q, \mathbb{1} \otimes T(\rho) \rangle \\ &= \mathrm{tr}(Q\rho^{T_B}) \geq 0\end{aligned}$$

onde usamos a equação (2.3) no penúltimo passo. □

Vemos que as testemunhas e os mapas estão intimamente ligados; a existência de uma testemunha que detecta um dado estado pode ser utilizada para descobrir mapa positivo que também o detecta, e vice-versa. Portanto, não podemos pesquisar um esperando um milagre que não ocorreria na pesquisa do outro. Em particular, como o problema da separabilidade é NP-HARD a descoberta de um algoritmo eficiente para resolvê-lo, seja através de mapas ou de testemunhas, seria equivalente a uma prova que P = NP. Não obstante, as testemunhas são muito mais flexíveis na prática; ao contrário dos mapas positivos, conhecemos algoritmos probabilísticos para encontrá-las no caso mais geral [1, 25]. Além disso, elas permitem um conhecimento mais detalhado da estrutura do espaço de estados, pois podem ser utilizadas para implementar uma grande família de quantificadores de emaranhamento [26], que inclui vários dos mais conhecidos.

Capítulo 4

Geometria do espaço de estados

ΑΣΠΟΥΔΑΣΤΟΣ ΠΕΡΙ ΓΕΩΜΕΤΡΙΑΣ
ΜΗΔΕΙΣ ΕΙΣΙΤΩ[1]
Inscrição na entrada do Perimeter Institute

Nos três capítulos anteriores desenvolvemos uma boa compreensão teórica do emaranhamento e da estrutura do espaço de estados. Infelizmente, o desenvolvimento foi um tanto quanto árido e analítico, dificultando o uso de nossa intuição. Pretendo remediar isso neste capítulo, dando forma geométrica ao que foi exposto. Lembre-se que dispomos de um produto interno, então podemos nos dar ao luxo de entender o que estamos fazendo: é possível construir uma geometria com as propriedades esperadas, *e.g.*, a regra do paralelogramo. Uma referência geral para o assunto de geometria de estados quânticos é a [5].

Para podermos ser mais concretos, precisamos primeiro descobrir a dimensão real do espaço de estados. Neste capítulo utilizaremos a notação $\mathcal{M}^{(n)}$ para designar o subconjunto de $\mathcal{M}_n$ que representa os estados quânticos. Lembrando da definição 1.1: um estado ρ de dimensão n é representado por uma matriz complexa de ordem n, positiva e de traço um. Como ela é positiva, ela é obrigatoriamente auto-adjunta, e podemos utilizar um simples argumento de contagem para determinar sua dimensão real. Sua diagonal principal precisa ser necessariamente real, e os demais elementos podem ser complexos, mas a parte triangular superior determina completamente a parte triangular inferior. Assim precisamos contar apenas uma delas, ou melhor: eliminar metade dos parâmetros livres de cada uma. Assim a dimensão é equivalente à de uma matriz com apenas elementos reais. Tiramos mais um elemento por conta da normalização, e chegamos à conclusão que

$$\dim \mathcal{M}^{(n)} = n^2 - 1$$

Isso é um pouco desanimador, pois o menor espaço de estados que contém estados emaranhados é $\mathcal{M}^{(4)} = \mathcal{M}^{(2)} \otimes \mathcal{M}^{(2)}$; que portanto pode ser mergulhado em $\mathbb{R}^{15}$. Ou seja, não seremos capazes de visualizar diretamente

[1] "Não entre ninguém negligente em geometria". Tradução cortesia de Jacyntho Lins Brandão.

nenhum espaço de estados mais interessante. O único representável em $\mathbb{R}^3$ é o espaço de estados de um sistema quântico de dois níveis: o famoso qubit. Vamos construir explicitamente sua representação para nos familiarizar com as ferramentas, para depois partirmos para espaços com estrutura mais complexa.

4.1 Qubit

Como estamos num subespaço vetorial do espaço de Hilbert composto por operadores auto-adjuntos, o natural é escolher uma base ortonormal de matrizes auto-adjuntas. A minha base será composta pelos geradores de $\mathfrak{su}(2)$, as familiares matrizes de Pauli:

$$\sigma_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Escolhendo a origem de $\mathcal{M}^{(2)}$ como a identidade normalizada, podemos expandir um estado arbitrário nessa base:

$$\rho = \frac{1}{2}\mathbb{1} + \langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle \tag{4.1}$$

onde $\boldsymbol{r}$ é um vetor real de três componentes, conhecido como vetor de Bloch[2], e o abuso de notação tem definição intuitiva:

$$\langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle := \sum_i r_i \sigma_i$$

É interessante calcular as restrições necessárias no vetor de Bloch para que todo operador escrito na forma (4.1) seja um estado válido. Como a base é auto-adjunta e de traço nulo, a única condição que nos resta exigir é a positividade. Neste caso, é trivial fazer a conta explicitamente, e chegamos à conclusão que

$$\rho \in \mathcal{M}^{(2)} \Leftrightarrow |\boldsymbol{r}| \leq \frac{1}{\sqrt{2}}$$

ou seja, $\mathcal{M}^{(2)}$ pode ser representado por uma bola fechada em $\mathbb{R}^3$. Para completar a figura, vamos verificar mais uma característica: onde estão os estados puros? Ora, eles são os pontos puros de $\mathcal{M}^{(2)}$, e os pontos puros de uma bola são toda sua superfície.

4.2 Qudit

Já começa a surgir uma figura geométrica bem-definida: o espaço de estados como um conjunto convexo altamente simétrico, com interior não-vazio e estados puros contidos em sua fronteira. Veremos que essa idéia geral é correta para as dimensões mais altas.

[2] O uso mais antigo que encontrei dessa representação foi num livro de Hermann Weyl de 1928 [27]; a nomenclatura é portanto apenas uma homenagem a Felix Bloch, por seu extenso estudo de sistemas quânticos de dois níveis.

Para tal, precisamos generalizar de alguma forma a construção feita para o qubit. Essa generalização não é simples nem única; podendo variar muito de acordo com a aplicação desejada. Uma discussão do assunto, bem como apresentação de resultados recentes na área, pode ser encontrada na ref. [28].

Mostrarei aqui a forma que considero mais simples matematicamente, seguindo as linhas de [29, 30]: se exigirmos que nossa base continue auto-adjunta, ortogonal e de traço nulo, conseguimos generalizar de forma canônica as matrizes de Pauli, utilizando os geradores de $\mathfrak{su}(n)$; são as chamadas matrizes de Gell-Mann. Só resta a decisão um tanto quanto espinhosa da normalização. Para o nosso caso o mais conveniente é continuar usando uma base ortonormal[3], o que é uma escolha relativamente rara na literatura.

Dito isso, vamos repetir a equação (4.1) para o caso geral:

$$\rho = \frac{1}{n}\mathbb{1} + \langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle \tag{4.2}$$

Nada muito impressionante. Mas ao tentarmos repetir os passos anteriores e determinar as condições para que o lado direito represente sempre um estado válido, vemos que essa tarefa é altamente não-trivial [29]; de qualquer forma, o resultado é complexo demais para apelar à nossa intuição. O ponto interessante que podemos tirar dele é que para $n \geq 3$ o espaço de estados deixa de ser uma bola; em particular, se $\boldsymbol{r}$ corresponde a um estado puro, então certamente $-\boldsymbol{r}$ está fora do espaço de estados.

4.2.1 Insfera e circunsfera

Para demonstrar isso precisamos primeiro estabelecer alguns fatos sobre a geometria do espaço de estados de dimensão n. Primeiramente, como se trata de um conjunto convexo compacto, podemos sempre definir uma insfera e uma circunsfera. Para encontrar o raio da circunsfera, posso simplesmente encontrar os estados puros, pois por definição eles têm de estar na fronteira de $\mathcal{M}^{(n)}$. Como eles são projetores segue direto da definição que ρ é puro sse $\rho^2 = \rho$. Para simplificar as contas, trabalharemos apenas com a condição necessária $\mathrm{tr}(\rho^2) = \mathrm{tr}(\rho) = 1$. Utilizando a forma (4.2), e as propriedades $\mathrm{tr}(\sigma_i) = 0$ e $\mathrm{tr}(\sigma_i\sigma_j) = \delta_{ij}$, obtemos:

$$\begin{aligned} 1 &= \mathrm{tr}(\rho^2) \\ &= \mathrm{tr}\left(\frac{1}{n^2}\mathbb{1} + \frac{2}{n}\langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle + \langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle^2\right) \\ &= \frac{1}{n} + |\boldsymbol{r}|^2 \\ &\Rightarrow |\boldsymbol{r}_{\max}| = \sqrt{\frac{n-1}{n}} \end{aligned}$$

e portanto os estados puros estão restritos à circunsfera (n^2-2)-dimensional de $\mathcal{M}^{(n)}$. Além disso, isso mostra que a identidade normalizada é o circuncentro de $\mathcal{M}^{(n)}$.

[3] Se quiséssemos escrever explicitamente o vetor de Bloch na base produto tensorial de um sistema bipartite, conhecido como forma de Fano [31], o mais conveniente seria escolher $\mathrm{tr}(\sigma_i\sigma_j) = \frac{1}{n}\delta_{ij}$.

Mas como não exigimos a condição de positividade, não é verdade que todo ponto da circunsfera corresponde a um estado puro. Podemos ver de forma precisa "quanto sobra": lembre-se que projetores unidimensionais em $\mathcal{M}_n$ representam direções no espaço, que são apenas vetores em $\mathbb{C}\mathbf{P}^n$; portanto seu conjunto tem $2(n-1)$ dimensões. Ou seja, o conjunto dos estados puros é um subconjunto bem pequeno da circunsfera. Apenas no caso bem degenerado de $\mathcal{M}^{(2)}$ ocorre que a fronteira do espaço de estados coincide com sua circunsfera.

Para encontrar o raio da insfera utilizaremos um processo diferente. Primeiro, note que a condição de positividade dos estados quânticos não retira nenhuma dimensão, quando estamos lidando com o espaço inteiro: então se exigirmos apenas que o operador seja auto-adjunto e de traço um, ainda estaremos no mesmo espaço vetorial, podendo porém ir além das bordas de $\mathcal{M}^{(n)}$. Faremos isso fazendo uma combinação afim entre a identidade normalizada e um projetor unidimensional qualquer:

$$\tilde{\rho} = (1-\alpha)\frac{1}{n}\mathbb{1} + \alpha P$$

onde α pode assumir qualquer valor real. Queremos que $\tilde{\rho}$ esteja numa fronteira do espaço de estados, ou seja, seu menor autovalor seja igual a 0. Como a identidade é invariante por transformações unitárias, podemos trabalhar na base em que P é diagonal. O menor autovalor é portanto

$$\lambda_{\min} = \frac{1}{n}(1-\alpha) + \alpha \quad \text{ou} \quad \lambda_{\min} = \frac{1}{n}(1-\alpha)$$

correspondendo às duas direções pelas quais podemos sair do espaço de estados: pelo projetor ou pela identidade. Como o projetor já se encontra na circunsfera, estamos interessados no primeiro caso, que corresponde a partir da identidade e encontrar a fronteira mais próxima. Ela está em

$$\alpha = -\frac{1}{n-1} \tag{4.3}$$

Temos assim uma cota superior para o "tamanho" da bola em torno da identidade que pertence a $\mathcal{M}^{(n)}$. Mas esta também é uma cota inferior, pois se perturbarmos mais de um autovalor ao mesmo tempo precisaremos de um α maior em módulo para levar o menor deles a zero; estaremos "desperdiçando" a negatividade nos autovalores que não irão a zero.

Note que se $n = 2$, temos que $\alpha = -1$, confirmando o fato de que em $\mathcal{M}^{(2)}$ a insfera coincide com a circunsfera.

Precisamos agora relacionar esse α com a norma do vetor de Bloch. Mas isso é muito fácil, pois a representação de $\tilde{\rho}$ com o vetor de Bloch é simplesmente

$$\tilde{\rho} = \frac{1}{n}\mathbb{1} + \alpha\langle \boldsymbol{r}, \boldsymbol{\sigma}\rangle$$

onde é necessário que $|\boldsymbol{r}| = \sqrt{\frac{n-1}{n}}$ para que $\alpha = 1$ corresponda a um estado puro. Portanto, usando a equação (4.3), o raio da insfera é

$$|\boldsymbol{r}_{\min}| = \frac{1}{\sqrt{n(n-1)}}$$

Em particular, isso implica que $\alpha = -1$ não corresponde a um estado válido para $n \geq 3$, o que demonstra meu comentário anterior. Na verdade, demonstramos algo mais forte: um estado puro P, na circunsfera, determina unicamente um estado misto $\rho^\star$ na insfera, através da fórmula

$$\rho^\star = \frac{1}{n-1}(\mathbb{1} - P)$$

Desta forma, podemos dizer que existe na insfera uma cópia homotética dos estados (puros) da circunsfera. Provavelmente isso dará origem a alguma bela representação, mas ainda não fui capaz de encontrar uma projeção em $\mathbb{R}^3$ que a exiba.

Além disso, este estado misto tem necessariamente posto $n-1$, pois por construção ele possui apenas um autovalor nulo. Esta dualidade entre os pontos puros e os pontos de posto $n-1$ é uma característica marcante da geometria de um simplexo; e é possível transformar esta reminiscência numa ferramenta de representação, nos possibilitando um vislumbre dos espaços de dimensão maior.

4.3 Simplexo dos autovalores

A idéia por trás dessa representação é simples: toda matriz auto-adjunta pode ser diagonalizada através de uma transformação unitária. Então para qualquer estado quântico posso escrever

$$\rho = UdU^*$$

onde d é uma matriz diagonal com os autovalores de ρ. Então podemos fazer uma projeção em $\mathcal{M}^{(n)}$ fixando uma unitária e representando apenas os autovalores. O surpreendente é que essa representação é bastante poderosa, sendo capaz de mostrar várias características essenciais do espaço de estados. Utilizarei a notação $\boldsymbol{M}^{(n)}$ para designar o simplexo de autovalores de $\mathcal{M}^{(n)}$.

Lembre-se que um estado $\rho \in \mathcal{M}^{(n)}$ possui n autovalores positivos que somam para 1. Ora, essa é a definição de um $(n-1)$-simplexo. Isso significa que agora seremos capazes de desenhar também $\boldsymbol{M}^{(3)}$ e $\boldsymbol{M}^{(4)}$, tendo finalmente uma visualização dos estados emaranhados.

Por enquanto, vamos descrever apenas a estrutura que vale para qualquer unitária. Logo mais, estudaremos a estrutura que surge com a escolha de uma U específica.

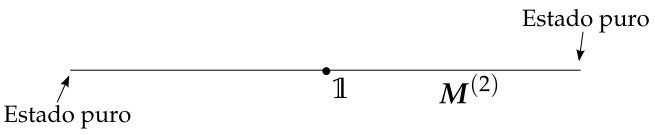

Figura 4.1: Simplexo dos autovalores para $\mathcal{M}^{(2)}$.

No caso de $\boldsymbol{M}^{(2)}$, a figura 4.1 é útil apenas para mostrar o quão radical é a simplificação: a bola de Bloch se reduz a uma linha e os estados puros a dois

pontos; mas a estrutura convexa se mantém: a combinação convexa de dois pontos puros cai necessariamente no interior do simplexo de autovalores, e o seu centro é a identidade normalizada. Não há o que falar sobre a insfera e a circunsfera, pois ambas coincidem com a fronteira do espaço de estados.

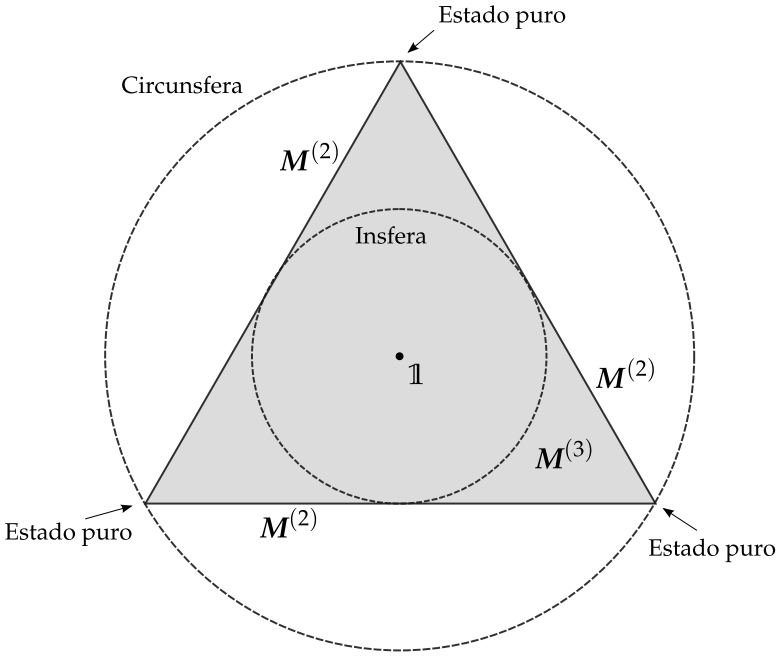

Figura 4.2: Simplexo dos autovalores para $\mathcal{M}^{(3)}$ (em cinza), incluindo insfera e circunsfera.

Na figura 4.2 você encontra o simplexo dos autovalores para $\mathcal{M}^{(3)}$, que já possui uma estrutura mais rica. Primeiro note a estrutura convexa: a combinação de três pontos puros fica no interior do simplexo, enquanto as combinações de apenas dois pontos puros formam os lados do triângulo. Mas o conjunto das combinações convexas de dois pontos puros é a estrutura que acabamos de descrever para $\boldsymbol{M}^{(2)}$! Isso é verdade num sentido mais amplo: qualquer subespaço vetorial de $\mathcal{M}^{(3)}$ formado pelas combinações convexas de dois pontos puros ortogonais é de fato uma cópia de $\mathcal{M}^{(2)}$, mesmo se considerarmos toda a estrutura de ambos os espaços.

Também podemos ver a estrutura descrita no final do capítulo anterior: se estamos num estado puro, e refletimos o vetor em torno da identidade, estamos no ponto da circunsfera o mais longe possível de $\boldsymbol{M}^{(3)}$.

O simplexo de autovalores para $\mathcal{M}^{(4)}$ segue a mesma lógica, conforme visto na figura 4.3: ele é um 3-simplexo com uma bola maximal em seu interior. Seus vértices são estados puros, suas arestas são cópias de $\boldsymbol{M}^{(2)}$ e suas faces cópias de $\boldsymbol{M}^{(3)}$.

Essa estrutura recursiva ocorre em todas dimensões: as $(n-2)$-faces de $\boldsymbol{M}^{(n)}$ são cópias de $\boldsymbol{M}^{(n-1)}$, e o mesmo é verdade para $\mathcal{M}^{(n)}$, embora agora estejamos falando de subespaços vetoriais e não de faces.

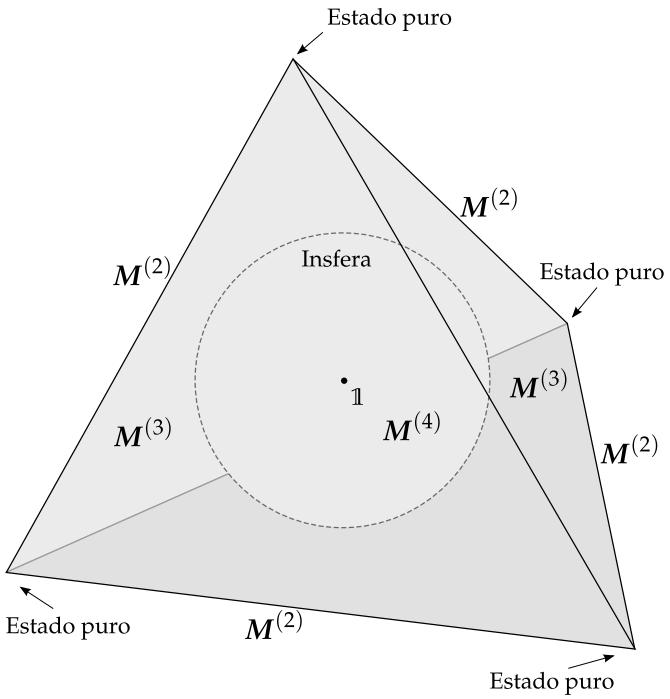

Figura 4.3: Simplexo dos autovalores para $\mathcal{M}^{(4)}$ (em cinza), incluindo sua insfera.

4.3.1 Estados emaranhados

Até agora não falamos de emaranhamento; ora, era de fato impossível, pois essa é uma propriedade que enfaticamente depende da base. E é precisamente escolhendo uma unitária que vou desenhar estados emaranhados. Mas como? Existe uma representação simples e bela feita pelos Horodeccy [32], conhecida como *stella octangula*[4], que vou reconstruir aqui usando a idéia do simplexo de autovalores. Essa construção será bem mais simples que a deles, pois temos a vantagem de saber o poderoso critério da transposta parcial positiva.

Para tal, vamos primeiro interpretar geometricamente a operação de transposição.

Teorema 4.1. *O mapa $T : \mathcal{M}_2 \to \mathcal{M}_2$ é equivalente ao mapa $\neg : \mathcal{M}_2 \to \mathcal{M}_2$, $\neg(\rho) := \mathbb{1} - \rho$ a menos de uma transformação unitária.*

Demonstração. Representando ρ em seu vetor de Bloch

$$\rho = \frac{1}{2}\mathbb{1} + \langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle$$

vemos que precisamos analisar o efeito da transposição apenas em $\boldsymbol{\sigma}$. Ora, é imediato que

$$T(\sigma_1) = \sigma_1 \quad T(\sigma_2) = -\sigma_2 \quad T(\sigma_3) = \sigma_3$$

[4]Em 2002, essa representação ganhou uma extensão elegante por Ericsson [33], que não abordarei aqui.

e portanto a transposição é apenas uma reflexão em relação ao plano $r_2 = \langle \rho, \sigma_2 \rangle = 0$. Além disso, através da matriz unitária $\sqrt{2}\sigma_2$ conseguimos definir um mapa positivo $R : \mathcal{M}_2 \to \mathcal{M}_2$

$$R(\rho) := 2\sigma_2 \, \rho \, \sigma_2$$

que tem a propriedade complementar

$$R(\sigma_1) = -\sigma_1 \quad R(\sigma_2) = \sigma_2 \quad R(\sigma_3) = -\sigma_3$$

Compondo ambas as operações eu tenho um mapa positivo $\neg : \mathcal{M}_2 \to \mathcal{M}_2$ definido por $\neg(\rho) := R \circ T(\rho) = \mathbb{1} - \rho$, que tem a simples interpretação geométrica

$$\rho = \frac{1}{2}\mathbb{1} + \langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle \Rightarrow \neg(\rho) = \frac{1}{2}\mathbb{1} - \langle \boldsymbol{r}, \boldsymbol{\sigma} \rangle,$$

ou seja, de refletir o vetor de Bloch em relação à identidade. □

Em dimensões mais altas esses mapas deixam de ser equivalentes. Surge então a idéia de usar a generalização natural desse mapa de inverter o vetor de Bloch

$$\neg(\rho) := \frac{1}{n-1}(\mathbb{1} - \rho)$$

para construir um critério de separabilidade análogo ao da transposição parcial. Mas essa idéia é sem futuro: o critério resultante é estritamente mais fraco[5] que a transposição parcial [17, 34], pois se trata de um mapa completamente copositivo.

Mas voltemos ao problema em mãos: escolhendo uma unitária determinamos de forma única n projetores ortonormais que formam uma base para o conjunto de estados puros de $\mathcal{M}^{(n)}$. E o $(n-1)$-simplexo é simplesmente o conjunto das combinações convexos desses n pontos puros. A base que escolheremos é a base de Bell[6], composta por quatro estados maximamente emaranhados de $\mathcal{M}^{(4)}$:

$$B_{ell} = \{\psi_-, \psi_+, \phi_-, \phi_+\}$$

Esta base tem a interessante propriedade de formar um subespaço vetorial fechado[7] em relação ao mapa $\mathbb{1} \otimes R$. Mais precisamente

$$\psi_- = \mathbb{1} \otimes R(\phi_+) \qquad \phi_+ = \mathbb{1} \otimes R(\psi_-)$$
$$\psi_+ = \mathbb{1} \otimes R(\phi_-) \qquad \phi_- = \mathbb{1} \otimes R(\psi_+)$$

Além disso, para qualquer $\beta \in B_{ell}$ é verdade que

$$\beta^{T_A} = \mathbb{1} \otimes T(\beta) = \mathbb{1} \otimes \neg \circ R(\beta)$$

e portanto seremos capazes de representar no mesmo espaço o 3-simplexo da base de Bell, e o espaço de suas transpostas parciais. Isso é interessante pois

[5] Apesar de ter aplicações interessantes.

[6] Essa base extremamente famosa é definida e explorada em [6].

[7] Essa propriedade é compartilhada apenas pela base computacional, que só vai produzir estados separáveis [33].

para qualquer dimensão é verdade que $\rho^{T_A} \geq 0 \Leftrightarrow \rho \in \mathcal{M}^{(n)} \cap T_A\left(\mathcal{M}^{(n)}\right)$. Como estamos em $\mathcal{M}^{(4)}$ isso é suficiente para afirmar que ρ é separável. Portanto, os estados separáveis que podem ser escritos como combinação convexa de estados de Bell são exatamente a intersecção entre esses dois 3-simplexos, conforme vemos na figura 4.4.

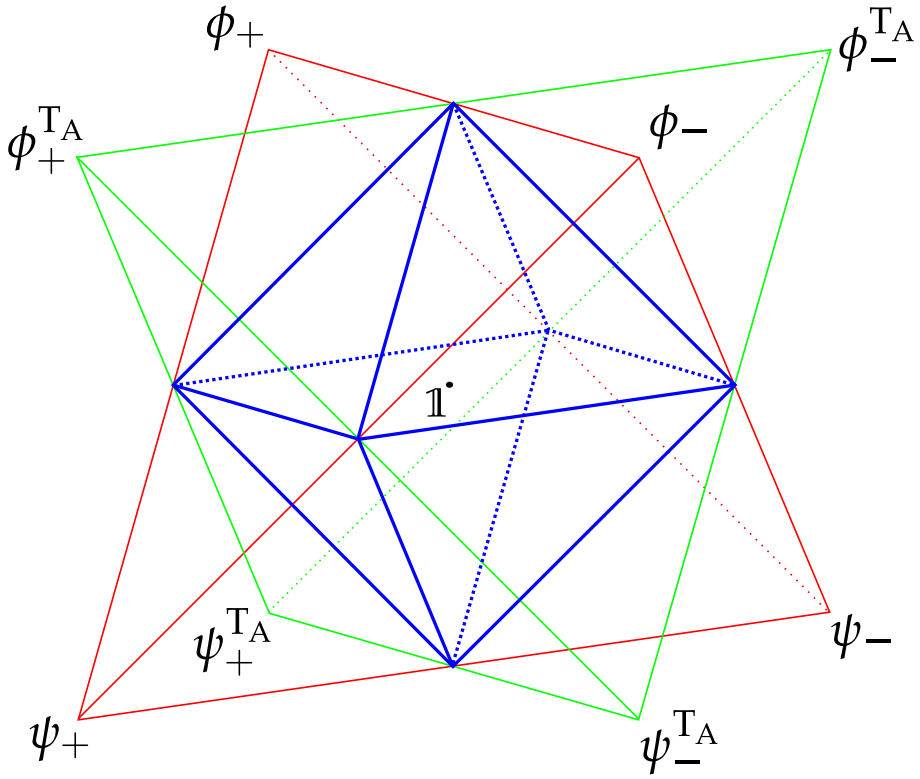

Figura 4.4: *Stella octangula*. Em vermelho, o 3-simplexo da base de Bell. Em verde, o espaço de suas transpostas parciais. Em azul, sua intersecção: o octaedro dos estados separáveis desta base.

A geometria resultante é bem interessante: podemos ver claramente que o espaço dos estados emaranhados não é convexo, e está restrito a regiões próximas aos estados puros. Mas não se deixe enganar pela simplicidade da fronteira dos estados separáveis: esse é um caso muito especial. Para uma base qualquer a imagem resultante é de um cone truncado, e em dimensões mais altas ninguém sabe.

Note também que a insfera do espaço de estados ficou toda dentro do espaço dos separáveis. Isso não é mera coincidência. Pode ser facilmente provado que em qualquer dimensão a insfera só contém estados PPT[8]; isso implica separabilidade para os estados de dimensão mais baixa. Mais recentemente, surgiu um critério de separabilidade[9] [35] que prova a separabilidade

[8] Veja a secção 15.5 da ref. [5].
[9] Consciente de estar sendo deselegante, não recomendo a ninguém a leitura deste artigo.

de *todos* os estados que pertencem à insfera: especificamente, ele diz que se

$$|\boldsymbol{r}| \leq \frac{1}{\sqrt{n(n-1)}}$$

um estado é separável. Além disso, esse também é o critério mais forte possível que depende somente do módulo do vetor de Bloch, existindo estados emaranhados a uma distância ε da superfície da insfera.

4.4 Volume do espaço de estados

Nada mais natural que fechar um capítulo sobre geometria com algumas considerações sobre o (hiper)volume do espaço de estados[10]. Embora o volume de $\mathcal{M}^{(n)}$ possa ser calculado[11], não faremos isso; este número não tem muito significado, e vamos defini-lo como sendo 1.

Estamos interessados no volume relativo dos espaços de estados emaranhados e separáveis. Esse número sim pode nos revelar várias coisas sobre a geometria do espaço de estados, ou mesmo sobre a física da mecânica quântica. Sabemos, por exemplo, que se nos restringirmos a estados puros, o conjunto dos estados separáveis tem medida nula[12].

Podemos estender essa afirmação para todo o espaço de estados? Lembre-se da discussão no final da secção anterior. Como temos uma bola separável de raio finito em todas as dimensões, isso já é suficiente para dizer que qualquer medida sensata vai retornar um valor não-nulo para o conjunto dos separáveis. Para a mesma afirmação em relação aos emaranhados, basta notar que eles são um conjunto aberto, pois eles são o complementar dos separáveis, que é fechado. Idem para o conjunto dos estados PPT-emaranhados: se considerarmos nosso espaço como o conjunto dos estados PPT, ele é o complementar do conjunto dos estados separáveis, e portanto um conjunto aberto.

Poderíamos avançar um pouco mais e utilizar essas propriedades para tirar analiticamente cotas inferiores e superiores para o volume do espaço de estados separáveis. Mas como essas cotas são muito ruins e o cálculo desinteressante, vamos passar duma vez para o cálculo do volume em si.

Como fazê-lo? Não dispomos de uma parametrização da fronteira do espaço de estados separáveis. Só nos resta fazer o cálculo numérico, definindo uma medida e gerando estados aleatoriamente. Como definimos o volume total do espaço de estados como sendo 1, o volume do espaço dos estados separáveis será simplesmente a probabilidade do estado gerado ser separável, e o mesmo para o volume do espaço dos estados emaranhados.

Lembrando da idéia do simplexo dos autovalores, fica claro que um estado é completamente determinado pela escolha de uma matriz unitária e de um simplexo. Mais precisamente, podemos escrever uma função $f : \Delta_{n-1} \times U_n \to \mathcal{M}^{(n)}$, onde Δ_{n-1} é o $(n-1)$-simplexo, U_n é o conjunto das

[10] Esta secção é baseada nos resultados de [36, 37].

[11] Isso é feito em [38], usando a medida de Hilbert-Schmidt, e em [39], usando a medida de Bures.

[12] Isso pode ser provado facilmente usando o mergulho de Segre [6].

matrizes unitárias de ordem n e f é dada por

$$\rho = f(d,U) := UdU^*$$

onde d é uma matriz diagonal cujos elementos são as coordenadas de Δ.

Contudo, essa função não é bijetiva. Em primeiro lugar, U tem $n-1$ parâmetros redundantes em relação ao que nos interessa: o conjunto $\boldsymbol{P}$ das famílias completas de projetores ortonormais. Mas isso não será problema, pois uma medida uniforme em U induz uma medida uniforme em $\boldsymbol{P}$. Além disso, mesmo trabalhando em $\Delta \times \boldsymbol{P}$ temos uma redundância causada pela existência de degenerescência nos autovalores. Mas esse conjunto tem medida nula, então existe um aberto denso em $\Delta \times \boldsymbol{P}$ no qual f é bijetiva, e portanto podemos caracterizar $\mathcal{M}^{(n)}$ através de uma medida produto em $\Delta \times U$.

É difícil justificar fisicamente qual medida utilizar, então vamos nos focar apenas nos aspectos estéticos. Para Δ, vamos utilizar a distribuição uniforme no $(n-1)$-simplexo. Isso é fácil de fazer; alguns algoritmos simples podem ser encontrados em [40]. Falta escolher a medida em U. Utilizaremos a única medida uniforme no grupo das matrizes unitárias: a medida de Haar. Um algoritmo para gerar matrizes unitárias uniformes sob essa medida é descrito em [41].

A partir disso desenvolvemos um algoritmo numérico[13] para calcular os variados volumes que desejamos. O resultado pode ser visto na figura 4.5.

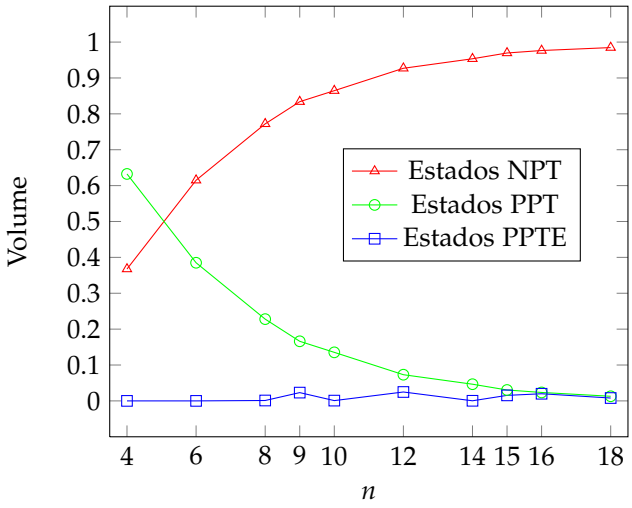

Figura 4.5: Volume dos espaços de estados emaranhados com transposta parcial negativa (NPT, △), estados com transposta parcial positiva (PPT, ◯) e estados PPT-emaranhados (PPTE, □).

A classificação dos estados emaranhados com transposta parcial positiva é feita através do algoritmo descrito em [1]; por isso seu volume é apenas uma cota superior, pois o algoritmo é feito para considerar como emaranhados os estados na região de incerteza. Não os chamei de estados com emaranhamento

[13] Código-fonte disponível via email para `mas@fisica.ufmg.br`.

preso, pois ainda é uma conjectura em aberto se existem estados NPT que têm emaranhamento preso [42].

Note duas características essenciais: o volume do espaço de estados PPT parece decair exponencialmente com a dimensão (isso é explorado com mais rigor em [36]), e consequentemente o volume dos separáveis. Isso dá base à afirmação de que em dimensões altas só existem estados emaranhados. Outra é que o comportamento do volume dos estados PPTE em relação à dimensão é tudo menos simples: ele oscila bastante, e depende fortemente do particionamento do espaço de estados (*e.g.*, podemos considerar $\mathcal{M}^{(12)}$ como $\mathcal{M}^{(2)} \otimes \mathcal{M}^{(6)}$ ou $\mathcal{M}^{(3)} \otimes \mathcal{M}^{(4)}$), sendo maior quanto mais bem-distribuída é a partição. Mostramos apenas o maior valor encontrado. Já o volume dos estados PPT também depende da partição, mas de forma tão fraca que a diferença desaparece dentro de nosso erro estatístico.

Note que o volume dos estados PPTE é sempre muito pequeno, chegando a no máximo 0.02; isso diminui sua importância com vista a aplicações práticas, se a distribuição deles na natureza tem algo a ver com a medida que escolhemos. Porém, eles ainda são interessantes do ponto de vista matemático, devido a sua grande complexidade, e ao tanto que eles podem nos revelar sobre a estrutura do espaço de estados.

E o que acontece se mudamos nossa medida? Essa questão é explorada em [37], e respondida de forma tentativa: apesar do valor numérico dos volumes mudar, o comportamento deles em função da dimensão permanece essencialmente inalterado.

Bibliografia

[1] F. G. Brandão e R. O. Vianna. "Separable Multipartite Mixed States: Operational Asymptotically Necessary and Sufficient Conditions". *Phys. Rev. Lett.* **93**, 22 (2004). arXiv:quant-ph/0405063.

[2] Erhard Schmidt. "Zur Theorie der linearen und nichtlinearen Integralgleichungen. 1. Entwicklung willküriger Funktionen nach Systemevorgeschriebener". *Mathematische Annalen* **63** (4 1907), pp. 433–476.

[3] Artur Ekert e Peter L. Knight. "Entangled quantum systems and the Schmidt decomposition". *Am. J. Phys.* **63**, 5 (1995), pp. 415–423.

[4] R. Horodecki *et al.* "Quantum entanglement". (2007). arXiv:quant-ph/0702225.

[5] Karol Życzkowski e Ingmar Bengtsson. *Geometry of Quantum States*. Cambridge University Press, 2006.

[6] Marcelo Oliveira Terra Cunha. *Noções de Informação Quântica*. IMPA, 2007.

[7] Michael Nielsen e Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[8] A. Sanpera, R. Tarrach e G. Vidal. "Quantum separability, time reversal and canonical decompositions". (1997). arXiv:quant-ph/9707041.

[9] Dagmar Bruß e Chiara Macchiavello. "How the First Partial Transpose was Written". *Foundations of Physics* **35** (11 2005), pp. 1921–1926.

[10] Stephen Boyd e Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004. URL: http://www.stanford.edu/~boyd/cvxbook/.

[11] H. G. Eggleston. *Convexity*. Cambridge University Press, 1958.

[12] S. L. Woronowicz. "Positive maps of low dimensional matrix algebras". *Rep. Math. Phys* **10**, 2 (1976), pp. 165–183.

[13] A. Jamiołkowski. "Linear transformations which preserve trace and positive semidefiniteness of operators". *Rep. Math. Phys* **3**, 4 (1972), pp. 275–278.

[14] P. Arrighi e C. Patricot. "On quantum operations as quantum states". *Ann. Phys.* **311** (2004), pp. 26–52. arXiv:quant-ph/0307024.

[15] M. Horodecki, P. Horodecki e R. Horodecki. "Separability of mixed states: necessary and sufficient conditions". *Phys. Lett. A* **223** (1996), pp. 1–8. arXiv:quant-ph/9605038.

[16] Man-Duen Choi. "Positive semidefinite biquadratic forms". *Linear Algebra Appl.* **12**, 2 (1975), pp. 95–100.

[17] D. Chruściński e A. Kossakowski. "Geometry of quantum states: New construction of positive maps". *Phys. Lett. A* **373** (2009), pp. 2301–2305. arXiv:0902.0885 [quant-ph].

[18] Wai-Shing Tang. "On positive linear maps between matrix algebras". *Linear Algebra Appl.* **79** (1986), pp. 33–44.

[19] A. Peres. "Separability Criterion for Density Matrices". *Phys. Rev. Lett.* **77** (1996), pp. 1413–1415. arXiv:quant-ph/9604005.

[20] Marco Túlio Coelho Quintino. "Não-localidade como recurso para a comunicação". Monografia. 2010. URL: http://www.mat.ufmg.br/~tcunha/MonografiaMTulio.pdf.

[21] M. Horodecki, P. Horodecki e R. Horodecki. "Mixed-State Entanglement and Quantum Communication". *Quantum Information*. Ed. por G. Alber. 2001, pp. 151–195. arXiv:quant-ph/0109124.

[22] M. Horodecki, P. Horodecki e R. Horodecki. "Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?" *Phys. Rev. Lett.* **80** (1998), pp. 5239–5242. arXiv:quant-ph/9801069.

[23] Maurice Sion. "On general minimax theorems". *Pacific J. Math.* **8**, 1 (1958), pp. 171–176. URL: http://projecteuclid.org/euclid.pjm/1103040253.

[24] M. Horodecki, P. Horodecki e R. Horodecki. "Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps". *Phys. Lett. A* **283** (2001), pp. 1–7. arXiv:quant-ph/0006071.

[25] M. Lewenstein *et al.* "Optimization of entanglement witnesses". *Phys. Rev. A* **62**, 5 (2000). arXiv:quant-ph/0005014.

[26] F. G. S. L. Brandão. "Quantifying entanglement with witness operators". *Phys. Rev. A* **72**, 2 (2005). arXiv:quant-ph/0503152.

[27] Hermann Weyl. *Gruppentheorie und Quantenmechanik*. Leipzig, S. Hirzel, 1928.

[28] R. A. Bertlmann e P. Krammer. "Bloch vectors for qudits". *J. Phys. A: Math. Theor.* **41**, 23 (2008). arXiv:0806.1174 [quant-ph].

[29] G. Kimura. "The Bloch vector for N-level systems". *Phys. Lett. A* **314** (2003), pp. 339–349. arXiv:quant-ph/0301152.

[30] G. Kimura e A. Kossakowski. "The Bloch-vector space for N-level systems – the spherical-coordinate point of view". *Open Systems & Information Dynamics* **12** (3 2004), pp. 207–229. arXiv:quant-ph/0408014.

[31] U. Fano. "Pairs of two-level systems". *Rev. Mod. Phys.* **55**, 4 (1983), pp. 855–874.

[32] R. Horodecki e M. Horodecki. "Information-theoretic aspects of inseparability of mixed states". *Phys. Rev. A* **54** (1996), pp. 1838–1843. arXiv:quant-ph/9607007.

[33] Åsa Ericsson. "Separability and the stella octangula". *Phys. Lett. A* **295** (2002), pp. 256–258. arXiv:quant-ph/0109099.

[34] M. Horodecki e P. Horodecki. "Reduction criterion of separability and limits for a class of protocols of entanglement distillation". *Phys. Rev. A* **59**, 6 (1997), pp. 4206–4216. arXiv:quant-ph/9708015.

[35] L. Gurvits e H. Barnum. "Largest separable balls around the maximally mixed bipartite quantum state". *Phys. Rev. A* **66**, 6 (2002). arXiv:quant-ph/0204159.

[36] K. Życzkowski *et al.* "On the volume of the set of mixed entangled states". *Phys. Rev. A* **58** (1998), pp. 883–892. arXiv:quant-ph/9804024.

[37] K. Życzkowski. "On the volume of the set of mixed entangled states II". *Phys. Rev. A* **60** (1999), pp. 3496–3507. arXiv:quant-ph/9902050.

[38] K. Życzkowski e H.J. Sommers. "Hilbert-Schmidt volume of the set of mixed quantum states". *J. Phys. A: Math. Gen.* **36** (2003), pp. 10115–10130. arXiv:quant-ph/0302197.

[39] H.J. Sommers e K. Życzkowski. "Bures volume of the set of mixed quantum states". *J. Phys. A: Math. Gen.* **36** (2003), pp. 10083–10100. arXiv:quant-ph/0304041.

[40] Wikipedia. *Simplex*. URL: http://en.wikipedia.org/wiki/Simplex (acesso em 24/09/2010).

[41] Marcin Poźniak, Karol Życzkowski e Marek Kuś. "Composed ensembles of random unitary matrices". *J. Phys. A: Math. Gen.* **31**, 3 (1998), p. 1059. arXiv:chao-dyn/9707006.

[42] Reinhard F. Werner. *Quantum Information: Problems*. URL: http://www.imaph.tu-bs.de/qi/problems/2.html (acesso em 24/09/2010).