

Universidade Federal de Juiz de Fora

Departamento de Matemática

Pós-Graduação em Matemática

Sobre a Catálise em Sistemas Quânticos

Cristhiano André Duarte

Orientador: Professor Marcelo de Oliveira Terra Cunha

cristhianoduarte@gmail.com

Juiz de Fora

2013

Aluno: Cristhiano André Gamarano Duarte Carneiro Silva

Sobre a Catálise em Sistemas Quânticos

Dissertação apresentada como parte da obtenção do grau de Mestre em Matemática pela Universidade Federal de Juiz De Fora, elaborada sob a orientação do Prof. Marcelo de Oliveira Terra Cunha.

Juiz de Fora-MG

2013

“There is a loneliness in this world so great
that you can see it in the slow movement of
the hands of a clock.

people so tired

mutilated

either by love or no love.

people just are not good to each other
one on one.

the rich are not good to the rich

the poor are not good to the poor.

we are afraid.

our educational system tells us

that we can all be

big-ass winners.

it hasn't told us

about the gutters

or the suicides.

or the terror of one person

aching in one place

alone

untouched

unspoken to

watering a plant.”

Charles Bukowski, Love is a Dog from Hell

“Goodbye everybody, I've got to go

Gotta leave you all behind

And face the truth...”

Queen, Bohemian Rhapsody

“I've been working from seven to eleven every night

I said it kinda makes my life a drag, drag, drag, drag, Lord, that ain't right

Since I've been loving you

I'm about to lose my worried mind

Said I've been crying, my tears they fell like rain

Don't you hear, don't you hear them falling...”

Led Zeppelin, Since I've been loving you.

Agradecimentos

À medida que o tempo passa, o número de pessoas que entram e saem de nossas vidas aumenta ainda mais. Geralmente todas elas contribuem de alguma maneira para o aprendizado, seja direta ou indiretamente. Agradecer a todas uma por uma é impossível (até porque não tenho boa memória e não me lembraria de todos os nomes), por outro lado fazer referência a só algumas é correr o risco de deixar alguém chateado. Mas vou fazer assim mesmo...

*Aos meus pais, meus mais sinceros agradecimentos, vocês me aguentaram 24 anos debaixo de suas asas, e estavam do meu lado em todas as dificuldades (todas!), ainda que eu não os apoiasse vocês sempre me apoiaram, incondicionalmente. Obrigado! A família do Poker do fim de semana (Karl, Marcelo, Monica, Sérgio, Virgininha), todos vocês me ensinaram, as vezes sem saber, que rir é o melhor remédio pra todo tipo tristeza (especialmente vocês, Fia e Fabiano). A turma dos churrascos (Zé Luiz, Piada, Fernanda, Alysson, Amâncio, Podolsky e cia.) nossos micro churrascos me fizeram, surpreendentemente, crescer como pessoa, aonde mais eu poderia discutir política, sexo, religião, ciência, música e relações interpessoais alheias (fofoca), ouvindo um bom Led Zeppelin? Piada, a combinação uísque + Ziggy Stardust vai ficar pra sempre na minha memória... valeu por tudo pessoal! À todos os meus professores do mestrado (Flaviana, Régis, Crocco, Luiz Fernando) e aos meus coordenadores (Fábio e Flaviana) muito obrigado, vocês sempre foram pacientes comigo e me tornaram um aluno/tutor melhor. Para todos alunos da tutoria, obrigado! Todas as turmas me mostraram que eu tenho muito que aprender e que posso fazer alguma coisa pela educação, mesmo enquanto pesquisador. Obrigado também a Laura, que sempre foi muito solícita e me salvou de alguns apuros. Ao pessoal do SubEnLight por me acolher. Um obrigado especial ao Raphael pelas discussões e ajudas! Deixei por último duas pessoas a quem devo demais: Ao meu orientador, Marcelo Terra Cunha, por ter uma enorme paciência comigo (e algumas poucas vezes falta dela), por ter me deixado pensar com minhas próprias pernas, por me deixar trabalhar num tema que tanto me chamou atenção e por topa essa orientação a distância, e acima de tudo por ser **orientador**: muito obrigado! Ao meu amigo/professor/co-orientador Amâncio, por ter me aturado e me ajudado em **todas** as vezes que te pedi, por ter saca pra me ensinar (as vezes coisas bem complicadas, as vezes coisas banais), por mostrar que eu acreditava em variáveis ocultas, por todas as discussões científicas e filosóficas e por me mostrar que quanto mais aprendemos, menos sabemos, **muito obrigado**. Não há palavras pra te agradecer, ó mestre dos magos!*

RESUMO

Deixado de lado durante anos na Mecânica Quântica, o *Emaranhamento* é visto hoje em dia como uma fonte, um recurso a ser utilizado. Cabendo a cada pesquisador aproveitá-lo da melhor forma possível. Usado para gerar algoritmos mais eficientes, teleportar estados quânticos, e realizar tarefas antes impossíveis, o emaranhamento pode ser um recurso ainda mais estranho. Basta ver o fenômeno da *catálise*, onde o emaranhamento extra utilizado não é consumido. Aqui nosso objetivo é estudar um pouco mais sobre a catálise em sistemas quânticos e obter uma maneira de dizer quais estados são catalisadores em potencial.

Palavras-chave: Mecânica Quântica, Emaranhamento, Catálise, Majoração, Álgebra Linear, Operadores.

ABSTRACT

Left aside for years in quantum theory, the entanglement is today a source, a resource to be utilised. Each researcher should use it of the best way possible. Used to generate faster algorithms, to teleport states and perform tasks before impossibles, the entanglement may be a more strange source. Just watch the catalysis phenomenon, where the extra entanglement utilized is not consumed. Here our goal is studying just a little bit of catalysis in quantum systems and get a way to say which states are potential catalysts.

Key-words: Quantum Mechanics, Entanglement, Catalysis, Majorization, Linear Algebra, Linear Operators.

Lista de Símbolos e Notações

I_n	$\{1, 2, 3, \dots, n\}$
\otimes	Produto Tensorial. Multiplicação componente a componente
\prec	Majoração 1.1
$\{e_1, e_2, \dots, e_n\}$	Base Canônica
\prec_w	Sub Majoração 1.5
\prec^w	Super Majoração 1.5
$\lambda(A)$	Vetor contendo os auto-valores do operador $A : V \rightarrow V$. 1.18
x^\downarrow	Reordenamento, em ordem não-crescente, das componentes de x
$(\mathbb{R}^n)^\downarrow$	$\{(x_1, \dots, x_n) \in \mathbb{R}^n; x_1 \geq x_2 \geq \dots \geq x_n\}$ 1.2
$f^+ : \mathbb{R}^n \rightarrow \mathbb{R}$	Parte positiva da função f
\mathbb{V}^n	Simplexo de Probabilidades 1.3
BON	Base Ortonormal
$ \psi\rangle\langle\psi $	Projeter na direção de $ \psi\rangle$
$ \psi\rangle \propto \phi\rangle$	O vetor $ \psi\rangle$ tem a mesma direção de $ \phi\rangle$
$ \psi\rangle \sim (\lambda_1, \dots, \lambda_n)$	Identificação entre o vetor $ \psi\rangle$ e sua Decomposição de Schmidt
$\mathbb{M}_{n,m}(\mathbb{K})$	Conjunto das Matrizes $n \times m$, com entradas em \mathbb{K} 2.21
$ X $	Cardinalidade do conjunto X
$\mathfrak{D} = \{\rho \in \mathbb{M}; \text{tr}(\rho) = 1\}$	Matrizes com traço igual a 1 2.21
λ_ψ	Vetor cujas entras são os coeficientes de Schmidt do estado $ \psi\rangle$
$v \ll \mu$	v é absolutamente contínua com respeito a μ [57]
$\mathbb{M}_n \ni A \geq 0$	A é Positiva (semi-definida) [8]
$[[A_{ij}]]$	Matriz cujas entradas são as matrizes $\mathcal{A} = A_{ij}$

Sumário

Introdução	ix
1 Majoração	1
1.1 Introdução	1
1.2 Definições	2
1.3 Alguns Lemas importantes	7
2 Um pouco de Mecânica Quântica	12
2.1 Postulados Básicos da Mecânica Quântica	12
2.1.1 Qubits	12
2.1.2 2 Qubits	15
2.1.3 Generalizações	16
2.1.4 Estados Reduzidos	19
2.2 O Emaranhamento	19
2.2.1 Critérios de Separabilidade Operacionais	22
2.2.2 Critérios de Separabilidade Não-Operacionais	23
2.3 Purificação	23
2.4 Operações Quânticas	25
2.5 O Teorema	28
3 Catálise	31
3.1 Introdução	31
3.2 Pedindo Emprestado	32
3.3 Quando a Catálise não é Possível e a Anti-Catálise	34
3.4 Algumas Perguntas	36
3.5 Sobre a existência do Catalisador	37
3.6 Conjectura de Nielsen	41
4 Poder Catalítico	46

<i>SUMÁRIO</i>	viii
4.1 Algumas Palavras	46
4.2 Poder Catalítico Total	48
4.3 Um pequeno exemplo: Poder Catalítico Parcial - Fixando o estado final	50
5 Comentários Finais e Trabalhos Futuros	59
A Aplicações Completamente Positivas	62
B Uma Calculadora para a Catálise	68
C Mensurabilidade de certos conjuntos	70
Referências Bibliográficas	74

Introdução

Simples: Vamos estudar a Catálise de estados puros em sistemas quânticos, e definir Poderes Catalíticos para estados bipartites. Muito embora o tema seja claro e direto, é necessário algum arcabouço teórico para que, no mínimo, a frase em destaque faça sentido. Devemos primeiro entender o que significa catálise, estados puros, sistemas quânticos e estados bipartites. Feito isso deverão ser claras a motivação e a necessidade de se definir o “Poder Catalítico”.

Entender o significado desses termos quer dizer estudar um pouco de Física Quântica, e é basicamente para isso que escrevemos o Capítulo 2. Esta é uma dissertação de Matemática Aplicada, ou Física-Matemática, escrita para um público alvo que (infelizmente) talvez nunca tenha aberto um livro de Mecânica Quântica, e é para esse leitor que o grosso do segundo capítulo é escrito. Lá, numa abordagem muito próxima àquela presente em [16, 22], vamos dar uma pequena pincelada em Mecânica Quântica. Iremos desde os postulados básicos (numa visão axiomática), passando por assuntos centrais como o emaranhamento, até tópicos um pouco mais delicados, que não são usualmente vistos nos cursos regulares sobre o assunto, tais como critérios de separabilidade, decomposição de Schmidt e purificação. Palavras como Oscilador Harmônico, Poços de Potencial, Função de Onda, Métodos Perturbativos, Espalhamento, Adição de Momento Angular, Bons Números Quânticos... não serão vistas por aqui, apesar de serem de interesse histórico, didático e fundamental para outras áreas de pesquisa. Esse não é um texto padrão em Mecânica Quântica, para tanto citamos os usuais [2, 17, 12, 13, 14] e o menos usual, mas ótimo [18]. Mas tudo isso não é suficiente, apenas necessário. Para entender completamente o texto como um todo, também é fundamental saber um pouco de Majoração, e é com esse assunto que esta dissertação se inicia. Lá, numa maneira bem matemática (definição, lema, demonstração, exemplos, proposição, demonstração, teorema, demonstração,

definição...), definimos a relação de ordem parcial que será amplamente utilizada no terceiro capítulo, mas além disso, também enunciamos vários dos lemas que serão úteis nos capítulos que se seguem. Também definimos matrizes duplamente estocásticas e (infelizmente apenas) enunciamos o Teorema de Birkhoff.

Alguém poderia se perguntar porque começamos com Majoração e não com Mecânica Quântica, como seria de esperar. Por dois simples motivos:

Primeiro, veremos que a teoria da majoração entrará, sem ser convidada, mas naturalmente, na seção destinada aos critérios de separabilidade. Segundo, terminaremos o Capítulo 2 com uma pergunta que pode ser prontamente respondida no Capítulo 3. Nesse último (central nesse trabalho) começaremos revendo o artigo [39]. Algumas perguntas podem surgir, e para aquelas que vieram na cabeça do autor, serão encontradas respostas, pelo menos parciais em casos particulares. Os Poderes Catalíticos (parcial e total) serão abordados nas últimas seções da dissertação. Concluimos o trabalho com algumas palavras finais. Seguem também três apêndices, a intenção destes é ilustrar, definir, ou mesmo discutir fatos importantes que não caberiam no corpo do texto, mas que não poderiam ser deixados de lado. Lá vamos definir Aplicações Completamente Positivas; apresentar a Calculadora para Catálise (numa versão *beta*); e por último discutir um pouco de não-mensurabilidade. Comentários Gerais: Quis deixar a dissertação o mais leve possível, num eterno diálogo com o leitor. Com notas de rodapé e comentários entre parênteses por todos os lados. Mas nem por isso a mesma perde a profundidade ou mesmo o caráter científico. Está tudo aqui, organizado, documentado, enunciado e em quase todos os casos **provado**. Apenas alguns resultados foram enunciados sem demonstração, seja por questão de espaço ou porque a prova demandaria muito mais definições e lemas auxiliares que fariam com que perdêssemos o caminho original. Todas as demonstrações tem alguma contribuição do presente autor, pelo menos no clareamento de alguma passagem ou outra. Fiz um tremendo esforço para que demonstrações não originais fossem vistas como tais (citando referências), não me apossando dos créditos. Além disso, o texto é cheio de links, então para aqueles que lêem no computador, basta passar a seta do mouse sobre um texto em [azul](#) e você será levado diretamente para a página certa. Experimente o exemplo: Definição [1.1](#). Agora chega de blábláblá e vamos ao que interessa...

Capítulo 1

Majoração

“Comparison of two vectors quantities often leads to interesting inequalities...”

(R. Bhatia)

1.1 Introdução

Mesmo sendo vaga a noção de “mais espalhado” ou “mais próximos”, dados dois vetores $x, y \in \mathbb{R}^n$ podemos, com alguma boa vontade e muita intuição, diferenciá-los em termos do quanto suas componentes estão “mais próximas” ou “mais espalhadas”. Não surpreendentemente essa noção aparece numa variedade de contextos e pode ser apresentada rigorosamente. O fato é que essas situações motivam a definição de uma relação de ordem dada pela sentença “ x é majorado por y ”, $x \prec y$.

Por exemplo, a desigualdade $\sum_{i=1}^n g(\bar{y}) \leq \sum_{i=1}^n g(y_i)$, $\forall y \in \mathbb{R}^n$, t.q. $\bar{y} = \frac{1}{n} \sum_{i=1}^n y_i$ é verdadeira para todas funções convexas¹ $g : \mathbb{R} \rightarrow \mathbb{R}$. Podemos então nos perguntar quais são as condições necessárias, e suficientes, para que $\sum_{i=1}^n g(x_i) \leq \sum_{i=1}^n g(y_i)$ seja verdadeira quaisquer que sejam as funções convexas. De fato² afim de que dados $x, y \in \mathbb{R}^n$ tenha-se $\sum_{i=1}^n g(x_i) \leq \sum_{i=1}^n g(y_i)$, $\forall g : \mathbb{R} \rightarrow \mathbb{R}$ convexa, é necessário e suficiente que $x \prec y$.

Não só em Matemática Pura, mas mesmo em Economia, onde é necessária uma comparação entre aquilo que é recebido com aquilo que é possuído, usa-se a relação de majoração. Além disso, veremos que a noção rigorosa

¹Lembre-se que um conjunto $X \in V$ é convexo quando $tx + (1-t)y \in X, \forall x, y \in X, t \in [0, 1]$ e que uma função $f : X \rightarrow \mathbb{R}$, com domínio no convexo X , é convexa quando $f[tx + (1-t)y] \leq tf(x) + (1-t)f(y), \forall x, y \in X, e t \in [0, 1]$.

²Veja [3].

de “mais espalhados” ou “mais próximos” também é utilizada em Mecânica Quântica.

1.2 Definições

Começaremos com a seguinte definição:

Definição 1.1. Sejam $x, y \in \mathbb{R}^n$ vetores arbitrários e $x^\downarrow \in \mathbb{R}^n$ um vetor cujas componentes são as componentes de x reescritas em ordem não-crescente. Então x é majorado por y , e escrevemos $x \prec y$, quando $\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow, \forall k \in \{1, 2, 3, \dots, n-1\}$ com a igualdade verdadeira se $k = n$.

Proposição 1.2. A majoração é uma relação reflexiva e transitiva sobre \mathbb{R}^n . Além disso é simétrica³ sobre $(\mathbb{R}^n)^\downarrow$.

Demonstração. Sejam $x, y, z \in \mathbb{R}^n$ arbitrários.

i)

Como $x^\downarrow = x^\downarrow$, então $\sum_{i=1}^k x_{i=1}^\downarrow = \sum_{i=1}^k x_{i=1}^\downarrow, \forall k \in I_n$, com a igualdade verdadeira se $k = n$. Portanto $x \prec x$.

ii)

Suponha que $x \prec y$ e $y \prec x$, então:

$x_1^\downarrow \leq y_1^\downarrow \leq x_1^\downarrow$, donde $x_1^\downarrow = y_1^\downarrow$. Logo $x_1^\downarrow + x_2^\downarrow \leq y_1^\downarrow + y_2^\downarrow \leq x_1^\downarrow + x_2^\downarrow$, portanto $x_2^\downarrow = y_2^\downarrow$. Prosseguindo obtemos $x_i^\downarrow = y_i^\downarrow, \forall k \in I_n$, donde $x^\downarrow = y^\downarrow$.

iii)

Suponha que $x \prec y$ e $y \prec z$, então:

Seja $k \in I_n$ qualquer. Como $x \prec y$ e $y \prec z$, então $\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow \leq \sum_{i=1}^k z_i^\downarrow$. Além disso $\sum_{i=1}^n x_i^\downarrow = \sum_{i=1}^n y_i^\downarrow = \sum_{i=1}^n z_i^\downarrow$. Portanto $x \prec z$. \square

-Exemplos-

1)

$$\left(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}\right) \prec \left(\frac{1}{n-1}, \dots, \frac{1}{n-1}, 0\right) \prec \dots \prec \left(\frac{1}{2}, \frac{1}{2}, 0, \dots, 0\right) \prec (1, 0, \dots, 0)$$

³Como veremos mais a frente, esta proposição garante que a majoração é uma relação de ordem parcial sobre o conjunto dos estados quânticos.

2)

$$(0.4, 0.4, 0.1, 0.1) \not\prec (0.5, 0.25, 0.25, 0) \text{ e } (0.5, 0.25, 0.25, 0) \not\prec (0.4, 0.4, 0.1, 0.1)$$

3)

$$(0.4, 0.4, 0.1, 0.1) \otimes (0.6, 0.4) \prec (0.5, 0.25, 0.25, 0) \otimes (0.6, 0.4)$$

4)

$$(0.5, 0.4, 0.1) \prec (0.6, 0.33, 0.07)$$

Definição 1.3. Seja $\mathbb{V}^n = \{x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n; \sum_{i=1}^n x_i = 1 \text{ e } x_i \geq 0, \forall i \in I_n\} \subset \mathbb{R}^n$ o *simplexo de probabilidades*.

Lema 1.4. Seja $x \in \mathbb{V}^n$ arbitrário, então $(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}) \prec x$, e $x \prec (1, 0, 0, \dots, 0)$.

Demonstração. Sem perda de generalidade suponha que x esteja já ordenado de forma não-crescente. Além disso para fixar as ideias suponha que $x_n > 0$. Vamos mostrar a primeira afirmação, a segunda é trivialmente satisfeita.

Suponha, por absurdo, que $(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}) \not\prec x$, então existe $l \in I_{n-1}$, t.q. $\frac{1}{n} > x_1 + \dots + x_l$, logo $1 = \sum_{i=1}^n x_i = x_1 + \dots + x_l + x_{l+1} + \dots + x_n < \frac{1}{n} + x_{l+1} + \dots + x_n$, donde $x_{l+1} + \dots + x_n > 1 - \frac{1}{n} = \frac{n-1}{n}$. Como $x_1 \geq \dots \geq x_l \geq x_{l+1} \geq \dots \geq x_n$, então $\frac{n-1}{n} < x_{l+1} + \dots + x_n < (n-l)x_{l+1}$, logo $x_1 \geq x_2 \geq \dots \geq x_l \geq x_{l+1} > \frac{1}{n}$, portanto $x_1 + x_2 + \dots + x_l > \frac{1}{n} + \dots + \frac{1}{n} = \frac{l}{n}$, um absurdo. \square

Definição 1.5. Sejam $x, y \in \mathbb{R}^n$. Dizemos que x é (fracamente) *submajorado* por y , e escrevemos $x \prec_{\omega} y$ quando $\sum_{i=1}^k x_i^{\downarrow} \leq \sum_{i=1}^k y_i^{\downarrow}, \forall k \in \{1, 2, 3, \dots, n\}$. Analogamente, se $x, y \in \mathbb{R}^n$ e $x^{\uparrow} \in \mathbb{R}^n$ é um vetor cujas componentes são as componentes de x reescritas em ordem não-decrescente, então dizemos que x é (fracamente) *supermajorado* por y , e escrevemos $x \prec^{\omega} y$, quando $\sum_{i=1}^k x_i^{\uparrow} \geq \sum_{i=1}^k y_i^{\uparrow}, \forall k \in \{1, 2, 3, \dots, n\}$.

Proposição 1.6. Sejam $x, y \in \mathbb{R}^n$ então:

1. $x \prec_{\omega} y$ se, e somente se, $\sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+, \forall t \in \mathbb{R}$;
2. $x \prec^{\omega} y$ se, e somente se, $\sum_{i=1}^n (t - x_i)^+ \leq \sum_{i=1}^n (t - y_i)^+, \forall t \in \mathbb{R}$.

Demonstração. 1)

(\implies)

Suponha que $x \prec_{\omega} y$.

Seja $t \in \mathbb{R}$ arbitrário, então:

Se $t > x_1^{\downarrow}$, como x^{\downarrow} está em ordem não-crescente, então $t > x_1^{\downarrow} \geq x_2^{\downarrow} \geq \dots \geq x_n^{\downarrow}$, donde $0 = (x_i - t)^+$, $\forall i \in I_n$, portanto $0 = \sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+$.

Se $x_{k+1}^{\downarrow} \leq t \leq x_k^{\downarrow}$, $k \in I_{n-1}$, então:

$\sum_{i=1}^n (x_i - t)^+ = \sum_{i=1}^k (x_i^{\downarrow} - t)^+ = \sum_{i=1}^k x_i^{\downarrow} - kt \leq \sum_{i=1}^k y_i^{\downarrow} - kt = \sum_{i=1}^k (y_i^{\downarrow} - t) \leq \sum_{i=1}^n (y_i - t)^+$.

(\Leftarrow)

Suponha que $\sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+$, $\forall t \in \mathbb{R}$.

Se $t = y_k^{\downarrow}$, então $\sum_{i=1}^n (y_i - t)^+ = \sum_{i=1}^k (y_i^{\downarrow} - t) = \sum_{i=1}^k y_i^{\downarrow} - kt$.

Por outro lado $\sum_{i=1}^k x_i^{\downarrow} - kt = \sum_{i=1}^k (x_i^{\downarrow} - t)^+ \leq \sum_{i=1}^n (x_i^{\downarrow} - t)^+ = \sum_{i=1}^n (x_i - t)^+$. Como $\sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+$, $\forall t \in \mathbb{R}$, então $\sum_{i=1}^k x_i^{\downarrow} - kt \leq \sum_{i=1}^k y_i^{\downarrow} - kt$, $\forall k \in I_n$. Portanto $x \prec_{\omega} y$.

2)

(\implies)

Suponha que $x \prec_{\omega} y$. Seja $t \in \mathbb{R}$ arbitrário.

Se $t \leq x_1^{\uparrow} \leq x_2^{\uparrow} \leq \dots \leq x_n^{\uparrow}$, então $t - x_j \leq 0$, $\forall j \in I_n$, donde $\sum_{i=1}^n (t - x_i)^+ = 0 \leq \sum_{i=1}^n (t - y_i)^+$.

Se $x_k^{\uparrow} \leq t \leq x_{k+1}^{\uparrow}$, $k \in I_{n-1}$, então $x_i^{\uparrow} \leq \dots \leq x_k^{\uparrow} \leq t \leq x_{k+1}^{\uparrow} \leq \dots \leq x_n^{\uparrow}$, portanto $\sum_{i=1}^n (t - x_i)^+ = \sum_{i=1}^k (t - x_i^{\uparrow}) = kt - \sum_{i=1}^k x_i^{\uparrow} \leq kt - \sum_{i=1}^k y_i^{\uparrow} = \sum_{i=1}^k (t - y_i)^+ \leq \sum_{i=1}^n (t - y_i)^+$.

(\Leftarrow)

Suponha que $\sum_{i=1}^n (t - x_i)^+ \leq \sum_{i=1}^n (t - y_i)^+$, $\forall t \in \mathbb{R}$.

Se $t = y_k^{\uparrow}$, $k \in I_n$, então $\sum_{i=1}^n (t - y_i)^+ = \sum_{i=1}^k (t - y_i^{\uparrow}) = kt - \sum_{i=1}^k y_i^{\uparrow}$. Por outro lado $kt - \sum_{i=1}^k x_i^{\uparrow} = \sum_{i=1}^k (t - x_i^{\uparrow}) \leq \sum_{i=1}^k (t - x_i^{\uparrow})^+ \leq \sum_{i=1}^n (t - x_i)^+$, portanto $kt - \sum_{i=1}^k x_i^{\uparrow} \leq \sum_{i=1}^n (t - x_i)^+ \leq \sum_{i=1}^n (t - y_i)^+ = kt - \sum_{i=1}^k y_i^{\uparrow}$, logo $\sum_{i=1}^k x_i^{\uparrow} \geq \sum_{i=1}^k y_i^{\uparrow}$. Como $k \in I_n$ é arbitrário, então $x \prec_{\omega} y$. \square

Lema 1.7. *Sejam $x, y \in \mathbb{R}^n$ arbitrários. A fim de que $x \prec y$ é necessário e suficiente que $\sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+, \forall t \in \mathbb{R}$ e $\sum_{i=1}^n x_i = \sum_{i=1}^n y_i$.*

Demonstração. (\implies)

Suponha que $x \prec y$.

Como $x \prec y$, então $\sum_{i=1}^n x_i = \sum_{i=1}^n y_i$ e $x \prec_{\omega} y$, logo $\sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+, \forall t \in \mathbb{R}$.

(\impliedby)

Suponha que $\sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+, \forall t \in \mathbb{R}$ e $\sum_{i=1}^n x_i = \sum_{i=1}^n y_i$.

Como $\sum_{i=1}^n (x_i - t)^+ \leq \sum_{i=1}^n (y_i - t)^+, \forall t \in \mathbb{R}$, então $x \prec_{\omega} y$, donde $\sum_{i=1}^k x_i^{\downarrow} \leq \sum_{i=1}^k y_i^{\downarrow}, \forall k \in \{1, 2, 3, \dots, n\}$. Além disso, como $\sum_{i=1}^n x_i = \sum_{i=1}^n y_i$, então $x \prec y$. \square

Antes de prosseguir, vamos fazer uma pequena parada e definir um novo conceito que ajudará na visualização “geométrica” da afirmação $x \prec y$. Nosso objetivo é mostrar que se $x \prec y$, então podemos obter x apenas permutando e multiplicando as componentes de y numa forma bonitinha.

Definição 1.8. *Uma matriz quadrada $D \in M_n(\mathbb{R})$ é (simplesmente) Estocástica quando todos os seus elementos são não-negativos e cada linha tem soma igual a unidade. Se em adição a ser Estocástica, cada coluna de D tem soma igual a um, então dizemos que a matriz D é Duplamente Estocástica.*

Definição 1.9. *Uma matriz quadrada $P \in M_n(\mathbb{R})$ é uma Matriz de Permutação quando cada linha e cada coluna tem uma única unidade e todas as outras entradas nulas.*

Segue diretamente das definições acima que toda matriz de Permutação é uma matriz Duplamente Estocástica, e que toda matriz Duplamente Estocástica é (simplesmente) Estocástica.

-Exemplos-

1)

O exemplo trivial (e recorrente):

$$\mathbb{1} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

2)

Seja $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$ uma aplicação linear dada por $T(e_1) = e_j$, $T(e_j) = e_1$ e $T(e_i) = e_i$, $\forall i \in I_n - \{1, j\}$. Portanto:

$$[T] = \begin{pmatrix} 0 & 0 & \dots & 1 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

3)

$$M_n(\mathbb{R}) \ni D = \frac{1}{n} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix}.$$

Note que a matriz D acima é Duplamente Estocástica, mas não é de Permutação.

4)

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix}.$$

Já a matriz A , no exemplo 4) é Estocástica, mas não é Duplamente Estocástica, e muito menos é de Permutação.

Lema 1.10. *Sejam $P, Q \in \mathbb{M}_n\mathbb{R}$ matrizes duplamente estocásticas. Afirmamos que $T = PQ$ é duplamente estocástica.*

Demonstração. Como $P_{ij}, Q_{ij} \geq 0, \forall i, j \in I_n$, então $T_{ij} = \sum_{k=1}^n P_{ik}Q_{kj} = P_{i1}Q_{1j} + P_{i2}Q_{2j} + \dots + P_{in}Q_{nj} \geq 0, \forall i, j \in I_n$. Além disso, $\sum_{i=1}^n T_{ij} = \sum_{i=1}^n \sum_{k=1}^n P_{ik}Q_{kj} = \sum_{k=1}^n (\sum_{i=1}^n P_{ik})Q_{kj} = 1 \cdot \sum_{k=1}^n Q_{kj} = 1, \forall j \in I_n$. Analogamente $\sum_{j=1}^n T_{ij} = \sum_{j=1}^n \sum_{k=1}^n P_{ik}Q_{kj} = 1, \forall i \in I_n$. Portanto T é duplamente estocástica. \square

Proposição 1.11. *O conjunto $\mathfrak{D} = \{D \in \mathbb{M}_n(\mathbb{R}); D \text{ é uma matriz duplamente estocástica}\}$ é um conjunto convexo.*

Demonstração. Sejam $P, Q \in \mathfrak{D}$ e $t \in [0, 1]$ arbitrários.

Defina $T = tP + (1 - t)Q$. Basta mostrar que T é duplamente estocástica.

Como $P_{ij}, Q_{ij} \geq 0, \forall i, j \in I_n$ e $t \in [0, 1]$ então $T_{ij} = tP_{ij} + (1 - t)Q_{ij} \geq 0, \forall i, j \in I_n$. Além disso $\sum_{i=1}^n T_{ij} = \sum_{i=1}^n (tP_{ij} + (1 - t)Q_{ij}) = t \sum_{i=1}^n P_{ij} + (1 - t) \sum_{i=1}^n Q_{ij} = t + 1 - t = 1, \forall j \in I_n$. Analogamente $\sum_{j=1}^n T_{ij} = 1, \forall i \in I_n$.

\square

Para terminar nosso pequeno *pit stop* enunciamos o teorema de Birkhoff[4]:

Teorema (Birkhoff) 1.12. *As matrizes de permutação constituem os pontos extremos do conjunto das matrizes duplamente estocásticas. Além disso, o conjunto das matrizes duplamente estocásticas é o fecho convexo das matrizes de permutação.*

1.3 Alguns Lemas importantes

Começaremos com o:

Lema 1.13. *Sejam $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{R}^n$, t.q. $y_1 \geq y_2 \geq \dots \geq y_n$. Seja $X = \{x_1, \dots, x_n\}$. A fim de que $x \prec y$ é necessário e suficiente que $\max_{X' \subset X, |X'|=l} \{\sum_{x_i \in X'} x_i\} \leq \sum_{i=1}^l y_i, \forall l \in I_{n-1}$, com a igualdade verdadeira se $l = n$.*

Demonstração. (\implies)

Suponha que $x \prec y$.

Como $x \prec y$, então $\sum_{i=1}^l x_i^\downarrow \leq \sum_{i=1}^l y_i^\downarrow, \forall l \in I_{n-1}$ e $x_1^\downarrow + \dots + x_n^\downarrow = y_1 + \dots + y_n$. Seja $l \in I_{n-1}$ qualquer, como $\max_{X' \subset X, |X'|=l} \{\sum_{x_i \in X'} x_i\} \leq \sum_{i=1}^l x_i^\downarrow$, então $\max_{X' \subset X, |X'|=l} \{\sum_{x_i \in X'} x_i\} \leq \sum_{i=1}^l x_i^\downarrow \leq \sum_{i=1}^l y_i$.

(\Leftarrow)

Suponha que $x_1 + \dots + x_n = y_1 + \dots + y_n$ e $\max_{X' \subset X, |X'|=l} \{\sum_{x_i \in X'} x_i\} \leq \sum_{i=1}^l y_i, \forall l \in I_{n-1}$.

Em particular $\sum_{i=1}^l x_i^\downarrow \leq \sum_{i=1}^l y_i, \forall l \in I_n$. Donde $x \prec y$. \square

Lema 1.14. Afim de que $x \prec y$ é necessário e suficiente que $x = Dy$, t.q. D é uma matriz duplamente estocástica.

Demonstração. (\Leftarrow)

Suponha que $x = Dy$.

Como D é duplamente estocástica, o teorema de Birkhoff garante que existem uma distribuição de probabilidade (p_1, p_2, \dots, p_m) e matrizes de permutação P_1, P_2, \dots, P_m t.q. $D = \sum_{i=1}^m p_i P_i$. Portanto $x = \sum_{i=1}^m p_i P_i y$. Como $P_j y \prec y, \forall j \in I_m$, então $x = \sum_{i=1}^m p_i P_i y \prec y$.

(\Rightarrow)

Suponha que $x \prec y$. Sem perda de generalidade suponha que $x = x^\downarrow$ e $y = y^\downarrow$.

Indução em n .

i) Se $n = 1$,

Como $n = 1$ e $x \prec y$, então $x = y = \mathbb{1}y$.

ii) Suponha o resultado válido para $x, y \in \mathbb{R}^k$, logo:

Sejam $x, y \in \mathbb{R}^{k+1}$, t.q. $x \prec y$. Como $x \prec y$, então $x_1 \leq y_1$. Defina $J = \{i \in I_{k+1} - \{1\}; y_i \leq x_1 \leq y_1\} \neq \emptyset$. Seja $j_0 = \min J$, então $y_{j_0} \leq x_1 \leq y_1$, portanto $\exists t \in [0, 1]$ t.q. $x_1 = ty_1 + (1-t)y_{j_0}$. Defina $D' : \mathbb{R}^{k+1} \rightarrow \mathbb{R}^{k+1}$ dada por $D' = t\mathbb{1} + (1-t)T$, T a permutação que troca a primeira com a j_0 -ésima entrada. Portanto $D'y = D'(y_1, \dots, y_{k+1}) = (y_1, y_2, y_3, \dots, y_{j_0-1}, ty_{j_0} + (1-t)y_1, y_{j_0+1}, \dots, y_{k+1})$.

Defina $x' = (x_2, \dots, x_{k+1})$ e $y' = (y_2, y_3, \dots, y_{j_0-1}, ty_{j_0} + (1-t)y_1, y_{j_0+1}, \dots, y_{k+1})$. Afirmamos que $x' \prec y'$, portanto existem uma distribuição de probabilidade $\{p'_1, \dots, p'_m\}$ e matrizes de permutação P'_1, P'_2, \dots, P'_m t.q. $x' = \sum_{i=1}^m p'_i P'_i y'$, logo $x = \sum_{i=1}^m p'_i P_i D y$, onde P_1, P_2, \dots, P_m, D são extensões de $P'_1, P'_2, \dots, P'_m, D'$ naturais que atuam trivialmente na primeira entrada. Como o produto de duas matrizes duplamente estocásticas é uma matriz duplamente estocástica, veja Lema 1.10, então o resultado é válido para $k+1$.

Como $x \prec y$, então $\sum_{i=1}^m x_i \leq \sum_{i=1}^m y_i, \forall m \in I_{k+1}$ e $\sum_{i=1}^{k+1} x_i \leq \sum_{i=1}^{k+1} y_i$. Além disso $y' = (y_2, y_3, \dots, y_1 - x_1 + y_{j_0}, \dots, y_{k+1})$. Como

$y_{j_0} \leq x_1 \leq y_1$, então $-y_{j_0} \geq -x_1 \geq -y_1$, donde $y_1 + y_{j_0} - x_1 \geq y_{j_0}$ e $y_1 + y_{j_0} - x_1 \leq y_1$, portanto, com $a = y_1 + y_{j_0} - x_1$ tem-se que $y_1 \geq a \geq y_{j_0} \geq y_{j_0+1} \geq \dots \geq y_{k+1}$. Como $j_0 = \min J$, então $y_1 \geq \dots \geq y_{j_0-1} \geq a \geq y_{j_0} \geq \dots \geq y_{k+1}$.

Seja $m \in \{1, 2, \dots, j_0 - 2\}$, como $y_1 \geq \dots \geq y_{j_0-1} \geq x_1 \geq x_2 \geq \dots \geq x_k$, então $\sum_{i=1}^m x'_i \leq \sum_{i=1}^m y'_i$. Por outro lado, se $m \in I_k$, então $\sum_{i=1}^m y'_i = \sum_{i=2}^{m+1} y_i = \sum_{i=2}^{j_0-1} y_i + y_1 y_{j_0} - x_1 + \sum_{i=j_0+1}^m = \sum_{i=1}^m y_i - x_1 \geq \sum_{i=1}^m x_i - x_1 = \sum_{i=2}^m x_1 = \sum_{i=1}^m x'_i$.

□

Corolário 1.15. O conjunto $T(y) = \{x \in \mathbb{R}^n; x \prec y\}$ é convexo, $\forall y \in \mathbb{R}^n$.

Demonstração. Sejam $x, z \in T(y)$ e $t \in [0, 1]$ arbitrários. Defina $\zeta = tx + (1 - t)z$.

Como $x, z \in T(y)$, então o Lema 1.14 garante que existem matrizes D_x, D_z duplamente estocásticas t.q. $x = D_x y$ e $z = D_z y$. Portanto:

$$\zeta = tx + (1 - t)z = tD_x y + (1 - t)D_z y = [tD_x + (1 - t)D_z]y.$$

Por outro lado, o conjunto das matrizes duplamente estocásticas é convexo, logo $D = tD_x + (1 - t)D_z$ é duplamente estocástica. Então $\zeta = Dy$, D duplamente estocástica, donde $\zeta \in T(y)$. □

Corolário 1.16. Sejam $x, y \in \mathbb{R}^n$. A fim de que $x \prec y$ é necessário, e suficiente que $x = \sum_{i=1}^m p_i P_i y$, t.q. (p_1, p_2, \dots, p_m) é uma distribuição de probabilidade e P_1, P_2, \dots, P_m são matrizes de permutação.

O Corolário 1.16 garante que se $x \prec y$, então x vive na envoltória convexa da órbita de y sob o grupo das matrizes de permutação [5].

Corolário 1.17. Sejam $x, y \in \mathbb{R}^n$. Se $x \prec y$, então $x \otimes z \prec y \otimes z$, qualquer que seja $z \in \mathbb{R}^k$.

O Lema acima vai se mostrar importante no decorrer do texto. O fato a ser ressaltado é que a “volta” dele não é, em geral, verdadeira.

Demonstração. Sejam $x, y \in \mathbb{R}^n$ e $z \in \mathbb{R}^k$ arbitrários, t.q. $x \prec y$, então:

O lema 1.14 garante que existe uma matriz duplamente estocástica B t.q. $x = By$. Como $\mathbb{1}$ é duplamente estocástica, então $B \otimes \mathbb{1}$ é também duplamente estocástica, logo $x = By \implies x \otimes z = (B \otimes \mathbb{1})y \otimes z$. Portanto $x \otimes z \prec y \otimes z$. □

Definição 1.18. *Sejam H, K dois operadores auto-adjuntos, e $\lambda(H)$ o vetor contendo todos os auto-valores de H . Dizemos que $H \prec K$ quando $\lambda(H) \prec \lambda(K)$.*

Teorema 1.19. *Sejam H, K operadores auto-adjuntos sobre \mathbb{C}^n . A fim de que $H \prec K$ é necessário e suficiente que existam uma distribuição de probabilidade (p_1, p_2, \dots, p_m) e matrizes unitárias $\{U_1, U_2, \dots, U_m\}$ t.q. $H = \sum_{j=1}^m p_j U_j K U_j^*$.*

Demonstração. ⁴ (\implies)

Suponha que $H \prec K$.

Como H, K são auto adjuntos, então existem bases ortonormais de \mathbb{C}^n , $\{u_1, u_2, \dots, u_n\}$ e $\{v_1, v_2, \dots, v_n\}$, t.q. $H = \sum_{i=1}^n \lambda(H)_i u_i u_i^*$ e $K = \sum_{i=1}^n \lambda(K)_i v_i v_i^*$. Além disso, como $H \prec K$ e portanto $\lambda(H) \prec \lambda(K)$, então existem uma distribuição de probabilidade $\{p_\pi; \pi \in S \subset S_m\}$ e matrizes de permutação $\{P_\pi; \pi \in S \subset S_m\}$, t.q.⁵ $\lambda(H) = \sum_{\pi \in S} p_\pi P_\pi \lambda(K)$.

Para cada $\pi \in S$ defina $U_\pi = \sum_{j=1}^n u_j v_{\pi(j)}^*$, logo:

$$U_\pi U_\pi^* = \sum_{i,j=1}^n u_j v_{\pi(j)}^* \cdot v_{\pi(i)} u_i^* = \sum_{i,j=1}^n u_j u_i^* \delta_{\pi(i)\pi(j)} = \sum_{i=1}^n u_i^* u_i = \mathbb{1}, \forall \pi \in S,$$

e analogamente

$$U_\pi^* U_\pi = \mathbb{1}, \forall \pi \in S.$$

Portanto,

$$T = \sum_{\pi \in S} p_\pi U_\pi K U_\pi^* = \sum_{\pi, j, i} p_\pi u_j v_{\pi(j)}^* K v_{\pi(i)} u_i^* = \sum_{\pi, j, i} p_\pi v_{\pi(j)}^* K v_{\pi(i)} u_j u_i^*.$$

Como $K = \sum_{l=1}^n \lambda(K)_l v_l v_l^*$, então $v_{\pi(j)} K v_{\pi(i)} = \sum_{l=1}^n \lambda(K)_l \delta_{\pi(j)l} \delta_{\pi(i)l} = \lambda(K)_{\pi(i)}$ $\delta_{\pi(j)\pi(i)}$, donde $T = \sum_{\pi, i, j} p_\pi \lambda(K)_{\pi(i)} \delta_{\pi(i)\pi(j)} u_j u_i^* = \sum_{\pi, i} p_\pi \lambda(K)_i u_i u_i^*$. Por outro lado, como $\lambda(H) = \sum_{\pi \in S} p_\pi P_\pi \lambda(K)$, então $\lambda(H)_j = \sum_{\pi \in S} p_\pi \lambda(K)_{\pi(j)}$, portanto $T = \sum_{i=1}^n \lambda(H)_i u_i u_i^* = H$.

(\Leftarrow)

Suponha que exista uma distribuição de probabilidade $\{p_\pi\}$ e operadores unitários $\{U_\pi\}$ t.q. $H = \sum_{\pi \in S \subset S_n} p_\pi U_\pi K U_\pi^*$, além disso seja $\{u_1, \dots, u_n\}$ uma base de auto-vetores de H , então:

$$\lambda(H)_i = \sum_{\pi} p_\pi u_i^* U_\pi K U_\pi^* u_i = \sum_{\pi, j} p_\pi \lambda(K)_j u_i^* U_\pi v_j v_j^* U_\pi^* u_i = \sum_{\pi, j} \|u_i^* U_\pi v_j\|^2 \lambda(K)_j.$$

⁴Uma demonstração alternativa, numa roupagem que agradará muito mais aos físicos, pode ser encontrada em [22].

⁵No espírito de [6], cada $\pi \in S \subset S_n$ representa uma permutação nos índices dos vetores, portanto $P_\pi \lambda(K) = (\lambda(K)_{\pi(1)}, \dots, \lambda(K)_{\pi(n)})$.

Defina $D_{ij} = \sum_{\pi \in S} p_{\pi} \|u_i^* U_{\pi} v_j\|^2$, $\forall i, j \in I_n$, então $\lambda(H)_i \sum_{j=1}^n D_{ij} \lambda(K)_j$, donde $\lambda(H) = D\lambda(K)$. Afirmamos que D é duplamente estocástica, portanto o lema 1.14 garante que $\lambda(H) \prec \lambda(K)$, logo $H \prec K$.

Como $p_{\pi} \geq 0$, $\forall \pi \in S$ e $\|u_i^* U_{\pi} v_j\|^2 \geq 0$, $\forall i, j \in I_n$, então $D_{ij} \geq 0$, $\forall i, j \in I_n$. Além disso, $\sum_{i=1}^n D_{ij} = \sum_{\pi \in S} \sum_{i=1}^n p_{\pi} u_i^* U_{\pi} v_j v_j^* U_{\pi}^* u_i = \sum_{\pi \in S} p_{\pi} v_j^* U_{\pi}^* (\sum_{i=1}^n u_i u_i^*) v_j = \sum_{\pi \in S} p_{\pi} v_j^* U_{\pi}^* U_{\pi} v_j = \sum_{\pi \in S} p_{\pi} = 1$, $\forall j \in I_n$. Analogamente $\sum_{j=1}^n D_{ij} = 1$, $\forall i \in I_n$.

□

É claro que a Teoria da Majoração não se resume a meia-dúzia de Lemas, Teoremas e Proposições. Ela é uma subárea da Matemática Pura por direito, e existem grandes textos dedicados inteiramente a esse ordenamento parcial [4, 7]. Os resultados acima demonstrados são necessários (suficientes?) e serão amplamente utilizados nos próximos capítulos desta dissertação. Podemos agora prosseguir com nosso caminho e adentrar no maravilhoso mundo da Mecânica Quântica.

Capítulo 2

Um pouco de Mecânica Quântica

*“Quantum physics makes me so happy... It’s like looking at the universe naked.”
(Sheldon Cooper)*

Nesse capítulo vamos discutir os postulados básicos da Mecânica Quântica. Não abordaremos aqui muito dos assuntos que são usualmente encontrados em livros padrões na área [2, 12, 13, 15]. Estamos mais interessados nos conceitos de Estados, Testes, Medições, Emaranhamento, Estados Reduzidos, Purificação e Decomposição de Schmidt, além claro de suas implicações e aplicações. Esse capítulo é uma condição necessária para que não só as seções seguintes, mas a motivação desta Dissertação, sejam entendidas. O ponto de vista adotado aqui é parecido com aquele visto em [16, 22].

2.1 Postulados Básicos da Mecânica Quântica

2.1.1 Qubits

Na Mecânica Clássica [1] o estado de um sistema é representado por um ponto no espaço de fase. Iremos adotar provisoriamente a seguinte definição para um sistema governado pela Mecânica Quântica:

Axioma 2.1. *Para cada sistema quântico está associado um Espaço Vetorial H sobre o corpo dos complexos, dotado de produto interno¹ e completo, chamado de Espaço de Estados². O estado de um sistema é representado por um vetor normalizado $\psi \in H$.*

¹Por razões históricas produtos escalares em Mecânica Quântica são lineares na segunda entrada.

²Veja que não dizemos qual espaço vetorial é esse. Apenas dizemos que ele existe!

Existe uma notação mnemônica devida a Dirac que iremos usar por todo o texto e que é padrão na maioria dos textos envolvendo Mecânica Quântica³: Para Dirac, o estado do sistema é representado por um vetor $|\psi\rangle \in H$ (lê-se *ket psi*), e tão importante quanto os *kets* e o espaço H é o seu dual $H' = \{l : H \rightarrow \mathbb{C}; l \text{ é linear}\}$. Fixado $|\psi\rangle \in H$ podemos definir o funcional linear *fazer produto interno com $|\psi\rangle$* por:

$$PI_{|\psi\rangle} : H \rightarrow \mathbb{C}$$

$$PI_{|\psi\rangle}(|\phi\rangle) = \langle |\psi\rangle, |\phi\rangle \rangle, \forall \phi \in H.$$

Vamos fazer $PI_{|\psi\rangle} = \langle \psi|$ e escrever $PI_{|\psi\rangle}(|\phi\rangle) = \langle \psi||\phi\rangle = \langle \psi|\phi\rangle = \langle |\psi\rangle, |\phi\rangle \rangle$. A aplicação que acabamos de definir é conhecida como *bra psi*.

A um conjunto de alternativas classicamente distintas será associado um conjunto de vetores ortogonais em H , logo a dimensão do espaço de estados está diretamente associada com o número dessas alternativas.

Na teoria clássica da informação um Bit é a menor unidade de informação que pode ser armazenada e transmitida de uma fonte para um receptor, assumindo somente dois valores possíveis: Zero ou Um, Mais ou Menos, Sim ou Não, Para cima ou Para baixo, Com corrente ou Sem corrente... A situação é análoga quando tentamos passar informação usando sistemas que são regidos pela Mecânica Quântica. Agora qualquer sistema com espaço de estados de dimensão igual a 2 realiza um bit quântico⁴ (qubit) e devemos sempre observar qual sistema está sendo usado para transmitir informação, como o receptor receberá a informação passada, como o envio de informação será feito, quais são as influências externas e se elas são ou não controláveis. Vários são os sistemas que realizam qubits: Spin dos átomos de prata no aparato de Stern-Gerlach[2], Polarização de fótons[2] ou ainda um Experimento de fenda dupla[17].

Mesmo sabendo como representar um estado e que um conjunto de alternativas clássicas distintas está associado a um conjunto de vetores ortogonais, ainda não sabemos por exemplo como confirmar que um sistema está ou não num dado estado (ou que um qubit está ou não no estado inicial de interesse). Logo precisamos definir a noção de medição ou teste.

³Existem ótimos livros sobre Teoria Quântica, que não usam a notação de Dirac, veja: [18, 19, 24]. Aqui mantemos a notação simplesmente pela tradição!

⁴Por isso nos interessam somente os espaços vetoriais de dimensão finita!

Axioma 2.2. Para um teste B com alternativas classicamente distintas a e b associa-se a uma base ortonormal de H , $\beta = \{|a\rangle, |b\rangle\}$. Aplicar um teste pode ser visto como decompor um vetor na base, para em seguida selecionar apenas uma das alternativas.

Assim se estamos interessados em aplicar um teste B com duas alternativas classicamente distintas a e b então, $|\psi\rangle \in H \implies |\psi\rangle = \alpha|a\rangle + \lambda|b\rangle$; $\alpha, \lambda \in \mathbb{C}$. Os escalares α e λ foram chamados por Feynman de amplitudes de probabilidade⁵, $|\alpha|^2$ é a probabilidade de que no teste B obtenhamos o resultado rotulado por a e $|\lambda|^2$ é a probabilidade que no mesmo teste B obtenhamos o resultado rotulado por b .

Proposição 2.3. Seja $\beta = \{|a\rangle, |b\rangle\}$ uma base ortonormal para o espaço de estados, então $H \ni |\psi\rangle = \alpha|a\rangle + \lambda|b\rangle \implies |\alpha|^2 + |\lambda|^2 = 1$.

Demonstração. Seja dado $H \ni |\psi\rangle = \alpha|a\rangle + \lambda|b\rangle$, então $1 = \langle |\psi\rangle, |\psi\rangle \rangle = \langle \alpha|a\rangle + \lambda|b\rangle, \alpha|a\rangle + \lambda|b\rangle \rangle = \bar{\alpha}.\alpha \langle |a\rangle, |a\rangle \rangle + \bar{\alpha}.\lambda \langle |a\rangle, |b\rangle \rangle + \bar{\lambda}.\alpha \langle |b\rangle, |a\rangle \rangle + \bar{\lambda}.\lambda \langle |b\rangle, |b\rangle \rangle = |\alpha|^2 + |\lambda|^2 \implies |\alpha|^2 + |\lambda|^2 = 1. \quad \square$

Já sabemos como representar um estado, como fazer medições nesse estado e também como prever probabilisticamente quais resultados são possíveis num experimento. Mas ainda resta uma dúvida: “Após um experimento que discrimina entre duas alternativas distintas, para onde vai o sistema?”.

Axioma 2.4. (Reprodutibilidade.) Seja B um teste com alternativas classicamente distintas a e b , com uma base $\beta = \{|a\rangle, |b\rangle\}$ associada. Após a medição, se o resultado obtido foi a , então o sistema passa a ser descrito por $|a\rangle$, se o resultado obtido foi b , então o sistema passa a ser descrito por $|b\rangle$.

Sejam B um teste que discrimina entre as alternativas a e b e $|\psi\rangle = \alpha|a\rangle + \lambda|b\rangle$ o estado do sistema antes da realização da medição. Suponha que o resultado b foi obtido. Logo depois do teste o sistema é descrito por $|\psi\rangle = |b\rangle$, portanto se realizarmos o mesmo teste novamente sobre esse mesmo representante do sistema, a definição 2.4 garante que sempre vamos obter o resultado b com 100% de certeza. Contudo se realizarmos o mesmo teste em outro representante do sistema podemos obter ao invés do resultado b o resultado a [2].

⁵Diferentemente da Mecânica Estatística [21], a Mecânica Quântica é uma teoria probabilística a priori.

2.1.2 2 Qubits

Podemos agora dar um passo além e discutir sistemas formados por duas partes. A motivação natural é poder trabalhar com dois ou mais bits quânticos simultaneamente.

Axioma 2.5. *Sejam A e B dois sistemas regidos pela Mecânica Quântica, com espaço de estados H_A e H_B tais que $\dim H_A = n$ e $\dim H_B = m$, então o espaço de estados conjunto é $H_A \otimes H_B$.*

Portanto, se $\{|a_1\rangle, |a_2\rangle, \dots, |a_n\rangle\}$ é uma base ortonormal de H_A e $\{|b_1\rangle, |b_2\rangle, \dots, |b_m\rangle\}$ é uma base ortonormal de H_B , então $\{|a_1\rangle \otimes |b_1\rangle, |a_1\rangle \otimes |b_2\rangle, \dots, |a_1\rangle \otimes |b_m\rangle, |a_2\rangle \otimes |b_1\rangle, |a_2\rangle \otimes |b_2\rangle, \dots, |a_n\rangle \otimes |b_m\rangle\}$ é uma base ortonormal de $H_A \otimes H_B$. Logo a dimensão de $H_A \otimes H_B$ é nm . No caso de bits quânticos cada espaço de estados tem dimensão igual a dois, portanto o sistema conjunto tem dimensão igual a 4 e usaremos a base computacional⁶ $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Apesar de $H_A \otimes H_B$ ser gerado por vetores $|a_i\rangle \otimes |b_j\rangle$, esse espaço não se restringe somente a esses casos⁷. Citamos por exemplo os seguintes estados:⁸

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle); \quad (2.1)$$

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (2.2)$$

Ainda temos a associação entre alternativas distintas e vetores ortogonais em H , mas agora pode acontecer que o número de alternativas classicamente distintas seja menor que o número de vetores ortogonais, logo pode ocorrer que para a mesma alternativa tenhamos dois ou mais vetores ortogonais associados. Precisamos generalizar a definição 2.2.

Axioma 2.6. *Seja H um espaço de estados e $|\psi\rangle \in H$ um vetor normalizado. Um teste com alternativas classicamente distintas, cada uma indexada por i , corresponde a uma decomposição ortogonal $\bigoplus_i H_i$. Seja $P_i : H \rightarrow H$ o projetor ortogonal sobre H_i , então a probabilidade de obter o i -ésimo resultado é dada por $\langle \psi | P_i | \psi \rangle$.*

Além disso:

⁶Por questões de economia, e aonde não houver confusão, a partir de agora vamos escrever $|a\rangle \otimes |b\rangle = |ab\rangle$

⁷De fato, os outros vetores que compõem $H_A \otimes H_B$ são os responsáveis pelas tarefas que somente a Teoria Quântica da Informação e a Computação Quântica podem realizar, tais como: Teleportação, Codificação Superdensa, Fatoração de números primos em tempo polinomial, Catálise, Algoritmos de busca mais rápidos, entre outros[16, 22].

⁸Iremos vê-los novamente mais a frente.

Definição 2.7. *Seja B um teste que discrimina entre alternativas classicamente distintas indexadas por i ao qual está associada a decomposição $\bigoplus_i H_i$. Então se o teste for aplicado ao estado representado por $|\psi\rangle$ e a alternativa i for obtida, o estado passará a ser descrito por $|\psi_i\rangle = \frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$.*

2.1.3 Generalizações

Pode acontecer que não tenhamos como, ao preparar um sistema, conseguir tirar o máximo de informação possível para escrever seu representante $|\psi\rangle$ apenas como uma combinação linear simples de alguns outros *kets*. Tudo o que sabemos é que o sistema pode assumir os estados $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ com respectivas probabilidades $\{p_1, p_2, p_3, \dots, p_n\}$, então podemos nos perguntar: “Como representar o estado de um sistema quando temos um conhecimento incompleto⁹ sobre ele?”.

Axioma 2.8. *Para um sistema descrito pelo conjunto de pares $\{(p_i, |\psi_i\rangle); i \in \{1, 2, 3, \dots, n\}\}$ seu estado é dado pelo operador*

$$\rho = \sum_{i=1}^n p_i |\psi_i\rangle \langle \psi_i|.$$

Axioma 2.9. *Se o estado do sistema é inicialmente $|\psi_i\rangle$, então a probabilidade de se obter o resultado m numa medição generalizada descrita pelos operadores $\{M_1, M_2, \dots, M_n; \sum_{k=1}^n M_k^* M_k = \mathbb{1}\}$ é $p(m|i) = \langle \psi_i | M_m^* M_m | \psi_i \rangle$.*

Proposição 2.10. *Afirmamos que $p(m|i) = \langle \psi_i | M_m^* M_m | \psi_i \rangle = \text{tr}(M_m^* M_m | \psi_i \rangle \langle \psi_i |)$.*

Demonstração. De fato:

$$\text{tr}(M_m^* M_m | \psi_i \rangle \langle \psi_i |) = \sum_{k=1}^n \langle \psi_k | M_m^* M_m | \psi_i \rangle \langle \psi_i | \psi_k \rangle = \sum_{k=1}^n \langle \psi_k | M_m^* M_m | \psi_i \rangle \delta_{ik} = \langle \psi_i | M_m^* M_m | \psi_i \rangle. \quad \square$$

Como $p(m) = \sum_{i=1}^n p_i p(m|i)$ é a probabilidade de obter o resultado m a partir das probabilidades condicionais, então $p(m) = \sum_{i=1}^n p_i \text{tr}(M_m^* M_m | \psi_i \rangle \langle \psi_i |) = \text{tr}(M_m^* M_m \sum_{i=1}^n p_i |\psi_i\rangle \langle \psi_i|) = \text{tr}(M_m^* M_m \rho)$. A próxima pergunta natural é: “Qual é o operador densidade que representará o sistema quando obtemos

⁹U. Fano diz que um estado é misto quando não existe um conjunto de experimentos que determina completamente todas as características deste estado[28].

o resultado com rótulo m ”. De fato se $|\psi_i\rangle$ é o estado antes da medição, então definimos o estado do sistema após obtido o resultado m por $|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^*M_m|\psi_i\rangle}}$.

Proposição 2.11. O operador densidade que descreve o sistema após obtido o resultado com rótulo m é $\rho_m = \frac{M_m\rho M_m^*}{\text{tr}(M_m^*M_m\rho)}$.

*Demonstração.*¹⁰

$$\begin{aligned}\rho_m &= \sum_{i=1}^n p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \\ &= \sum_{i=1}^n \frac{p(m|i)p_i}{p(m)} \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^*}{\langle\psi_i|M_m^*M_m|\psi_i\rangle} = \\ &= \frac{\sum_{i=1}^n p_i \left[\frac{\text{tr}(M_m^*M_m|\psi_i\rangle\langle\psi_i|) \cdot M_m|\psi_i\rangle\langle\psi_i|M_m^*}{\text{tr}(M_m^*M_m|\psi_i\rangle\langle\psi_i|)} \right]}{p(m)} = \\ &= \frac{M_m\rho M_m^*}{p(m)} = \frac{M_m\rho M_m^*}{\text{tr}(M_m^*M_m\rho)}.\end{aligned}$$

□

Poderíamos também supor que para um dado sistema conhecemos somente um conjunto de operadores densidade $\{\rho_1, \rho_2, \dots, \rho_n\}$ com distribuição de probabilidades $\{p_1, p_2, \dots, p_n\}$, então o operador densidade que descreve o sistema nesse caso é $\rho = \sum_{i=1}^n p_i\rho_i$.

Feitas as motivações podemos passar para uma estrutura mais formal e enfim enunciar a forma definitiva dos postulados básicos da Mecânica Quântica:

- Para cada sistema governado pela Mecânica Quântica existe associado um espaço vetorial H sobre o corpo dos complexos, munido de produto interno e completo, chamado de Espaço de Estados. O estado do sistema é representado por um operador $\rho : H \rightarrow H$ auto-adjunto, positivo-semidefinido, de traço 1;
- Medições (Generalizadas) são descritas por operadores $\{M_i : H \rightarrow H; \sum_{i=1}^n M_i^*M_i = 1\}$ tal que $i \in \{1, 2, 3, \dots, n\}$. A probabilidade de obter o resultado com rótulo m é $\text{tr}(M_m^*M_m\rho)$ e se esse resultado é obtido então o sistema passa a ser descrito pelo operador $\rho_m : H \rightarrow H$ dado por $\rho_m = \frac{M_m^*\rho M_m}{\text{tr}(M_m^*M_m\rho)}$;

¹⁰Aqui usaremos o Teorema de Bayes [29].

- O Espaço de Estados de um sistema composto de várias partes é o produto tensorial dos Espaços de Estados de cada parte.

Podemos então nos perguntar: “Como os casos inicialmente discutidos podem ser recuperados com a descrição de um estado pelo operador densidade ρ ?”. De fato, se temos o conhecimento completo do estado de um sistema¹¹, então o conjunto $\{(p_1, |\psi_1\rangle), (p_2, |\psi_2\rangle), \dots, (p_n, |\psi_n\rangle)\}$ tem a seguinte característica: $p_k = 1$ para algum $k \in \{1, 2, 3, \dots, n\}$ e $p_j = 0, \forall j \neq k \in \{1, 2, 3, \dots, n\}$. Logo $\rho = |\psi_k\rangle\langle\psi_k|$ e simplesmente podemos escrever que o ket $|\psi_k\rangle$ é o representante do sistema. Reescreveremos esse resultado sob a forma de um teorema:

Teorema 2.12. *Seja A um sistema descrito pelo operador densidade $\rho : H \rightarrow H$, então $\text{tr}(\rho^2) \leq 1$ com a igualdade verdadeira se, e somente se, A está num estado puro.*

Demonstração. Seja $\rho : H \rightarrow H$ o operador densidade que representa A . Seja a decomposição espectral de ρ dada por $\rho = \sum_{i=1}^n p_i |\psi_i\rangle\langle\psi_i|$, então $\rho^2 = \rho \circ \rho = \sum_{i=1}^n \sum_{j=1}^n p_i p_j |\psi_j\rangle\langle\psi_j| |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^n \sum_{j=1}^n p_i \cdot p_j |\psi_j\rangle\langle\psi_i| \delta_{ij} = \sum_{i=1}^n p_i^2 |\psi_i\rangle\langle\psi_i| \implies \text{tr}(\rho^2) = \sum_{k=1}^n \langle\psi_k| (\sum_{i=1}^n p_i^2 |\psi_i\rangle\langle\psi_i|) |\psi_k\rangle = \sum_{i=1}^n \sum_{k=1}^n p_i^2 \delta_{ik} = \sum_{k=1}^n p_k^2$.

Afirmamos que $\sum_{k=1}^n p_k^2 \leq 1$. De fato $1 = (\sum_{i=1}^n p_i)(\sum_{j=1}^n p_j) = \sum_{i=1}^n \sum_{j=1}^n p_i \cdot p_j = \sum_{i=j=1}^n p_i \cdot p_j + \sum_{j=1}^n \sum_{i \neq j=1}^n p_i \cdot p_j \geq \sum_{i=1}^n p_i^2$.

(\Leftarrow)

Suponha que o sistema esteja num estado puro, então $p_k = 1$ para algum $k \in \{1, 2, 3, \dots, n\}$. Como $\sum_{i=1}^n p_i = 1$ e $0 \leq p_i \leq 1, \forall i \in \{1, 2, 3, \dots, n\}$, então $p_i = 0, \forall i \neq k$ e portanto $\sum_{i=1}^n p_i^2 = p_k^2 = 1$.

(\implies)

Suponha que $\sum_{k=1}^n p_k^2 = 1$, então $\sum_{k=1}^n p_k = 1 = \sum_{k=1}^n p_k^2 \implies \sum_{k=1}^n (p_k - p_k^2) = 0$. Como $0 \leq p_i \leq 1, \forall i \in \{1, 2, 3, \dots, n\}$ então $0 \leq p_i^2 \leq p_i \leq 1$, logo $(p_i - p_i^2) \geq 0, \forall i \in \{1, 2, 3, \dots, n\}$, portanto $\sum_{k=1}^n (p_k - p_k^2) = 0 \implies p_k = p_k^2, \forall k \in \{1, 2, 3, \dots, n\}$. Logo:

- Se todos termos forem nulos, então $\sum_{k=1}^n p_k = 0$, um absurdo.

¹¹U. Fano chama esses estados de Estados Puros

ii) Se existirem dois ou mais termos iguais a 1, então $\sum_{k=1}^n p_k > 1$, um absurdo.

Portanto exatamente um termo é igual a 1. Logo A é um estado puro \square

2.1.4 Estados Reduzidos

Definição 2.13. Sejam H_A, H_B dois espaços vetoriais munidos de produto interno sobre o corpo dos complexos, $\{|a_1\rangle, |a_2\rangle, \dots, |a_n\rangle\}$ uma base de H_A , $\{|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle\}$ uma base de H_B e $T : H_A \otimes H_B \rightarrow H_A \otimes H_B$ um operador. O traço parcial de T sobre H_B é um operador $tr_B(T) : H_A \rightarrow H_A$ com componentes¹² $[tr_B(T)]_{ij} = \sum_{k=1}^n \langle a_i b_k | T | a_j b_k \rangle$.

Seja ρ o operador densidade do sistema composto AB, então $tr_B(\rho) = \rho^A : H_A \rightarrow H_A$ é o operador densidade reduzido para o sistema A. Seja também M uma propriedade (local) que queremos medir no subsistema A a qual associamos um operador auto-adjunto $M : H_A \rightarrow H_A$. Como ρ^A é o único¹³ operador com a propriedade $tr(M\rho^A) = tr[(M \otimes 1_{H_B})\rho]$, então os resultados probabilísticos que seriam obtidos a partir da extensão $M \otimes 1_{H_B}$ podem ser também obtidos apenas olhando para o teste local M aplicado sobre o operador ρ^A . Nesse sentido, o operador densidade reduzido é um bom representante para o sistema A.

-Exemplos-

1) Se $\rho^{AB} = \rho \otimes \sigma$ é o operador densidade do sistema AB então $\rho^A = \rho$ é o operador densidade reduzido para o sistema A e $\rho^B = \sigma$ é o operador densidade reduzido para o sistema B.

2) Seja $\rho = |\phi_+\rangle\langle\phi_+| = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)$ o operador densidade para o sistema AB num dos estados de Bell. Então $\rho^A = \frac{1}{2}\mathbb{1}$.

2.2 O Emaranhamento

“...um truque que os mágicos quânticos usam para produzir fenômenos que não podem ser imitados pelos mágicos clássicos...”

(Asher Peres, sobre o emaranhamento)

¹²Poderíamos definir: $tr_B(|\psi_1\rangle\langle\psi_2| \otimes |\phi_1\rangle\langle\phi_2|) = |\psi_1\rangle\langle\psi_2| tr(|\phi_1\rangle\langle\phi_2|) = |\psi_1\rangle\langle\psi_2| \langle\phi_2|\phi_1\rangle$; $|\psi_1\rangle, |\psi_2\rangle \in H_A$ e $|\phi_1\rangle, |\phi_2\rangle \in H_B$, e estender por linearidade para os outros casos. Além disso, assim como o produto tensorial, o traço parcial independe da escolha de bases, veja [16].

¹³Veja [22].

Começaremos com a:

Definição 2.14. *Sejam H_A o espaço de estados do sistema A, H_B o espaço de estados do sistema B, e ρ o operador densidade que representa o sistema composto AB. Então o estado composto é Separável quando pode ser representado por $\rho = \sum_{i=1}^m p_i \rho_i^A \otimes \rho_i^B$ tal que ρ_i^A e ρ_i^B são operadores densidades sobre H_A e H_B qualquer que seja $i \in \{1, 2, 3, \dots, m\}$, e (p_1, p_2, \dots, p_m) é um vetor de probabilidades. Caso contrário o sistema AB é emaranhado.*

Um caso particular de estados separáveis são aqueles representados por $\rho = \rho^A \otimes \rho^B$, ρ^A um operador densidade sobre H_A e ρ^B um operador densidade sobre H_B . Esses estados são chamados de decomponíveis.

Contudo, em várias situações, não é possível apenas com a definição saber se um estado é ou não emaranhado. Portanto devemos buscar outros critérios para decidir sobre a separabilidade de estados em sistemas compostos.

Teorema (Schmidt) 2.15. ¹⁴ *Seja $|\psi\rangle$ o estado puro de um sistema composto AB, então existem vetores ortonormais $\{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\} \in H_A$ e $\{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_n\rangle\} \in H_B$, t.q. $|\psi\rangle = \sum_{i=1}^n \lambda_i |\alpha_i \beta_i\rangle$, $\lambda_i \geq 0$, $\forall i \in \{1, 2, 3, \dots, n\}$ e $\sum_{i=1}^n \lambda_i^2 = 1$.*

Demonstração. Suponha que $\dim H_A = n = \dim H_B$. Sejam $\{|a_1\rangle, |a_2\rangle, \dots, |a_n\rangle\}$ uma BON de H_A e $\{|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle\}$ uma BON de H_B , logo $|\psi\rangle \in H_A \otimes H_B \implies |\psi\rangle = \sum_{i,j=1}^n \gamma_{ij} |a_i b_j\rangle$. Se M é uma matriz, então existem duas matrizes unitárias U e V , e uma matriz D diagonal com elementos não-negativos tais que $M = UDV$, então:

$$|\psi\rangle = \sum_{i,j,k=1}^n u_{ik} d_{kk} v_{kj} |a_i\rangle \otimes |b_j\rangle.$$

Defina $|\alpha_k\rangle = \sum_{i=1}^n u_{ik} |a_i\rangle \in H_A$, $|\beta_k\rangle = \sum_{j=1}^n v_{kj} |b_j\rangle \in H_B$ e $d_{kk} = \lambda_k$, logo $|\psi\rangle = \sum_{k=1}^n \lambda_k |\alpha_k \beta_k\rangle$. Afirmamos que $\{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\}$ é ortonormal. De fato $\langle \alpha_l | \alpha_m \rangle = \sum_{i,j=1}^n (u_{il})^* u_{jm} \langle a_i | a_j \rangle = \sum_{i,j=1}^n (u_{il})^* u_{jm} \delta_{ij} = \sum_{i=1}^n (u_{il})^* u_{im} = \delta_{lm}$. Analogamente, $\{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_n\rangle\}$ é ortonormal. \square

Uma segunda demonstração¹⁵ é dada abaixo:

Demonstração. Sejam $\{|a_i\rangle; i \in I_n\}$ uma base para o espaço H_A e $\{|b_i\rangle; i \in I_m\}$ uma base para o espaço H_B . Como $|\psi\rangle \in H_A \otimes H_B$, então $|\psi\rangle =$

¹⁴A Decomposição de Schmidt será de extrema importância mais a frente!

¹⁵Esta feita pelo autor do presente texto.

$\sum_{i=1}^n \sum_{j=1}^m \gamma_{ij} |a_i b_j\rangle$ t.q. $\gamma_{ij} \in \mathbb{C}, \forall (i, j) \in I_n \times I_m$. Portanto existe uma transformação $T : \mathbb{C}^m \rightarrow \mathbb{C}^n$ tal que $[T]_{ij} = \gamma_{ij}, \forall (i, j) \in I_n \times I_m$.

O teorema de decomposição a valores singulares [34] garante que existem bases ortonormais $\alpha = \{\alpha_i; i \in I_n\} \subset \mathbb{C}^n$ e $\beta = \{\beta_i; i \in I_m\} \subset \mathbb{C}^m$ t.q.:

$$[T]_{\beta}^{\alpha} = \begin{pmatrix} D_1 & 0 \\ 0 & 0 \end{pmatrix},$$

com $D_1 = \text{diag}(\mu_1, \mu_2, \dots, \mu_r)$, r o posto de T^*T e $\mu_1, \mu_2, \dots, \mu_r \geq 0$ os valores singulares da aplicação $T : \mathbb{C}^m \rightarrow \mathbb{C}^n$.

Portanto na base produto $\{|\alpha_i \beta_j\rangle; (i, j) \in I_n \times I_m\}$ o estado do sistema conjunto é representado por $|\psi\rangle = \sum_{i=1}^r \mu_i |\alpha_i \beta_i\rangle$.

Além disso, $1 = \langle \psi | \psi \rangle = \sum_{i=1}^r \sum_{j=1}^r \mu_i \mu_j \langle \alpha_i \beta_i | \alpha_j \beta_j \rangle = \sum_{i=1}^r \mu_i^2$. \square

Segue diretamente do Teorema acima:

Corolário 2.16. $|\psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ é um estado produto se, e somente se, $\lambda_i^2 = 1$ para algum $i \in I_{\min\{m, n\}}$.

Teorema 2.17. Seja AB um sistema composto num estado puro. Então AB é separável se, e somente se, as matrizes densidades reduzidas correspondem a estados puros.

Demonstração. Seja AB um sistema representado por $|\psi\rangle \in H_A \otimes H_B$.

(\implies)

O Teorema de decomposição de Schmidt garante que $|\psi\rangle = \sum_{i=1}^n \lambda_i |a_i b_i\rangle$. Então existe somente um $k \in \{1, 2, 3, \dots, n\}$ tal que $\lambda_k \neq 0$. Portanto o operador densidade que representa o sistema AB é $\rho = |a_k b_k\rangle \langle a_k b_k|$, logo $\rho^A = \text{tr}_B(\rho) = |a_k\rangle \langle a_k|$ e $\rho^B = \text{tr}_A(\rho) = |b_k\rangle \langle b_k|$. Então os sistemas A e B correspondem a estados puros.

(\impliedby)

Suponha que ρ^A e ρ^B correspondam a estados puros. Suponha, por absurdo, que AB seja um sistema puro não-separável (emaranhado) representado por $|\psi\rangle = \sum_{i=1}^n \lambda_i |a_i b_i\rangle$, então existe mais de um coeficiente de Schmidt não-nulo. Sem perda de generalidade, suponha que $\{\lambda_1, \lambda_2, \dots, \lambda_k\}$ são coeficientes de Schmidt não nulos, logo $|\psi\rangle = \sum_{i=1}^k \lambda_i |a_i b_i\rangle$, $k \geq 2$, donde $\rho = \sum_{i,j=1}^k \lambda_i \lambda_j |a_i b_i\rangle \langle a_j b_j|$, logo $\rho^A = \sum_{i,j=1}^k \lambda_i \lambda_j |a_i\rangle \langle a_j| \delta_{ji} = \sum_{i=1}^k \lambda_i^2 |a_i\rangle \langle a_i|$ um absurdo, uma vez que A corresponde a um estado puro. \square

-Exemplo-

1)

Os seguintes estados são emaranhados.¹⁶

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle);$$

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

Caracterizamos o emaranhamento em sistemas compostos que são puros, agora o próximo passo é obter critérios de separabilidade para estados mistos. Para esses casos a situação muda de figura, e existem vários métodos que permitem identificar se um estado é, ou não, emaranhado. Alguns deles são ditos **operacionais**, ou seja, uma simples conta determina se um dado estado é (ou não) emaranhado. Mas como nem tudo são flores, é de se esperar que existam estados que se encaixem somente numa classe de critérios mais “complicados”, mais técnicos, **não-operacionais**. Como o objetivo central deste texto não é um conhecimento profundo acerca dos critérios de separabilidade para estados mistos, omitiremos todas as demonstrações que virão, muito embora elas possam ser encontradas nas referências citadas.

2.2.1 Critérios de Separabilidade Operacionais

Seja $T : H_1 \otimes H_2 \rightarrow H_1 \otimes H_2$ um operador sobre um espaço vetorial dotado de produto interno sobre o corpo dos complexos, $\beta_1 = \{|a_1\rangle, |a_2\rangle, \dots, |a_n\rangle\}$ uma base para H_1 e $\beta_2 = \{|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle\}$ uma base para H_2 , então podemos obter as componentes de T na base produto β : $T = (1_A \otimes 1_B)T(1_A \otimes 1_B) = (\sum_{m,\mu} |a_m b_\mu\rangle \langle a_m b_\mu|)T(\sum_{n,\nu} |a_n b_\nu\rangle \langle a_n b_\nu|) = \sum_{n,m,\mu,\nu} \langle a_m b_\mu|T|a_n b_\nu\rangle |a_m b_\mu\rangle \langle a_n b_\nu| \implies [T]_\beta = \langle a_m b_\mu|T|a_n b_\nu\rangle$.

Definição 2.18. *Sejam β uma base produto para $H_A \otimes H_B$ e L um operador sobre $H_A \otimes H_B$, com componentes $[L]_\beta = L_{m\mu,n\nu}$, então a transposta parcial de L com respeito a uma base de H_A é um operador sobre $H_A \otimes H_B$ com componentes na base produto dadas por $[L_\beta^{T_A}] = L_{m\mu,n\nu}^{T_A} = L_{n\nu,m\mu}$.*

¹⁶Estes estados “maximamente emaranhados”, mais conhecidos como Estados de Bell, estão associados com violações de localidade em Mecânica Quântica. Não é o objetivo dessa dissertação abordar Não-Localidade ou Contextualidade, para tanto veja [25, 23, 27, 26].

Critério de Peres-Horodecki [30, 31]: Seja ρ o operador densidade do sistema composto AB, se ρ representa um estado separável então os operadores ρ^{T_A}, ρ^{T_B} são positivos semidefinidos. Para sistemas com espaços de estado com dimensão 2×2 ou 2×3 , vale a recíproca do enunciado, logo: se ρ^{T_A} é positivo semidefinido então AB é separável.¹⁷

Critério de Redução [33]: Seja AB um sistema composto descrito pelo operador densidade ρ . Se ρ é separável então $(\rho^A \otimes 1_B) - \rho$ é positivo semidefinido e $(1_A \otimes \rho^B) - \rho$ é positivo semidefinido, tal que ρ^A e ρ^B são as matrizes densidade reduzidas para H_A e H_B .

Critério da Majoração[32]: Sejam¹⁸ ρ o operador densidade que representa AB, λ o vetor cujas entradas são os autovalores de ρ , λ_A e λ_B vetores cujas componentes são os autovalores dos operadores densidade reduzidos ρ^A e ρ^B . Se ρ é separável, então $\lambda^\downarrow \prec \lambda_A^\downarrow, \lambda_B^\downarrow$.

2.2.2 Critérios de Separabilidade Não-Operacionais

Mapas Positivos[33]: ρ representa um estado separável se, e somente se, para cada mapa positivo Λ tem-se $(1 \otimes \Lambda)(\rho) \geq 0$.

Testemunhas do Emaranhamento[33]: A fim de que a matriz densidade ρ seja emaranhada, é necessário e suficiente que exista um operador auto-adjunto W tal que $\text{tr}(W\rho) < 0$ e $\text{tr}(W\rho_{sep}) \geq 0$ qualquer que seja o estado separável ρ_{sep} . Dizemos que a Testemunha W detecta o emaranhamento de ρ .

2.3 Purificação

Uma técnica amplamente utilizada em Teoria Quântica da Informação e em Computação Quântica, e que será usada também nesse texto, é a chamada Purificação. Como o próprio nome já diz, a ideia por trás da Purificação é tornar algo não-puro em puro, no nosso caso, vamos mostrar como enxergar (em algumas situações) um estado misto como estado puro.

Suponha que é dado um estado representado por $\rho_A : H_A \rightarrow H_A$. Afir-mamos que é possível obter um espaço de estados H_R , tal que o sistema composto tem espaço de estados $H = H_A \otimes H_R$, e é representado pelo vetor

¹⁷Para dimensões superiores pode-se exibir estados que têm transposta parcial positiva e que são emaranhados [20].

¹⁸Vale lembrar que a Majoração foi o assunto tema do nosso primeiro Capítulo, certo!?

$|AR\rangle$ e $\text{tr}_R(|AR\rangle\langle AR|) = \rho_A$, ou seja o estado $|AR\rangle$ se reduz a ρ_A quando olhamos somente para a parte original do sistema.

Este processo, puramente matemático, é chamado de Purificação. O sistema R acrescentado¹⁹ não tem interpretação física direta, é apenas um apoio, uma ferramenta de cálculo.

Falta mostrar que a Purificação é sempre possível, para isso enunciaremos uma proposição:

Proposição 2.19. *Seja $\rho_A : H_A \rightarrow H_A$ um operador densidade que representa um sistema A . Então existem um espaço de estados H_R , e um vetor²⁰ $|AR\rangle \in H_A \otimes H_R$, t.q. $\text{tr}_R(|AR\rangle\langle AR|) = \rho_A$.*

Demonstração. Como ρ_A é auto-adjunto, então existe uma base ortonormal $\{|1_A\rangle, |2_A\rangle, \dots, |n_A\rangle\}$ de H_A tal que $\rho_A = \sum_{i=1}^n p_i |i_A\rangle\langle i_A|$, $p_1, \dots, p_n \geq 0$. Seja H_R um espaço vetorial com a mesma dimensão de H_A , e seja $|i_R\rangle$ uma base de H_R . Defina $|AR\rangle = \sum_{i=1}^n \sqrt{p_i} |i_A i_R\rangle \in H_A \otimes H_B$. Portanto $|AR\rangle\langle AR| = \sum_{i,j=1}^n \sqrt{p_i \cdot p_j} |i_A i_R\rangle\langle j_A j_R|$, logo $\text{tr}_R(|AR\rangle\langle AR|) = \sum_{k=1}^n \mathbb{1} \otimes \langle k_R|(|AR\rangle\langle AR|)\mathbb{1} \otimes |k_R\rangle = \sum_{i,j,k=1}^n \sqrt{p_i p_j} \delta_{ki} \delta_{kj} |i_A\rangle\langle j_A| = \sum_{i=1}^n p_i |i_A\rangle\langle i_A| = \rho_A$.

□

Terminamos a seção enunciando mais um Lema:

Lema 2.20. *Sejam $|AR_1\rangle$ e $|AR_2\rangle$ purificações por um mesmo sistema de referência, do estado $\rho_A : H_A \rightarrow H_A$. Afirmamos que existe um operador unitário U atuando sobre o segundo sistema t.q. $|AR_1\rangle = (\mathbb{1} \otimes U)|AR_2\rangle$.*

Demonstração. Como $|AR_1\rangle$ e $|AR_2\rangle$ são purificações do mesmo sistema, representado por $\rho_A : H_A \rightarrow H_A$, $\dim H_A = n$, então existem duas bases ortonormais de H_R , $\beta_1 = \{|i_1\rangle; i \in I_n\}$ e $\beta_2 = \{|i_2\rangle; i \in I_n\}$, t.q. $|AR_1\rangle = \sum_{i=1}^n \sqrt{p_i} |i_A i_1\rangle$ e $|AR_2\rangle = \sum_{i=1}^n \sqrt{p_i} |i_A i_2\rangle$.

Defina $U : H_R \rightarrow H_R$ uma aplicação linear dada por $U|i_2\rangle = |i_1\rangle$, $\forall i \in I_n$. Como β_1, β_2 são ortonormais, então U é unitária. Além disso $(\mathbb{1} \otimes U)|AR_2\rangle = (\mathbb{1} \otimes U) \sum_{i=1}^n \sqrt{p_i} |i_A i_2\rangle = \sum_{i=1}^n \sqrt{p_i} |i_A i_1\rangle = |AR_1\rangle$. □

¹⁹Em geral o chamamos de Sistema de Referência.

²⁰De uma certa maneira estamos aumentando a dimensão do espaço de estados, numa forma "esperta", a fim de poder enxergar o sistema como puro. Mas sempre sabendo como voltar a descrição original.

2.4 Operações Quânticas

Nas próximas seções iremos usar, várias e várias vezes, a frase “Operações Locais com Comunicação Clássica” (LOCC)²¹, portanto nada mais natural que reservar um espaço para definir, discutir e entender o que são Operações (locais) em Mecânica Quântica. Existem várias maneiras de defini-las, algumas tem mais apelo intuitivo e outras mais operacionais. Para deixar a discussão mais limpa e concisa²², vamos usar uma definição com “axiomas fisicamente motivados”²³. Antes disso fixemos algumas notações:

Definição 2.21. Chamamos de \mathbb{M} o espaço das matrizes quadradas com um tamanho fixado, e $\mathfrak{D} = \{\rho \in \mathbb{M}; \text{tr}(\rho) = 1\}$ o conjunto dos elementos em \mathbb{M} que têm traço igual a um.

Definição 2.22. Uma Operação Quântica é representada por uma aplicação $\Phi : \mathbb{M}_1 \rightarrow \mathbb{M}_2$ que cumpre as seguintes condições:

1. Φ é linear²⁴;
2. $\Phi : \mathbb{M}_1 \rightarrow \mathbb{M}_2$ é completamente positiva²⁵;
3. $\text{tr}[\Phi(\rho)] \in [0, 1]$, $\forall \rho \in \mathfrak{D}_1 = \{\rho \in \mathbb{M}_1; \text{tr}(\rho) = 1\}$. Além disso, $\text{tr}[\Phi(\rho)]$ é a probabilidade de ocorrência do processo representado por ρ .

O item 3 é uma abstração matemática conveniente, garantindo que medições também possam ser representadas via Operações Quânticas. Por exemplo, se queremos realizar um teste representado por $\{|0\rangle, |1\rangle\}$, podemos então definir as operações quânticas $\Phi_i(\rho) = |i\rangle\langle i|\rho|i\rangle\langle i|$, $\forall \rho$, com $i \in \{0, 1\}$. A probabilidade de obter o resultado i , dado que o estado ρ está em jogo é dada por $\text{tr}[\Phi_i(\rho)]$. Após a medição o sistema é descrito²⁶ por $\frac{\Phi_i(\rho)}{\text{tr}[\Phi_i(\rho)]}$. Numa situação em que nenhuma medição é feita, não há probabilidades, então a Operação Quântica Φ deve preservar o traço. Temos $p = 1 = \text{tr}(\rho) = \text{tr}[\Phi(\rho)]$ de certeza da evolução do estado.²⁷

²¹Em inglês *Local Operation with Classical Communication*.

²²E também melhor adaptada à uma dissertação em matemática

²³Veja [22].

²⁴Portanto, para todo vetor de probabilidades $p = (p_1, \dots, p_m)$ e para toda lista $\rho_1, \dots, \rho_m \in \mathbb{M}_1$, tem-se que $\Phi(\sum_{i=1}^m p_i \rho_i) = \sum_{i=1}^m p_i \Phi(\rho_i)$

²⁵Definições e Resultados envolvendo aplicações completamente positivas se encontram no Apêndice A.

²⁶Lembrando que em Mecânica Quântica sempre usamos estados com representantes normalizados.

²⁷O termo Canal Quântico é por vezes utilizado quando Φ preserva o traço.

O item 1 garante que preparar um estado $\sum_{i=1}^k p_i \rho_i$ e realizar uma Operação $\Phi(\sum_{i=1}^k p_i \rho_i)$, é equivalente a aplicar, em cada estado ρ_i , a mesma Operação Φ é preparar o estado $\sum_{i=1}^k p_i \Phi(\rho_i)$.

O item 2 também tem uma motivação física importante. Sejam R , e Φ uma Operação Quântica que atua sobre R . É natural imaginar que para qualquer outro sistema Q a extensão trivial de Φ ao o sistema composto RQ , também leve matrizes positivas em matrizes positivas²⁸.

Nos textos de Informação Quântica e Computação Quântica é muito comum rotular os sistemas em questão com as letras A, B . Mais ainda, para dar um caráter mais descontraído (e aplicado) também se imagina que existem dois cientistas, Alice e Bob, em dois laboratórios que são os responsáveis respectivamente pelos sistemas A, B . Assim muito da Teoria Quântica da Informação e da Computação tem usualmente a seguinte construção (historinha): “Suponha que Alice e Bob compartilhem um estado $|\psi\rangle$... Alice então realiza uma operação no seu sistema... agora, condicionado (ou não) ao resultado comunicado por Alice, Bob pode realizar a seguinte operação... e passando o resultado para Alice, ela realiza uma operação em seu próprio laboratório...”.

Definição 2.23. Sejam A, B dois sistemas físicos. Uma Operação Local com Comunicação Clássica é um protocolo composto de operações locais, em que o resultado de cada etapa pode ser comunicado classicamente²⁹ entre as partes, de maneira que o passo seguinte pode (ou não) estar condicionado a tal comunicação.³⁰

-Exemplo-

1) Obtenção de Estados puros não-emaranhados.

Suponha que Alice e Bob possuam um qubit no estado $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

i) Primeira ação de Alice:

Alice realiza um experimento, no subsistema dela, descrito pelos operadores $M_1 = \text{diag}(\cos \theta \ \sin \theta)$, $M_2 = \text{diag}(\sin \theta \ \cos \theta) \in \mathbb{M}_2$. Note que $\sum_{i=1}^2 M_i^* M_i = \mathbb{1}$.

ii) Segunda ação de Alice:

Após a medição, se for obtido o resultado 1, o sistema é descrito por $|\psi_1\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle$, analogamente, se for obtido o resultado 2, a descrição será $|\psi_2\rangle = \sin \theta |00\rangle + \cos \theta |11\rangle$.

²⁸E portanto, a menos de normalizações, matrizes densidade em matrizes densidade.

²⁹Via telefone, e-mail, Skype, Facebook...

³⁰Por isso Local.

Se $\mathbb{1}$ for o resultado obtido, ela aplica uma operação **NOT** dada por:

$$\text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Então $\text{NOT} \otimes \mathbb{1}|\psi_2\rangle = \cos\theta|01\rangle + \sin\theta|10\rangle$. Alice agora envia o resultado do experimento para Bob.

iii) Ação de Bob:

Se o resultado for $\mathbb{1}$ Bob não faz nada, caso contrário realiza uma operação **NOT** no subsistema dele, obtendo $|\psi_1\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$. Portanto em qualquer um dos casos, Alice e Bob transformaram o estado inicial, com máximo emaranhamento, $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ no estado $|\psi_1\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$. Note que se $\theta \in \{0, \frac{\pi}{2}, \pi, \dots\}$ o estado final não é emaranhado!

O exemplo acima levanta várias perguntas: “Dado um estado puro, quantos pares de estados de Bell (estados com máximo emaranhamento) podem ser obtidos via LOCC³¹?”, “Dados n pares de Bell, quais são os estados atingíveis por LOCC³²?”, “Dados dois estados, existe um protocolo envolvendo apenas LOCC que leva um no outro?”, “LOCC pode aumentar, diminuir ou manter constante funções como a Entropia?”...

Existem vários trabalhos na direção de Transformações que envolvem emaranhamento. Inicialmente o problema foi introduzido, e resolvido, em dois diferentes caminhos: A Destilação de Emaranhamento e o Custo de Emaranhamento (relacionados às duas primeiras perguntas anteriores) [35, 36, 37]. Aqui, como veremos mais adiante, nossa preocupação será outra. Nessa dissertação, estamos focados em responder a terceira pergunta.

Terminamos essa seção com a

Definição 2.24. Dizemos que $|\chi\rangle$ é acessado a partir de $|\psi\rangle$, quando existe um protocolo envolvendo somente LOCC que leva $|\psi\rangle$ em $|\chi\rangle$, e escrevemos $|\psi\rangle \rightarrow |\chi\rangle$.

³¹Na situação em que várias cópias do estado inicial estão disponíveis (Limite Assintótico).

³²Também no limite Assintótico.

2.5 O Teorema

Após tantas definições, lemas, teoremas, proposições, mais definições, mais teoremas e alguns comentários, podemos enfim enunciar o Teorema central desta Dissertação:

Teorema (Nielsen) 2.25. *Sejam H_A, H_B, H_C, H_D espaços de estado de dimensão finita, $|\psi\rangle \in H_A \otimes H_B$ e $|\phi\rangle \in H_C \otimes H_D$. A fim de que $|\phi\rangle$ seja acessado por $|\psi\rangle$, é necessário e suficiente que $\lambda_\psi \prec \lambda_\phi$, λ_ψ um vetor cujas entradas são os coeficientes de Schmidt do estado $|\psi\rangle$.*

Demonstração. (\implies)

Suponha que $|\psi\rangle \rightarrow |\phi\rangle$ por LOCC. Sem perda de generalidade podemos assumir que o processo é feito com uma medição de Alice $\{M_1, M_2, \dots, M_m\}$ sobre o sistema dela, e um envio do resultado para Bob.

Do ponto de vista de Alice, ela começa com o estado $\rho_\psi = \text{tr}_B(|\psi\rangle\langle\psi|)$ e termina com o estado $\rho_\phi = \text{tr}_B(|\phi\rangle\langle\phi|)$, então $\rho_\phi = \frac{M_j \rho_\psi M_j^*}{p_j}$, para algum $j \in I_m$

Como $M_j \sqrt{\rho_\psi} = \sqrt{M_j \sqrt{\rho_\psi} \sqrt{\rho_\psi} M_j^*} V_j$ é a decomposição polar de $M_j \sqrt{\rho_\psi}$ com V_j unitária, e $\sqrt{\rho_\psi} M_j^* M_j \sqrt{\rho_\psi} = V_j^* p_j \rho_\phi V_j$, então $\sum_{j=1}^m \sqrt{\rho_\psi} M_j^* M_j \sqrt{\rho_\psi} = \sum_{j=1}^m p_j V_j^* \rho_\phi V_j$, donde $\rho_\psi = \sum_{i=1}^m p_i V_i^* \rho_\phi V_i$. Logo, o teorema 1.19 garante que $\rho_\psi \prec \rho_\phi$, portanto $\lambda_\psi \prec \lambda_\phi$.

(\impliedby)

Suponha que $\lambda_\psi \prec \lambda_\phi$.

Como $\lambda_\psi \prec \lambda_\phi$, o teorema 1.19 garante que existem uma distribuição de probabilidades $\{p_1, p_2, \dots, p_m\}$ e operadores unitários $\{U_1, U_2, \dots, U_m\}$ t.q. $\rho_\psi = \sum_{i=1}^m p_i U_i \rho_\phi U_i^*$.

Para fixar as ideias, suponha que ρ_ψ é inversível³³. Defina $M_1, M_2, \dots, M_m : H_A \rightarrow H_C$ dadas por $M_i = \sqrt{p_i \rho_\phi} U_i^* \rho_\psi^{-\frac{1}{2}}$, $i \in I_m$, logo $\sum_{i=1}^m M_i^* M_i = \sum_{i=1}^m \rho_\psi^{-\frac{1}{2}} U_i \sqrt{p_i \rho_\phi} \sqrt{p_i \rho_\phi} U_i^* \rho_\psi^{-\frac{1}{2}} = \rho_\psi^{-\frac{1}{2}} (\sum_{i=1}^m U_i p_i \rho_\phi U_i^*) \rho_\psi^{-\frac{1}{2}} = \mathbb{1}$. Portanto, $\{M_i : H_A \rightarrow H_C; i \in I_m\}$ é uma medição no subsistema de Alice.

Suponha que Alice realiza a medição $\{M_1, M_2, \dots, M_m\}$ e obtém o resultado j , então $|\phi_j\rangle \propto (M_j \otimes \mathbb{1})|\psi\rangle$, portanto $\rho_j \propto M_j \rho_\psi M_j^* = M_j \sqrt{\rho_\psi} \sqrt{\rho_\psi} M_j^* =$

³³Caso ρ_ψ não seja inversível, basta definir cada M_i como acima em $H_A - \text{Ker}\{\rho_\psi\}$ e sendo identicamente nula em $\text{Ker}\{\rho_\psi\}$.

$\sqrt{p_j \rho_\phi} U_j^* U_j \sqrt{p_j \rho_\phi} = p_j \rho_\phi$, donde $\rho_j = K p_j \rho_\phi$. Como $1 = \text{tr}(\rho_j) = K p_j$, então $\rho_j = \rho_\phi$.

Portanto $|\phi_j\rangle$ e $|\phi\rangle$ são purificações do mesmo estado quântico. O lema 2.20 garante que Bob pode realizar uma operação unitária V t.q. $|\phi\rangle = (\mathbb{1} \otimes V)|\phi_j\rangle$. \square

Em linhas gerais o Teorema de Nielsen funciona da seguinte maneira: Se $|\psi\rangle \rightarrow |\phi\rangle$, então $|\psi\rangle$ pode ser colocado (via Teorema A1.1 se preferir) numa forma “bonitinha” envolvendo $|\phi\rangle$, mas ora, essa forma “bonitinha” nada mais é do que a majoração para operadores. Por outro lado, quando $\lambda_\psi \prec \lambda_\phi$ então também temos uma forma “bonitinha” para $|\psi\rangle$, muito parecida com a anterior, logo basta extrair dela uma medição para mostrar como obter $|\phi\rangle$. Existem, claro, várias outras demonstrações do Teorema de Nielsen. A original, feita pelo próprio, se encontra em [38]. Nas elegantes³⁴ notas de aula do Watrous [19] aparece outro enunciado e outra demonstração, rigorosa e elegante, mas muito mais extensa. Aqui, por motivos práticos, usamos uma prova mais limpa e concisa, muito parecida com aquela encontrada em [22].

-Exemplos-

1)

Suponha que Alice e Bob compartilhem o estado $|\psi_1\rangle$, com vetor de Schmidt³⁵ dados por $\lambda_1 = (0.4, 0.4, 0.1, 0.1)$. O Teorema de Nielsen garante que Alice e Bob não conseguem atingir, apenas com LOCC, o estado $|\psi_2\rangle$ com vetor de Schmidt $\lambda_2 = (0.5, 0.25, 0.25)$.

2)

Ainda no exemplo acima, note que $\lambda_1 \not\prec \lambda_2$ e também $\lambda_2 \not\prec \lambda_1$. Assim, como já era de se esperar, a acessibilidade via LOCC é uma relação de ordem parcial.³⁶

3)

Se $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, afirmamos que $|\psi_1\rangle \rightarrow |\psi_2\rangle$ ou $|\psi_2\rangle \rightarrow |\psi_1\rangle$.

Como $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, então existem $p, q \in (0.5, 1]$ t.q. $\lambda_i = (p, 1-p)$ e $\lambda_2 = (q, 1-q)$. Se $|\psi_1\rangle \rightarrow |\psi_2\rangle$ não há o que mostrar, caso contrário $\lambda_1 \not\prec \lambda_2$, logo $p > q$, donde $\lambda_2 = (q, 1-q) \prec (p, 1-p) = \lambda_1$.

³⁴Apesar de conter alguns erros.

³⁵Na verdade, em geral, pra tornar a discussão mais limpa, olharemos para o quadrado dos Coeficientes de Schmidt.

³⁶Note que esses exemplos já fora discutidos na seção 1.1.

4)

Os Estados de Bell, $|\psi_{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$, $|\phi_{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$, só são atingíveis via LOCC por eles mesmos.

5)

Os estados com vetores de Schmidt $\lambda_1 = (0.5, 0.4, 0.1)$ e $\lambda_2 = (0.6, 0.2, 0.2)$ não são comparáveis, ou seja, nem $|\psi_2\rangle \rightarrow |\psi_1\rangle$, nem $|\psi_1\rangle \rightarrow |\psi_2\rangle$.

6)

Sejam $\lambda_1 = (0.4, 0.4, 0.2)$ e $\lambda_2 = (0.5, 0.4, 0.1)$. Como $\lambda_1 \prec \lambda_2$, mas $\lambda_2 \not\prec \lambda_1$, tem-se que $|\psi_2\rangle \rightarrow |\psi_1\rangle$ e $|\psi_2\rangle \not\rightarrow |\psi_1\rangle$.

No exemplos 1), 2) e 6) vimos que existem estados que não são diretamente atingíveis via LOCC. Portanto existem pares de estados $|\psi_1\rangle, |\psi_2\rangle$ tais que $|\psi_1\rangle \rightarrow |\psi_2\rangle$, mas será esse o fim?

Capítulo 3

Catálise

“Então você está estudando as enzimas da Mecânica Quântica!”

(S. R. Barbosa)

3.1 Introdução

Terminamos o capítulo anterior com o Teorema de Nielsen, alguns exemplos e uma pergunta no ar: “*Mas será esse o fim?*”. Obviamente a resposta é *NÃO*, como poderia ser deduzido pelo leitor mais malicioso. Temos, portanto, que explicar porque não consideramos $|\psi_1\rangle \rightarrow |\psi_2\rangle$ como um ponto final da nossa discussão.

A ideia central, não só deste capítulo, mas da dissertação inteira, veio do trabalho de D. Jonathan e M. Plenio, sobre a possibilidade de tornar uma transformação antes impossível em possível [39]. Em linhas gerais, eles mostraram que existem casos onde Alice e Bob não conseguem, via **LOCC**, levar $|\psi_1\rangle$ em $|\psi_2\rangle$, mas com a ajuda de um $|\phi\rangle$ advindo de um repositório de estados emaranhados (ou de um Banqueiro de Emaranhamento), Alice e Bob poderiam agora realizar a tarefa, sem danificar o estado que foi a eles confiado.

Em geral, o Emaranhamento é sempre visto como um recurso para realizar tarefas em Informação e Computação Quânticas [40], mas sempre é natural que como recurso ele seja consumido, total ou parcialmente, durante o processo. Contudo, o emaranhamento é um recurso tão estranho e complexo, que pode ser usado sem ser consumido. Esse é o ponto chave, fundamental da Ref. [39].

3.2 Pedindo Emprestado

Imagine a seguinte situação: Alice e Bob compartilham um estado emaranhado $|\psi_1\rangle \in H_A \otimes H_B$, e querem por meio de LOCC obter o estado $|\psi_2\rangle \in H_C \otimes H_D$. Sabemos, via Teorema 2.25, que para alguns pares de estados existe um protocolo garantindo que $|\psi_1\rangle \rightarrow |\psi_2\rangle$ (basta que $\lambda_1 \prec \lambda_2$). Para tornar a situação mais interessante, suponha que não seja esse o caso, logo $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$.

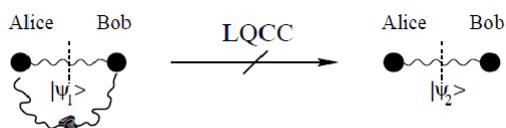


Figura 3.1: Primeira tentativa. [39]

Suponha agora que uma terceira pessoa (Chris)¹ entra em cena, e concorda em emprestar um outro estado emaranhado $|\phi\rangle$ para Alice e Bob, mas com a seguinte condição: Alice e Bob deverão devolver para Chris o mesmo estado $|\phi\rangle$ intacto ao final do processo! Será que agora Alice e Bob podem, usando $|\phi\rangle$, transformar $|\psi_1\rangle$ em $|\psi_2\rangle$ sem estragar o empréstimo de Chris?

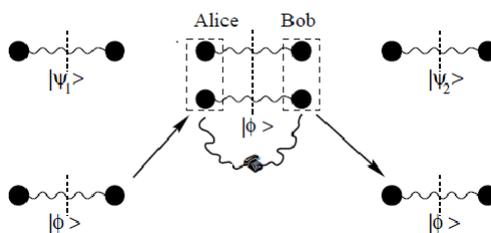


Figura 3.2: Tentativa com ajuda.

Definição 3.1. Uma transformação entre dois estados quaisquer $|\psi_1\rangle, |\psi_2\rangle$ é uma transformação local auxiliada pelo emaranhamento (ELOCC) quando $|\psi_1\rangle \rightarrow |\psi_2\rangle$ via LOCC, mas existe um estado $|\phi\rangle$ t.q. $|\psi_1\phi\rangle \rightarrow |\psi_2\phi\rangle$ via LOCC. Ao estado

¹Originalmente Chris seria um Banqueiro ou um Agiota, mas como veremos é melhor que Chris seja somente um amigo da dupla dinâmica Alice e Bob.

$|\phi\rangle$ damos o nome de Catalisador².

-Exemplos-

1)

Suponha que Alice e Bob compartilhem o estado $|\psi_1\rangle = \sqrt{0.4}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.1}|22\rangle + \sqrt{0.1}|33\rangle$ e querem levá-lo ao estado $|\psi_2\rangle = \sqrt{0.5}|00\rangle + \sqrt{0.25}|11\rangle + \sqrt{0.25}|22\rangle$. Já vimos que $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$. Contudo, se Chris empresta o estado $|\phi\rangle = \sqrt{0.6}|00\rangle + \sqrt{0.4}|11\rangle$, então:

$$|\psi_1\rangle \otimes |\phi\rangle \sim (0.24, 0.24, 0.16, 0.16, 0.06, 0.06, 0.04, 0.04),$$

e

$$|\psi_2\rangle \otimes |\phi\rangle \sim (0.30, 0.20, 0.15, 0.15, 0.10, 0.10, 0.00, 0.00).$$

Donde $|\psi_1\phi\rangle \rightarrow |\psi_2\phi\rangle$, ou seja, agora a transformação é possível e o estado emaranhado $|\phi\rangle$, emprestado por Chris, não é consumido durante o processo. Portanto $|\psi_1\rangle \xrightarrow{\text{ELOCC}} |\psi_2\rangle$.

2)

Via de regra, todos os artigos sobre catálise sempre apresentam o exemplo anterior, originalmente em [39], nunca um exemplo diferente. Cabe então produzir um novo exemplo:

Suponha que Alice e Bob compartilhem o estado $|\psi_1\rangle = \sqrt{0.5}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.05}|22\rangle + \sqrt{0.05}|33\rangle$ e querem por meio de LOCC leva-lo até $|\psi_2\rangle = \sqrt{0.7}|00\rangle + \sqrt{0.15}|11\rangle + \sqrt{0.15}|22\rangle$. O teorema de Nielsen garante que $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$ e também $|\psi_2\rangle \not\rightarrow |\psi_1\rangle$. Contudo $|\phi\rangle = \sqrt{0.7}|00\rangle + \sqrt{0.3}|11\rangle$ e $|\chi\rangle = \sqrt{0.75}|00\rangle + \sqrt{0.25}|11\rangle$, são dois possíveis catalisadores.

3)

Afirmamos que nenhuma transformação pode ser catalisada por um estado “balanceado” $|\phi\rangle = \frac{1}{\sqrt{p}}(\sum_{i=1}^p |ii\rangle)$, qualquer que seja $p \in \mathbb{N}$.

Seja $p \in \mathbb{N}$ qualquer. Suponha por absurdo que existe um par de estados $|\psi_i\rangle$ e $|\psi_f\rangle$, com vetores de Schmidt ordenados $(\alpha_1, \dots, \alpha_n)$ e $(\beta_1, \dots, \beta_m)$ t.q. $|\psi_i\rangle \not\rightarrow |\psi_f\rangle$, mas $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$. Como $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$, então, em particular, $\sum_{i=1}^l \frac{\alpha_i}{\sqrt{p}} \leq \sum_{i=1}^l \frac{\beta_i}{\sqrt{p}}, \forall l \in \{1, 2, \dots, \max\{np, mp\}\}$, logo

²A imagem aqui é bem clara, o estado adicional atua como um catalisador em química, facilitando ou permitindo reações químicas.

$\sum_{i=1}^l \alpha_i \leq \sum_{i=1}^l \beta_i, \forall l \in \{1, 2, \dots, \max\{n, m\}\}$. Portanto $\lambda_{\psi_i} \prec \lambda_{\psi_f}$, donde $|\psi_i\rangle \rightarrow |\psi_f\rangle$, um absurdo.

O exemplo 1) simplesmente mostra que existem ELOCC. Por outro lado, exemplo 2) responde a uma pergunta que poderia já ter surgido: “O catalisador de cada transformação é único?” e levanta uma conjectura: Podem existir infinitos catalisadores para uma dada transformação! Voltaremos nesse mesmo exemplo na seção 3.4. O exemplo 3) aborda uma outra questão: a possibilidade de um dado estado $|\phi\rangle$ ser catalisador, lá mostramos que existe, sim, um estado que não pode catalisar ninguém³.

3.3 Quando a Catálise não é Possível e a Anti-Catálise

Começamos pelo:

Teorema 3.2. Não existe catálise em $\mathbb{C}^2 \otimes \mathbb{C}^k; k \geq 2$.

Demonstração. Sejam $|\psi_i\rangle, |\psi_f\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^k$ t.q. $|\psi_i\rangle \not\rightarrow |\psi_f\rangle$. Suponha, por absurdo, que existe $|\phi\rangle$ com coeficientes de Schmidt ordenados $(\delta_1, \delta_2, \dots, \delta_k)$, t.q. $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$.

Como $|\psi_i\rangle, |\psi_f\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^k$, então existem $p, q \in [0.5, 1)$ t.q. os coeficientes de Schmidt de $|\psi_i\rangle$ e $|\psi_f\rangle$ são $\lambda_i = (p, 1-p), \lambda_f = (q, 1-q)$. Além disso, como $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$, então $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$. Portanto $\delta_1 p \leq \delta_1 q$, donde $p \leq q$. Por outro lado, como $|\psi_i\rangle \not\rightarrow |\psi_f\rangle$, e $|\psi_i\rangle, |\psi_f\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, então $p > q$, um absurdo. \square

Lema 3.3. Sejam $\lambda_i = (\alpha_1, \dots, \alpha_n), \lambda_f = (\beta_1, \dots, \beta_n) \in \mathbb{R}^n$ os vetores de Schmidt ordenados de $|\psi_i\rangle, |\psi_f\rangle$. A fim de que $|\psi_i\rangle \xrightarrow{\text{ELOCC}} |\psi_f\rangle$ é necessário que $\alpha_1 \leq \beta_1$ e $\alpha_n \geq \beta_n$.

Demonstração. Seja $\lambda_\phi = (\delta_1, \dots, \delta_k)$ o vetor de Schmidt ordenado do catalisador $|\phi\rangle$, t.q. $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$. Sejam $\lambda_i \otimes \lambda_\phi = (\gamma_1, \dots, \gamma_{nk})$ e $\lambda_f \otimes \lambda_\phi = (\gamma'_1, \dots, \gamma'_{nk})$ os vetores de Schmidt ordenados dos estados $|\psi_i\phi\rangle$ e $|\psi_f\phi\rangle$.

Como $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$, então $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$. Portanto $\alpha_1 \cdot \delta_1 = \gamma_1 \leq \gamma'_1 = \beta_1 \cdot \delta_1$, donde $\alpha_1 \leq \beta_1$. Por outro lado $\sum_{i=1}^{nk-1} \gamma_i \leq \sum_{i=1}^{nk-1} \gamma'_i$, logo

³Veja a seção “Sobre a conjectura de Nielsen”.

$1 - \sum_{i=1}^{nk-1} \gamma_i \geq 1 - \sum_{i=1}^{nk-1} \gamma'_i$, como $\gamma_{nk} = 1 - \sum_{i=1}^{nk-1} \gamma_i$ e $\gamma'_{nk} = \sum_{i=1}^{nk-1} \gamma'_i$, então $\alpha_n \cdot \delta_k = \gamma_{nk} \geq \gamma'_{nk} = \beta_n \delta_k$. Portanto $\alpha_n \geq \beta_n$. \square

Teorema 3.4. *Não existe catálise em $\mathbb{C}^3 \otimes \mathbb{C}^k$; $k \geq 3$*

Demonstração. Sejam $\lambda_i = (\alpha_1, \alpha_2, \alpha_3), \lambda_f = (\beta_1, \beta_2, \beta_3) \in \mathbb{R}^3$, t.q. $\lambda_i \not\prec \lambda_f$.

Como $\lambda_i \not\prec \lambda_f$, então $\alpha_1 > \beta_1$, ou $\alpha_1 \leq \beta_1$ e $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$.

Se for $\alpha_1 > \beta_1$, então o Lema 3.3 garante que não pode existir catálise, caso contrário $\alpha_1 \leq \beta_1$. Se for $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$, e portanto $\alpha_3 < \beta_3$, então, novamente, o Lema 3.3 garante que não pode existir catálise, caso contrário $\alpha_3 \geq \beta_3$. Portanto não existe catálise em $\mathbb{C}^3 \otimes \mathbb{C}^k$; $k \geq 3$. \square

Teorema 3.5. *Não existe catálise entre $|\psi_i\rangle \in \mathbb{C}^4 \otimes \mathbb{C}^n$ e $|\psi_f\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^m$, t.q. $n \geq 4$ e $m \geq 2$.*

Demonstração. Sejam $|\psi_i\rangle \in \mathbb{C}^4 \otimes \mathbb{C}^n$ e $|\psi_f\rangle \in \mathbb{C}^3 \otimes \mathbb{C}^m$. A decomposição de Schmidt Teorema 2.15 garante que podemos olhar somente para os respectivos vetores de Schmidt $\lambda_i = (\alpha_1, \dots, \alpha_4) \in \mathbb{R}^4$ e $\lambda_f = (\beta_1, \beta_2)$. Suponha, por absurdo, que existe $\lambda_\phi = (\delta_1, \dots, \delta_k) \in \mathbb{R}^k$, t.q. $\lambda_i \not\prec \lambda_f$ e $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$.

Como $\lambda_i \not\prec \lambda_f$, então $\alpha_1 > \beta_1$, caso contrário obtém-se ou $\alpha_1 + \alpha_2 > 1$, um absurdo, ou $\alpha_1 + \alpha_2 + \alpha_3 > 1$, um absurdo. Por outro lado $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$, então $\alpha_1 \delta_1 \leq \beta_1 \delta_1$, donde $\alpha_1 \leq \beta_1$, um absurdo. \square

Lema 3.6. *Sejam $|\psi_i\rangle, |\psi_f\rangle$ estados tais que $|\psi_i\rangle \xrightarrow{ELOCC} |\psi_f\rangle$, com catalisador $|\phi\rangle$. Então $|\phi\rangle^{\otimes k}$ é também um catalisador (da mesma transformação), qualquer que seja $k \in \mathbb{N}$.*

Demonstração. Basta usar o corolário 1.17. \square

Em linhas gerais, o Teorema 3.2 mostra que, para 2 qubits, se $|\psi_i\rangle \rightarrow |\psi_f\rangle$, então $|\psi_f\rangle \rightarrow |\psi_i\rangle$, se além disso tivéssemos $|\psi_i\rangle \xrightarrow{ELOCC} |\psi_f\rangle$, então $|\psi_i\rangle$ teria os mesmos coeficientes de Schmidt⁴ de $|\psi_f\rangle$, um absurdo. Por outro lado, o Teorema 3.4 mostra que em $\mathbb{C}^3 \otimes \mathbb{C}^3$, não há liberdade suficiente para que ocorra a majoração $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$. Os Teoremas 3.2, 3.4 e 3.5 são, portanto, teoremas de impossibilidade e, aliados ao exemplo 1), fixam a dimensão mínima onde pode acontecer a catálise. É necessário que o estado inicial more pelo menos em $\mathbb{C}^4 \otimes \mathbb{C}^k$, com $k \geq 4$. O que mostra que os casos mais simples da catálise não ocorrem em espaços, assim, tão triviais! Já o Lema 3.6 diz que

⁴Sendo portanto equivalentes por uma rotação unitária [39].

se um dado estado é um catalisador de uma transformação, então qualquer potência dele mesmo é um catalisador da mesma transformação. Aqui a conclusão óbvia é que aumentar a liberdade (usando o mesmo catalisador) de onde já ocorre a majoração não leva a nenhum resultado novo. Podemos também usar o mesmo Lema 3.6 para afirmar que não existe algo como anti-catálise, ou seja, se uma dada transformação já ocorre (via LOCC), então o acréscimo de um estado (tal como feito em [39]) não impede o acontecimento dessa transformação. Não podemos, por exemplo, proteger o sistema de uma transformação indesejada usando o mesmo truque de adicionar um estado extra.⁵

Dito isto, iremos nos concentrar nos mais simples dentre os casos mais simples. Nesse texto iremos apenas olhar para catalisadores com coeficientes de Schmidt da forma $\lambda_\phi = (p, 1 - p)$; $p \in [0.5, 1)$ e mesmo assim, como veremos, eles são extremamente interessantes, bonitos e complicados.

Terminamos com a definição:

Definição 3.7. *Sejam⁶ $\lambda_i \in \mathbb{R}^n$, $\lambda_f \in \mathbb{R}^m$ e $\lambda_\phi \in \mathbb{R}^k$. Dizemos que $|\psi_i\rangle$ acessa diretamente $|\psi_f\rangle$ quando $\lambda_i \prec \lambda_f$. Por outro lado, dizemos que $|\psi_i\rangle$ ϕ -acessa $|\psi_f\rangle$ quando $\lambda_i \not\prec \lambda_f$, mas $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$. Analogamente, dizemos que $|\psi_f\rangle$ é ϕ -acessado por $|\psi_i\rangle$ quando $\lambda_i \not\prec \lambda_f$, mas $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$.*

3.4 Algumas Perguntas

A discussão acima pode ter levantado algumas perguntas, como por exemplo:

1. Dado $\lambda_\phi \in \mathbb{R}^k$, existem $\lambda_i, \lambda_f \in \mathbb{R}^n$, t.q. $\lambda_i \not\prec \lambda_f$, mas $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$?
2. Dados $\lambda_\phi \in \mathbb{R}^k$, $\lambda_i, \lambda_f \in \mathbb{R}^n$, existem condições necessárias e suficientes para que tenhamos $\lambda_i \not\prec \lambda_f$ e $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$?
3. Dado $\lambda_\phi \in \mathbb{R}^k$, como deve ser o conjunto dos $\lambda_i, \lambda_f \in \mathbb{R}^n$; $\lambda_i \not\prec \lambda_f$, e $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$?
4. Dados $\lambda_\phi \in \mathbb{R}^k$ e $\lambda_f \in \mathbb{R}^n$, como deve ser o conjunto dos $\lambda_i \in \mathbb{R}^n$, t.q. $\lambda_i \not\prec \lambda_f$, mas $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$?

⁵Esse fato poderia ser considerado como um *Non Watchdog effect* [42]. Veja também [43], [44].

⁶Via de regra, $\lambda_i, \lambda_f, \lambda_\phi$ são os coeficientes de Schmidt (ao quadrado) dos estados $|\psi_i\rangle, |\psi_f\rangle, |\phi\rangle$ respectivamente.

5. Dados $\lambda_\phi \in \mathbb{R}^k$ e $\lambda_i \in \mathbb{R}^n$, como deve ser o conjunto dos $\lambda_f \in \mathbb{R}^n$, t.q. $\lambda_i \not\prec \lambda_f$, mas $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$?

O primeiro questionamento está diretamente ligado a conjectura de Nielsen, ou seja, das condições em que um estado $|\phi\rangle$ pode atuar como um catalisador. Já o segundo item é de ordem mais operacional: normalmente, em matemática, temos uma definição e queremos obter um método, uma caracterização que facilite a vida, e que permita não ter que aplicar a definição recorrentemente⁷. As três últimas perguntas, que *a priori* podem parecer meio forçadas, versam sobre a estrutura geométrica, topológica, e por que não algébrica, dos conjuntos, ou seja, se eles são convexos, abertos, fechados, densos, conexos, compactos... ou mesmo admitem uma medida natural, com respeito à qual podemos comparar diferentes conjuntos?

Nas próximas seções nos dedicaremos a tentar responder as perguntas acima. Para algumas, como veremos mais adiante, conseguiremos apenas uma resposta parcial, num caso particular, uma vez que a solução geral se mostra mais complicada. Mas mesmo as respostas parciais têm se mostrado satisfatórias.

3.5 Sobre a existência do Catalisador

Começaremos com o:

Teorema (Sun, Duang e Ying) 3.8. *Sejam $\lambda_i = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $\lambda_f = (\beta_1, \beta_2, \beta_3, \beta_4) \in \mathbb{V}^4$, t.q. $\lambda_i^\downarrow = \lambda_i$, $\lambda_f^\downarrow = \lambda_f$ e $\lambda_i \not\prec \lambda_f$. A fim de que exista um catalisador com coeficientes de Schmidt $\lambda_\phi = (p, 1-p)$; $p \in (0.5, 1)$, é necessário e suficiente que $\max\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1 - \frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\} \leq \min\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1 - \frac{\beta_4}{\alpha_3+\alpha_4}\}$ e $\alpha_1 \leq \beta_1$, $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$, $\alpha_4 \geq \beta_4$. Além disso, no caso afirmativo, se $\max\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1 - \frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\} \leq p \leq \min\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1 - \frac{\beta_4}{\alpha_3+\alpha_4}\}$, então $|\psi_i\rangle$ ϕ -acessa $|\psi_f\rangle$.*

Demonstração. (\implies)

Suponha que $\lambda_i \not\prec \lambda_f$ e $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$.

⁷Apenas para ilustrar: em \mathbb{R} sabemos que uma sequência converge, se e só se, é de Cauchy, ou que toda sequência monótona limitada é convergente. Para convergência de séries temos o critério da integral, ou os testes da razão, o da raiz, e o teste de Raabe[45, 46].

Sejam $\lambda_i \otimes \lambda_\phi = (\alpha_1 p, \dots, \alpha_4 p, \alpha_1(1-p), \dots, \alpha_4(1-p))$ e $\lambda_f \otimes \lambda_\phi = (\beta_1 p, \dots, \beta_4 p, \dots, \beta_1(1-p), \dots, \beta_4(1-p))$. Sejam $(\lambda_i \otimes \lambda_\phi)^\downarrow = (a_1, a_2, \dots, a_n)$ e $(\lambda_f \otimes \lambda_\phi)^\downarrow = (b_1, b_2, \dots, b_n)$. Como $(\beta_1, \beta_2, \dots, \beta_n)$ é ordenado e $p \in (0.5, 1)$, então:

$$\beta_1 p \geq \beta_2 p \geq \beta_3 p \geq \beta_4 p. \quad (3.1)$$

$$\beta_1(1-p) \geq \dots \geq \beta_4(1-p). \quad (3.2)$$

$$\beta_i p \geq \beta_i(1-p), \quad \forall i \in I_4. \quad (3.3)$$

Afirmamos que $\beta_1 p \geq \beta_1(1-p) > \beta_2 p \geq \beta_3 p > \beta_2(1-p) \geq \beta_3(1-p) > \beta_4 p \geq \beta_4(1-p)$.

Como $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$, então $\sum_{i=1}^l a_i \leq \sum_{i=1}^l b_i$, $\forall l \in I_8$, donde $b_1 + b_2 \geq a_1 + a_2 \geq \alpha_1 p + \alpha_2 p$. Além disso, como $\lambda_i \not\prec \lambda_f$ e $\lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi$, então segue da definição⁸ que $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$, portanto $b_1 + b_2 > \beta_1 p + \beta_2 p$, donde $b_2 > \beta_2 p$. Usando a desigualdade (3.1) obtem-se que $b_2 = \beta_1(1-p)$ e $b_3 = \beta_2 p$.

Analogamente, como $a_1 + a_2 + a_3 + a_4 \geq \alpha_1 p + \alpha_2 p + \alpha_1(1-p) + \alpha_2(1-p) = \alpha_1 + \alpha_2$, então $b_1 + b_2 + b_3 + b_4 \geq a_1 + \dots + a_4 \geq \alpha_1 + \alpha_2 > \beta_1 + \beta_2$, donde $b_4 > -\beta_1 p - \beta_1(1-p) - \beta_2 p + \beta_1 + \beta_2 = \beta_2(1-p)$, logo $b_4 > \beta_2(1-p)$, portanto $b_4 = \beta_3 p$.

Como $\lambda_i \prec \lambda_f$, então $a_7 + a_8 \geq b_7 + b_8$. Além disso, $a_7 + a_8 \leq \alpha_3(1-p) + \alpha_4(1-p)$, donde $b_7 + b_8 \leq (\alpha_3 + \alpha_4)(1-p) < (\beta_3 + \beta_4)(1-p)$. Como $b_8 = \beta_4(1-p)$, então $\beta_7 < \beta_3(1-p)$, logo $b_7 = \beta_4 p$. As desigualdades (3.1), (3.2), (3.3) implicam que $b_6 = \beta_3(1-p)$, $b_5 = \beta_2(1-p)$.

Afirmamos que $\frac{\beta_2}{\beta_2 + \beta_3} < p < \min\left\{\frac{\beta_1}{\beta_1 + \beta_2}, \frac{\beta_3}{\beta_3 + \beta_4}\right\}$.

$$\frac{\beta_2}{\beta_2 + \beta_3} < p \iff \beta_2 < \beta_2 p + \beta_3 p \iff p\beta_3 > \beta_2(1-p);$$

$$\frac{\beta_1}{\beta_1 + \beta_2} > p \iff (1-p)\beta_1 > p\beta_2;$$

$$\frac{\beta_3}{\beta_3 + \beta_4} > p \iff (1-p)\beta_3 > p\beta_4.$$

Como as desigualdades (3.1), (3.2), (3.3) são verdadeiras, segue que $\frac{\beta_2}{\beta_2 + \beta_3} < p < \min\left\{\frac{\beta_1}{\beta_1 + \beta_2}, \frac{\beta_3}{\beta_3 + \beta_4}\right\}$.

Daqui pra frente usaremos repetidas vezes⁹ o Lema 1.13.

⁸Veja a Definição 1.1.

⁹Mais ainda, essa é a parte mais "chatinha" da demonstração. Para facilitar a leitura, omitiremos algumas passagens, mas não tantas quantas foram omitidas no original [47].

i)

$$a_1 \leq b_1 \iff \alpha_1 \leq \beta_1$$

ii)

Como $a_1 + a_2 \leq b_1 + b_2$ pode ser reescrita como $b_1 + b_2 \geq \max\{\alpha_1 p + \alpha_1(1-p), \alpha_1 p + \alpha_2 p\}$, então $\beta_1 = \beta_1 p + \beta_1(1-p) = b_1 + b_2 \geq \max\{\alpha_1 p + \alpha_1(1-p), \alpha_1 p + \alpha_2 p\}$, portanto $a_1 + a_2 \leq b_1 + b_2 \iff \beta_1 \geq \alpha_1$ e $\beta_1 \geq (\alpha_1 + \alpha_2)p \iff p \leq \frac{\beta_1}{\alpha_1 + \alpha_2}$ e $\beta_1 \geq \alpha_1$.

iii)

$$\begin{aligned} a_1 + a_2 + a_3 \leq b_1 + b_2 + b_3 &\iff \max\{\alpha_1 p + \alpha_2 p + \alpha_3 p, \alpha_1 p + \alpha_1(1-p) + \alpha_2 p\} \leq \\ &\leq b_1 + b_2 + b_3 = \beta_1 + \beta_2 p \iff p \leq \frac{\beta_1}{\alpha_1 + \alpha_2 + \alpha_3 - \beta_2} \text{ e } p \leq \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}. \end{aligned}$$

iv)

$$\begin{aligned} \sum_{i=1}^4 a_i \leq \sum_{i=1}^4 b_i &\iff \beta_1 p + \beta_1(1-p) + \beta_2 + \beta_3 p \geq \\ &\geq \max\{\alpha_1 p + \alpha_1(1-p) + \alpha_2 p + \alpha_2(1-p), \alpha_1 p + \alpha_2 p + \alpha_3 p + \alpha_1(1-p), \\ &\quad p(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)\} \iff p \geq \frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_1 + \beta_3}, \text{ e} \\ &\quad p \leq \frac{\beta_1 - \alpha_1}{\alpha_2 + \alpha_3 - \beta_2 - \beta_3}, \frac{\beta_1}{1 - \beta_2 - \beta_3} \end{aligned}$$

Se $\alpha_2 + \alpha_3 - \beta_2 - \beta_3 = 0$, então a respectiva desigualdade pode ser descartada.

v)

$$\begin{aligned} \sum_{i=1}^5 a_i \leq \sum_{i=1}^5 b_i &\iff \beta_3(1-p) + \beta_4 p + \beta_4(1-p) = b_6 + b_7 + b_8 \leq a_6 + a_7 + a_8 \leq \\ &\leq \min\{\alpha_2(1-p) + \alpha_3(1-p) + \alpha_4(1-p), \alpha_3(1-p) + \alpha_4 p + \alpha_4(1-p)\} \iff \\ &\iff p \leq 1 - \frac{\beta_4}{\alpha_2 + \alpha_3 + \alpha_4 - \beta_3} \text{ e } p \geq 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3}. \end{aligned}$$

vi)

$$\begin{aligned} \sum_{i=1}^6 a_i \leq \sum_{i=1}^6 b_i &\iff a_7 + a_8 \geq b_7 + b_8 \iff \beta_4 p + \beta_4(1-p) \leq \min\{\alpha_4, \alpha_3(1-p) + \alpha_4(1-p)\} \iff \\ &\iff \beta_4 \leq \alpha_4 \text{ e } p \leq 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}. \end{aligned}$$

vii)

$$\sum_{i=1}^7 a_i \leq \sum_{i=1}^7 b_i \iff a_8 \geq b_8 \iff \alpha_4 \geq \beta_4.$$

$$\text{Portanto } p \leq \frac{\beta_1}{\beta_1 + \beta_2}, \frac{\beta_3}{\beta_3 + \beta_4}, \frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1}{\alpha_1 + \alpha_2 + \alpha_3 - \beta_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}$$

$$\frac{\beta_1 - \alpha_1}{\alpha_2 + \alpha_3 - \beta_2 - \beta_3}, \frac{\beta_1}{1 - \beta_2 - \beta_3}, 1 - \frac{\beta_4}{\alpha_2 + \alpha_3 + \alpha_4 - \beta_3}, 1 - \frac{\beta_4}{\alpha_3 + \alpha_4} \text{ e}$$

$$p \geq 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3}, \frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_2 + \beta_3}.$$

Por outro lado, como $\beta_1 \geq \alpha_1 \geq \alpha_2 > \beta_2 \geq \beta_3 > \alpha_3 \geq \alpha_4 \geq \beta_4$ e $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$, então:

$$\frac{\beta_1}{\beta_1 + \beta_2} > \frac{\beta_1}{\alpha_1 + \alpha_2}; \quad (3.4)$$

$$\frac{\beta_3}{\beta_3 + \beta_4} = 1 - \frac{\beta_4}{\beta_3 + \beta_4} > 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}; \quad (3.5)$$

$$\frac{\beta_1}{\alpha_1 + \alpha_2} < \frac{\beta_1}{\alpha_1 + \alpha_2 - \beta_1 - \beta_2}; \quad (3.6)$$

$$\frac{\beta_1}{\alpha_1 + \alpha_2} < \frac{\beta_1}{\beta_1 + \beta_2} < \frac{\beta_1}{\beta_1 + \beta_4} = \frac{\beta_1}{1 - \beta_2 - \beta_3}; \quad (3.7)$$

$$1 - \frac{\beta_4}{\alpha_2 + \alpha_3 + \alpha_4 - \beta_3} > 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}; \quad (3.8)$$

$$\frac{\beta_1 - \alpha_1}{\alpha_2 + \alpha_3 + \beta_1 - \beta_3} > \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}. \quad (3.9)$$

Logo existem 6 desigualdades desnecessárias envolvendo p e os coeficientes de Schmidt $\alpha_1, \alpha_2, \dots, \beta_1, \dots, \beta_4$. Portanto $\max\left\{\frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_2 + \beta_3}, 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3}\right\} \leq p \leq \min\left\{\frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}, 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}\right\}$.

(\Leftarrow)

Suponha que $\alpha_1 \leq \beta_1$, $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$, $\alpha_4 \geq \beta_4$, e $\max\left\{\frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_2 + \beta_3}, 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3}\right\} \leq p \leq \min\left\{\frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}, 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}\right\}$, então:

Seja $p \in (0.5, 1.0) \cap \left[\max\left\{\frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_2 + \beta_3}, 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3}\right\}, \min\left\{\frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}, 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}\right\}\right]$ arbitrário. Como todas as setas da parte (\Rightarrow) da demonstração têm dois sentidos, então $\sum_{i=1}^l a_i \leq \sum_{i=1}^l b_i$, $\forall l \in I_8$, e $\sum_{i=1}^8 a_i = \sum_{i=1}^8 b_i$.

Em particular $|\psi_i\rangle$ ϕ -acessa $|\psi_f\rangle$. \square

-Exemplos-

1)

Sejam $|\psi_i\rangle, |\psi_f\rangle$ com vetor de Schmidt dados por $\lambda_i = (0.4, 0.4, 0.1, 0.1)$ e $\lambda_f = (0.5, 0.25, 0.25)$. Logo:

$$\max\left\{\frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_2 + \beta_3}, 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3}\right\} = \max\left\{\frac{3}{5}, \frac{1}{3}\right\} = \frac{3}{5},$$

$$\min\left\{\frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}, 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}\right\} = \min\left\{\frac{5}{8}, \frac{2}{3}\right\} = \frac{5}{8}.$$

Portanto $|\psi_i\rangle \rightarrow |\psi_f\rangle$, mas $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$, qualquer que seja $|\phi\rangle$ com coeficientes de Schmidt $\lambda_\phi = (p, 1-p)$; $p \in [0.600, 0.625]$.

2)

Sejam $|\psi_i\rangle, |\psi_f\rangle$ com coeficientes de Schmidt dados por $\lambda_i = (0.5, 0.4, 0.05, 0.05)$ e $\lambda_f = (0.7, 0.15, 0.15)$. Logo:

$$\max\left\{\frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_2 + \beta_3}, 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3}\right\} = \max\left\{\frac{2}{3}, \frac{1}{2}\right\} = \frac{2}{3},$$

$$\min\left\{\frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}, 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}\right\} = \min\left\{\frac{7}{9}, \frac{4}{5}\right\} = \frac{7}{9}.$$

Portanto $|\psi_i\rangle \rightarrow |\psi_f\rangle$, mas $|\psi_i\phi\rangle \rightarrow |\psi_f\phi\rangle$, qualquer que seja $|\phi\rangle$ com coeficientes de Schmidt $\lambda_\phi = (p, 1-p)$; $p \in [\frac{2}{3}, \frac{7}{9}]$.

Estabelecemos portanto as condições (necessárias e suficientes) onde faz sentido falar de catálise, mas não só isso, o Teorema 3.8 garante que exceto em alguns casos existe não somente um único catalisador, mas uma infinidade deles, basta olhar para os exemplos 1) e 2). Contudo, note que a existência do catalisador só é garantida para estados finais e iniciais vivendo em até $\mathbb{C}^4 \otimes \mathbb{C}^4$ e catalisadores em $\mathbb{C}^2 \otimes \mathbb{C}^2$, ou seja, apenas uma resposta parcial é obtida para a pergunta: "Quais são as condições necessárias e suficientes para a catálise?". Ainda assim, como vimos, a demonstração do teorema é árdua e cheia de detalhes técnicos.¹⁰

É esse teorema, ou uma variante dele, que transformará a conjectura de Nielsen em um teorema e permitirá a discussão sobre o volume de certos conjuntos.

3.6 Conjectura de Nielsen

"I conjecture that if z is a non-uniform vector, then there exist x and y such that $x \not\prec y$, but

$$x \otimes z \prec y \otimes z."$$

(M. A. Nielsen)

Teorema 3.9. *Seja $z = (z_1, z_2, \dots, z_k)$ um vetor de probabilidade não-uniforme, com $z_1 > z_k > 0$, então existem $x = (x_1, x_2, x_3, x_4), y = (y_1, y_2, y_3, y_4) \in \mathbb{R}^4$ t.q. $x \not\prec y$ e $x \otimes z \prec y \otimes z$.*

¹⁰Só para registrar, o artigo original de Jonathan e Plenio [39] veio em 1999 e somente seis anos depois, em 2005, vieram as condições necessárias e suficientes, no caso particular, para a ocorrência da catálise [47].

A fim de demonstrar o Teorema acima, vamos usar a seguinte ideia: dado um vetor z de probabilidades não-uniforme, iremos obter (espertamente) dois outros vetores auxiliares x e y , com $x \prec y$, e $x \otimes z \prec y \otimes z$, tal que todas as desigualdades da segunda relação de majoração são estritas. Veja um exemplo na figura abaixo.

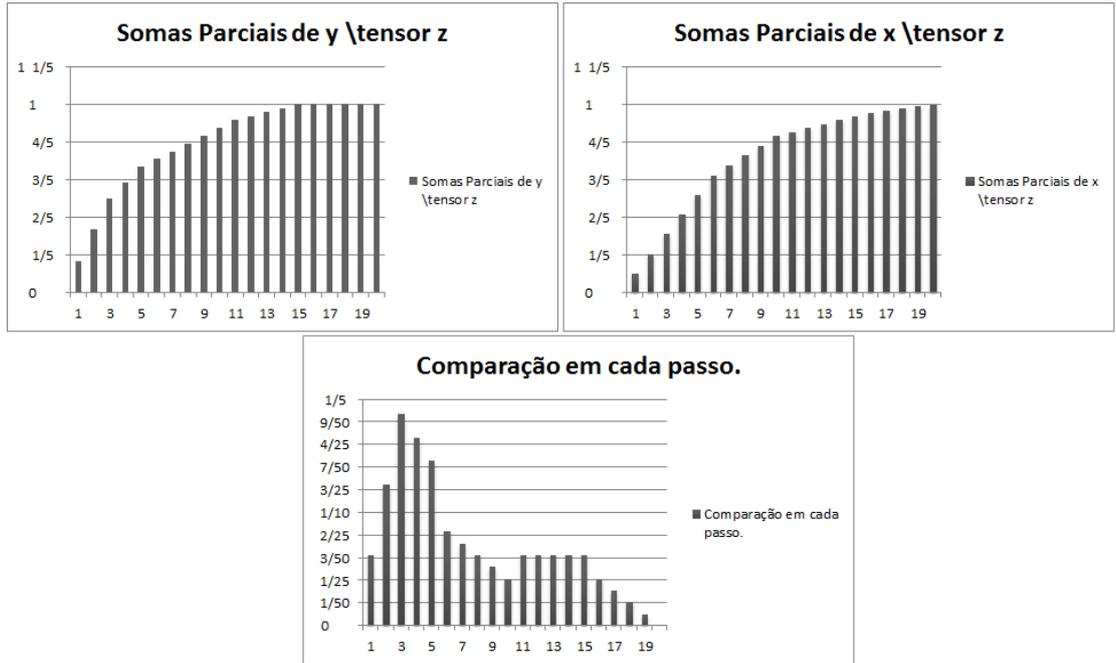


Figura 3.3: Aqui $x = (\frac{5}{12}, \frac{5}{12}, \frac{1}{12}, \frac{1}{12})$, $y = (\frac{4}{6}, \frac{1}{6}, \frac{1}{6}, 0)$ e $z = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8})$.

Feito isso, uma pequena perturbação em x, y leva aos vetores procurados no enunciado do Teorema 2.25.

Demonstração. Para fixar as ideias suponha que $z_1 \geq z_2 \geq \dots > z_k > 0$. Sejam α, β dados por $\alpha + \beta = 1$ e $\frac{z_1}{z_k} = \frac{\alpha}{\beta}$. Note que como $z_1 > z_k > 0$, então $\alpha \frac{z_1}{z_k} > \beta$. Logo $\alpha > \beta$.

Sejam $x = (x_1, \dots, x_4), y = (y_1, \dots, y_4) \in \mathbb{R}^4$ dados por $x_1 = x_2 = \frac{1}{2}\alpha + \frac{1}{4}\beta$, $x_3 = x_4 = \frac{1}{4}\beta$ e $y_1 = \alpha$, $y_2 = y_3 = \frac{1}{2}\beta$, $y_4 = 0$. Como $\alpha > \beta > 0$ e $\alpha + \beta = 1$, então $x = x^\downarrow$, $y = y^\downarrow$ e $\sum_{i=1}^4 x_i = 1 = \sum_{i=1}^4 y_i$. Afiramos que $x \prec y$.

Como $x_1 = \frac{1}{2}\alpha + \frac{1}{4}\beta < \alpha = y_1$, $x_1 + x_2 = \alpha + \frac{1}{2}\beta = y_1 + y_2$, e $x_1 + x_2 + x_3 = \alpha + \frac{3}{4}\beta < 1 = y_1 + y_2 + y_3$, então $x \prec y$.

Além disso, o corolário 1.17 garante que $x \otimes z \prec y \otimes z$. Afiramos que todas as desigualdades da majoração entre $x \otimes z$ e $y \otimes z$ são estritas, ou seja, $\sum_{i=1}^l (x \otimes z)_i^\downarrow < \sum_{i=1}^l (y \otimes z)_i^\downarrow$, $\forall l \in \{1, 2, 3, \dots, 4k-1\}$.

Suponha inicialmente que l é um número par.

i) Se $1 \leq l \leq k$, então:

$$\sum_{i=1}^l (x \otimes z)_i^\downarrow = \left(\alpha + \frac{1}{2}\beta\right) \sum_{i=1}^{l/2} z_i \text{ e } \sum_{i=1}^l (y \otimes z)_i^\downarrow = \alpha \sum_{i=1}^l z_i,$$

donde $\sum_{i=1}^l (y \otimes z)_i^\downarrow - \sum_{i=1}^l (x \otimes z)_i^\downarrow = \sum_{i=1}^{l/2} (\alpha z_{i+1/2} - \beta z_i) > 0$;

ii) Se $k+1 \leq l < 2k$, então:

$\sum_{i=1}^l (x \otimes z)_i^\downarrow = \left(\alpha + \frac{1}{2}\beta\right) \sum_{i=1}^{l/2} z_i$ e $\sum_{i=1}^l (y \otimes z)_i^\downarrow = \sum_{i=1}^k (y \otimes z)_i^\downarrow + \sum_{i=k+1}^l (y \otimes z)_i^\downarrow = \alpha \sum_{i=1}^k z_i + \sum_{i=k+1}^l (y \otimes z)_i^\downarrow$. Note que como z é um vetor de probabilidades, tem-se que $\sum_{i=1}^k z_i = 1$, por outro lado uma expressão fechada para $\sum_{i=k+1}^l (y \otimes z)_i^\downarrow$ demanda a análise da paridade de k . Vamos nos contentar somente com a limitação $\sum_{i=k+1}^l (y \otimes z)_i^\downarrow \geq \frac{1}{2}\beta \sum_{i=1}^{l-k} z_i$. Assim $\sum_{i=1}^l (y \otimes z)_i^\downarrow \geq \alpha + \frac{1}{2}\beta \sum_{i=1}^{l-k} z_i$, então $\sum_{i=1}^l (y \otimes z)_i^\downarrow - \sum_{i=1}^l (x \otimes z)_i^\downarrow \geq \alpha \sum_{i=l/2+1}^k z_i - \frac{1}{2}\beta \sum_{i=l-k+1}^{l/2} z_i$. Como as duas somas contém $k - \frac{l}{2}$ termos e $\alpha z_i > \frac{\beta}{2} z_j$, $\forall i, j \in I_k$, então $\sum_{i=1}^l (y \otimes z)_i^\downarrow - \sum_{i=1}^l (x \otimes z)_i^\downarrow \geq \alpha \sum_{i=l/2+1}^k z_i - \frac{1}{2}\beta \sum_{i=l-k+1}^{l/2} z_i > 0$;

iii) Se $l = 2k$, então:

Analogamente, $\sum_{i=1}^l (x \otimes z)_i^\downarrow = \sum_{i=1}^{2k} (x \otimes z)_i^\downarrow = \alpha + \frac{\beta}{2}$ e $\sum_{i=1}^{2k} (y \otimes z)_i^\downarrow = \alpha + \sum_{i=k+1}^{2k} (y \otimes z)_i^\downarrow \geq \alpha + \frac{1}{2}\beta z_1 + \frac{\beta}{2} \sum_{i=1}^{k-1} z_i$, donde $\sum_{i=1}^{2k} (x \otimes z)_i^\downarrow - \sum_{i=1}^{2k} (y \otimes z)_i^\downarrow = \frac{1}{2}\beta z_1 - \frac{1}{2}\beta z_k > 0$;

iv) Se $2k+1 \leq l \leq 3k$, então:

$$\sum_{i=1}^l (x \otimes z)_i^\downarrow = \alpha + \frac{1}{2}\beta + \frac{1}{2}\beta \sum_{i=1}^{l/2-k} z_i.$$

Com o mesmo argumento do item iii) tem-se que:

$$\sum_{i=1}^l (y \otimes z)_i^\downarrow = \sum_{i=1}^k (y \otimes z)_i^\downarrow + \sum_{i=k+1}^{2k} (y \otimes z)_i^\downarrow + \sum_{i=2k+1}^l (y \otimes z)_i^\downarrow \geq \alpha + \frac{1}{2}\beta + \frac{1}{2}\beta \sum_{i=1}^{l-2k} z_i$$

Donde $\sum_{i=1}^l (y \otimes z)_i^\downarrow - \sum_{i=1}^l (x \otimes z)_i^\downarrow \geq \alpha + \frac{1}{2}\beta + \frac{1}{2}\beta \sum_{i=1}^{l-2k} z_i - \alpha - \frac{1}{2}\beta - \frac{1}{2}\beta \sum_{i=1}^{l/2-k} z_i > 0$;

v) Se $3k+1 \leq l < 4k$.

Como $y_4 = 0$ tem-se que $\sum_{i=1}^l (y \otimes z)_i^\downarrow = 1$, obtemos facilmente que $\sum_{i=1}^l (y \otimes z)_i^\downarrow - \sum_{i=1}^l (x \otimes z)_i^\downarrow > 0$.

Por outro lado, suponha que, l é ímpar.

Como l é ímpar, então $l + 1$ é par e $l - 1$ é par. Portanto todas as somas do tipo $\sum_{i=1}^{l \pm 1} (x \otimes z)_i^\downarrow$ recaem sobre algum dos casos anteriores, logo:

$$\sum_{i=1}^{l-1} (x \otimes z)_i^\downarrow + \sum_{i=1}^{l+1} (x \otimes z)_i^\downarrow < \sum_{i=1}^{l-1} (y \otimes z)_i^\downarrow + \sum_{i=1}^{l+1} (y \otimes z)_i^\downarrow, \quad \forall l \in \{1, 3, 5, \dots, 4k - 1\}.$$

Como l é ímpar, então os termos do lado esquerdo da desigualdade aparecem aos pares, donde $\sum_{i=1}^l (x \otimes z)_i^\downarrow = \frac{1}{2} \left[\sum_{i=1}^{l-1} (x \otimes z)_i^\downarrow + \sum_{i=1}^{l+1} (x \otimes z)_i^\downarrow \right]$. Por outro lado $\sum_{i=1}^l (y \otimes z)_i^\downarrow \geq \frac{1}{2} \left[\sum_{i=1}^{l-1} (y \otimes z)_i^\downarrow + \sum_{i=1}^{l+1} (y \otimes z)_i^\downarrow \right]$. Portanto $\sum_{i=1}^l (y \otimes z)_i^\downarrow - \sum_{i=1}^l (x \otimes z)_i^\downarrow > 0$, $\forall l \in \{1, 2, \dots, 4k - 1\}$.

Como todas as desigualdades na majoração são estritas, então existe $\epsilon > 0$, t.q. $\tilde{x} = (x_1 + \epsilon, x_2 + \epsilon, x_3 - \epsilon, x_4 - \epsilon) \otimes z \prec (y_1, y_2, y_3, y_4) \otimes z$. Como $\tilde{x}_1 + \tilde{x}_2 = \alpha + \frac{1}{2}\beta + 2\epsilon > \alpha + \frac{1}{2}\beta = y_1 + y_2$, então $\tilde{x} \not\prec y$. \square

A demonstração acima não é original, e os créditos vão para S. Daftuar e M. Klimesh [48]. Aqui apenas modificamos uma passagem ou outra, expandindo alguns passos e suprimindo outros com o intuito de deixá-la mais clara ao leitor. Para o caso particular em que z é um vetor de probabilidade não uniforme em \mathbb{R}^2 existe um resultado com um *approach* diferente daquele proposto por Daftuar e Klimesh, veja o teorema 3.11 ao fim desta seção.

Corolário 3.10. *Os únicos estados que não atuam como catalisadores têm a seguinte forma $|\Psi_p\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^p |ii\rangle$, $p \in \mathbb{N}$.*

O corolário anterior mostra que nem estados produtos ($p = 1$), nem estados “maximamente emaranhados” ($p \neq 1$) podem atuar como catalisadores. Claro, que tecnicamente, esse fato já era esperado, uma vez que ambos os tipos de estados têm vetores de Schmidt que não contribuem para a relação de majoração, logo acrescentá-los ao jogo não leva a qualquer mudança. Por outro lado a força do corolário 3.10 reside no fato que esses são os **únicos** vetores que não podem atuar como catalisadores, ou seja, qualquer que seja o estado ϕ , se seu representante é diferente daquele $|\Psi_p\rangle$, é possível obter uma transformação que tem ϕ como catalisador.

Admitiremos sem provas o resultado de P. Anspanch:

Teorema 3.11. *Sejam $\lambda_i = (\alpha_1, \dots, \alpha_4)$, $\lambda_f = (\beta_1, \dots, \beta_4)$ os coeficientes de Schmidt ordenados dos estados $|\psi_i\rangle, |\psi_f\rangle$. A fim de que $\lambda_i \not\prec \lambda_f$, mas $\lambda_i \otimes \lambda_\phi \prec \lambda_\phi; \lambda_\phi =$*

$(p, 1 - p)$, $p \in (0.5, 1.0)$, é necessário e suficiente que $\exists \epsilon_1 \leq 0, \epsilon_2 > 0, \epsilon_3 > 0$ t.q. $\beta_1 = \alpha_1 + \epsilon_1$, $\beta_2 = \alpha_2 - \epsilon_1 - \epsilon_2$, $\beta_3 = \alpha_3 \epsilon_2 + \epsilon_3$, $\beta_4 = \alpha_4 - \epsilon_3$ e $M = \max\left(\frac{\alpha_2 - \epsilon_1}{\alpha_1 + \epsilon_1}, \frac{\alpha_4 - \epsilon_3}{\alpha_3 - \epsilon_3}, \frac{\epsilon_2}{\epsilon_1}\right) \leq \min\left(\frac{\alpha_3 + \epsilon_3}{\alpha_2 - \epsilon_1}, \frac{\epsilon_3}{\epsilon_2}\right) = M$. No caso afirmativo $|\phi\rangle$ é um catalisador quando $M \leq \frac{1-p}{p} \leq m$.

Ainda em [49], Anspach mostrou que dados quaisquer $M_0 > 0$, e $0 < m_0 < 1$, existem estados $|\psi_i\rangle, |\psi_f\rangle$ com coeficientes de Schmidt $\lambda_i = (\alpha_1, \dots, \alpha_4)$, $\lambda_f = (\beta_1, \dots, \beta_4)$, t.q. $M = M_0$ e $m = m_0$. Mas ora, seja $p \in (0.5, 1.0)$, então $1 > \frac{1-p}{p} > 0$, portanto para $M_0 = \frac{1-p}{p} = m_0$, existem $\lambda_i, \lambda_f \in \mathbb{R}^4$, t.q. $\lambda_i \not\prec \lambda_f$, mas $\lambda_i \otimes (p, 1 - p) \prec \lambda_f \otimes (p, 1 - p)$. Ou seja, qualquer estado com coeficiente de Schmidt $\lambda_\phi = (p, 1 - p)$; $p \in (0.5, 1.0)$ é um catalisador!

O leitor mais curioso verá que a demonstração de 3.11 é tão trabalhosa¹¹ quanto 3.8. Por outro lado a afirmação acima é construtiva: é possível, dado p , construir os estados em questão, sem apelar para a continuidade das funções na majoração. Não há, em [49] nenhuma menção a “vetores de probabilidade não uniforme atuam como catalisadores”..¹²

¹¹E por isso não está presente aqui.

¹²Como o autor não deixou nenhum modo de comunicação (eletrônico) explícito no artigo, então não tem como saber se o mesmo não percebeu o fato (indiretamente provado, no caso particular), ou se foi somente lapso no momento da escrita.

Capítulo 4

Poder Catalítico

“...algo como o Poder Catalítico...”

(Marcelo Terra Cunha)

4.1 Algumas Palavras

Sabemos desde o colégio que temos $\frac{2}{6}$ de chance de tirar a face 4 ou a face 2 num jogo honesto de dados, que temos $\frac{1}{2}$ de chance de ganhar um cara-ou-cora, e que temos $\frac{1}{C_{60}^1}$ de chance de ganhar na Mega-Sena. Basicamente o que estamos fazendo é o seguinte processo: Primeiro contamos quais são os resultados possíveis (no caso do jogo de dados: $\{1, 2, 3, 4, 5, 6\}$), depois contamos quais são os resultados que nos interessam ($\{2, 4\}$) e então dividimos o segundo número pelo primeiro para saber quais são nossas chances. Poderíamos reescrever a última setença usando teoria da medida: Usando sempre a medida de contagem, primeiro obtemos o volume do conjunto de resultados possíveis, depois o volume dos resultados que nos interessam, e então fazendo a divisão obtemos nossas “chances” (quanto de um volume cabe no outro).

O leitor poderia se perguntar: “Ora, o que tem tudo isso a ver com Catálise, ou com Mecânica Quântica?”, e a resposta seria... tudo! Falamos nos capítulos anteriores de estados puros, mistos, emaranhados, com transposta parcial positiva, e maximamente emaranhados. É uma pergunta legítima saber se é mais provável encontrar estados puros do que mistos, ou se estados emaranhados ocorrem com mais frequência em Mecânica Quântica, ou ainda, se em dimensões superiores é fácil encontrar estados emaranhados com

transposta parcial positiva¹. Ok! Falamos o que essa história de probabilidades tem a ver com Mecânica Quântica, mas para fazer sentido, falta mostrar como tudo isso se encaixa no nosso caso.

Já sabemos que para qualquer vetor de probabilidades não-uniforme z , existe um par de vetores $x, y \in \mathbb{R}^4$ t.q. x z -acessa y (teoremas 3.9 e 3.11, no caso particular). Mas dentro do contexto de catálise uma pergunta razoável seria: “Dados z_1 e z_2 não uniformes, quem catalisa mais transformações?”². Para tanto, é claro que vamos acabar calculando o tamanho, o volume (mesmo que abstrato) de alguns conjuntos. A título de exemplo e tendo em vista o teorema 3.8, vamos posteriormente nos concentrar só naqueles casos³ em que os estados finais e iniciais tem vetores de Schmidt λ_i, λ_f morando em \mathbb{R}^4 e os catalisadores tem a forma $\lambda_\phi = (p, 1 - p)$; $p \in [0.5, 1.0]$, pois aqui a catálise é muito bem caracterizada em termos dos coeficientes de Schmidt, no sentido de que existem critérios para determiná-la. Mas por enquanto tentaremos manter a maior generalidade possível.

A pergunta acima tem ótimas motivações⁴, é simples, direta e até está bem formulada. Mas sua resposta não é nem de longe igualmente simples e direta. Note que a catálise é um processo que envolve a transformação de dois estados: um inicial $|\psi_i\rangle$ e um final $|\psi_f\rangle$. Logo existem duas maneiras de se calcular o “Poder Catalítico Total” de um candidato a catalisador $|\phi\rangle$. Podemos começar olhando para o **Poder Catalítico Parcial - Fixado o estado inicial**, ou seja, para o tamanho, o volume com respeito a medida μ conjunto $\tilde{E}_{\phi,i} = \{|\psi_f\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m; |\psi_i\rangle \xrightarrow{ELOCC} |\psi_f\rangle, \text{ com catalisador } |\phi\rangle\}$ e depois integrar sobre o conjunto A de todos os possíveis estados iniciais, obtendo algo como:

$$PC_{\mu,\nu}(\phi) = \int_A \mu(\tilde{E}_{\phi,i}) d\nu. \quad (4.1)$$

Mas também poderíamos começar olhando para o **Poder Catalítico Parcial - Fixado o estado final**, ou seja, o volume com respeito a ν do conjunto $\tilde{E}_{\phi,f} = \{|\psi_i\rangle \in \mathbb{C}^r \otimes \mathbb{C}^l; |\psi_i\rangle \xrightarrow{ELOCC} |\psi_f\rangle, \text{ com catalisador } |\phi\rangle\}$, integrar sobre o conjunto B de todos possíveis estados finais e obter:

¹Veja por exemplo: [50], [51], [53], [54] e [55].

²É mais provável achar pares de estados que são catalisados por z_1 ou z_2 ?

³Possíveis generalizações serão brevemente discutidas.

⁴Basta pensar que um laboratório quer saber qual produção de catalisadores é mais rentável.

$$PC'_{\mu,\nu}(\phi) = \int_B \nu(\tilde{E}_{\phi,f}) d\mu. \quad (4.2)$$

Mas a primeira pergunta que vem a mente é: “Os dois Poderes Catalíticos Totais acima definidos são iguais?”. Com uma boa dose de intuição podemos acreditar que sim, mas existe uma assimetria na demonstração do teorema 3.8 que poderia ser transmitida para essa definição, devendo assim ser interpretada fisicamente, pois seria no mínimo estranho ter importância no resultado final o fato de começar fixando o conjunto $\tilde{E}_{\phi,i}$ ou $\tilde{E}_{\phi,f}$. Outro ponto a se destacar, e esse não tem como escapar, é que o Poder Catalítico depende diretamente das medidas adotadas. Ademais, ainda que tenha ficado oculto na discussão acima, o conjunto que estamos interessados em medir é dado por

$$\tilde{E}_\phi = \{(|\psi_i\rangle, |\psi_f\rangle) \in \mathbb{C}^r \otimes \mathbb{C}^l \times \mathbb{C}^n \otimes \mathbb{C}^m; |\psi_i\rangle \xrightarrow{ELOCC} |\psi_f\rangle, \text{ com catalisador } |\phi\rangle\},$$

cujas fatias são os já conhecidos $\tilde{E}_{\phi,i}$ e $\tilde{E}_{\phi,f}$, o que permite reconhecer A como $\tilde{E}_{\phi,f}$, e B como $\tilde{E}_{\phi,i}$. É o tamanho do conjunto \tilde{E}_ϕ que nos dirá quanto um catalisador $|\phi\rangle$ é (quantitativamente) melhor que outro.

É claro que numa primeira (e intencionalmente bem geral) abordagem não estamos preocupados em discriminar quais medidas iremos adotar. Como veremos na próxima seção, exigiremos delas apenas algumas propriedades que são úteis (e razoáveis) para obter resultados interessantes. Contudo seria um pecado deixar dizer que destacadamente existe uma classe de medidas que faz sentido não só em Mecânica Quântica, mas que reúne uma condição necessária para que o nosso problema fique bem posto. Estamos falando daquelas medidas que são invariantes perante Transformações Unitárias, da qual a Medida de Haar é um exemplo [59].⁵

Tornemos agora a discussão anterior um pouco mais rigorosa...

4.2 Poder Catalítico Total

“Dados dois possíveis catalisadores $|\phi\rangle, |\phi'\rangle$, quem catalisa mais transformações?”

Quando dizemos que estamos interessados em saber o volume do conjunto \tilde{E}_ϕ , ou de suas fatias $\tilde{E}_{\phi,i}, \tilde{E}_{\phi,f}$, o que está em jogo é a definição de uma medida bem adaptada ao nosso caso e a aplicação dessa medida no conjunto

⁵Lembre-se que estamos sempre olhando para os Coeficientes de Schmidt de um estado!

\tilde{E}_ϕ . Mas para definir uma medida devemos antes tomar alguma σ -álgebra que se encaixe bem na nossa situação. Antes de definir quais estruturas iremos considerar, uma discussão deve ser feita: Como o fenômeno da Catálise depende exclusivamente dos Coeficientes de Schmidt, sendo irrelevante considerar unitárias locais, faz todo sentido, então, descrever nossos conjuntos de interesse olhando somente para a Decomposição de Schmidt de cada estado. Cada conjunto fica associado a uma contra-parte que mora no simplexo de probabilidades correspondente:

$$\tilde{E}_\phi \mapsto E_\phi = \{(\lambda_i, \lambda_f) \in \mathbb{V}^{\min\{r,l\}} \times \mathbb{V}^{\min\{m,n\}}; \lambda_i \not\prec \lambda_f \text{ e } \lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi\}; \quad (4.3a)$$

$$\tilde{E}_{\phi,i} \mapsto E_{\phi,i} = \{\lambda_f \in \mathbb{V}^{\min\{m,n\}}; \lambda_i \not\prec \lambda_f \text{ mas } \lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi\}; \quad (4.3b)$$

$$\tilde{E}_{\phi,f} \mapsto E_{\phi,f} = \{\lambda_i \in \mathbb{V}^{\min\{r,l\}}; \lambda_i \not\prec \lambda_f \text{ mas } \lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi\}. \quad (4.3c)$$

A fim de poder determinar o volume de $E_{\phi,i}$ seja $(X, \mathbf{X}, \mu : \mathbf{X} \rightarrow \mathbb{R})$ um espaço de medida t.q. cada $E_{\phi,i}$ é \mathbf{X} -mensurável. Analogamente seja $(Y, \mathbf{Y}, \nu : \mathbf{Y} \rightarrow \mathbb{R})$ um espaço de medida t.q. $E_{\phi,f}$ é \mathbf{Y} -mensurável. Dessa maneira, podemos determinar o “tamanho” de cada uma das fatias de E_ϕ , mas podemos ir além. De posse das σ -álgebras \mathbf{X}, \mathbf{Y} é possível definir a menor σ -álgebra $\mathbf{Z} = \mathbf{X} \times \mathbf{Y}$ que contém todos os conjuntos da forma $A \times B$, $A \in \mathbf{X}$ e $B \in \mathbf{Y}$, agora com a ajuda do Teorema da medida produto [57] obtemos uma medida⁶ $(\mu \times \nu) : \mathbf{Z} \rightarrow \mathbb{R}$ t.q. $(\mu \times \nu)(A \times B) = \mu(A)\nu(B), \forall A \times B; A \in \mathbf{X}$ e $B \in \mathbf{Y}$. É essa medida $\mu \times \nu$ que nos dirá o volume do conjunto dos estados que são catalisados por ϕ . Se o conjunto E_ϕ for \mathbf{Z} -mensurável⁷, e cada medida μ, ν for σ -finita (e portanto também $\mu \times \nu$), então o Teorema de Fubini [57] garante que:

$$PC_{\mu,\nu}(\phi) = \int_A \mu(E_{\phi,i}) d\nu = \int_{E_\phi} d(\mu \times \nu) = \int_B \nu(E_{\phi,f}) d\mu = PC'_{\mu,\nu}(\phi). \quad (4.4)$$

Ou seja, obtemos o seguinte resultado: Para espaços de medida bem adaptados o Poder Catalítico Total **independe** da ordem em que começamos a calcular. Podemos fixar os estados iniciais e integrar, e posteriormente integrar sobre os possíveis inícios, ou fixar os finais e depois integrar sobre estes. É

⁶Que é única caso μ, ν sejam σ -finitas.

⁷Veja Apêndice 4.

apenas uma questão de escolha, comodidade, facilidade, ou tratabilidade das contas começar por um, ou outro, Poder Catalítico Parcial. Contudo devemos destacar que apesar de independer da ordem de integração, o Poder Catalítico Total depende da estrutura dos espaços de medidas que irão ser adotados.⁸

Antes de passar para o exemplo final que fecha este capítulo, seria injusto deixar de comentar com o leitor mais alguns fatos. Estamos interessados apenas em medidas com caráter, ou interpretação geométrica razoáveis, no seguinte sentido⁹: se dado o conjunto E_ϕ , for possível colocar uma bola, um bloco de medida de Lebesgue não-nula dentro dele, então diremos que E_ϕ tem um tamanho considerável (não tem-medida nula), e da mesma forma se E_ϕ for magro o suficiente para que nenhuma bola, ou bloco seja inserido dentro dele, então ele tem tamanho desprezível (medida-nula), em outras palavras vamos nos concentrar apenas naquelas medidas que são bem comportadas com respeito a medida de Lebesgue.¹⁰ Dito isso ficamos livres para, pelo menos num primeiro momento, nos concentrar apenas nas medidas usuais de Lebesgue. Além disso, pode não ter ficado clara a mensurabilidade (em geral) do conjunto E_ϕ , para tanto recomendamos a leitura do Apêndice C.

4.3 Um pequeno exemplo: Poder Catalítico Parcial - Fixando o estado final

“... with a few rare exceptions the entities which are studied and analyzed in mathematics may be regarded as certain particular sets or classes of objects...”
(P. Suppes)

Nosso¹¹ objetivo aqui é usar um exemplo para “por a mão na massa” e medir, de uma maneira que ficará clara mais abaixo, o tamanho, o volume do conjunto dos estados iniciais $|\psi_i\rangle$ que ϕ -acessam um certo estado final $|\psi_f\rangle$, onde $|\psi_f\rangle$ e $|\phi\rangle$ são previamente fixados. É claro que a situação será discutida em termos dos coeficientes de Schmidt (ordenados) de cada estado em jogo, e como já foi dito anteriormente, vamos nos preocupar apenas com estados iniciais e finais que têm no máximo 4 coeficientes de Schmidt não-nulos, e catalisadores da forma $(p, 1 - p)$.

⁸De qualquer maneira devemos ressaltar, mais uma vez, que é interessante obter um resultado geral, “independente” das medidas adotadas.

⁹Lembre-se que escolhemos trabalhar apenas num simplexo de probabilidades, ou seja, num sub-conjunto do espaço euclidiano.

¹⁰Algo como $\mu(S) = 0 \iff \lambda(S) = 0, \forall S$, onde λ é a medida de Lebesgue.

¹¹O exemplo aqui tratado, foi obtido com a colaboração de J. A. dos Santos.

Para evitar repetições desnecessárias durante o resto desta seção, vamos fixar algumas notações: $\lambda_i = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, t.q. $\alpha_4 > 0$, $\lambda_f = (\beta_1, \beta_2, \beta_3, \beta_4)$ e $\lambda_\phi = (p, 1 - p)$, t.q. $p \in (0.5, 1.0)$ serão respectivamente os vetores de Schmidt dos estados $|\psi_i\rangle$, $|\psi_f\rangle$ e $|\phi\rangle$. Além disso pediremos também que $\beta_1 > \beta_2 \geq \beta_3 > \beta_4 \geq 0$. Essa última cadeia de desigualdades¹² será a garantia que algumas das condições que obteremos são, além de necessárias, suficientes. Agora podemos começar.

Estamos interessados no conjunto:¹³

$$E_{p,f} = \left\{ \lambda_i = (\alpha_1, \dots, \alpha_4) \in \mathbb{V}^4; \lambda_i \not\prec \lambda_f, \lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi \right\}. \quad (4.5)$$

Mas ora, se $\lambda_i \in E_{p,f}$, então o estado inicial não acessa diretamente o estado final, mas o ϕ -acessa. Portanto, da demonstração do teorema 3.8, tem-se que $\lambda_i = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ obedece às desigualdades:

$$\alpha_1 + \alpha_2 > \beta_1 + \beta_2; \quad (4.6a)$$

$$\beta_1 \geq \alpha_1 \geq \alpha_2 > \beta_2 \geq \beta_3 > \alpha_3 \geq \alpha_4 \geq \beta_4; \quad (4.6b)$$

$$\alpha_1 \leq \beta_1 \text{ e } \alpha_1 + \alpha_2 \leq \frac{\beta_1}{p}; \quad (4.6c)$$

$$\alpha_1 + \alpha_2 p \leq \beta_1 + \beta_2 p \text{ e } \alpha_1 + \alpha_2 + \alpha_3 \leq \frac{\beta_1}{p} + \beta_2; \quad (4.6d)$$

$$1 \leq \frac{\beta_1}{p} + \beta_2 + \beta_3, \text{ e } \alpha_1 + \alpha_2 \leq \beta_1 + (\beta_2 + \beta_3)p; \quad (4.6e)$$

$$\alpha_1 + (\alpha_2 + \alpha_3)p \leq \beta_1 + (\beta_2 + \beta_3)p; \quad (4.6f)$$

$$\alpha_2 + \alpha_3 + \alpha_4 \geq \beta_3 + \frac{\beta_4}{1-p} \text{ e } \alpha_3(1-p) + \alpha_4 \geq \beta_3(1-p) + \beta_4; \quad (4.6g)$$

$$\alpha_3 + \alpha_4 \geq \frac{\beta_4}{1-p} \text{ e } \alpha_4 \leq \beta_4. \quad (4.6h)$$

Portanto o conjunto para o qual devemos olhar inicialmente é formado pelos $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathbb{V}^4$ que satisfazem as desigualdades (4.6). Explicitamente:

$$E_{p,f} = \left\{ \alpha \in \mathbb{V}^4; \alpha_1 + \alpha_2 > \beta_1 + \beta_2, \beta_1 \geq \alpha_1 \geq \alpha_2 > \beta_2 \geq \beta_3 > \alpha_3 \geq \alpha_4 \geq \beta_4, \right.$$

$$\left. \alpha_1 + \alpha_2 \leq \frac{\beta_1}{p}, \alpha_1 + \alpha_2 p \leq \beta_1 + \beta_2 p, \alpha_1 + \alpha_2 + \alpha_3 \leq \frac{\beta_1}{p} + \beta_2, \alpha_2 + \alpha_3 + \alpha_4 \geq \right.$$

¹²Note: Pedir que algumas desigualdades sejam estritas não altera, em geral, os resultados que envolvem medidas.

¹³Aqui $\mathbb{V}^4 = \{(x_1, \dots, x_4) \in \mathbb{R}^4; \sum_{i=1}^4 x_i = 1, 1 > x_1 \geq x_2 \geq x_3 \geq x_4 > 0\}$, e o índice p diz respeito ao catalisador $\phi = (p, 1 - p)$.

$$\beta_3 + \frac{\beta_4}{1-p}, \alpha_3(1-p) + \alpha_4 \geq \beta_3(1-p) + \beta_4, \alpha_3 + \alpha_4 \geq \frac{\beta_4}{1-p},$$

$$\alpha_1 + \alpha_2 \leq \beta_1 + (\beta_2 + \beta_3)p, \alpha_1 + (\alpha_2 + \alpha_3)p \leq \beta_1 + (\beta_2 + \beta_3)p\}.$$

Note que sempre teremos $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$, ou seja uma variedade de dimensão 3 dentro do espaço euclidiano \mathbb{R}^4 . Portanto qualquer medida em \mathbb{R}^4 com algum apelo geométrico, como por exemplo a medida de Lebesgue, nos dará a informação de que o conjunto $E_{p,f}$ tem medida nula. Para contornar esse fato, vamos usar a projeção canônica $\pi : \mathbb{R}^4 \rightarrow \mathbb{R}^3$ dada por $\pi(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3), \forall (x_1, \dots, x_4) \in \mathbb{R}^4$, e nos concentrar no conjunto $\pi(E_{p,f}) \in \mathbb{R}^3$. Feita a projeção, um pouco de trabalho com as desigualdades nos leva ao seguinte conjunto:

$$\pi(E_{p,f}) = \left\{ (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^3; \frac{\beta_1 + \beta_2}{2} < \alpha_1 < \beta_1, \beta_1 + \beta_2 - \alpha_1 < \alpha_2 \leq \right.$$

$$\left. \min \left\{ \alpha_1, \min \left\{ \frac{\beta_1}{p}, \beta_1 + (\beta_2 + \beta_3)p, 1 - \frac{\beta_4}{1-p} \right\} - \alpha_1, \frac{\beta_1}{p} + \beta_2 - \frac{\alpha_1}{p}, \right\}, \right.$$

$$\left. \frac{1 - \alpha_1 - \alpha_2}{2} \leq \alpha_3 \leq \frac{1}{p}(\beta_1 + \beta_2 + p\beta_3 - \alpha_1 - \alpha_2) \right\}.$$

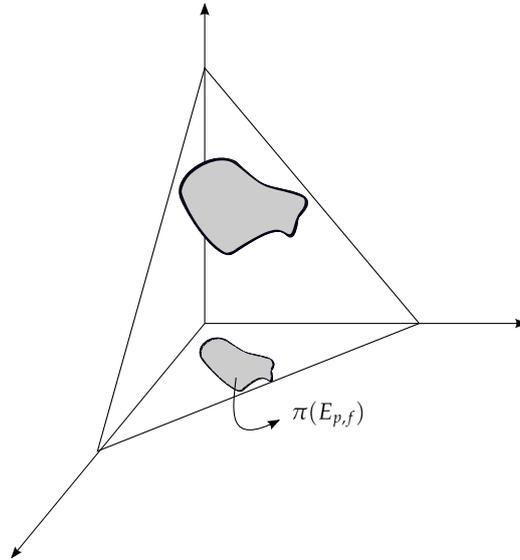


Figura 4.1: Representação esquemática da projeção.

Antes de prosseguir, devemos analisar quais são as condições necessárias, e suficientes (se essas existirem), para que o conjunto ao qual estamos olhando seja não-vazio.

Lema 4.1. *A fim de que $\pi(E_{p,f})$ seja não-vazio é necessário e suficiente que $p \in \left(\frac{\beta_2}{\beta_2+\beta_3}, \min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}\right) \subset (\frac{1}{2}, 1)$.*

Demonstração. A fim de que $\pi(E_{p,f})$ seja não-vazio é necessário, e suficiente, que tenhamos $\min\left\{\frac{\beta_1}{p}, 1 - \frac{\beta_4}{1-p}, \beta_1 + p(\beta_2 + \beta_3)\right\} > \beta_1 + \beta_2$. Logo:

$$\beta_1 + \beta_2 < \frac{\beta_1}{p} \iff p < \frac{\beta_1}{\beta_1 + \beta_2}. \quad (4.7a)$$

$$\beta_1 + \beta_2 < 1 - \frac{\beta_4}{1-p} \iff \frac{\beta_4}{1-p} < \beta_3 + \beta_4 \iff 1-p > \frac{\beta_4}{\beta_3 + \beta_4} \iff p < \frac{\beta_3}{\beta_3 + \beta_4}. \quad (4.7b)$$

$$\beta_1 + \beta_2 < \beta_1 + p(\beta_2 + \beta_3) \iff p > \frac{\beta_2}{\beta_2 + \beta_3}. \quad (4.7c)$$

Logo $\pi(E_{p,f})$ é não vazio se, e somente se, $p \in \left(\frac{\beta_2}{\beta_2+\beta_3}, \min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}\right)$. \square

Alguém poderia se perguntar porque não analisamos a desigualdade que vem com α_3 , ou seja, $\frac{1}{p}(\beta_1 + \beta_2 + p\beta_3 - \alpha_1 - \alpha_2) - \frac{1}{2}(1 - \alpha_1 - \alpha_2) = \frac{2-p}{2p} \left[\beta_1 + \beta_2 + \frac{p(\beta_3 - \beta_4)}{2-p} - (\alpha_1 + \alpha_2)\right] > 0$. Essa última desigualdade é equivalente a $\alpha_1 + \alpha_2 < \beta_1 + \beta_2 + \frac{p(\beta_3 - \beta_4)}{2-p}$. Contudo a construção de $\pi(E_{p,f})$ já é suficiente para mostrar que $\min\left\{\alpha_1, \min\left\{\frac{\beta_1}{p}, \beta_1 + (\beta_2 + \beta_3)p, 1 - \frac{\beta_4}{1-p}\right\}\right\} \leq \beta_1 + \beta_2 + \frac{p(\beta_3 - \beta_4)}{2-p}$, deixando portanto a análise desnecessária.

O Lema 4.1 é fundamental para a definição do poder catalítico parcial, uma vez que se $\pi(E_{p,f}) = \emptyset$, **então não existe estado inicial que ϕ -acessa $\left|\psi_f\right\rangle$** . Além disso, para o leitor mais atento poderia ter surgido a pergunta: “O intervalo $\left(\frac{\beta_2}{\beta_2+\beta_3}, \min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}\right)$ é sempre não-degenerado?”

Lema 4.2. *O intervalo $\left(\frac{\beta_2}{\beta_2+\beta_3}, \min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}\right)$ é não-degenerado se, e somente se, $\beta_1\beta_3 - \beta_2^2 > 0$ e $\beta_3^2 - \beta_2\beta_4 > 0$.*

Demonstração. Basta analisar a desigualdade $\min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\} > \frac{\beta_2}{\beta_2+\beta_3}$. \square

Veja que o Lema 4.2 pode ser parafraseado em termos de médias geométricas, ou seja, o intervalo em questão é não-degenerado se, e somente se, β_2 for maior que a média geométrica de β_1, β_3 , e, além disso, β_3 , for menor que a média geométrica entre β_2, β_4 .

Para aquelas questões que envolvem geometria, e para alguns tipos de medida também, o interior do conjunto $\pi(E_{p,f})$ é importante. Portanto faz total sentido enunciar o seguinte resultado:

Lema 4.3. *O interior do conjunto $\pi(E_{p,f})$ é:*

$$A = \left\{ (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^3; \frac{\beta_1 + \beta_2}{2} < \alpha_1 < \beta_1, \beta_1 + \beta_2 - \alpha_1 < \alpha_2 < \min \left\{ \alpha_1, \min \left\{ \frac{\beta_1}{p}, \beta_1 + (\beta_2 + \beta_3)p, 1 - \frac{\beta_4}{1-p} \right\} - \alpha_1, \frac{\beta_1}{p} + \beta_2 - \frac{\alpha_1}{p}, \right\}, \frac{1 - \alpha_1 - \alpha_2}{2} < \alpha_3 < \frac{1}{p}(\beta_1 + \beta_2 + p\beta_3 - \alpha_1 - \alpha_2) \right\}.$$

A fim de demonstrar o Lema 4.4 basta lembrar que para obter o interior de qualquer conjunto definido por um número finito de desigualdades, basta tornar todas aquelas desigualdades que não são estritas em desigualdades estritas. Vale notar que tanto $\pi(E_{p,f})$ quanto seu interior pode ser visto como uniões e interseções finitas de imagens inversas de funções contínuas.¹⁴

Aqui há um ponto muito peculiar, o lema 4.3 garante que o conjunto $\pi(E_{p,f})$ é razoavelmente parecido com seu interior, apenas algumas desigualdades foram transformadas em desigualdades estritas. Sendo assim, para medidas μ (bem comportadas) tem-se que $\mu(\pi(E_{p,f})) = \mu(\text{int}(\pi(E_{p,f})))$. Ademais:

Lema 4.4. *O conjunto $\pi(E_{p,f})$ é vazio se, e somente se, $\text{int}(\pi(E_{p,f}))$ é vazio.*

Demonstração. (\implies)

Se $\pi(E_{p,f})$ for vazio, então $\text{int}(\pi(E_{p,f}))$ é vazio, uma vez que $\text{int}A \subset A$ qualquer que seja o conjunto A .

(\impliedby)

Se $\text{int}(\pi(E_{p,f})) = \emptyset$, pelos mesmos argumentos usados no Lema 4.1, segue que $p \notin \left(\frac{\beta_2}{\beta_2 + \beta_3}, \min \left\{ \frac{\beta_1}{\beta_1 + \beta_2}, \frac{\beta_3}{\beta_3 + \beta_4} \right\} \right)$, donde $\pi(E_{p,f}) = \emptyset$. □

O lema 4.3 diz que naqueles casos em que $\text{int}(\pi(E_{p,f}))$ é não-vazio¹⁵, existem estados iniciais que são ϕ -levados em $|\psi_f\rangle$ com a seguinte propriedade: Pequenas variações desses estados, perturbações nos coeficientes de Schmidt, geram estados com a mesma característica (são ϕ -levados em $|\psi_f\rangle$). Ainda independente da medida adotada podemos enunciar mais um resultado:

¹⁴Esse fato será amplamente usado no Apêndice C.

¹⁵Veja as proposições 4.1, 4.2, 4.4.

Teorema 4.5. *A fim de que $|\psi_f\rangle$ seja acessível via catálise é necessário, e suficiente que $\min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\} > \frac{\beta_2}{\beta_2+\beta_3}$. No caso afirmativo $|\psi_f\rangle$ é ϕ -acessível desde que $p \in \left(\frac{\beta_2}{\beta_2+\beta_3}, \min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}\right)$, com $\lambda_i \otimes \lambda_\phi \rightarrow \lambda_f \otimes \lambda_\phi, \forall \lambda_i \in E_{p,f}$.*

-Exemplos-

1)

Seja $\lambda_f = \frac{1}{20}(9, 8, 2, 1)$.

Como $\frac{\beta_2}{\beta_2+\beta_3} = \frac{8}{10}$, $\frac{\beta_1}{\beta_1+\beta_2} = \frac{9}{11}$ e $\frac{\beta_3}{\beta_3+\beta_4} = \frac{2}{3}$, então $\pi(E_{p,f}) = \emptyset, \forall p \in (0.5, 1.0)$. Mostramos assim que existe pelo menos um estado final tal que a catálise via $|\phi\rangle \sim (p, 1-p)$ é impossível! Portanto, se ele não for acessado diretamente, então também não o é com a ajuda de ϕ .

2) Fixados β_i :

Seja $D_f = \left\{(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^3; \frac{\beta_1+\beta_2}{2} < \alpha_1 \leq \beta_1, \beta_1 + \beta_2 - \alpha_1 < \alpha_2 \leq \min\{\alpha_1, 1 - 2\beta_4 - \alpha_1\}, \frac{1-\alpha_1-\alpha_2}{2} \leq \alpha_3 \leq 1 - \beta_4 - \alpha_1 - \alpha_2\right\}$ o conjunto dos estados que podem acessar $(\beta_1, \beta_2, \beta_3, \beta_4)$ via catálise. Apenas a título de exemplo, usando a medida de Lebesgue, tem-se que:

$$\begin{aligned} \mu(D_f) &= \int_{\frac{\beta_1+\beta_2}{2}}^{\beta_1} d\alpha_1 \int_{\max\{\beta_1+\beta_2-\alpha_1, \frac{1-\alpha_1}{3}\}}^{\min\{\alpha_1, 1-\alpha_2-2\beta_4\}} d\alpha_2 \int_{\frac{1-\alpha_1-\alpha_2}{2}}^{1-\alpha_1-\alpha_2-\beta_4} d\alpha_3 = \\ &= \int_{\frac{\beta_1+\beta_2}{2}}^{\beta_1} d\alpha_1 \int_{\beta_1+\beta_2-\alpha_1}^{\min\{\alpha_1, 1-\alpha_2-2\beta_4\}} d\alpha_2 \int_{\frac{1-\alpha_1-\alpha_2}{2}}^{1-\alpha_1-\alpha_2-\beta_4} d\alpha_3. \end{aligned}$$

i) Se $\beta_1 \geq \frac{1}{2} - \beta_4$, então:

$$\begin{aligned} \lambda(D_f) &= \int_{\frac{\beta_1+\beta_2}{2}}^{\beta_1} d\alpha_1 \int_{\beta_1+\beta_2-\alpha_1}^{\alpha_1} d\alpha_2 \left(\frac{1}{2} - \frac{\alpha_1}{2} - \frac{\alpha_2}{2} - \beta_4\right) = \\ &= -\frac{\beta_1^3}{3} + \frac{(\beta_1 + \beta_2)^3}{24} + \frac{(\beta_1 - \beta_2)^2(1 - 2\beta_4)}{8} + \frac{(\beta_1^2 - \beta_2^2)(\beta_1 + \beta_2)}{8} \geq \\ &\geq -\frac{\beta_1^3}{3} + \frac{(\beta_1 + \beta_2)^3}{24} + \frac{(\beta_1 - \beta_2)^2\beta_1}{4} + \frac{(\beta_1^2 - \beta_2^2)(\beta_1 + \beta_2)}{8} = f(\beta_1, \beta_2). \end{aligned}$$

Como $\partial_2 f(\beta_1, \beta_2) = -\frac{(\beta_1 - \beta_2)^2}{4} \leq 0$ e $f(\beta_1, \beta_1) = 0$, então $\lambda(D_f) > 0$.

ii) Se $\beta_1 < \frac{1}{2} - \beta_4$, então:

$$\lambda(D_f) = \int_{\frac{\beta_1+\beta_2}{2}}^{1-2\beta_4} d\alpha_1 \int_{\beta_1+\beta_2-\alpha_1}^{\alpha_1} d\alpha_2 \left(\frac{1}{2} - \frac{\alpha_1}{2} - \frac{\alpha_2}{2} - \beta_4\right) +$$

$$\begin{aligned}
& + \int_{1-2\beta_4}^{\beta_1} d\alpha_1 \int_{\beta_1+\beta_2-\alpha_1}^{1-\alpha_1-2\beta_4} d\alpha_2 \left(\frac{1}{2} - \frac{\alpha_1}{2} - \frac{\alpha_2}{2} - \beta_4 \right) = \\
& = 2 \frac{(\frac{1}{2} - \beta_4)^3}{3} - \frac{7}{48} (\beta_1 + \beta_2)^3 - \frac{3}{2} (\frac{1}{2} - \beta_4)^2 (\frac{\beta_1 + \beta_2}{2}) + 2 (\frac{1}{2} - \beta_4) (\frac{\beta_1 + \beta_2}{2})^2 + \\
& \quad + [\beta_1 - (\frac{1}{2} - \beta_4)] (\frac{1}{2} - \beta_4 - \frac{\beta_1 + \beta_2}{2})^2 > 0.
\end{aligned}$$

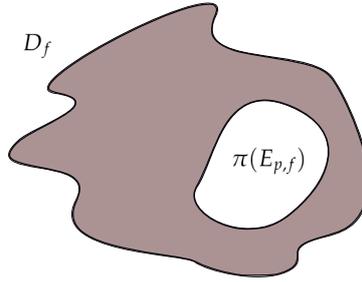


Figura 4.2: Relação entre D_f e $\pi(E_{p,f})$.

Mas o que todos esses Lemas, Teoremas e Proposições querem realmente dizer? Primeiro de tudo, deve-se notar que, com bastante esforço, obtivemos uma forma explícita e bonitinha para o interior do conjunto $\pi(E_{p,f})$. Nem sempre isso é possível, e a única garantia que se tem é que ele está contido em algum outro conjunto, ou que ele contém alguém. No nosso caso fica mais fácil saber quando ele é não-vazio, e portanto quando medidas com interpretações geométricas usuais são não-nulas.

Segundo, o teorema 4.5 pode parecer, num primeiro momento, contraditório com o resultado de Sun, Duang e Ying [47], mas não o é. A abordagem lá é diferente (apesar de ter sido amplamente utilizada aqui), e os interessava saber a existência de um catalisador se fossem dados estados finais e iniciais, enquanto que aqui é fixado somente o estado final $|\psi_f\rangle$, e a pergunta é: dado um estado com vetor de Schmidt $\lambda_\phi = (p, 1-p)$, qual o tamanho do conjunto dos estados iniciais que ϕ -acessam $|\psi_f\rangle$? Ou seja, os estados iniciais são livres!

Terceiro, contrariando as expectativas, o teorema 4.5 garante que existem vários estados que se não forem acessados diretamente, então também não o serão via catálise, com catalisadores da forma $(p, 1-p)$.

Quarto, era esperado que somente não atuariam como potenciais catalisadores¹⁶ estados com $p \in \{0.5, 1.0\}$, mas vimos que esse fato depende dos coeficientes $\beta_1, \beta_2, \beta_3, \beta_4$ e que por exemplo, se o poder catalítico parcial for a medida do conjunto $\pi(E_{p,f})$ e se a medida for a de Lebesgue então teríamos algo como:

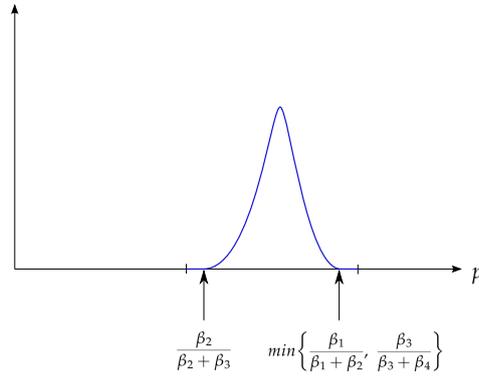


Figura 4.3: Poder Catalítico Parcial com medida de Lebesgue.

Por último, mas não menos importante, o exemplo 2) mostra que independente do estado final, existe sempre a necessidade de se falar em meios alternativos de acessá-lo, seja por catálise ou de outras maneiras ainda desconhecidas. Uma vez que D_f é sempre não-vazio e possui medida de Lebesgue não-nula¹⁷, então dado $\lambda_f = (\beta_1, \beta_2, \beta_3, \beta_4)$ é sempre possível construir vários estados com vetor de Schmidt $\lambda_i = (\alpha_1, \dots, \alpha_4)$ t.q. esses estados podem acessar via catálise $|\psi_f\rangle$.

Todos os fatos discutidos até aqui dizem que podemos encarar como um bom candidato a poder catalítico parcial (fixado o estado final) o valor de uma medida sobre o conjunto $\pi(E_{p,f})$. Chegamos então a definição:

Definição 4.6. *Seja $|\psi_f\rangle$ com coeficientes de Schmidt dados por $\beta_1 > \beta_2 \geq \beta_3 > \beta_4 > 0$, então o poder catalítico parcial (fixado o estado final) do catalisador $|\phi\rangle$ com vetor de Schmidt $\lambda_\phi = (p, 1 - p)$ é dado por $PC_f^\mu(\phi) = \mu(\pi(E_{p,f}))$, t.q. $\mu : \mathbf{X} \rightarrow \mathbb{R}$ é uma medida.*

Assim, independente da medida μ adotada, para alguns valores de $\beta_1, \beta_2, \beta_3, \beta_4$ sempre teremos $PC_f^\mu(\phi) = \mu(\pi(E_{p,f})) = 0, \forall p \in [0.5, 1.0]$ (veja

¹⁶No sentido de ter $\pi(E_{p,f})$ com medida nula.

¹⁷Apesar de ser altamente artificial!

os exemplos anteriores e também o lema 4.2). Mas mais ainda, sabemos que se $\beta_1\beta_3 > \beta_2^2$ e $\beta_3^2 > \beta_2\beta_4$, então ainda assim podemos ter $PC_f^\mu(\phi) = 0$, basta escolher p fora do intervalo $\left(\frac{\beta_2}{\beta_2+\beta_3}, \min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}\right)$, logo $\pi(E_{p,f}) = \emptyset$, uma vez que $\mu(\emptyset) = 0$. Por outro lado, se $\beta_1\beta_3 > \beta_2^2$ e $\beta_3^2 > \beta_2\beta_4$ e $p \in \left(\frac{\beta_2}{\beta_2+\beta_3}, \min\left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}\right)$, então $\text{int}(\pi(E_{p,f})) \neq \emptyset$, nesse caso usando μ como a medida de Lebesgue sabemos que $PC_f^\mu(\phi) \neq 0$. A fim de que não ganhemos mais nenhuma indesejada informação adicional sobre o poder catalítico, é natural pedir que trabalhemos somente com medidas μ tais que $\lambda \ll \mu$, onde λ é a medida de Lebesgue. Dessa forma asseguramos o caráter geométrico do poder catalítico parcial, pois se $PC_f^\lambda(\phi) \neq 0$, então também $PC_f^\mu(\phi) \neq 0$.

Capítulo 5

Comentários Finais e Trabalhos Futuros

Bom, chegamos ao final deste trabalho de dissertação¹, mas felizmente não chegamos ao final da pesquisa sobre poder catalítico, muito menos sobre a catálise. Além de termos cumprido com o que se espera de uma dissertação de mestrado ao:

- Rever, e ampliar com mais exemplos, o artigo de D. Jonathan e M. Plenio [39];
- Estudar a fundo o processo de catálise, para isso se baseando nos artigos [47, 49, 38] e como consequência tendo que gastar algum tempo debruçado em textos sobre Majoração [3, 4, 7, 8] e Aplicações Completamente Positivas [8, 9, 11];
- Rever bibliografia padrão da área a fim de ampliar os horizontes e buscar uma boa definição de volume em conjuntos advindos da Mecânica Quântica [52, 53, 54, 50, 51];

Também nos deperamos com o interessante fato de que escrever um texto de Mecânica Quântica para um público alvo não-físico nos levou ao encontro de ótimas referências sobre o assunto (ótimas mesmo), tais como: [19, 24]. Mas mais ainda, aqui também produzimos conhecimento novo, ao enunciar vários resultados na Seção 3.6.2 e propor alguns quantificadores (O Poder Catalítico Parcial e Total). Muito embora obtemos resultados relevantes,

¹Espero que tenham gostado.

nosso trabalho ainda não terminou, muito pelo contrário, isso foi só um começo. Aqui apenas olhamos para os casos em que λ_i, λ_f têm no máximo 4 componentes não-nulas, mas pode-se tentar também generalizar um pouco mais os resultados, mais especificamente o teorema² 3.8, permitindo agora que $|\psi_i\rangle$ e $|\psi_f\rangle$ morem em $\mathbb{C}^5 \otimes \mathbb{C}^5$, com catalisador ainda em $\mathbb{C}^2 \otimes \mathbb{C}^2$, feito isso, um caminho natural para se encontrar versões mais fortes do teorema 3.8 deve surgir. Também pode-se procurar atacar as situações acima numericamente, principalmente nos casos de dimensões muito altas, sorteando vetores de Schmidt de acordo com a medida adotada e comparar os volumes obtidos. Já que falamos de medidas, pode também ser interessante entender quais restrições aparecem quando pedimos que duas medidas sejam absolutamente contínuas (além do teorema de Radon-Nykodim [56, 57, 58, 59], é claro) ou equivalentes;

Para aqueles que leram o original [39], sabem que aqui apenas falamos de transformações determinísticas, mas é de conhecimento geral que anexar um emaranhamento extra também aumenta a probabilidade de ocorrência de uma transformação. Ou seja podemos refazer toda essa dissertação (e também as bolinhas acima) pensando somente naqueles catalisadores que aumentam a probabilidade total de ocorrência (claro que para isso devemos entender um pouco mais sobre transformações assistidas que aumentam a probabilidade, bons pontos de partida seriam: [60, 61]). Além disso, aqui apenas falamos de transformações entre estados puros (o teorema de Nielsen 2.25 só é válido nesses casos), mas bem poderíamos tentar fazer o mesmo para estados mistos (descritos exclusivamente por um operador densidade), estando inclusive mais próximos de realizações experimentais. Artigos com essa tônica também têm sido escritos, veja por exemplo: [63, 64].

Saindo um pouco da discussão acerca do poder catalítico, mas ainda dentro do contexto de catálise, o Lema 3.6 levanta uma pergunta interessante e que pode ser formulada num contexto "aplicado": Suponha que uma fábrica de estados-catalisadores consegue produzir³ apenas um dado estado, digamos $|\phi\rangle$. Será que é possível, apenas com várias cópias desse vetor, catalisar qualquer transformação⁴? Rigorosamente: Sejam $|\alpha\rangle, |\beta\rangle$ dois estados tais que $|\alpha\rangle \xrightarrow{ELOCC} |\beta\rangle$, com catalisador $|\chi\rangle$. Dado $|\phi\rangle$ arbitrário, existe $k \in \mathbb{N}$ t.q. $|\phi\rangle^{\otimes k}$ é também um catalisador para $|\alpha\rangle, |\beta\rangle$? É claro que se $|\phi\rangle$

²Basicamente tem-se que se preocupar com o reordenamento dos coeficientes

³com rapidez, agilidade, baixo custo, com boa margem de lucro...

⁴Qualquer transformação que admite um catalisador, claro!

for alguém do tipo $(\frac{1}{n}, \dots, \frac{1}{n})$ ou $(1, 0, 0, \dots, 0)$, então não existe tal $k \in \mathbb{N}$, mas todas as outras possibilidades precisam ser exploradas. Convém notar que alguém do tipo $(\frac{1}{n}, \dots, \frac{1}{n})$ apesar de não ser um catalisador, pode ser transformado em um, para então a posteriori poder realizar catálise, de maneira que no final do processo ele não aparece (como é requerido pela teoria), mas sim um “subproduto” deste. Acabamos de ver que relaxar uma das hipóteses sobre a catálise também gera resultados interessantes, nesse sentido obtemos uma resposta **positiva** (pelo menos no caso $\mathbb{C}^2 \otimes \mathbb{C}^2$) para a pergunta: “Todo estado emaranhado é útil?”.[\[68\]](#)

Em resumo acho que o trabalho cumpriu e superou as expectativas. Rendendo frutos e deixando pontos para pesquisas futuras...

Apêndice A

Aplicações Completamente Positivas

Destinamos este primeiro apêndice para definir Aplicações Completamente Positivas, além, é claro, de obter e discutir alguns resultados. Em vista da proximidade da abordagem feita aqui com a que pode ser encontrada em [8], vamos começar fixando algumas notações e só então partir para uma definição formal. Terminamos o capítulo com uma aplicação direta em Mecânica Quântica.

Notações: Aqui $A = [a_{ij}]$ representará uma matriz com entradas números complexos a_{ij} , enquanto que $\mathcal{A} = [[A_{ij}]]$ significará uma matriz cujas entradas são matrizes A_{ij} . A menos que dito explicitamente o contrário, $\{e_i\}_{i=1}^n$ é a base canônica do \mathbb{R}^n e $\{E_{ij} = e_i e_j^*\}_{i,j=1}^n$ é a base canônica do espaço de matrizes $m \times m$, com entradas reais. Passemos agora para as definições:

Definição A.1. *Uma aplicação linear $\Phi : \mathbb{M}_n \longrightarrow \mathbb{M}_k$ é positiva quando $\Phi(A) \geq 0$, $\forall A \geq 0 \in \mathbb{M}_n$.*

Definição A.2. *Seja $\mathbb{M}_m(\mathbb{M}_n)$ o conjunto das matrizes $m \times m$ t.q. a i, j -ésima entrada é uma matriz $[a_{ij}] \in \mathbb{M}_n(\mathbb{C})$. Cada aplicação linear $\Phi : \mathbb{M}_n \longrightarrow \mathbb{M}_k$ induz outra aplicação linear $\Phi_m : \mathbb{M}_m(\mathbb{M}_n) \longrightarrow \mathbb{M}_m(\mathbb{M}_k)$ dada por $\Phi_m(\mathcal{A}) = \Phi_m([[A_{ij}]]) = [[\Phi(A_{ij})]]$, $\forall \mathcal{A} = [[A_{ij}]] \in \mathbb{M}_m(\mathbb{M}_n)$. A aplicação Φ é m -positiva quando Φ_m é positiva. A aplicação Φ é completamente positiva¹ quando é m -positiva para todo $m \in \mathbb{N}$.*

¹Uma definição equivalente a esta diz que uma aplicação Φ é completamente positiva quando $\Phi \otimes \mathbb{1}_H$ é positiva, qualquer que seja o espaço de estados H , veja [62].

-Exemplos-

1)

Seja $\Phi : \mathbb{M}_2 \rightarrow \mathbb{M}_2$ dada por $\Phi(A) = A^T$. Afirmamos que Φ é positiva, mas não é 2-positiva, e portanto não é completamente positiva.

Seja $\mathbb{M}_2 \ni A \geq 0$ arbitrária. Como $A \geq 0$, então existe uma matriz B t.q. $A = B^*B$. Portanto $A^T = (B^*B)^T = B^T B^*$, defina $C = B^*$, então $A^T = B^T B^* = C^*C$. Donde $\Phi(A) = A^T$ é positiva², portanto $\Phi : \mathbb{M}_2 \rightarrow \mathbb{M}_2$ é positiva.

Por outro lado, vamos agora mostrar que existe uma matriz \mathcal{A} positiva com $\Phi_2(\mathcal{A})$ não positiva. Seja $\mathcal{A} = [[E_{ij}]]$, então:

$$[[E_{ij}]] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \implies \Phi_2([[E_{ij}]]) = [[\Phi(E_{ij})]] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Portanto $\det(\Phi_2([[E_{ij}]]) - \lambda \mathbf{1}) = (1 - \lambda)^3(1 + \lambda)$. Logo Φ_2 não é positiva.

2)

Seja $V \in \mathbb{M}_{n \times k}(\mathbb{C})$. Afirmamos que a aplicação $\Phi : \mathbb{M}_n \rightarrow \mathbb{M}_k$ dada por $\Phi(A) = V^*AV$, é completamente positiva.

Seja $m \in \mathbb{N}$ arbitrário, então:

$$\Phi_m[[A_{ij}]] = [[\Phi(A_{ij})]] = (\mathbf{1} \otimes V^*)[[A_{ij}]](\mathbf{1} \otimes V), \forall [[A_{ij}]] \in \mathbb{M}_m(\mathbb{M}_n).$$

Em particular, se $[[A_{ij}]] \geq 0$, então $\langle x, (\mathbf{1} \otimes V^*)[[A_{ij}]](\mathbf{1} \otimes V)x \rangle = \langle (\mathbf{1} \otimes V)x, [[A_{ij}]](\mathbf{1} \otimes V)x \rangle \geq 0, \forall x \in \mathbb{C}^{nk}$.³

O exemplo 2 permite enunciar a proposição:

Proposição A.3. Se $V_1, V_2, \dots, V_l \in \mathbb{M}_{n \times k}(\mathbb{C})$, então a aplicação $\Phi : \mathbb{M}_n \rightarrow \mathbb{M}_k$ dada por $\Phi(A) = \sum_{i=1}^l V_i^*AV_i, \forall A \in \mathbb{M}_n$ é completamente positiva.

Demonstração. Seja $m \in \mathbb{N}$ arbitrário, então:

$$\Phi_m[[A_{ij}]] = [[\Phi(A_{ij})]] = [[\sum_{i=1}^l V_i^*AV_i]] = \sum_{i=1}^l [[V_i^*AV_i]].$$

²Veja [8].

³Analogamente V^*AV é positivo para todo $A \geq 0$.

Como a soma de matrizes positivas é uma matriz positiva, então $\Phi_m[[A_{ij}]] \geq 0$, se $[[A_{ij}]] \geq 0$. Logo Φ_m é m -positiva, donde Φ é completamente positiva. \square

Vimos então que toda aplicação que é expressa na forma de uma soma $A \mapsto \sum_{i=1}^l V_i^* A V_i$ é completamente positiva. Por outro lado, pedir que uma aplicação seja completamente positiva é uma exigência muito restritiva, e portanto cabe naturalmente a pergunta: "Qual a consequência de uma aplicação Φ ser completamente positiva?"

Teorema (Choi, Kraus) 1. *Se $\Phi : \mathbb{M}_n \rightarrow \mathbb{M}_k$ é uma aplicação linear completamente positiva, então existem $V_1, V_2, \dots, V_{nk} \in \mathbb{M}_{n \times k}(\mathbb{C})$, t.q. $\Phi(A) = \sum_{i=1}^{nk} V_i^* A V_i$.*

Demonstração. ⁴

Seja $v \in \mathbb{C}^{nk}$ arbitrário. Podemos então escrever:

$$v = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}; \quad x_i \in \mathbb{C}^k$$

Cada $v \in \mathbb{C}^{nk}$ é portanto identificado com a matriz $V^* = (x_1, x_2, \dots, x_n)$ t.q. $x_1, \dots, x_n \in \mathbb{C}^k$ são as colunas de V^* .

Além disso:

$$\begin{aligned} V^* E_{rs} V &= (x_1, \dots, x_n) e_r e_s^* (x_1, \dots, x_n)^* = \begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1k} & x_{2k} & \cdots & x_{nk} \end{pmatrix} e_r e_s^* \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \cdots & \bar{x}_{1k} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{n1} & \bar{x}_{n2} & \cdots & \bar{x}_{nk} \end{pmatrix} = \\ &= \begin{pmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1k} & x_{2k} & \cdots & x_{nk} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1_r \\ \vdots \\ 0 \end{pmatrix} (0 \dots 1_s \dots 0) \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \cdots & \bar{x}_{1k} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{n1} & \bar{x}_{n2} & \cdots & \bar{x}_{nk} \end{pmatrix} = \end{aligned}$$

⁴Demonstração, sem nenhuma contribuição original, apenas esclarecimentos, retirada de [8].

$$\begin{pmatrix} x_{r1} \\ x_{r2} \\ \vdots \\ x_{rn} \end{pmatrix} (\bar{x}_{s1}, \dots, \bar{x}_{sn}) = x_r x_s^*.$$

Como $v \in \mathbb{C}^{nk}$, então vv^* pode ser representado por uma matriz em $\mathbb{M}_{nk \times nk}(\mathbb{C})$, portanto pode ser representado por uma matriz em blocos em $\mathbb{M}_n(\mathbb{M}_k)$, logo:

$$\begin{aligned} vv^* &= \begin{pmatrix} x_{11} \\ \vdots \\ x_{1k} \\ \vdots \\ x_{n1} \\ \vdots \\ x_{nk} \end{pmatrix} (\bar{x}_{11}, \dots, \bar{x}_{1k}, \dots, \bar{x}_{n1}, \dots, \bar{x}_{nk}) = \begin{pmatrix} x_{11}\bar{x}_{11} & \cdots & x_{11}\bar{x}_{1k} & \cdots & x_{11}\bar{x}_{n1} & \cdots & x_{11}\bar{x}_{nk} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{1k}\bar{x}_{11} & \cdots & x_{1k}\bar{x}_{1k} & \cdots & x_{1k}\bar{x}_{n1} & \cdots & x_{1k}\bar{x}_{nk} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{nk}\bar{x}_{11} & \cdots & x_{nk}\bar{x}_{1k} & \cdots & x_{nk}\bar{x}_{n1} & \cdots & x_{nk}\bar{x}_{nk} \end{pmatrix} = \\ &= [[x_r x_s^*]] = [[V^* E_{rs} V]]. \end{aligned}$$

Além disso, como $[[E_{ij}]] = [[e_r e_s^*]]$ é uma matriz em blocos cuja a r, s -ésima entrada é E_{rs} , então:

$$[[E_{rs}]] = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} (e_1, e_2, \dots, e_n).$$

Donde $[[E_{rs}]]$ é positiva.

Como $\Phi : \mathbb{M}_n \rightarrow \mathbb{M}_k$ é completamente positiva, e portanto n -positiva, então $[[\Phi(E_{rs})]]$ é positiva em $\mathbb{M}_n(\mathbb{M}_k) = \mathbb{M}_{nk}(\mathbb{C})$. O teorema espectral garante que existem vetores $v_1, v_2, \dots, v_{nk} \in \mathbb{C}^{nk}$ t.q. $[[\Phi(E_{rs})]] = \sum_{i=1}^{nk} v_i v_i^* = \sum_{i=1}^{nk} [[V_i^* E_{rs} V_i]] = [[\sum_{i=1}^{nk} V_i^* E_{rs} V_i]]$. Portanto $\Phi(E_{rs}) = \sum_{i=1}^l V_i^* E_{rs} V_i, \forall r, s \in I_n$.

Como Φ é linear, então $\Phi(A) = \Phi(\sum_{i,j=1}^n a_{ij} E_{ij}) = \sum_{i,j=1}^n a_{ij} \Phi(E_{ij}) = \sum_{i,j=1}^n \sum_{l=1}^{nk} a_{ij} V_l^* E_{ij} V_l = \sum_{l=1}^{nk} V_l^* A V_l, \forall A \in \mathbb{M}_n$. \square

Escólio 2. Toda aplicação linear $\Phi : \mathbb{M}_n \rightarrow \mathbb{M}_k$ n -positiva é completamente positiva.

Corolário 3. *Seja $\Phi : \mathbb{M}_n \longrightarrow \mathbb{M}_k$ como no teorema 1. Se $\sum_{i=1}^{nk} V_i V_i^* = \mathbb{1}$, então $\text{tr}(A) = \text{tr}(\Phi(A))$, $\forall A \in \mathbb{M}_n$.*

Demonstração. Seja $A \in \mathbb{M}_n$ arbitrária:

$$\begin{aligned} \text{Como } \Phi(A) = \sum_{i=1}^{nk} V_i^* A V_i, \text{ então } \text{tr}(\Phi(A)) &= \text{tr}\left(\sum_{i=1}^{nk} V_i^* A V_i\right) = \sum_{i=1}^{nk} \text{tr}(V_i^* A V_i) = \\ \text{tr}\left(A \sum_{i=1}^{nk} V_i V_i^*\right) &= \text{tr}(A \mathbb{1}_n) = \text{tr}(A). \quad \square \end{aligned}$$

Corolário 4. *Seja $\Phi : \mathbb{M}_n \longrightarrow \mathbb{M}_k$ como no teorema 1. Se Φ preserva o traço, então $\sum_{i=1}^{nk} V_i V_i^* = \mathbb{1}$.*

Demonstração. Sejam $r, s \in I_n$ arbitrários. Como Φ é completamente positivo e preserva o traço, tem-se que:

$$\begin{aligned} \delta_{rs} = \text{tr}(E_{rs}) = \text{tr}(\Phi(E_{rs})) &= \text{tr}\left(\sum_{i=1}^{nk} V_i^* E_{rs} V_i\right) = \sum_{i=1}^{nk} \text{tr}(E_{rs} V_i V_i^*) = \\ \text{tr}\left(E_{rs} \sum_{i=1}^{nk} V_i V_i^*\right) &= \left(\sum_{i=1}^{nk} V_i V_i^*\right)_{rs}. \quad \square \end{aligned}$$

A representação tal como no teorema 1 é um dos motivos do amplo uso de aplicações completamente positivas. Esforços em obter uma representação “bonitinha” para aplicações positivas não foram muito bem sucedidos. Veja por exemplo [9, 10, 11]. Apesar de ser uma representação bem útil e agradável de se trabalhar, a representação em soma também tem seus pontos fracos, uma vez que pode acontecer dela não ser única.

-Exemplo-

1)

Sejam $\Phi, \Psi : \mathbb{M}^2 \longrightarrow \mathbb{M}^2$ aplicações completamente positivas dadas por $\Phi(M) = \sum_{i=1}^2 E_i^* M E_i$ e $\Psi(M) = \sum_{i=1}^2 F_i^* M F_i$, tais que:

$$\begin{aligned} E_1 &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad e \quad E_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \\ F_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad e \quad F_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Como $F_1 = \frac{1}{\sqrt{2}} E_1 + E_2$ e $F_2 = \frac{1}{\sqrt{2}} E_1 - E_2$, então $\Psi(M) = F_1^* M F_1 + F_2^* M F_2 = \frac{1}{2} ((E_1^* + E_2^*) M (E_1 + E_2) + (E_1^* - E_2^*) M (E_1 - E_2)) = E_1^* M E_1 + E_2^* M E_2 = \Phi(M)$, qualquer que seja $M \in \mathbb{M}_2$.

Esse último exemplo tem bastante interesse físico, pois diz que medições na base $\{|0\rangle, |1\rangle\}$ sem registro do resultado obtido (descrito por Ψ), são

equivalentes ao seguinte processo (descrito por Φ): condicionado ao resultado de um jogo de cara ou coroa, aplicamos ou o operador $\mathbb{1}$, ou o operador Z no sistema. Mais exemplos de aplicações completamente positivas (operações quânticas) podem ser encontradas em [22].

Apêndice B

Uma Calculadora para a Catálise

Aqui a automação das “continhas” envolvidas com a catálise, mais precisamente com a majoração e o produto tensorial, surgiu quando ansiamos responder à conjectura de Nielsen¹.

A tentativa inicial foi pegar um vetor de probabilidade qualquer e mostrar que ele poderia ser um catalisador, contudo fizemos isso com “números” e não “letras” para ver como o processo poderia funcionar. São, portanto, vários ansatz, ou chutes, produtos, somas e comparações simples, mas laboriosas e que tomam tempo. A solução encontrada foi escrever e implementar uma rotina que fazia tudo isso automaticamente, não importando a dimensão dos estados em jogo.

Para evitar perda “desnecessária” de espaço, e aproveitar as facilidades do mundo virtual, escolhemos colocar na grande rede o código fonte da rotina citada acima e algumas figurinhas da mesma em ação.² Seguem abaixo os links para visualização, ou mesmo o *download*, da “Calculadora para a Catálise”, qualquer sugestão visando um algoritmo mais limpo, ou mais rápido, é muito bem-vinda³!

- [Código em C](#);
- [Início do Programa](#);
- [Definindo os estados](#);

¹Todo vetor de probabilidade não uniforme pode atuar como um catalisador.

²Os leitores interessados verão que a combinação *código em C + imagens* ocupariam cerca de 10 páginas aproximadamente. Além disso, para aqueles que possuem apenas a versão impressa deste texto, os links estão disponíveis em www.mat.ufmg.br/~tcunha/dissertacristhiano.pdf.

³Uma nova versão com mais funcionalidades, e mais eficiente está em fase de preparação.

- Verificando a Majoração-Parte I;
- Etapa do Catalisador;
- Verificando a Majoração-Parte II.

Apêndice C

Mensurabilidade de certos conjuntos

"... o fato relevante é que a não mensurabilidade não ocorre quando os conjuntos são definidos construtivamente, por leis de pertinência, nem quando as funções são definidas por fórmulas, como ocorre usualmente nas aplicações." (C. Isnard)

Na seção 3.6.2 fizemos a seguinte afirmação: *"É essa medida $\mu \times \nu$ que nos dirá o volume do conjunto dos estados que são catalisados por ϕ . Se o conjunto E_ϕ for \mathbf{Z} -mensurável, e cada medida μ, ν for σ -finita (e portanto também $\mu \times \nu$), então o Teorema de Fubini [57] garante que..."*. É claro que o ponto-fino dessa afirmação é o condicional **Se**, pois para que as afirmações posteriores façam sentido desejamos que o conjunto E_ϕ esteja na σ -álgebra \mathbf{Z} que foi construída de maneira peculiar, ela é o produto de σ -álgebras em que cada fatia de E_ϕ é mensurável. Para o leitor mais preocupado com os detalhes pode surgir a pergunta: *"Pode-se caracterizar a mensurabilidade de um conjunto via mensurabilidade de cada uma de suas fatias?"*. *A priori* sabemos o seguinte resultado:

Teorema C.1. [57]

Sejam \mathbf{X}, \mathbf{Y} duas σ -álgebras e $\mathbf{Z} = \mathbf{X} \times \mathbf{Y}$. Se $E \in \mathbf{Z}$, então cada uma das fatias $E_x = \{y \in Y; (x, y) \in E\}$ e $E_y = \{x \in X; (x, y) \in E\}$ é mensurável.

Basicamente o que estamos procurando é uma recíproca para este teorema. Seria ideal que a seguinte conjectura fosse verdade:

Conjectura C.2. *Sejam X, Y duas σ -álgebras e $Z = X \times Y$. Seja $E \subset Z = X \times Y$, um conjunto tal que $E_x \in Y$, e $E_y \in X$, $\forall (x, y) \in X \times Y$, então $E \in Z$.*

Valendo a conjectura acima, não precisaríamos nos preocupar com a mensurabilidade do nosso conjunto de interesse E_ϕ , uma vez que cada uma de suas fatias já são mensuráveis. Mas como veremos, isso nem sempre é verdade! Acompanhe:

-Contra-Exemplo-

1)

Sejam (X, \mathbf{X}, μ) , (Y, \mathbf{Y}, ν) dois espaços de medida t.q. $X = [0, 1] = Y$, $\mathbf{X} = \mathbf{Y} = \mathfrak{B}$ os borelianos sobre $[0, 1]$ e $\mu = \nu$ a medida de Lebesgue. Seja T um conjunto não-enumerável, com a cardinalidade de \mathbb{R} , bem-ordenado, com a propriedade de que cada $t \in T$ tem no máximo um número enumerável de antecessores. Defina $s : [0, 1] \rightarrow T$ como uma bijeção.

Defina $E = \{(x, y) \in [0, 1] \times [0, 1]; s(y) \leq s(x)\}$. Logo $E_y = \{x \in [0, 1]; (x, y) \in E\} = \{x \in [0, 1]; s(y) \leq s(x)\} \subset [0, 1]$ tem complementar enumerável qualquer que seja $y \in [0, 1]$, donde $\mu(E_y) = \mu([0, 1] - C(E_y)) = \mu[0, 1] - \mu(E_y) = 1$, $\forall y \in [0, 1]$. Analogamente $E_x = \{y \in [0, 1]; s(y) \leq s(x)\} \in [0, 1]$, é enumerável, portanto mensurável e possui medida nula qualquer que seja $x \in [0, 1]$. Cada fatia de E é mensurável, suponha por absurdo que o próprio E seja um conjunto mensurável.

Como E é mensurável, o Teorema de Fubini garante que:

$$0 = \int_0^1 \nu(E_x) d\mu = \int_0^1 \mu(E_y) d\nu = 1.$$

Donde $0 = 1$, um absurdo. Logo E não é mensurável. Portanto obtemos um conjunto E t.q. cada seção é mensurável, mas ele mesmo não o é!

Note que o exemplo acima é extremamente dependente do conjunto não-enumerável, bem-ordenado T , t.q. cada elemento tem no máximo enumeráveis antecessores [65]. Bom, por um lado tal resultado é esperado, pois respeita o “princípio de Isnard” segundo o qual apenas conjuntos bem patológicos não são mensuráveis. Imagine (se é que isso é possível) o quanto estranho não é o conjunto E definido no exemplo acima! Podemos citar também uma construção, devida a Sierpinski, parecida com a anterior [66]. Contudo, por outro lado, provamos que a conjectura é muito forte e é, em geral, falsa. Portanto a mensurabilidade de E_ϕ não é em geral garantida! Esse fato poderia

por todo o trabalho a perder, pois poderia ser inclusive que o nosso conjunto de estados que são catalisáveis não fosse mensurável, nem mesmo a Lebesgue. Mas aqui invocamos novamente o “princípio de Isnard” para salvar nossa vida: O conjunto E_ϕ é dado de maneira construtiva, com relações de pertinência e fórmulas/expressões, portanto o mesmo deve ser mensurável! Seria no mínimo estranho que um conjunto definido por várias desigualdades não fosse Lebesgue mensurável, e é esse aspecto que vamos explorar:

Proposição C.3. *O conjunto E_ϕ é mensurável a Lebesgue.*

Demonstração. Para fixar as idéias, e sem perda de generalidade, suponha que $\lambda_\phi \in \mathbb{V}^k$, $\lambda_i = (\alpha_1, \dots, \alpha_m) \in \mathbb{V}^m$, $\lambda_f = (\beta_1, \dots, \beta_m) \in \mathbb{V}^m$. Logo $E_\phi = \{(\lambda_i, \lambda_f) \in \mathbb{V}^m \times \mathbb{V}^m; \lambda_i \not\prec \lambda_f, \text{ e } \lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi\}$.

Defina $M = \{(\lambda_i, \lambda_f) \in \mathbb{V}^m \times \mathbb{V}^m; \lambda_i \not\prec \lambda_f\}$ e $M_\phi = \{(\lambda_i, \lambda_f) \in \mathbb{V}^m \times \mathbb{V}^m; \lambda_i \otimes \lambda_\phi \prec \lambda_f \otimes \lambda_\phi\}$, logo $E_\phi = M \cap M_\phi$. Como a interseção de conjuntos mensuráveis é um conjunto mensurável, então basta mostrar que M, M_ϕ são mensuráveis. Vamos mostrar apenas que M é mensurável, e um raciocínio completamente análogo garante que M_ϕ é mensurável.¹

Defina $M_1 = \{(\lambda_i, \lambda_f) \in \mathbb{V}^m \times \mathbb{V}^m; \alpha_1 > \beta_1\}$, $M_2 = \{(\lambda_i, \lambda_f) \in \mathbb{V}^m \times \mathbb{V}^m; \alpha_1 \leq \beta_1, \alpha_1 + \alpha_2 > \beta_1 + \beta_2\}, \dots, M_{m-1} = \{(\lambda_i, \lambda_f) \in \mathbb{V}^m \times \mathbb{V}^m; \alpha_1 \leq \beta_1, \alpha_1 + \alpha_2 \leq \beta_1 + \beta_2, \dots, \sum_{i=1}^{m-2} (\alpha_i - \beta_i) \leq 0, \sum_{i=1}^{m-1} (\alpha_i - \beta_i) > 0\}$. Logo $M = \bigcup_{i \in I_{m-1}} M_i$. Afirmamos que M_i é mensurável qualquer que seja $i \in I_{m-1}$, portanto M é mensurável.

Defina $f : \mathbb{V}^m \times \mathbb{V}^m \rightarrow \mathbb{R}^m$ dada por $f(\alpha, \beta) = (\alpha_1 - \beta_1, \alpha_1 - \beta_1 + \alpha_2 - \beta_2, \dots, \sum_{i=1}^{m-1} (\alpha_i - \beta_i), 0)$. Como as componentes de f são combinações lineares das variáveis, então f é contínua.

Seja $i \in I_{m-1}$ arbitrário. Então $(\lambda_i, \lambda_f) \in M_i$ implica que $\alpha_1 \leq \beta_1, \dots, \alpha_1 + \dots + \alpha_{i-1} \leq \beta_1 + \dots + \beta_{i-1}$, e $\alpha_1 + \dots + \alpha_i > \beta_1 + \dots + \beta_i$. Logo $(\lambda_i, \lambda_f) \in M_i \iff \sum_{j=1}^t (\alpha_j - \beta_j) \leq 0, \forall t \in \{1, 2, 3, \dots, i-1\}$, e $\sum_{j=1}^i (\alpha_j - \beta_j) > 0 \iff (\lambda_i, \lambda_f) \in f^{-1}([-1, 0] \times [-1, 0] \times \dots \times (0, 1] \times [-1, 1] \times [-1, 1] \times \dots \times \{0\})$. Como $[-1, 0] \times [-1, 0] \times \dots \times (0, 1] \times [-1, 1] \times [-1, 1] \times \dots \times \{0\}$ é um retângulo em \mathbb{R}^m tem-se que M_i é mensurável. \square

A proposição acima mostra que enquanto nos concentramos na medida de Lebesgue, o conjunto E_ϕ é mensurável, independente de ϕ , inclusive também independente da dimensão do catalisador. Como já foi discutido na

¹Na verdade esta demonstração foi obtida por Raphael Drumond e o autor.

seção 3.6.2, vamos olhar, num primeiro momento, apenas para a medida de Lebesgue, portanto estando dentro das hipóteses, garantimos que nosso E_ϕ é “sempre” mensurável! Dessa maneira, podemos dizer que a partícula **Se**, que originou a discussão, pode ser desprezada.

Aqui nesse texto o que queríamos, e conseguimos num caso bem adaptado, era que nosso conjunto de interesse fosse mensurável. Mas essa não é a primeira vez que uma discussão desse tipo é feita em Mecânica Quântica, em [67], I. Pitowski propõe um modelo determinístico para o spin, usando para tal a não-mensurabilidade de certas funções (e para esse último o Axioma da Escolha e a Hipótese do contínuo²). Não deixa de ser surpreendente como tópicos sutis de teoria de conjuntos possam aparecer “naturalmente” dentro de outras áreas do conhecimento.

²Como já era de se esperar, pelo “Princípio de Isnard”.

Referências Bibliográficas

- [1] H. Goldstein, C. Poole e J. Saiko. **Classical Mechanics**. E.U.A.: Addison-Wesley, 2000;
- [2] J. J. Sakurai. **Modern Quantum Mechanics**. E.U.A.: Addison-Wesley Publishing Company, 1994;
- [3] G. H. Hardy, J. E. Littlewood e G. Pólya. Some simple inequalities satisfied by convex functions. **Messenger Math**, v. 58, 145-152, 1929;
- [4] Marshall. A. W. e Olkin. I. **Inequalities: Theory of Majorization and its Applications**. Inglaterra: Academic Press, 1979;
- [5] R. Rado. An Inequality. **J. London. Math. Soc**, v. 27, 1-6, 1953;
- [6] T. W. Hungerford. **Algebra**. E.U.A.: Springer-Verlag, 2003;
- [7] B. C. Arnold. Majorization and the Lorenz Order: A Brief Introduction. **Springer-Verlag Lecture Notes in Statistics**, vol. 43, 1987;
- [8] R. Bathia. **Positive Definite Matrices**. E.U.A.: Princeton University Press, 2007;
- [9] S. L. Woronowicz. Positive maps on low dimensional matrix algebras. **Reports Math. Phys.**, v. 10, 166-183, 1976;
- [10] E. Stormer. Positive linear maps of operator algebras. **Acta Math.**, v, 110, 233-278, 1963)
- [11] M. Choi. Some assorted inequalities for positive linear maps on C^* -algebras. **J. Operator Theory**, v. 4, 271-285, 1980;
- [12] R. P. Feynman. **The Feynman Lectures On Physics**. Vol. 3. E.U.A.: Addison Wesley Longman, 1970;

- [13] L. E. Ballentine. **Quantum Mechanics a Modern Development**. Singapura: World Scientific Publishing Company, 2000;
- [14] A. Messiah. **Quantum Mechanics: Two Volumes Bound as One**. E.U.A.: Dover Publications, 1999;
- [15] S. Gasiorowicz. **Quantum Physics**. E.U.A.: John Wiley and Sons, 2003;
- [16] M. O. Terra Cunha. **Noções de Informação Quântica**. Brasil: IMPA, 2006;
- [17] T. C. Cohen, et. al., **Quantum Mechanics**. vol. 1. E.U.A.: Wiley and Sons, 1977;
- [18] A. Peres. **Quantum Theory: Concepts and Methods**. E.U.A.: Kluwer Academic Publishers, 2002;
- [19] J. Watrous. **Theory of Quantum Information: Lecture notes from Fall 2008**, Institute for Quantum Computing, University of Waterloo, Waterloo, Canada, 2008;
- [20] D. C. Santos. **Em busca de um entendimento completo acerca do Emarranhamento**. 2006. Dissertação (Mestrado em Física, Física Geral) - Universidade Federal de Minas Gerais, Belo Horizonte, 2006;
- [21] F. Reif. **Fundamentals of Statistical and Thermal Physics**. Japão: Mc.Grow-Hill, 1965;
- [22] M. A. Nielsen. I. L. Chuang. **Quantum Information and Quantum Computation**. E.U.A.: Cambridge University Press, 2000;
- [23] A. Bárbara, A. T. Baraviera e M. O. Terra Cunha, **Mecânica Quântica para Matemáticos em Formação**. 28^o Colóquio Brasileiro de Matemática. Brasil: IMPA, 2011;
- [24] K. Kraus. States, Effects, and Operations, **Fundamental Notions of Quantum Theory: Lectures in Mathematical Physics at the University of Texas at Austin**. Alemanha: Springer-Verlag, 1983;
- [25] A. Cabello. **Pruebas algebraicas de imposibilidad de variables ocultas en mecánica cuántica**: Memoria que presenta para optar al grado de Doctor en Ciencias Físicas. Tese (Doutorado em Física, Física Geral) - Facultad de Ciencias Físicas, Univesidad Complutense de Madri, Madri, 1996;

- [26] S. Abramsky e A. Brandenburger. The Sheaf-Theoretic Structure Of Non-Locality and Contextuality, arxiv:1102.0264 (2011);
- [27] M. A. Santos e M. T. Quintino. **Desigualdades de Bell**: Uma introdução à não-localidade quântica. (Brasil, 2011)
- [28] U. Fano. Description of States in Quantum Mechanics by Density Matrix and Operator Techniques. **Rev. Mod. Phys.**, vol. 29, n. 1, 74-93, 1957;
- [29] A. Papoulis. Bayes' Theorem in Statistics and Bayes' Theorem in Statistics (Reexamined). **Probability, Random Variables, and Stochastic Processes**, 2nd ed. New York: McGraw-Hill, pp. 38-39, 78-81, and 112-114, 1984);
- [30] M. Horodecki, P. Horodecki, R. Horodecki. Separability of mixed states: necessary and sufficient conditions. **Phys. Lett. A**, v. 223,1-8, 1996;
- [31] A. Peres. Separability Criterion for Density Matrices. **Phys. Rev. Lett.**, v. 77, 1413-1415, 1996;
- [32] M. Nielsen, J. Kempe. Separable states are more disordered globally than locally. arXiv: quant-ph/0011117. Disponível em <http://arxiv.org/abs/quant-ph/0011117>;
- [33] B. M. Terhal. Bell inequalities and The Separability Criterion. arXiv: quant-ph/9911057. Disponível em <http://arxiv.org/abs/quant-ph/9911057>;
- [34] H. P. Bueno. **Álgebra Linear**: Um segundo curso. Coleção Textos Universitários. Brasil: SBM, 2006;
- [35] C. H. Bennett, H. J. Bernstein, S. Popescu, e B. Schumacher, Concentrating partial entanglement by local operations. **Phys. Rev. A**, v. 53, 2046-2052, 1996;
- [36] C. H. Bennett et al. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. **Physical Review Letters**, v. 76, 722-725, 1996;
- [37] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, e W. K. Wootters. Mixed-state entanglement and quantum error correction. **Phys. Rev. A**, v. 54, 3824-3851, 1996;

- [38] M. A. Nielsen. Conditions for a Class of Entangled Transformations. **Phys. Rev. Lett.**, v. 83, 436-439, 1999;
- [39] D. Jonathan e M. B. Plenio. Entanglement-assisted local manipulation of pure quantum states. arXiv: quant-ph/9905071, **Phys. Rev. Lett.** 83, 3566, (1999);
- [40] M.B. Plenio e V. Vedral. Contemp. Teleportation, entanglement and thermodynamics in the quantum world. **Cont. Phys.** v. 39, 431-446, 1998;
- [41] M. A. Nielsen. An introduction to majorization and its applications to quantum mechanics. Lecture Notes, Department of Physics, University of Queensland (Australia,2002);
- [42] E. Joos. Continuous Measurement: Watchdog effect versus golden rule. **Phys. Rev. D.** v. 29, 1626–1633, 1984;
- [43] S. Haroche, et. al. Quantum jumps of light recording the birth and death of a photon in a cavity. arXiv:quant-ph/0612031. Disponível em <http://arxiv.org/abs/quant-ph/0612031>;
- [44] S. Haroche, M. Brune e J. M. Raimond. Colloquium: Manipulating quantum entanglement with atoms and photons in a cavity. **Rev. Mod. Physics**, v. 73, 565-582, 2011;
- [45] E. L. Lima. **Curso de Análise**. Vol. 1. Brasil: IMPA, 2008;
- [46] R. G. Bartle. **The Elements of Real Analysis**. E.U.A.: John Wiley and Sons, 1964;
- [47] X. Sun, R. Duan, M. Ying. The Existence of Quantum Entanglement Catalysts. **IEEE Transaction on Information Theory**, v. 51, n. 1, 75-80, 2005;
- [48] S. Daftuar e M. Klimesh. A mathematical structure of entanglement catalysis. **Phys. Rev. A**, 64, 042314 (2001);
- [49] P. Anspach. Two qubit catalysis in a four-state pure bipartite system. arXiv: quant-ph/0102067. Disponível em <http://arxiv.org/abs/quant-ph/0102067>;

- [50] K. Życzkowski e H. J. Sommers. Induced measures in the space of mixed states. arXiv: quant-ph/0012101. Disponível em <http://arxiv.org/abs/quant-ph/0012101>;
- [51] K. Życzkowski e H. J. Sommers. Bures volume of the set of mixed quantum states. **J. Phys. A: Math. Gen.**, v.36,10083-10100, 2006);
- [52] I. Bengtsson e K. Życzkowski. **Geometry of Quantum States: An Introduction to Quantum Entanglement**. E.U.A.: Cambridge University Press, 2006;
- [53] K. Życzkowski, P. Horodecki, A. Sapper e M. Lewenstein. On volume of the set of mixed quantum states. arXiv: quant-ph/9804024. Disponível em <http://arxiv.org/abs/quant-ph/9804024>;
- [54] K. Życzkowski. Volume of the set of mixed entangled states II. arXiv: quant-ph/9902050 (1999). Disponível em <http://arxiv.org/abs/quant-ph/9902050>;
- [55] D. Ye. On the Bures Volume of Separable Quantum States. arXiv: quant-ph/0902.1505. Disponível em <http://arxiv.org/abs/quant-ph/0902.2505>;
- [56] C. Isnard. **Introdução à medida e integração**. Brasil: IMPA, 2007;
- [57] R. G. Bartle. **The elements of Integration**. E.U.A.: John Wiley and Sons, 1966;
- [58] A. A. Castro Júnior. **Curso de Teoria da Medida**. Projeto Euclides. Brasil: IMPA, 2008;
- [59] P. R. Halmos. **Measure Theory**. E.U.A.: Springer-Verlag New York Inc., 1974;
- [60] Y. Feng, R. Duan, e M. Ying. Catalyst-Assisted Probabilistic Entanglement Transformation. **IEEE TRANSACTIONS ON INFORMATION THEORY**, v. 51, n. 3, 1090-1101, 2005;
- [61] Y. Feng, R. Duan, e M. Ying. When catalysis is Useful for probabilistic entanglement transformation. arXiv: quant-ph/0403170. Disponível em <http://arxiv.org/abs/quant-ph/0403170>;

- [62] M. Raginsky. Radon-Nikodym Derivatives of Quantum Operations. arXiv: math-ph/ 0303056. Disponível em <http://arxiv.org/abs/math-ph/0303056>;
- [63] J. Eisert e M. Wilkens. Catalysis of entanglement manipulation for mixed states. arXiv: quant-ph/ 9912080. Disponível em <http://arxiv.org/abs/quant-ph/9912080>;
- [64] B. Terhal e P. Horodecki. A Schmidt number for density Matrices. arXiv: quant-ph/9911117. Disponível em <http://arxiv.org/abs/quant-ph/9911117>;
- [65] P. J. Cohen. Set Theory and the Continuum Hypothesis. W. A. Benjamin (New York, 1966);
- [66] W. Sierpinski. Sur un problème concernant les ensembles mesurables superficiellement. **Found. Math**, v.1 , 112-115, 1920;
- [67] I. Pitowski. Deterministic model of spin and statistic. **Phys. Rev. D**, v. 27, 2316–2326, 1982;
- [68] C. A. Duarte. **Emaranhamento**: Uma Introdução. 2010. Monografia (Curso de Física, Física Geral) - Universidade Federal de Juiz de Fora, Juiz de Fora, 2010.