UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

EMARANHADORES, ESTADOS QUÂNTICOS E UMA CONTRIBUIÇÃO À CONJECTURA DE LEHMER

TESE DE DOUTORADO

HEVANS VINICIUS PEREIRA

Porto Alegre, dezembro de 2018

Hevans Vinicius Pereira

EMARANHADORES, ESTADOS QUÂNTICOS E UMA CONTRIBUIÇÃO À CONJECTURA DE LEHMER

Tese apresentada ao Programa de Pós Graduação em Matemática da Universidade Federal do Rio Grande do Sul como requisito parcial para obtenção do título de Doutor em Matemática.

Orientador: Prof. Dr. Alexandre Tavares Baraviera.

Porto Alegre, dezembro de 2018

Tese submetida por Hevans Vinicius Pereira[1] como requisito parcial para a obtenção do grau de Doutor em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Banca Examinadora

Dr. Eduardo Brietzke (IME-UFRGS)

Dra. Marília Luiza Matte (CMPA)

Dr. Leonardo Guidi (IME-UFRGS)

Dra. Sandra Prado (IF-UFRGS)

Dr. Alexandre Tavares Baraviera (orientador, IME-UFRGS)

[1] Bolsista da Conselho Nacional de Desenvolvimento Cientifíco e Tecnológico (CNPq).

Dedicatória

Dedico este trabalho para os meus pais e para minha esposa, por sempre me apoiarem.

Agradecimentos

Gostaria de agradecer ao Professor Doutor Alexandre Tavares Baraviera por ter me recebido muito bem e por ter aceito me orientar nesses temas e principalmente por ser sempre muito paciente.

Também gostaria de agradecer aos professores da UFRGS que sempre me trataram muito bem e contribuíram muito para a minha formação e à CAPES e ao CNPq pois sem o apoio destas instituições de fomento este trabalho e toda minha jornada pós graduação não teria sido possível.

Resumo

Este trabalho apresenta alguns problemas matemáticos ligados à Mecânica Quântica e à Teoria de Números; mais precisamente, este trabalho apresenta três problemas: dois deles no contexto da Mecânica Quântica e o terceiro no âmbito da Teoria de Números.

O primeiro problema, dentro do contexto da Mecânica Quântica, trata de determinar a geometria dos estados da esfera de Bloch que representem estados fisicamente realizáveis. Tal geometria herda uma simetria que é preservada por transformações isoespectrais que compõem um grupo abeliano; nesse sentido, obtivemos os mesmos resultados de Mendas, em [14], e Kimura, em [10] e [11], mas por um método diferente. Em [10] e [11] o problema é abordado inteiramente em coordenadas esféricas, o que conduz a uma formulação ligeiramente diferente na obtenção dos autolavores do operador densidade. Em [14], a mesma ideia de [10] e [11] é abordada mas em dimensão $d = 4$. Em ambas as referências o ponto principal foi tomar interseção da esfera de Bloch com hiperplanos especiais do espaço, isso permitiu aos autores utilizar métodos computacionais e ilustrar regiões de interesse na tentativa de compreender melhor a geometria do problema.

Já o segundo problema trata de descobrir propriedades de sistemas dinâmicos quânticos, como convergência e velocidade de convergência de produto de matrizes unitárias sorteadas aleatoriamente para emaranhadores universais. Conseguimos um resultado interessante que garante a convergência com velocidade exponencial, mesmo sob condições relativamente gerais. Tal resultado é importante devido ao interesse da comunidade acadêmica em entender melhor emaranhadores universais e usá-los em aplicações da computação quântica. Mais especificamente, nosso resultado garante que dado um número finito de elementos $u_1, \ldots, u_n \in U(n)$ escolhidos ao acaso, então o produto de elementos aleatoriamente sorteados na vizinhança dos elementos $u_1, \ldots, u_n$ converge fraco-estrela para um emaranhador universal na medida de Haar em $U(n)$. Tal resultado pode auxiliar no entendimento de propriedades de emaranhadores universais e em aplicações da computação quântica, tópicos que vêm sendo bastante estudados pela comunidade acadêmica.

Finalmente, o terceiro problema, pertencente à área de Teoria de Números. É

uma conjectura que encontra-se sem solução desde 1932, quando foi formulada por Derrick Henry Lehmer. Uma nova abordagem na tentativa de resolver este problema é apresentada.

Palavras-chave: Emaranhadores Universais; Grupo Unitário; Esfera de Bloch; Geometria de estados quânticos; Conjectura de Lehmer.

Abstract

This thesis presents some mathematical problems related to Quantum Mechanics and Number Theory; more precisely, this thesis presents three problems not correlated to each other, two of them on the field of Quantum Mechanics, and one on the field of Number Theory.

The first problem deals with geometric aspects of the Bloch Sphere that represent physically achievable states. Such geometry inherits a symmetry that is preserved by isospectral transformations that compose an abelian group.

The second deals with aspects of quantum dynamical systems, such as convergence and speed of convergence, which try to approximate universal entanglers through successive applications of unitary operators, randomly chosen. We have achieved an interesting result that guarantees convergence with exponential speed even under relatively general conditions, which is important because of the interest of the academic community to better understand universal entanglers and use them in applications of quantum computation.

The third problem belongs to the field of Number Theory and deals with a conjecture that has been unsolved since 1932, when it was formulated by Derrick Henry Lehmer. A new approach in trying to solve this problem is presented.

Keywords: Universal Entanglers; Unitary Group; Bloch's Sphere; Geometry of quantum states; Lehmer Conjecture.

Sumário

Introdução

Os estudos e soluções apresentados ao longo deste texto foram inspirados em Feng, MingXing, XiuBo, YiXian e XiaoJun ([8]), Kimura ([10] e [11]) e Lehmer ([12]), entre outros. Em [8] encontra-se o seguinte resultado: Para um espaço de Hilbert $\mathcal{H}$ de dimensão maior que 10 a probabilidade de se sortear um operador unitário agindo em $\mathcal{H}$ e este ser um emaranhador universal (operador unitário que pode emaranhar todo estado produto) é alta. Tal resultado é interessante pois, apesar de serem a quase totalidade, não se conhece nenhum exemplo de emaranhador universal. Em [10] pode-se encontrar um estudo interessante sobre a geometria de estados da esfera de Bloch em dimensão 8. Embora uma grande quantidade de técnicas tenham sido empregadas ainda não há uma descrição simples e completa deste objeto. Já em [12], publicado em 1932, encontra-se a Conjectura de Lehmer, uma conjectura sobre teoria de números, mais especificamente, sobre a função *totient* de Euler. Ainda que distintos, apresentando características e técnicas variadas, esses problemas inspiraram esta investigação.

Neste trabalho estudam-se aspectos matemáticos da Teoria Quântica ligados à dinâmica de emaranhamento no contexto dos emaranhadores universais e aspectos geométricos associados à estados quânticos via Teoria de Grupos. Num terceiro momento, faz-se uma contribuição ao problema conhecido como Conjectura de Lehmer: a conjectura estabelece que a função de Euler $\varphi(n)$ divide $n-1$ apenas quando n for um número primo. Nos parágrafos que seguem, encontra-se, um roteiro de leitura do trabalho.

O capítulo 1 apresenta uma maneira alternativa à encontrada na literatura, especialmente em [10], [11] e [14], para o problema de se estudar e determinar os aspectos geométricos de estados quânticos da Esfera de Bloch que correspondem realmente a estados físicos, em dimensão 8. Tal problema só foi resolvido em dimensão real igual a 4, isto é, para o caso da Esfera de Bloch do espaço $\mathbb{C}^2$ que é o modelo natural usado para se representar geometricamente com um único qubit.

Sabe-se que para $\mathbb{C}^2$ todo ponto da Esfera de Bloch corresponde a uma matriz densidade e portanto representa um estado físico. Mas, para dimensões maiores, não há uma correspondência biúnivoca entre pontos da Esfera de Bloch e matrizes

densidade, ou seja, em última análise não existe uma bijeção entre os pontos da esfera e estados físicos.

Surge, naturalmente, então a seguinte questão: Qual é a geometria, dentro da Esfera de Bloch, que corresponde aos estados físicos? Esta questão mostra-se muito difícil mesmo no caso mais simples, da Esfera de Bloch do Espaço $\mathbb{C}^3$, caso abordado neste capítulo.

Já o capítulo 2 apresenta os conceitos e definições relacionados aos Emaranhadores Universais, bem como o principal problema do capítulo, que é o de estudar a convergência e a velocidade de emaranhamento de estados sujeitos à aplicações sucessivas de operadores unitários escolhidos ao acaso. O trabalho [8] garante que para espaços de Hilbert bipartidos do tipo $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, com $\dim \mathcal{H}$ suficientemente grande, quase todo operador unitário agindo em $\mathcal{H}$ é um emaranhador universal, isto é, o conjunto **UE** (dos emaranhadores universais) tem medida de Haar $\mu(\mathbf{UE})$ quase 1 e aumenta conforme a dimensão de $\mathcal{H}$ aumenta. Todavia, surpreendentemente, nenhum exemplo de emaranhador universal é conhecido.

Emaranhamento é um fenômeno de grande importância na mecânica quântica, neste contexto é importante saber como emaranhar estados e conhecer operadores que conseguem emaranhar todo estado produto, operadores estes que são chamados de emaranhadores universais. Devido à importância descrita os autores de [8] obtiveram um resultado interessante do ponto de vista físico e matemático. Abordaremos o problema com o objetivo de investigar mais a questão e obter maior entendimento da parte matemática do problema, isto é, queremos estudar e entender algumas propriedades de certos operadores que possuem interesse físico.

Portanto, inspirados pelo exposto em [8] e em textos sobre sistemas dinâmicos, como [20], e sobre sistemas dinâmicos quânticos, como [18], tentamos uma nova abordagem para se aproximar de emaranhadores universais via sistemas dinâmicos quânticos.

Considerando-se que, ao atuar com um operador unitário em um qubit, estamos representando teoricamente uma operação física, e que esta possui um erro inerentemente associado, adotamos um ponto de vista prático ao considerar que não se executa efetivamente um dado operador unitário escolhido a priori, mas sim um operador que está na vizinhança deste.

Ainda, sobre o processo descrito, adotamos um ponto de vista dinâmico ao considerar que a dinâmica é dada por meio de aplicações sucessivas de operadores unitários escolhidos aleatoriamente em vizinhanças conforme descritas no parágrafo anterior. Mais precisamente, conseguimos provar o seguinte resultado:

Teorema 2.4.1: Considere um número finito de elementos $u_1, \ldots, u_n \in U(n)$ escolhidos aleatoriamente. Então o produto de elementos aleatoriamente escolhidos

na vizinhança de elementos $u_1, \ldots, u_n$ converge fraco-estrela para um elemento em **UE** na medida de Haar em $U(n)$.

Essencialmente, este teorema garante que, compondo-se operadores unitários escolhidos aleatoriamente, obtém-se com certeza a convergência do referido produto para o conjunto dos emaranhadores universais, no sentido fraco-estrela, e esta convergência se dá com uma velocidade exponencial que depende da dimensão do espaço $\mathcal{H}$ e da quantidade de operadores unitários escolhidos para se compor a dinâmica.

O capítulo 3 apresenta a Conjectura de Lehmer, também conhecida como Problema *Totient* de Lehmer. O problema foi proposto em 1932 por Derrick Henry Lehmer e consiste em saber se existe algum número não primo n tal que a função *totient* de Euler, aplicada em n, divide $n-1$, isto é, se $\varphi(n)$ divide $n-1$. Este problema foi abordado nas últimas décadas, principalmente na década de 80 por Cohen em [5]. Mais recentemente avanços parciais tem sido obtido com o auxílio de computadores.

Capítulo 1

Geometria de Estados Quânticos

O presente capítulo tem o objetivo de apresentar uma maneira alternativa à encontrada por Kimura, em [10] e [11], para se estudar a geometria dos estados quânticos associados a estados físicos representados por operadores densidade na Esfera de Bloch de dimensão 8. Nas referências citadas, Kimura partiu inicialmente para uma formulação do problema em coordenadas esféricas. Isto o levou a obter um tratamento diferente na obtenção dos autovalores e consequentemente nas simestrias do problema. Kimura não utilizou a abordagem via grupos e tentou compreender diretamente toda a geometria dos estados físicos dentro da esfera de Bloch. Nossa abordagem é diferente: construímos todo o grupo de simetrias que atua sobre a esfera de Bloch e, consequentemente, sobre os estados físicos; depois, tentamos compreender apenas a geometria de dois ortantes, região do espaço menor do que toda a esfera de Bloch, a fim de simplificar a determinação da geometria, que é a parte mais difícil de abordar. No entanto, mesmo para um ortante a obtenção precisa da geometria mostra-se um problema difícil de ser determinado.

Trataremos apenas de casos de dimensão finita e neste contexto os operadores podem ser pensados como as matrizes que os representam.

1.1 Esfera de Bloch e Operadores Densidade

Normalmente a mecânica quântica é desenvolvida sobre o conceito de vetor de estado, mas é possível fazer o desenvolvimento da mecânica quântica em termos de operadores densidade. Cada uma das abordagens têm vantagens e desvantagens, mas não vamos discutir tais pontos neste trabalho, vamos focar apenas nos resultados que precisamos para o desenvolvimento das seções posteriores. O leitor interessados nestes desenvolvimentos pode consultar [18].

Definição 1.1.1. *Um espaço de estados é um espaço vetorial complexo com pro-*

duto interno. Como estaremos sempre em dimensão finita podemos considerar, sem perda de generalidade, que nossos espaços serão sempre $\mathbb{C}^d$ *em que* d *é a dimensão do espaço, e o produto interno é o usual.*

Como exemplo de espaço de estados e de vetor de estado, podemos considerar um qubit, como definido a seguir.

Definição 1.1.2. *Um qubit é um vetor unitário no espaço vetorial* $\mathbb{C}^2$*. Mais formalmente, seja* $|0\rangle = (1,0)$ *e* $|1\rangle = (0,1)$ *base do espaço vetorial* $\mathbb{C}^2$*, um qubit é um vetor da forma* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$*, com* $\alpha, \beta \in \mathbb{C}$ *e* $|\alpha|^2 + |\beta|^2 = 1$*.*

Se um sistema quântico pode estar em um estado $|\psi_i\rangle \in \mathbb{C}^d$ com probabilidade p_i, chamamos $\{p_i, |\psi_i\rangle\}$ de um *ensemble de estados puros*.

O operador densidade (ou matriz densidade) para este sistema é definido por $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

Note que, da maneira como foi definido o operador densidade, tem-se que $\rho = \rho^*$, em que $*$ denota a operação de tomar a transposta conjugada da matriz ρ, de ordem $d \times d$, que representa o operador ρ. Os operadores que satisfazem a propriedade $\rho = \rho^*$ são chamados autoadjuntos ou hermitianos.

É possível caracterizar um operador densidade através de um operador hermitiano que satisfaz duas propriedades especiais, conforme teorema 1.1.1 a seguir.

Teorema 1.1.1. *Um operador hermitiano* ρ *é um operador densidade associado a um ensemble* $\{p_i, |\psi_i\rangle\}$ *se, e somente se, satisfaz:*

(1) $\mathrm{Tr}(\rho) = 1$*;*

(2) ρ *é operador positivo.*

Demonstração. ($\Rightarrow$) Suponha que $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ é um operador densidade, então $\mathrm{Tr}(\rho) = \sum_i p_i \,\mathrm{Tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1$. E, suponha que $|\phi\rangle$ é um vetor arbitrário no espaço de estados, então $\langle\phi|\rho|\phi\rangle = \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle = \sum_i p_i |\langle\phi|\psi_i\rangle|^2 \geq 0$.

($\Leftarrow$) Suponha que ρ é um operador hermitiano positivo qualquer satisfazendo $\mathrm{Tr}(\rho) = 1$. Como ρ é positivo admite decomposição espectral $\rho = \sum_j \lambda_j |j\rangle\langle j|$, em que os vetores $|j\rangle$ são ortogonais e λ_j os autovalores reais não negativos de ρ. De $\sum_i \lambda_j = 1$ conclui-se que um sistema no estado $|j\rangle$ com probabilidade λ_j vai ter operador densidade ρ. Isto é, o ensemble $\{\lambda_j, |j\rangle\}$ é um ensemble de estados que dá origem ao operador densidade ρ. □

No teorema 1.1.1 usamos o conceito de operado positivo que encontra-se definido na definição 1.1.3 a seguir.

Definição 1.1.3. *[Operador Positivo] Um operador T é positivo se para todo $|\psi\rangle \in \mathbb{C}^d$ ocorrer $\langle\psi|T|\psi\rangle \geq 0$.*

Sempre que quisermos considerar um sistema quântico com d níveis, conhecido como qudit (um análogo d dimensional do qubit) devemos escolher como espaço vetorial o espaço vetorial complexo que tenha dimensão d, isto é, $\mathbb{C}^d$.

Neste contexto, sempre que escolhermos um operador densidade, estaremos lidando com uma matriz quadrada de ordem $d \times d$. Os operadores densidade por se tratarem de matrizes podem ser expressos em termos de uma base de matrizes especiais, conhecidas como matrizes de Gell-Mann, que no caso de qubits é conhecida mais comumente como base das matrizes de Pauli. Para mais informações sobre matrizes de Gell-Mann, consultar [2].

Vejamos como obter uma base para os operadores densidade.

Como mencionado para o caso mais simples (qubit) temos que o espaço de estados de interesse é $\mathbb{C}^2$ e o operador densidade ρ_2 está definido e age neste espaço, isto é, $\rho_2 : \mathbb{C}^2 \to \mathbb{C}^2$, portanto ρ pode ser representado por uma matriz de ordem 2×2.

As matrizes de Pauli são definidas como

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

Neste caso, qualquer matriz densidade ρ_2 pode ser escrita como $\rho_2 = \frac{1}{2}(Id + \overrightarrow{r} \cdot \overrightarrow{\sigma})$, em que $\overrightarrow{r} = (x_1, x_2, x_3) \in \mathbb{R}^3$ e $\overrightarrow{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$, isto é,

$$\rho_2 = \frac{1}{2}\begin{pmatrix} 1 + x_3 & x_1 - ix_2 \\ x_1 + ix_2 & 1 - x_3 \end{pmatrix}$$

Segue do teorema 1.1.1 que $\det(\rho) \geq 0$, que é equivalente a $x_1^2 + x_2^2 + x_3^2 \leq 1$ portanto podemos fazer uma identificação entre os pontos da bola unitária de $\mathbb{R}^3$, centrada na origem, e os operadores densidade que representam qubits. Tal bola é chamada bola ou esfera de Bloch.

Tal representação é muito simples e útil pois nos permite pensar em operadores densidade (de qubit) como pontos ou vetores de $\mathbb{R}^3$.

Em dimensões maiores também é possível expressar os operadores densidade como pontos (ou vetores) dentro da bola unitária de dimensão $d^2 - 1$, mas o fato curioso é que apenas no caso de qubits cada estado da Esfera de Bloch corresponde a um estado físico [2]. Para dimensões maiores, nem todo ponto da esfera

de Bloch corresponde a um estado físico e determinar qual é a geometria dos vetores que representam estados físicos é tema complexo e de intensa pesquisa. As próximas seções tentam uma abordagem alternativa ao que se encontra na literatura a fim de tentar elucidar este problema.

Em geral, as matrizes de Gell-Mann de ordem $d \times d$ podem ser definidas como um conjunto de $d^2 - 1$ matrizes $\{A_i\}$ que possuem traço nulo e são ortogonais, isto é, $\mathrm{Tr}(A_i) = 0$ e $\mathrm{Tr}(A_i^* A_j) = c\delta_{ij}$, em que $\delta_{ij} = 1$ se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$ e $c \in \mathbb{R}$.

Essas d^2-1 matrizes juntamente com a matriz identidade formam uma base para os operadores densidade de ordem $d \times d$ e, neste contexto, um operador densidade pertencente à esfera de Bloch pode ser escrito como $\rho = \frac{1}{d}(Id + \vec{r} \cdot \vec{\Gamma})$, em que $\vec{r} \cdot \vec{\Gamma}$ é uma combinação linear de todas as matrizes A_i, $\vec{r} \in \mathbb{R}^{d^2-1}$ e $r_i = \mathrm{Tr}(\rho \Gamma_i)$.

É conhecido da literatura que as matrizes de Gell-Mann são definidas como três tipos de matrizes:

$i)$ $\frac{d(d-1)}{2}$ matrizes simétricas dadas por $\Lambda_s^{jk} = |j\rangle\langle k| + |k\rangle\langle j|$, com $1 \leq j < k \leq d$;

$ii)$ $\frac{d(d-1)}{2}$ matrizes anti-simétricas dadas por $\Lambda_a^{jk} = -i\,|j\rangle\langle k| + i\,|k\rangle\langle j|$, com $1 \leq j < k \leq d$;

$iii)$ $d-1$ matrizes diagonais $\lambda^l = \sqrt{\frac{2}{l(l+1)}}\left(\sum_{j=1}^{l} |j\rangle\langle j| - l\,|l+1\rangle\langle l+1|\right)$, com $1 \leq l \leq d-1$.

1.2 Simetrias

Para se estudar a simetria dos estados quânticos da Esfera de Bloch que representam estados físicos, vamos considerar os operadores densidade associados aos estados quânticos da Esfera de Bloch e tentar determinar qual é o grupo de transformações que preserva os autovalores do operador densidade.

Ortante é a generalização de octante e, neste trabalho, corresponde a uma das 128 divisões de um sistema de coordenadas de dimensão 7 definido pelos sinais das coordenadas. Por exemplo, o primeiro ortante corresponde a todos os pontos $(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{R}^7$ tais que $x_i \geq 0$ para $1 \leq i \leq 7$.

A ideia é tentar determinar para uma dada região, o primeiro ortante, qual é a região dos estados quânticos que representam de fato estados físicos (autovalores de ρ não negativos) e tentar levar essa região para outros ortantes via simetrias por ação de grupos, isto é, tentar aplicar as transformações do grupo para “espelhar” a região encontrada no primeiro ortante para os outros ortantes.

1.2.1 Caso $d = 2$

Sabe-se de [19] (página 4) que o polinômio característico de ρ_2 é

$$p_2(t) = t^2 - t + \frac{1}{4}\left(1 - x_1^2 - x_2^2 - x_3^2\right)$$

e nota-se que trocar o sinal de x_1, x_2 e\ou x_3 não altera o polinômio.

Denote por $[x_a, x_b, x_c]$ a troca de sinal que se obtém ao trocar $\overrightarrow{r}$ por $(-x_a, -x_b, -x_c)$, ou seja, troca-se ao mesmo tempo os sinais de x_a, x_b e x_c, deixando inalterado os sinais dos outros termos, se existirem.

Com a notação acima temos 7 possíveis simetrias: $S_{1,2} = [x_1]$, $S_{2,2} = [x_2]$, $S_{3,2} = [x_3]$, $S_{4,2} = [x_1, x_2]$, $S_{5,2} = [x_1, x_3]$, $S_{6,2} = [x_2, x_3]$ e $S_{7,2} = [x_1, x_2, x_3]$.

Seja $\mathbb{S}_2 = \{\mathrm{Id}, S_{1,2}, S_{2,2}, S_{3,2}, S_{4,2}, S_{5,2}, S_{6,2}, S_{7,2}\}$ o conjunto das simetrias citadas, e considere a operação binária $\circ : \mathbb{S}_2 \times \mathbb{S}_2 \to \mathbb{S}_2$ que a cada par de elementos de $\mathbb{S}_2$ associa um elemento de $\mathbb{S}_2$, definida por $[x_i, x_j] \circ [x_k, x_j] = [x_i, x_k]$, ou seja, elementos repetidos são desprezados e os demais são concatenados.

Com a operação acima, nota-se que $(\mathbb{S}_2, \circ)$ é um grupo abeliano cuja tabela de multiplicação encontra-se a seguir.

	$S_{1,2}$	$S_{2,2}$	$S_{3,2}$	$S_{4,2}$	$S_{5,2}$	$S_{6,2}$	$S_{7,2}$
$S_{1,2}$	Id	$S_{4,2}$	$S_{5,2}$	$S_{2,2}$	$S_{3,2}$	$S_{7,2}$	$S_{6,2}$
$S_{2,2}$	$S_{4,2}$	Id	$S_{6,2}$	$S_{1,2}$	$S_{7,2}$	$S_{3,2}$	$S_{5,2}$
$S_{3,2}$	$S_{5,2}$	$S_{6,2}$	Id	$S_{7,2}$	$S_{1,2}$	$S_{2,2}$	$S_{4,2}$
$S_{4,2}$	$S_{2,2}$	$S_{1,2}$	$S_{7,2}$	Id	$S_{6,2}$	$S_{5,2}$	$S_{3,2}$
$S_{5,2}$	$S_{3,2}$	$S_{7,2}$	$S_{1,2}$	$S_{6,2}$	Id	$S_{4,2}$	$S_{2,2}$
$S_{6,2}$	$S_{7,2}$	$S_{3,2}$	$S_{2,2}$	$S_{5,2}$	$S_{4,2}$	Id	$S_{1,2}$
$S_{7,2}$	$S_{6,2}$	$S_{5,2}$	$S_{4,2}$	$S_{3,2}$	$S_{2,2}$	$S_{1,2}$	Id

Vamos tentar determinar a geometria dos estados quânticos da esfera de Bloch que correspondem a estados físicos. Primeiramente, note que para o caso em questão, a Esfera de Bloch é a bola unitária centrada na origem de $\mathbb{R}^3$, denotada por $B_1[0, 0]$, e que os planos coordenados dividem $B_1[0, 0]$ em oito regiões correspondentes aos octantes de $\mathbb{R}^3$ que, por abuso de linguagem, serão também chamadas de octantes.

Vamos observar o que ocorre com os pontos do primeiro octante, isto é, com os pontos da forma (x_1, x_2, x_3) com todas as coordenadas positivas sem nos preocuparmos em determinar quais destes pontos representam estados físicos.

Note que aplicando $S_{1,2}$ em pontos do primeiro octante, estes serão levados em pontos $(-x_1, x_2, x_3)$, simétricos de (x_1, x_2, x_3) em relação ao plano coordenado $x_1 = 0$. De maneira análoga, vemos que todos os oito octantes irão conter pontos

da órbita do primeiro octante, portanto teremos uma simetria esférica, em relação à origem da Esfera de Bloch.

Sabe-se de [2] que todos os pontos do primeiro octante correspondem a estados físicos, portanto todo ponto da esfera de Bloch corresponde a algum estado físico; e sabe-se também que, curiosamente, apenas para esta dimensão há uma correspondência biúnivoca entre pontos da esfera e estados físicos. Para dimensões maiores, existem pontos da esfera de Bloch que correspondem a operadores que possuem algum autovalor negativo e, portanto, não correspondem a matrizes densidade e sendo assim não estão associados a estados físicos.

1.2.2 Caso $d = 3$

O próximo caso a se estudar é o caso de um qutrit, por ser ligeiramente mais complexo que o caso anterior e ser o mais simples dentre os casos de dimensão maior que 2.

Para $d = 3$ as matrizes de Gell-Mann são:

$$L_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad L_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad L_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$L_4 = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad L_5 = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix} \quad L_6 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}$$

$$L_7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad L_8 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

Neste caso, qualquer matriz densidade ρ_3 pode ser escrita como $\rho_3 = \frac{1}{3}\left(Id + \sqrt{3}\overrightarrow{r} \cdot \overrightarrow{L_3}\right)$, onde $\overrightarrow{r} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) \in \mathbb{R}^8$ e $\overrightarrow{L_3} = (L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8)$, isto é,

$$\rho_3 = \frac{1}{3} \begin{pmatrix} 1 + \sqrt{3}(x_7 + \sqrt{3}x_8) & \sqrt{3}(x_1 - ix_4) & \sqrt{3}(x_2 - ix_5) \\ \sqrt{3}(x_1 + ix_4) & 1 - \sqrt{3}(x_7 - \sqrt{3}x_8) & \sqrt{3}(x_3 - x_6) \\ \sqrt{3}(x_2 + ix_5) & \sqrt{3}(x_3 + ix_6) & 1 - 2x_8 \end{pmatrix}$$

Sabemos de [19] que o polinômio característico de ρ_3 é $p_3(t) = t^3 - t^2 + \frac{1}{3}(1 - |\overrightarrow{r}|^2)t + \frac{1}{9}(1 + x_8)|\overrightarrow{r}|^2 + \frac{2}{3\sqrt{3}}(x_2x_4x_6 - x_1x_2x_3 - x_3x_4x_5 - x_1x_5x_6) + \frac{1}{3\sqrt{3}}(x_3^2 - x_2^2 + x_6^2 - x_5^2)x_7 - \frac{1}{3}(x_1^2 + x_4^2 + x_7^2)x_8 - \frac{1}{27}(1 + x_8^3)$, e nota-se que existem 7 simetrias que preservam $p_3(t)$.

Estas simetrias são: $S_{1,3} = [x_1, x_3, x_4, x_6]$, $S_{2,3} = [x_1, x_3, x_5]$, $S_{3,3} = [x_1, x_2, x_4, x_5]$,

$S_{4,3} = [x_1, x_2, x_6]$, $S_{5,3} = [x_2, x_3, x_4]$, $S_{6,3} = [x_2, x_3, x_5, x_6]$ e $S_{7,3} = [x_4, x_5, x_6]$. Novamente, percebe-se que $(\mathbb{S}_3, \circ)$ é um grupo abeliano cuja tabela de multiplicação encontra-se a seguir.

	$S_{1,3}$	$S_{2,3}$	$S_{3,3}$	$S_{4,3}$	$S_{5,3}$	$S_{6,3}$	$S_{7,3}$
$S_{1,3}$	Id	$S_{7,3}$	$S_{6,3}$	$S_{5,3}$	$S_{4,3}$	$S_{3,3}$	$S_{2,3}$
$S_{2,3}$	$S_{7,3}$	Id	$S_{5,3}$	$S_{6,3}$	$S_{3,3}$	$S_{4,3}$	$S_{1,3}$
$S_{3,3}$	$S_{6,3}$	$S_{5,3}$	Id	$S_{7,3}$	$S_{2,3}$	$S_{1,3}$	$S_{4,3}$
$S_{4,3}$	$S_{5,3}$	$S_{6,3}$	$S_{7,3}$	Id	$S_{1,3}$	$S_{2,3}$	$S_{3,3}$
$S_{5,3}$	$S_{4,3}$	$S_{3,3}$	$S_{2,3}$	$S_{1,3}$	Id	$S_{7,3}$	$S_{6,3}$
$S_{6,3}$	$S_{3,3}$	$S_{4,3}$	$S_{1,3}$	$S_{2,3}$	$S_{7,3}$	Id	$S_{5,3}$
$S_{7,3}$	$S_{2,3}$	$S_{1,3}$	$S_{4,3}$	$S_{3,3}$	$S_{6,3}$	$S_{5,3}$	Id

1.3 Transformações Isoespectrais

Os autovalores de ρ_3 são preservados por transformações isoespectrais, isto é, por trocas de sinal e\ou permutações de algumas das coordenadas de $\overrightarrow{r}$, para ver isto basta mostrar que tais trocas preservam o polinômio característico.

Considere a transformação que leva o vetor $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ no vetor $(x_1, -x_6, x_3, x_4, x_5, x_2, x_7, x_8)$, ou seja, a transformação que troca x_2 por $-x_6$ e x_6 por x_2, essa transformação vai ser denotada por $(x_2, -x_6)(x_6, x_2)$, e note que a ordem em que se escreve os parênteses não é relevante para especificar uma transformação deste tipo.

Fazendo todas as possíveis combinações, conseguimos mostrar que existem ao todo 64 transformações isoespectrais:

$I_0 = \mathrm{Id}$
$I_1 = (x_1, -x_1)(x_3, -x_3)(x_4, -x_4)(x_6, -x_6)$
$I_2 = (x_1, -x_1)(x_3, -x_3)(x_5, -x_5)$
$I_3 = (x_1, -x_1)(x_2, -x_2)(x_4, -x_4)(x_5, -x_5)$
$I_4 = (x_1, -x_1)(x_2, -x_2)(x_6, -x_6)$
$I_5 = (x_2, -x_2)(x_3, -x_3)(x_4, -x_4)$
$I_6 = (x_2, -x_2)(x_3, -x_3)(x_5, -x_5)(x_6, -x_6)$
$I_7 = (x_4, -x_4)(x_5, -x_5)(x_6, -x_6)$
$I_8 = (x_2, x_6)(x_3, x_5)(x_5, x_3)(x_6, x_2)(x_7, -x_7)$
$I_9 = (x_2, -x_6)(x_3, -x_5)(x_5, -x_3)(x_6, -x_2)(x_7, -x_7)$
$I_{10} = (x_2, x_3)(x_3, x_2)(x_5, -x_6)(x_6, -x_5)(x_7, -x_7)$
$I_{11} = (x_2, -x_3)(x_3, -x_2)(x_5, x_6)(x_6, x_5)(x_7, -x_7)$
$I_{12} = (x_2, -x_5)(x_3, -x_6)(x_5, x_2)(x_6, x_3)$
$I_{13} = (x_2, x_5)(x_3, x_6)(x_5, -x_2)(x_6, -x_3)$

$$I_{14} = (x_2, -x_6)(x_3, -x_5)(x_4, -x_4)(x_5, x_3)(x_6, x_2)(x_7, -x_7)$$
$$I_{15} = (x_2, x_6)(x_3, x_5)(x_4, -x_4)(x_5, -x_3)(x_6, -x_2)(x_7, -x_7)$$
$$I_{16} = (x_2, x_3)(x_3, x_2)(x_4, -x_4)(x_5, x_6)(x_6, x_5)(x_7, -x_7)$$
$$I_{17} = (x_2, -x_3)(x_3, -x_2)(x_4, -x_4)(x_5, -x_6)(x_6, -x_5)(x_7, -x_7)$$
$$I_{18} = (x_2, x_5)(x_3, x_6)(x_4, -x_4)(x_5, x_2)(x_6, x_3)$$
$$I_{19} = (x_2, -x_5)(x_3, -x_6)(x_4, -x_4)(x_5, -x_2)(x_6, -x_3)$$
$$I_{20} = (x_1, -x_1)(x_2, x_6)(x_3, -x_5)(x_5, -x_3)(x_6, x_2)(x_7, -x_7)$$
$$I_{21} = (x_1, -x_1)(x_2, -x_6)(x_3, x_5)(x_5, x_3)(x_6, -x_2)(x_7, -x_7)$$
$$I_{22} = (x_1, -x_1)(x_2, -x_3)(x_3, x_2)(x_5, -x_6)(x_6, x_5)(x_7, -x_7)$$
$$I_{23} = (x_1, -x_1)(x_2, x_3)(x_3, -x_2)(x_5, x_6)(x_6, -x_5)(x_7, -x_7)$$
$$I_{24} = (x_1, -x_1)(x_2, x_5)(x_3, -x_6)(x_5, x_2)(x_6, -x_3)$$
$$I_{25} = (x_1, -x_1)(x_2, -x_5)(x_3, x_6)(x_5, -x_2)(x_6, x_3)$$
$$I_{26} = (x_1, -x_1)(x_2, x_6)(x_3, -x_5)(x_4, -x_4)(x_5, x_3)(x_6, -x_2)(x_7, -x_7)$$
$$I_{27} = (x_1, -x_1)(x_2, -x_6)(x_3, x_5)(x_4, -x_4)(x_5, -x_3)(x_6, x_2)(x_7, -x_7)$$
$$I_{28} = (x_1, -x_1)(x_2, -x_3)(x_3, x_2)(x_4, -x_4)(x_5, x_6)(x_6, -x_5)(x_7, -x_7)$$
$$I_{29} = (x_1, -x_1)(x_2, x_3)(x_3, -x_2)(x_4, -x_4)(x_5, -x_6)(x_6, x_5)(x_7, -x_7)$$
$$I_{30} = (x_1, -x_1)(x_2, x_5)(x_3, -x_6)(x_4, -x_4)(x_5, -x_2)(x_6, x_3)$$
$$I_{31} = (x_1, -x_1)(x_2, -x_5)(x_3, x_6)(x_4, -x_4)(x_5, x_2)(x_6, -x_3)$$
$$I_{32} = (x_1, x_4)(x_3, -x_6)(x_4, x_1)(x_5, -x_5)(x_6, -x_3)$$
$$I_{33} = (x_1, x_4)(x_2, x_5)(x_4, x_1)(x_5, x_2)(x_6, -x_6)$$
$$I_{34} = (x_1, x_4)(x_2, -x_2)(x_3, x_6)(x_4, x_1)(x_6, x_3)$$
$$I_{35} = (x_1, x_4)(x_2, -x_5)(x_3, -x_3)(x_4, x_1)(x_5, -x_2)$$
$$I_{36} = (x_1, -x_4)(x_3, x_6)(x_4, x_1)(x_6, -x_3)$$
$$I_{37} = (x_1, -x_4)(x_2, x_5)(x_3, -x_3)(x_4, x_1)(x_5, -x_2)(x_6, -x_6)$$
$$I_{38} = (x_1, -x_4)(x_2, -x_2)(x_3, -x_6)(x_4, x_1)(x_5, -x_5)(x_6, x_3)$$
$$I_{39} = (x_1, -x_4)(x_2, -x_5)(x_4, x_1)(x_5, x_2)$$
$$I_{40} = (x_1, x_4)(x_3, -x_6)(x_4, -x_1)(x_6, x_3)$$
$$I_{41} = (x_1, x_4)(x_2, x_5)(x_4, -x_1)(x_5, -x_2)$$
$$I_{42} = (x_1, x_4)(x_2, -x_2)(x_3, x_6)(x_4, -x_1)(x_5, -x_5)(x_6, -x_3)$$
$$I_{43} = (x_1, x_4)(x_2, -x_5)(x_3, -x_3)(x_4, -x_1)(x_5, x_2)(x_6, -x_6)$$
$$I_{44} = (x_1, -x_4)(x_3, x_6)(x_4, -x_1)(x_5, -x_5)(x_6, x_3)$$
$$I_{45} = (x_1, -x_4)(x_2, x_5)(x_3, -x_3)(x_4, -x_1)(x_5, x_2)$$
$$I_{46} = (x_1, -x_4)(x_2, -x_2)(x_3, -x_6)(x_4, -x_1)(x_6, -x_3)$$
$$I_{47} = (x_1, -x_4)(x_2, -x_5)(x_4, -x_1)(x_5, -x_2)(x_6, -x_6)$$
$$I_{48} = (x_1, x_4)(x_2, x_3)(x_3, x_5)(x_4, x_1)(x_5, x_6)(x_6, -x_2)(x_7, -x_7)$$
$$I_{49} = (x_1, x_4)(x_2, x_3)(x_3, x_5)(x_4, -x_1)(x_5, -x_6)(x_6, x_2)(x_7, -x_7)$$
$$I_{50} = (x_1, x_4)(x_2, -x_3)(x_3, -x_5)(x_4, -x_1)(x_5, x_6)(x_6, -x_2)(x_7, -x_7)$$
$$I_{51} = (x_1, x_4)(x_2, -x_3)(x_3, -x_5)(x_4, x_1)(x_5, -x_6)(x_6, x_2)(x_7, -x_7)$$

$I_{52} = (x_1, x_4)(x_2, x_6)(x_3, -x_2)(x_4, -x_1)(x_5, x_3)(x_6, x_5)(x_7, -x_7)$
$I_{53} = (x_1, x_4)(x_2, x_6)(x_3, -x_2)(x_4, x_1)(x_5, -x_3)(x_6, -x_5)(x_7, -x_7)$
$I_{54} = (x_1, x_4)(x_2, -x_6)(x_3, x_2)(x_4, x_1)(x_5, x_3)(x_6, x_5)(x_7, -x_7)$
$I_{55} = (x_1, x_4)(x_2, -x_6)(x_3, x_2)(x_4, -x_1)(x_5, -x_3)(x_6, -x_5)(x_7, -x_7)$
$I_{56} = (x_1, -x_4)(x_2, x_3)(x_3, -x_5)(x_4, -x_1)(x_5, x_6)(x_6, x_2)(x_7, -x_7)$
$I_{57} = (x_1, -x_4)(x_2, x_3)(x_3, -x_5)(x_4, x_1)(x_5, -x_6)(x_6, -x_2)(x_7, -x_7)$
$I_{58} = (x_1, -x_4)(x_2, -x_3)(x_3, x_5)(x_4, x_1)(x_5, x_6)(x_6, x_2)(x_7, -x_7)$
$I_{59} = (x_1, -x_4)(x_2, -x_3)(x_3, x_5)(x_4, -x_1)(x_5, -x_6)(x_6, -x_2)(x_7, -x_7)$
$I_{60} = (x_1, -x_4)(x_2, x_6)(x_3, x_2)(x_4, -x_1)(x_5, -x_3)(x_6, x_5)(x_7, -x_7)$
$I_{61} = (x_1, -x_4)(x_2, x_6)(x_3, x_2)(x_4, x_1)(x_5, x_3)(x_6, -x_5)(x_7, -x_7)$
$I_{62} = (x_1, -x_4)(x_2, -x_6)(x_3, -x_2)(x_4, x_1)(x_5, -x_3)(x_6, x_5)(x_7, -x_7)$
$I_{63} = (x_1, -x_4)(x_2, -x_6)(x_3, -x_2)(x_4, -x_1)(x_5, x_3)(x_6, -x_5)(x_7, -x_7)$

Essas transformações, que estão definidas de $\mathbb{R}^8$ para $\mathbb{R}^8$, formam um grupo abeliano com a operação de composição.

Nota-se que as transformações formadas apenas por troca de sinal de algumas coordenadas, conforme estudadas na seção anterior, formam um subgrupo do grupo das transformações isoespectrais.

Utilizando-se a mesma abordagem da seção anterior, em que se procurava determinar qual era a órbita de pontos do primeiro ortante, obtemos que, para o caso de uma matriz densidade de um qutrit, há duas órbitas (dois ortantes que são espelhados para diversos outros ortantes e nenhum destes dois é levado no mesmo ortante por qualquer transformação isoespectral). Sendo assim, precisamos olhar para a órbita de dois ortantes que não estejam na mesma classe para entender a geometria dos estados físicos.

1.4 Estados Físicos

Sabe-se que para dimensão 3 podemos escrever o polinômio característico de maneira mais conveniente como $p(t) = t^3 - t^2 + \frac{1}{3}(1-|r|^2)t - \det(\rho)$ ao invés de expressar os coeficientes em termos das coordenadas x_i.

Como o polinômio em questão é o polinômio característico de uma matriz densidade, este deve possuir todas as três raízes reais.

Um polinômio de grau 3 da forma $p(x) = ax^3 + bx^2 + cx + d$ possui todas as raízes reais se o discriminante $\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$ satisfizer $\Delta \geq 0$. Agora, considere a expressão $\delta = \left(\frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}\right)^2 + \frac{4}{27}\left(\frac{c}{a} - \frac{b^2}{3a^2}\right)^3$. Tal expressão satisfaz $\delta = -\frac{1}{27a^4}\Delta$.

Fazendo $\alpha = \frac{1}{3}(1-|r|^2)$ e $\beta = \det(\rho)$, temos que $27\delta = 4\beta - \alpha^2 - 18\alpha\beta + 4\alpha^3 + 27\beta^2$. Procurar os valores de α e β que tornam $\delta \geq 0$ é equivalente a procurar valores de α e β tal que $27\beta^2 - (18\alpha - 4)\beta - (\alpha^2 - 4\alpha^3) \geq 0$, isto é um polinômio do grau 2 na variável β, e estudar o sinal desta função é fácil. Tais valores também tornam $\Delta \leq 0$, e estão associados a estados que não apresentam realidade física.

O discriminante da equação do segundo grau é $\Delta = (18\alpha - 4)^2 + 108(\alpha^2 - 4\alpha^3) = 16(1-3\alpha)^3$, reescrevendo em termos de $|r|$ temos $\Delta = 16|r|^6$. Portanto, Δ é sempre positivos e teremos sempre duas raízes, a não ser quando $|r| = 0$. Essas raízes são $\beta_+ = \dfrac{-1 + 3|r|^2 + 2|r|^3}{-27}$ e $\beta_- = \dfrac{-1 + 3|r|^2 - 2|r|^3}{-27}$.

Primeiramente, note que $\beta_+ \leq \beta_-$ e $\beta_+ = \beta_-$ se, e somente se, $|r| = 0$.

Vamos analisar o comportamente de δ conforme variamos $|r|$.

• Se $|r| = 0$ então $\beta_+ = \beta_- = \dfrac{1}{27}$ e $\alpha = \dfrac{1}{3}$ e, consequentemente, $\delta = 0$ para $\beta = \dfrac{1}{27}$.

• Se $0 < |r| < \dfrac{1}{2}$ então $0 < \beta_+ < \beta_-$ e $\dfrac{1}{4} < \alpha < \dfrac{1}{3}$ e, consequentemente, $0 \leq \delta$ para $0 < \beta_+ \leq \beta \leq \beta_- < \dfrac{1}{54}$.

• Se $|r| = \dfrac{1}{2}$ então $\beta_+ = 0$, $\beta_- = \dfrac{1}{54}$ e $\alpha = \dfrac{1}{4}$ e, consequentemnte, $0 \leq \delta$ para $0 \leq \beta \leq \dfrac{1}{54}$.

• Se $\dfrac{1}{2} < |r| < 1$ então $-\dfrac{4}{27} < \beta_+ < 0 < \beta_- < \dfrac{1}{54}$ e $0 < \alpha < \dfrac{1}{4}$ e, consequentemente, $0 \leq \delta$ para $\beta_+ < \beta < \beta_-$.

• Se $|r| = 1$ então $\beta_- = 0$, $\beta_+ = -\dfrac{4}{27}$ e $\alpha = 0$ e, consequentemente, $0 \leq \delta$ para $-\dfrac{4}{27} \leq \beta \leq 0$.

Resumindo, para $0 \leq |r| \leq 1$ temos que $0 \leq \beta_-$ mas, $0 < \beta_+$ para $0 \leq |r| < \dfrac{1}{2}$, $0 = \beta_+$ para $|r| = \dfrac{1}{2}$ e $\beta_+ < 0$ para $\dfrac{1}{2} < |r| \leq 1$.

Infelizmente, as condições acima embora permitam especificar quais são os estados da esfera de Bloch que correspondem a estados físicos, em termos de $|r|$ e de $\det(\rho)$, deixam muita margem para obter estes valores em termos dos x_i, dado que há oito destas coordenadas e que a expressão dos coeficientes do polinômio característico em termos dos x_i não é trivial.

Tal dificuldade impõe uma restrição muito grande para se determinar qual é a geometria dos estados físicos dentro da esfera de Bloch. Uma maneira de se tentar contornar esta dificuldade é tomar a interseção da esfera de Bloch, sujeita às condições especificadas para $|r|$ e $\det(\rho)$, com retas e planos especiais que deixem parte das coordenadas x_i iguais a zero para facilitar a análise. Embora isso possa ser feito não será apresentado aqui pois tal método foi exaustivamente abordado

em [14], [10] e [11].

A abordagem descrita neste capítulo embora de simples entendimento resultou de um árduo e demorado processo de cálculo que tinha como objetivo determinar o grupo de transformações isoespectrais associadas a operadores densidade de um qutrit. Embora o caminho usado na abordagem do problema tenha sido diferente das abordagens encontradas em [14], [10] e [11], não houve maiores avanços.

Uma outra tentantiva para tentar simplificar um pouco o problema seria repetir o método descrito neste capítulo mas tentando utilizar outras bases para o conjunto das matrizes densidade. Em [2] encontram-se outras bases, como a base de operadores de Weyl, base de polarização dentre outras conhecidas na literatura; há ainda a possibilidade de se tentar construir uma base na qual o polinômio característico tenha a representação mais simples possível.

Não é claro se essa mesma abordagem com outras bases poderia resultar em novas simestrias; também não está claro se a utilização de tais simestrias conjuntamente com a interseção da Esfera de Bloch com certos subconjuntos especiais, diferentes dos já abordados, poderia trazer maiores esclarecimentos sobre a questão, mas esta é uma tarefa deixada para um momento futuro.

Capítulo 2

Emaranhadores Universais

O presente capítulo tem o objetivo de apresentar resultados referentes à convergência de estados produto de um sistema quântico fechado qualquer sob aplicações sucessivas de medições quânticas sorteadas aleatoriamente. Para tanto, iniciaremos o capítulo com uma seção que tem o objetivo de introduzir os conceitos necessários aos desenvolvimentos posteriores das demais seções do capítulo.

2.1 Preliminares

A maioria dos resultados desta seção podem ser encontrados no livros de Botelho, Pellegrino e Teixeira ([3]), Hognas ([9]) e Munkres ([17]) e estão reproduzidos aqui para o conforto do leitor.

Entendemos que a omissão, nessa etapa preliminar, de alguns tópicos de análise funcional, teoria da medida e topologia não prejudicará a sequência do texto, pois estaremos sempre tratando do caso de dimensão finita e, neste contexto, nossos espaços são homeomorfos a $\mathbb{R}^m$ e satisfarão automaticamente todas as referidas definições omitidas; além disso, as definições omitidas não terão papel relevante no restante do texto, a não ser como hipóteses de resultados que precisaremos.

2.1.1 Grupo Unitário

Estaremos interessados, nas seções posteriores, em sistemas quânticos fechados, isto é, sistemas que não interagem com o seu exterior. Nenhum sistema é realmente fechado, mas muitas vezes essa consideração é uma hipótese bem próxima da realidade e permite tratar a teoria de forma mais simples.

Conforme pode ser consultado em [18] página 81, o postulado 2 da mecânica quântica estabelece que a evolução de um sistema quântico fechado é descrita por meio de uma transformação unitária.

Definição 2.1.1 (Matriz Unitária)**.** *Uma matriz complexa quadrada u é chamada de unitária se a transposta conjugada de u^* é igual a u^{-1}, isto é, se* $uu^* = u^*u = \mathrm{Id}$.

O conjunto das matrizes unitárias possui uma propriedade especial conforme proposição 2.1.1.

Proposição 2.1.1 (Grupo Unitário)**.** *O conjunto das matrizes unitárias de ordem n com a operação de multiplicação usual de matrizes forma um grupo, chamado de grupo unitário, denotado por $U(n)$.*

Vale dizer que o grupo $U(n)$ é homeomorfo a um subconjunto de $\mathbb{C}^{n^2}$ e com a topologia induzida de $\mathbb{C}^{n^2}$ as operações de multiplicação e inversão são contínuas, por isso ele é chamado de um grupo topológico. Ainda, com a referida topologia, toda cobertura aberta de $U(n)$ admite subcobertura finita e, portanto, $U(n)$ é chamado grupo topológico compacto. Como $\mathbb{C}^{n^2}$ é metrizável e $U(n)$ é homeomorfo a um subconjunto de $\mathbb{C}^{n^2}$, segue que $U(n)$ é um grupo topológico compacto metrizável. Para mais informações, consultar [9].

Ainda, segundo o homeomorfismo citado, $U(n)$ pode ser considerado espaço métrico e portanto também é espaço Hausdoff e, além disso, $U(n)$ é segundo contável. Para ver as definições de Hausdorff e segundo contável, consultar [17].

2.1.2 Medida de Haar

A medida de Haar é uma forma de atribuir um tamanho para subconjuntos de grupos localmente compactos. Por comodidade a definição de localmente compacto encontra-se a seguir.

Definição 2.1.2. *Um espaço topológico X é localmente compacto se para cada $x \in X$ admite uma base de vizinhanças compactas.*

Como estaremos interessado em medir o tamanho de subconjuntos de matrizes unitárias que, conforme veremos na proposição 2.1.2, são localmente compactos somos então levados a considerar a medida de Haar como sendo a mais natural a ser usada neste problema.

Vejamos brevemente o conceito de medida de Haar.

Suponha que G seja um grupo topológico localmente compacto. A σ-álgebra de Borel, denotada por $\mathcal{G}$, é a σ-álgebra gerada por todos os subconjuntos abertos de G. Para mais detalhes, consultar [13].

Seja $a \in G$ e $S \subset G$, definimos a translação a esquerda de S como $aS = \{as; s \in S\}$, aqui está sendo empregada a notação multiplicativa para a operação do grupo.

Uma medida μ é chamada invariante por translação à esquerda em G se, e somente se, $\mu(aS) = \mu(S)$ para todo subconjunto de Borel $S \subset G$ e todo $a \in G$.

Conforme [13], é possível mostrar que, exceto por uma constante multiplicativa, existe apenas uma medida regular (ver definição 2.1.3) μ que é invariante por translação à esquerda tal que $\mu(U) > 0$, para qualquer conjunto aberto não vazio U. Esta medida é que chamaremos de agora em diante de medida de Haar e a denotaremos por μ.

Definição 2.1.3. *Seja $M(S)$ o conjunto das medidas atuando em S. Uma medida $\mu \in M(S)$ é chamada regular se para qualquer $\epsilon > 0$ existir um subconjunto compacto $K \subset \mathfrak{B}$ tal que $\mu(S - K) < \epsilon$, em que $\mathfrak{B}$ é a classe dos subconjuntos de Borel.*

Para que possamos medir subconjuntos de $U(n)$ com a medida de Haar precisamos mostrar que $U(n)$ é um grupo localmente compacto mas isso é uma consequência da proposição 2.1.2 encontrada em [13].

Proposição 2.1.2. *Um espaço Hausdorff X é localmente compacto se, e somente se, cada $x \in X$ tem pelo menos uma vizinhança compacta.*

Como cada espaço de Hausdorff compacto é localmente compacto e $U(n)$ é um grupo Hausdorff compacto, segue que $U(n)$ é localmente compacto e portanto a medida de Haar está bem definida para o grupo unitário.

Prosseguindo, trataremos agora sobre convergência de sequências de medidas.

Seja S um semigrupo topológico Hausdorff localmente compacto e segundo contável. Seja $\mathfrak{B}$ a classe dos subconjuntos de Borel de S e $P(S)$ o conjunto de todas as medidas de probabilidade regulares μ em $\mathfrak{B}$.

Seja $C(S)$ o espaço de todas as funções reais contínuas limitadas em S.

Definição 2.1.4 (Convergência fraca)**.** *Seja $\mu_n \in P(S)$ uma sequência de medidas. Dizemos que μ_n converge fracamente para $\mu \in P(S)$ se para toda função $f \in C(S)$, $\lim_{n\to\infty} \int f d\mu_n = \int f d\mu$.*

Seja $B(S)$ o conjunto de todas as medidas regulares em $\mathfrak{B}$ tal que $\mu(S) \leq 1$.

Definição 2.1.5 (Convergência fraca-estrela)**.** *Uma sequência $\mu_n \in B(S)$ converge fraco-estrela para $\mu \in B(S)$ se para toda função contínua $f \in S$ com suporte compacto $\lim_{n\to\infty} \int f d\mu_n = \int f d\mu$.*

2.2 Desenvolvimento

Vamos aplicar resultados sobre grupos unitários para estudar a evolução de um sistema quântico. A principal motivação para este estudo e, em particular, para este capítulo é prover um modelo simples no qual a evolução temporal sobre algum parâmetro de controle pode emaranhar todo estado produto. Isto é, começaremos agora a desenvolver o nosso principal resultado, deste capítulo, que trata da aproximação de emaranhadores universais via composição de aplicações unitárias.

Lembrando que um estado $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ é dito estado produto se podemos escrever $|\psi\rangle$ da forma $|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$, em que $|\psi\rangle_A \in \mathcal{H}_A$ e $|\psi\rangle_B \in \mathcal{H}_B$ e $\otimes$ denota o produto tensorial. Se $|\psi\rangle$ não é estado produto, então dizemos que é um estado emaranhado. Para maiores esclarecimentos sobre produto tensorial consultar [18].

Considere um espaço de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, em que $\mathcal{H}_A$ e $\mathcal{H}_B$ são espaços de Hilbert, e o grupo formado pelo conjunto $U(n)$ de transformações unitárias agindo em $\mathcal{H}$ com a operação do grupo sendo o produto usual de matrizes, em que n é a dimensão global do espaço, isto é, a dimensão de $\mathcal{H}$.

Conforme visto, este grupo pode ser dotado de uma medida natural de probabilidade invariante por translação, ou seja, uma medida de Haar μ associada ao grupo $U(n)$. Isto é, dado qualquer conjunto mensurável $A \subset U(n)$, vale que $\mu(A) = \mu(T_u(A))$ para todo $u \in U(n)$, em que $T_u : U(n) \mapsto U(n)$ é dado por $T_u(v) = uv$.

Neste trabalho pode-se considerar que uma porta quântica é um pequeno circuito quântico operando em uma quantidade pequena de qubits. Assim como um sistema elétrico clássico é composto de fios e portas lógicas, um circuito quântico é essencialmente um conjunto de fios e portas quânticas elementares que carregam e manipulam informação quântica. Para uma discussão mais detalhada, consultar [18].

Ainda conforme [18], cada matriz unitária representa alguma porta quântica, portanto ao encontrar a expressão porta quântica o leitor pode pensar em alguma matriz unitária.

Definição 2.2.1 (Emaranhador Universal)**.** *Uma porta quântica que pode transformar um estado produto em um estado emaranhado é chamada de emaranhador. Um emaranhador universal é um operador que pode transformar todo estado produto em algum estado emaranhado, isto é,* $u : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$ *é um emaranhador universal se, para qualquer estado produto* $|\psi\rangle_A \otimes |\psi\rangle_B \in \mathcal{H}_A \otimes \mathcal{H}_B$*,* $u(|\psi\rangle_A \otimes |\psi\rangle_B)$ *for estado emaranhado.*

Tal definição pode ser muito abrangente e pode levar o leitor a um questionamento natural: será que existe algum operador que satisfaz a definição? Isto é,

será que existe algum emaranhador universal?

Foi provado em [6] que existem emaranhadores universais em $U(n)$ se e somente se $\min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\} \geq 3$ e $(\dim \mathcal{H}_A, \dim \mathcal{H}_B) \neq (3,3)$.

Interessantemente, não é conhecido nenhum exemplo de tais transformações, embora haja muita pesquisa voltada para a identificação de tais transformações. Para mais detalhes ver [15].

Nós denotamos o conjunto dos emaranhadores universais por **UE**.

2.3 Dinâmica

Sabe-se de [8] que escolhendo aleatoriamente um $u \in U(n)$ de acordo com a medida de Haar tem-se um emaranhador universal com probabilidade $1 - e^{cn}$, para algum $c \in \mathbb{R}$ com $c < 0$. Isto quer dizer que se escolhermos um sistema quântico fechado cuja dinâmica é dada por u, então depois do primeiro passo do processo todos os estados do processo são quase emaranhados.

Agora, considere a sequência de iterações u^k.

Como a distribuição de u^k também é μ (e isto vale para todo $k \in \mathbb{Z}$, pois a medida de Haar μ satisfaz a equação $\mu * \mu = \mu$), temos que qualquer u^k é um emaranhador universal com probabilidade aproximadamente 1, pois u^k também possui distribuição μ. Neste parágrafo $*$ denota a convolução de medidas.

Assumindo um ponto de vista dinâmico, pode-se questionar quanto à ergodicidade do sistema (T_u, μ), em que T_u é a translação por u. Em outras palavras, pode-se questionar se aplicando inúmeras vezes T_u a órbita da sequência vai ser estacionária ou se acabará entrando e saindo várias vezes de **UE**.

Convém, para demais intentos, lembrar que o grupo $U(n)$ é compacto e metrizável e, para conforto do leitor, disponibilizamos a proposição abaixo que traz caracterizações importantes de ergodicidade. Para mais detalhes, consultar [20].

Proposição 2.3.1. *Seja G um grupo compacto metrizável, μ a medida de Haar associada a G e $g \in G$. Os seguintes resultados são equivalentes:*

a) (T_g, μ) *é ergódico;*

b) $\{g^n\}$ *é denso em* G. ■

De acordo com a Proposição 2.3.1, se os iterados de u forem densos em $U(n)$, então o sistema será unicamente ergódico e valerá

$$\frac{1}{n}\sum_{i=0}^{n-1} \chi_{\mathbf{UE}} \circ T_u^i(v) \to \mu(\mathbf{UE})$$

para todo $v \in U(n)$, em que $\chi_{\mathbf{UE}}$ é a função característica do conjunto **UE**. Para mais detalhes, consultar [20].

Retomando a discussão sobre emaranhadores universais, temos que se a dimensão do espaço de Hilbert $\mathcal{H}$ é grande (maior que 12), então o conjunto **UE** de emaranhadores universais agindo em $\mathcal{H}$ tem medida positiva de acordo com a medida de Haar.

No caso particular $v = u$, temos que o tempo médio de visita da sequência u^n para o conjunto dos emaranhadores universais é positivo.

Portanto, se a dinâmica do sistema quântico é dada por u, existe um inteiro positivo N (na realidade, uma quantidade infinita de valores de N) de maneira que depois de N passos o sistema está emaranhado para qualquer estado produto inicial.

Entretanto, não existe $u \in U(n)$ tal que u^k seja denso, conforme conseguimos demonstrar na seguinte proposição.

Proposição 2.3.2. *Não existe $u \in U(n)$ tal que u^k é denso em $U(n)$.*

Demonstração. Vamos chamar de G_s o conjunto de todas as matrizes unitárias diagonalizadas por s, isto é, a forma unitária $v = sd_vs^*$, em que $s \in U(n)$ e d_v é diagonal. Como todas as potências de v pertencem a este subgrupo, é suficiente mostrar que G_s não é denso em $U(n)$.

Considere inicialmente o conjunto das matrizes diagonais unitárias G_e, em que e é o elemento identidade do grupo. Este é um subconjunto próprio e fechado de $U(n)$, que implica que este não pode ser denso. Realmente, identificando elementos de $U(n)$ com vetores de $\mathbb{R}^{n^2}$, vê se que dado $d \in U(n)$ diagonal e $a \in U(n)$ não diagonal,

$$||d - v|| \geq \sqrt{\sum_i |a_i|^2} := \epsilon$$

em que os a_i são os elementos não diagonais de a e $||\cdot||$ denota a norma euclidiana.

Isto quer dizer que $d \notin B(a, \epsilon)$ para todo d diagonal e portanto G_e não é denso. Note que isso vale para qualquer a não diagonal.

Considere agora G_s, com $s \neq e$, e $a \notin G_s$. Se para cada $\epsilon > 0$ existe um $v = sd_vs^*$ em $B(a, \epsilon)$, então existe alguma matriz diagonal d_v em $B(s^*as, \epsilon)$.

Entretanto, como s^*as não é diagonal e ϵ é arbitrário, isto contradiz o fato anterior e o fato de que $s \neq e$. □

Não precisamos sequer do item (b) da Proposição 2.3.1 para concluir que neste caso o sistema não é ergódico: existe uma medida de Haar suportada em G_s e então a função T_u não será unicamente ergódica.

No caso geral, o fecho da órbita u^k gera uma subvariedade de dimensão dada por um número de autovalores racionais independentes. Isto é, no máximo dimensão n, enquanto $\dim(U(n)) = n^2$.

2.4 Caso aleatório

Agora considere o caso fisicamente relevante de uma evolução com parâmetros de controle. Vamos fixar uma transformação arbitrária u agindo em um sistema composto de dimensão grande, uma vizinhança $\mathcal{N} \ni u$ e a restrição de μ para $\mathcal{N}$, denotado por $\mu_{\mathcal{N}}$, isto é, a restrição da medida de Haar à vizinhança $\mathcal{N}$.

Embora a medida do conjunto dos emaranhadores universais **UE** seja aproximadamente 1, pode ser que u não pertença à **UE**.

Considere o processo estocástico

$$u_1, u_2u_1, u_3u_2u_1, \ldots \tag{2.1}$$

em que cada $u_i \in \mathcal{N}$ é independentemente escolhido de acordo com a medida de probabilidade $\mu_{\mathcal{N}}$.

No caso particular em que $u = e$, temos o seguinte resultado bem conhecido, encontrado em [1]:

Proposição 2.4.1. *Seja $\mathcal{H}$ um grupo topológico conexo e seja $\mathcal{N} \subset \mathcal{H}$ um subconjunto aberto tal que $e \in \mathcal{N}$ e $u \in \mathcal{N}$ implica em $u^{-1} \in \mathcal{N}$. Então*

$$\mathcal{H} = \bigcup_{j=1}^{\infty} \mathcal{N}^j, \tag{2.2}$$

em que $\mathcal{N}^1 = \mathcal{N}$ e $\mathcal{N}^j := \{u_j \cdots u_1; u_i \in \mathcal{N}, i = 1, \ldots, j\}$, para $j > 1$.

Demonstração. Note que o conjunto $\mathcal{N}^2 = \bigcup_{u \in \mathcal{N}} u\mathcal{N}$ é aberto pois é a união de conjuntos abertos. Procedendo indutivamente, vemos que $\mathcal{N}^n$ é aberto para qualquer n, e o mesmo vale para a união no lado direito de (2.2). Como $\mathcal{H}$ é um grupo conexo, para terminar a prova é suficiente mostrar, devido à proposição 24.2 (página 1268) de [1], que $\bigcup_{j=1}^{\infty} \mathcal{N}^j$ é um grupo.

Por hipótese, $e \in \mathcal{N}$. Se $g_1 \in \mathcal{N}^{n_1}$ e $g_2 \in \mathcal{N}^{n_2}$, então $g_1g_2 \in \mathcal{N}^{n_1+n_2} \subset \bigcup_{j=1}^{\infty} \mathcal{N}^j$. Finalmente, se $g \in \mathcal{N}^n$ e $g = u_1 \ldots u_n$, então $g^{-1} = u_n^{-1} \ldots u_1^{-1} \in \mathcal{N}^n \subset \bigcup_{j=1}^{\infty} \mathcal{N}^j$. □

Essencialmente o que a proposição estabelece é que se considerarmos uma vizinhança da identidade de um grupo conexo, então podemos gerar todo o grupo através do produto de elementos contidos na vizinhança considerada.

No caso mais geral, considere uma bola B_u centrado em um arbitrário $u \in U(n)$. Se todos os autovalores de u são da forma $e^{\frac{p}{q}i2\pi}$, então para cada autovalor de u existe algum $k \in \mathbb{N}$ tal que $u^k = e$.

Mas, se ao menos um dos autovalores é irracional então ainda é verdade que para qualquer $\epsilon > 0$ existe algum k tal que u^k é ϵ-fechado para e.

Portanto, o k-ésimo iterado de B_u contém alguma vizinhança B_e da identidade. Como u^{-1} e u são equidistantes de e, sem perda de generalidade podemos assumir que B_e está nas condições da Proposição 2.4.1, e conseguimos demonstrar o seguinte resultado.

Proposição 2.4.2. *Dado $u \in U(n)$, qualquer vizinhança aberta $B_u \ni u$ gera todo o grupo, isto é, $U(n) = \bigcup_{j=1}^{\infty} B_u^j$.*

No caso particular em que o grupo é também compacto, tal como o grupo unitário, a união em (2.2) acima é finita, pois pode-se sempre extrair uma subcobertura finita dela.

Portanto, se escolhermos algum $u \in U(n)$, a órbita de u pode não intersectar **UE**, mas se considerarmos qualquer bola centrada em u e realizar o processo estocástico (2.1), então é possível intersectar o conjunto **UE**.

Em outras palavras, provamos o seguinte corolário.

Corolário 2.4.1. *Seja $u \in U(n)$ uma matriz unitária arbitrária e B_u uma vizinhança aberta de u. Se cada u_i é escolhida de acordo com a medida de Haar restrita a B_u, então o processo estocástico gera um emaranhador universal, com probabilidade quase 1, em um número finito de passos (2.1).*

Vamos agora provar que o produto de elementos de $U(n)$ estará próximo de um emaranhador universal no sentido da convergência fraco-estrela para a medida de Haar, para isso usaremos o teorema 2.21 de [9], reproduzido abaixo por comodidade.

Teorema 2.21: Sejam S um grupo compacto e conexo e μ_n, $n \geq 1$, uma sequência de medidas. Seja $\beta \in P(S)$, $\beta_a \neq 0$, e $a > 0$ tal que $\mu_n \geq a.\beta$. Então existem um inteiro positivo p e $0 < r < 1$ tais que $||\mu_1 * \cdots * \mu_n - m|| \leq 2.r^{[n/p]+1}$ para $n \geq 1$, em que m é a medida de probabilidade de Haar em S.

Então temos, agora, o nosso principal resultado do capítulo:

Teorema 2.4.1. *Considere um número finito de elementos $u_1, \ldots, u_n \in U(n)$ escolhidos aletatoriamente, então o produto de elementos aleatoriamente escolhidos na vizinhança de elementos $u_1, \ldots, u_n$ converge fraco-estrela para um elemento em **UE** na medida de Haar em $U(n)$.*

Demonstração. Escolha de maneira aleatória um número finito de elementos $u_1, \ldots, u_{n_0} \in U(n)$ e considere bolas $B_i = B(u_i, \epsilon_i)$, com $\epsilon_i > 0$ e $i \in \{1, \ldots, n_0\}$, e considere μ_i (a medida de Haar de $U(n)$ restrita a B_i) a distribuição de probabilidade do elemento u_i, então a distribuição de probabilidade do produto $u_n \ldots u_1$ será a convolução $\mu_1 * \cdots * \mu_{n_0}$. Pelo Teorema 2.21 de [9], $\mu_1 * \cdots * \mu_{n_0}$ vai convergir fraco-estrela na medida de Haar em $U(n)$ exponencialmente rápido e por [8] temos $\chi(\textbf{UE}) \approx 1$, então o produto dos elementos $u_1, \ldots, u_{n_0}$ estará arbitrariamente próximo de um elemento de **UE**. □

Essencialmente, o teorema 2.3.2 garante que escolhidos aleatoriamente uma certa quantidade arbitrária de transformações unitárias $u_1, \ldots, u_n$ a aplicação sucessiva destas, ou de outras na vizinhança destas, converge fraco-estrela para um emaranhador universal. Esse é o caso que se observa na prática, devido ao fato de que qualquer porta quântica corresponde a uma interação entre parte do sistema quântico com algum aparelho que executa alguma manipulação sobre qubits e os aparelhos possuem naturalmente um erro associado de maneira que nossa manipulação do sistema não é perfeita.

2.5 Conclusão e resultados relacionados

Do exposto neste capítulo conclui-se que embora seja provada a existência de emaranhadores universais ainda não se conhece nenhum exemplo de tais operadores; mesmo assim é possível emaranhar qualquer estado produto pela aplicação sucessiva de portas quânticas, selecionadas aleatoriamente, com velocidade exponencialmente rápida.

Como as portas quânticas são a representação teórica de operações que se fazem na prática com qubits, e como todo experimento apresenta invariavelmete algum erro, temos na realidade uma ligeira indeterminação com relação à operação realizada, de forma que só se pode afirmar que realizou-se aproximadamente a operação indicada. Essa indeterminação se traduz matematicamente no sorteio de um operador na vizinhança das operações indicadas. Neste contexto, o presente capítulo mostrou que quanto maior a dimensão do sistema e quanto mais portas quânticas se escolhe, mais rapidamente essa aplicação sucessiva de portas quânticas emaranha qualquer estado produto inicial.

Além disso cabe ressaltar que estudos correlatos mostraram conclusões semelhantes. Por exemplo, em [4] estudaram-se dois processos semelhantes mas restritos a sortear duas ou três portas quânticas pré determinadas e notou-se que em ambos os casos qualquer estado produto inicial acabava evoluindo para um estado emaranhado mas com velocidade polinomial. Este resultado é de certa forma esperado pois há uma limitação com relação à quantidade de portas quânticas sorteadas; por outro lado, parece mostrar que com apenas poucas portas quânticas se pode gerar emaranhamento, sem a necessidade de se considerar que as portas sorteadas pertençam à vizinhanças.

O fato de tudo isso ser possível de ser feito com poucas portas é uma vantagem para a teoria da computação quântica, pois todos os circuitos quânticos são contruídos com base em poucas portas elementares e combinação destas.

Capítulo 3

Conjectura de Lehmer

O problema *totient* de Lehmer, proposto em 1932 por Derrick Henry Lehmer, consiste em saber se existe algum número não primo n tal que a função *totient* de Euler, aplicado em n, divide $n-1$, isto é, se $\varphi(n)$ divide $n-1$. Sabe-se que $\varphi(p) \mid (p-1)$ para p primo, e Lehmer conjecturou que isso não acontece para nenhum número composto.

Pretendemos aqui mostrar, para alguns casos particulares, o seginte resultado:

Teorema 3.0.1. *Seja n número um natural que não é primo. Então $\varphi(n)$ não é um divisor de $n-1$.*

De acordo com o dicionário Collins, de língua inglesa, o termo *totient* (sem correspondente em português) é um substantivo que significa "a quantidade de números menores do que, e não compartilhando fator comum, com um dado número" (em tradução livre).

Essencialmente, se Lehmer estiver certo então há mais uma maneira de caracterizar números primos, o que poderá trazer consequências para a área de Teoria de Números. Isto é, poderíamos definir que um número p é primo se, e somente se, $\varphi(p)$ dividir $p-1$.

O presente problema foi abordado por diversos matemáticos nas últimas décadas, principalmente na década de 80 por Cohen em [5]. Mais recentemente os avanços se deram devido ao auxílio de computadores, sendo o mais recente de 2017.

3.1 Preliminares

A presente seção tem o objetivo de fornecer ao leitor as definições básicas usadas no estudo da Conjectura de Lehmer. Todas as definições e resultados podem ser encontrados em [21] mas estão reproduzidas aqui para o conforto do leitor.

Definição 3.1.1 (Número primo)**.** *Um número natural n é chamado de número primo se n tem apenas dois divisores naturais distintos, 1 e o próprio n. Caso contrário é chamado número composto.*

Definição 3.1.2. *Sejam $a, b \in \mathbb{Z}$ e $a \neq 0$. Dizemos que a divide b, e denotamos por $a \mid b$, se existe $c \in \mathbb{Z}$ tal que $b = ac$.*

Existem infinitos primos. Este resultado era conhecido por Euclides, que trouxe uma demonstração simples e elegante deste fato.

Tal demonstração pode ser encontrada em [16] ou qualquer livro sobre Teoria de Números.

Teorema 3.1.1 (Teorema Fundamental da Aritmética)**.** *Todo inteiro positivo $n > 1$ pode ser escrito de modo único, exceto pela ordem dos fatores, como produto de números primos, isto é, $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ em que $p_1, \ldots, p_k$ são primos distintos e $\alpha_1, \ldots, \alpha_k$ são números inteiros positivos.*

Tal demonstração pode ser encontrada em [16] ou qualquer livro sobre Teoria de Números.

Vamos introduzir agora a função *totient* de Euler.

Definição 3.1.3. *Seja $n \in \mathbb{N}$, a função totient de Euler, denotada por φ, é definida por $\varphi(n) = \sum_{\substack{1 \leq k < n, \\ mdc(k,n)=1}} 1$.*

Essencialmente, $\varphi(n)$ é o número de inteiros positivos k menores que n que são relativamente primos com n.

Vejamos agora algumas propriedades da função *totient* de Euler, estas podem ser encontradas em [21], mas estão reproduzidas abaixo para o conforto do leitor..

Teorema 3.1.2. *Seja $n \in \mathbb{N}$, então*

$i)$ *Se a e b são primos entre si, então $\varphi(ab) = \varphi(a)\varphi(b)$;*

$ii)$ *Se p é primo, então $\varphi(p) = p - 1$;*

$iii)$ *Se p é primo e $\alpha > 1$ então $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$;*

$iv)$ *Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, então $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$.*

Demonstração. $i)$ Segue de uma aplicação simples de indução finita.

$ii)$ Se p é primo então $1, 2, \ldots, p-1$ são relativamente primos com p, e pela definição da função de Euler, temos $\varphi(p) = p-1$. Reciprocamente, se n não é primo então n tem algum divisor $d < n$, portanto existe pelo menos um inteiro menor que n que não é relativamente primo a n, e segue da definição da função de Euler que $\varphi(n) \leq n-2$.

$iii)$ Se $n = p^\alpha$, com p primo, então há exatamente $p^{\alpha-1}$ inteiros entre 1 e p^α, a saber $p, 2p, 3p, \ldots, p^{\alpha-1}$, que dividem p^α. Portanto, o conjunto $\{1, 2, \ldots, p^\alpha\}$ contém exatamente $p^\alpha - p^{\alpha-1}$ inteiros relativamente primos a p^α, e segue da definição da função de Euler que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

$iv)$ Segue de combinar os itens i e iii e usar indução finita.

□

3.2 Caso de números naturais que são múltiplos de ao menos um quadrado perfeito

Vamos aqui considerar o caso de números naturais que são múltiplos de ao menos um quadrado perfeito, caso já conhecido mas que incluímos em benefício do leitor.

Proposição 3.2.1. *Seja n um número natural que é múltiplo de ao menos um quadrado perfeito, isto é, pelo menos algum $\alpha_i \geq 2$. Então $\varphi(n)$ não é um divisor de $n-1$.*

Demonstração. Seja n um número composto, então pelo Teorema Fundamental da Aritmética n pode ser escrito na forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, em que p_i, $1 \leq i \leq k$, é primo e $\alpha_i \in \mathbb{N}$.

Sabe-se que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ para p primo; e que $\varphi(ab) = \varphi(a)\varphi(b)$ para a e b primos entre si.

Portanto, $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right)$.

Suponha que $\varphi(n)|(n-1)$. Então existe $c \in \mathbb{N}$ tal que $n - 1 = \varphi(n)c$.

Suponha que $\alpha_i > 1$ para algum $1 \leq i \leq k$ então

$$n - cn\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right) = 1$$

$$n\left(1 - c\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_n}\right)\right) = 1$$

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}\left(\frac{p_1 \cdots p_n - c(p_1 - 1)\cdots(p_n - 1)}{p_1 \cdots p_n}\right) = 1$$

$$p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}\left(p_1\cdots p_n - c(p_1-1)\cdots(p_n-1)\right) = 1$$

Note que na expressão acima temos o produto de dois termos (o primeiro é um produto de números naturais e o outro está entre parênteses), em que pelo menos um deles é maior que 1, resultando em 1. Isto é uma contradição que surgiu de supor $\varphi(n)|(n-1)$. □

Fica assim demonstrada a Conjectura de Lehmer para o caso $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ em que pelo menos um dos α_i é maior que 1, ou seja, a conjectura vale para números que são múltiplos de ao menos algum quadrado perfeito, e resta então compreender o que ocorre com números que são livres de quadrados.

3.3 Caso de números livres de quadrados

Vamos agora tratar do caso em que $n = p_1p_2\cdots p_k$ com $p_i \neq p_j$ para $i \neq j$. Mais precisamente, queremos mostrar o seguinte:

Proposição 3.3.1. *Seja n um número natural não primo livre de quadrados. Então $\varphi(n)$ não é divisor de $n-1$.*

A prova desta proposição, para casos particulares, ocupará o restante deste texto e será dividada em alguns lemas.

Lema 3.3.1. *Seja n um número natural não primo, livre de quadrados e par. Então $\varphi(n)$ não é divisor de $n-1$.*

Demonstração. Seja n par. Sem perda de generalidade, podemos considerar $n = 2p_2p_3\cdots p_k$. Então $\varphi(n) = \varphi(2)\varphi(p_2)\cdots\varphi(p_k)$.

Como $\varphi(p) = p-1$ para p primo, seque que $\varphi(2p_2\cdots p_k)$ é um número par; mas $2p_2\cdots p_k - 1$ é um número ímpar. Logo $\varphi(n)$ não pode ser divisor de $n-1$. □

Portanto, a conjectura vale se $p_i = 2$ para algum i.

Vamos nos concentrar, portanto, no caso $n = p_1p_2\cdots p_k$ e, sem perda de generalidade, vamos supor $3 \leq p_1$ e $p_i < p_j$ para $i < j$.

Comecemos com o caso em que n é o produto de dois primos distintos.

3.3.1 Produto de dois números primos distintos

Comecemos com o caso em que n é o produto de dois primos distintos, isto é, $n = p_1p_2$.

Lema 3.3.2. *Considere o natural $n = 3p$, para $5 \leq p$ primo. Então $\varphi(n)$ não é divisor de $n - 1$.*

Demonstração. Neste caso, $\varphi(3p) = 2(p-1)$ e $n-1 = 3p-1$. Supondo $\varphi(3p)|(3p-1)$, então existe $c \in \mathbb{N}$ tal que $3p-1 = c[2(p-1)]$, que equivale a $(2c-3)p+(1-2c) = 0$. Esta equação é verdadeira se $2c-3 = 0$ e $1-2c = 0$ ou se $p = \dfrac{2c-1}{2c-3}$.

Note que não é possível a primeira opção. Resta então $p = \dfrac{2c-1}{2c-3}$.

Note, ainda, que $c \neq 0$ e $c \neq 1$, pois isto implicaria, respectivamente, em $3p-1 = 0$ e $3p-1 = 2p-2$, ambas sem solução para p primo.

Considere a função $f : [2, \infty) \to \mathbb{R}$ dada por $f(x) = \dfrac{2x-1}{2x-3}$. Derivando esta função obtemos $f'(x) = -\dfrac{4}{(2x-3)^2} < 0$. Conclui-se, portanto, que f é decrescente. Note que $f(2) = 3$, $f(3) = \dfrac{5}{3} < 2$ e $f(x) < 2$ para $x > 3$, pois f é decrescente.

Portanto, o único primo na imagem da função f é o número 3 e, consequentemente, $p = \dfrac{2c-1}{2c-3}$ é o número primo 3 apenas para $c = 2$. Mas havíamos suposto $p \neq 3$. Desta contradição conclui-se que $\varphi(3p)$ não divide $(3p-1)$. □

Vejamos agora o produto de dois primos distintos maiores que 3.

Para fazer esta análise, e inspirados pela prova do lema anterior, consideraremos a família de funções

$$f_p(x) : [2, \infty) \to \mathbb{R}, \qquad f_p(x) = \frac{x(p-1)-1}{x(p-1)-p}$$

onde p é um inteiro, $p \geq 5$.

Lema 3.3.3. *Fixado p, $f_p(x)$ é função decrescente de x; fixado x, $f_p(x)$ é função decrescente de p. Ademais,*

$$2 < f_p(2) \leq \frac{7}{3} < 3 \qquad \textit{e} \qquad 1 < f_p(3) \leq \frac{11}{7} < 2$$

Demonstração. Note que podemos reescrever $f_p(x)$ na forma $f_p(x) = 1 + \dfrac{1}{x - \dfrac{p}{p-1}}$.

Derivando f_p obtemos $f_p'(x) = -\dfrac{1}{\left(x - \dfrac{p}{p-1}\right)^2} < 0$ e conclui-se que, para cada p, $f_p(x)$ é uma função decrescente.

Agora, sejam q_1 e q_2 dois primos com $5 < q_1 < q_2$. Para cada x fixo, tem-se que $\dfrac{1}{x - \dfrac{q_1}{q_1-1}} > \dfrac{1}{x - \dfrac{q_2}{q_2-1}}$, ou seja, para cada x fixo vale $f_{q_1}(x) > f_{q_2}(x)$.

Note também que para $p = 5$ tem-se $f_5(2) = \frac{7}{3} < 3$ e $f_5(3) = \frac{11}{7} < 2$. Portanto não há nenhum primo na imagem de f_5, pois f_5 é decrescente.

Como para cada x fixo $f_{q_1}(x) > f_{q_2}(x)$ para $q_1 < q_2$ primos, tem-se que $f_p(x) < 2$ para $5 \leq p$ primo e $x \geq 3$ e, consequentemente, não há nenhum primo na imagem de nenhuma das funções f_p para p primo e $p \geq 5$ e $x \geq 3$.

Resta analisar se para $x = 2$ alguma função da família f_p possui algum primo em sua imagem.

Note que $f_p(2) < f_5(2) = \frac{7}{3} < 3$; por outro lado,

$$2 < f_p(2) = 1 + \frac{1}{2 - \frac{p}{p-1}} \Leftrightarrow \frac{p}{p-1} > 1,$$

o que e verdade dado que $p \geq 5$. Portanto temos de fato $2 < f_p(2) < 3$ (e assim a imagem dessa função não contém nenhum primo). □

Estamos assim em posição de enunciar e provar o próximo resultado:

Lema 3.3.4. *Seja $n = p_1p_2$ com $5 \leq p_1 < p_2$ primos; então $\varphi(n)$ não é divisor de $n - 1$.*

Demonstração. Seja $n = p_1p_2$ para $5 \leq p_1 < p_2$.

Para $n = p_1p_2$ temos $\phi(p_1p_2) = (p_1 - 1)(p_2 - 1)$ e, $n - 1 = p_1p_2 - 1$. Suponha que $\phi(p_1p_2) \mid (p_1p_2 - 1)$, então existe $c \in \mathbb{N}$ tal que $p_1p_2 - 1 = c(p_1 - 1)(p_2 - 1)$.

Note que $c \neq 0$ e $c \neq 1$ pois $c = 0$ ou $c = 1$ implicariam, respectivamente, em $p_1p_2 - 1 = 0$ e $p_1 + p_2 = 2$, ambas contradições.

De $p_1p_2 - 1 = c(p_1 - 1)(p_2 - 1)$ temos $(cp_1 - c - p_1)p_2 + (1 + c - cp_1) = 0$, e esta equação é válida se $cp_1 - c - p_1 = 0$ e $1 + c - cp_1 = 0$ ou se $p_2 = \frac{cp_1 - c - 1}{cp_1 - c - p_1}$. Vamos analisar estes casos:

Se $cp_1 - c - p_1 = 0$ e $1 + c - cp_1 = 0$ simultaneamente, então somando-se as duas equações temos $p_1 = 1$, que é uma contradição.

Se $p_2 = \frac{cp_1 - c - 1}{cp_1 - c - p_1}$ e este quociente não é exato, então temos um absurdo pois p_2 é natural.

Se $p_2 = \frac{cp_1 - c - 1}{cp_1 - c - p_1} = \frac{c(p_1 - 1) - 1}{c(p_1 - 1) - p_1}$ é um número inteiro, considere a família de funções $f_p : [2, \infty) \to \mathbb{R}$ dada por $f_p(x) = \frac{x(p-1) - 1}{x(p-1) - p}$. Estamos então tentanto obter um ponto inteiro c no qual $p_2 = f_{p_1}(c)$, com $c \geq 2$.

Do exposto no Lema 3.3.3, $p_2 = \frac{cp_1 - c - 1}{cp_1 - c - p_1}$ não é primo, pois o lado direito da igualdade não é primo, independentemente do primo p_1 e do natural c que se escolha, e temos portanto uma contradição.

Em todos os casos a contradição surgiu de considerarmos que existia $c \in \mathbb{N}$ tal que $p_1p_2 - 1 = c(p_1 - 1)(p_2 - 1)$. Isto mostra que tal c não existe e portanto $\varphi(p_1p_2)$ não divide $p_1p_2 - 1$.

□

Conclui-se portanto que a conjectura de Lehmer vale para o produto de dois primos distintos.

3.3.2 Produto de três primos distintos

Nesse caso procuramos c inteiro tal que $p_1p_2p_3 - 1 = c(p_1 - 1)(p_2 - 1)(p_3 - 1)$, que é equivalente a

$$p_1p_2p_3 - 1 = c[p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3 + p_1 + p_2 + p_3 - 1].$$

Note que $c \neq 0$ e $c \neq 1$, pois $c = 0$ ou $c = 1$ implicariam, respectivamente, em $p_1p_2p_3 - 1 = 0$ e $p_1p_2 + p_1p_3 + p_2p_3 = p_1 + p_2 + p_3$. Mas, no lado esquerdo cada termo está multiplicado por um número primo que é no mínimo 2, logo o lado esquerdo é no mínimo
$2p_1 + 2p_2 + 2p_3$ e a igualdade impossível. Logo c deve ser maior ou igual a 2.

Reescrevendo a igualdade acima e isolando p_3 temos, por analogia ao caso com dois primos, $[(c - 1)p_1p_2 - cp_1 - cp_2 + c]p_3 + [-cp_1p_2 + cp_1 + cp_2 - c + 1] = 0$.

Uma solução seria ter os dois colchetes iguais a zero, mas o primeiro não pode ser zero, pois isso já é o caso para primos p_1 e p_2. Portanto nos resta saber se há $c \geq 2$ tal que $p_3 = \dfrac{(p_1p_2 - p_1 - p_2 + 1)c - 1}{(p_1p_2 - p_1 - p_2 + 1)c - p_1p_2}$.

Para mostrar que p_3 não pode ser primo vamos precisar de algumas funções.

Família de funções auxiliares

Considere a família de funções $f_{p_1,p_2} : [2, \infty) \to \mathbb{R}$ definida por

$$f_{p_1,p_2}(x) = \frac{(p_1p_2 - p_1 - p_2 + 1)x - 1}{(p_1p_2 - p_1 - p_2 + 1)x - p_1p_2}.$$

Vamos mostrar que dentro de uma mesma família de curvas (p_1 fixo) e para cada $x \in \mathbb{N}$, $x \geq 2$ (fixo), as curvas da família "decrescem" conforme p_2 cresce.

Mais precisamente, fixe p_1 primo e $x \in \mathbb{N}$, $x \geq 2$, e considere os primos p_j e p_k com $3 \leq p_1 < p_j < p_k$, vamos mostrar que $f_{p_1,p_j}(x) > f_{p_1,p_k}(x)$.

Considere $f_{p_1,p_k}(x)$ e note que existe $\theta \in \mathbb{N}$ tal que $p_k = p_j + \theta$, então

$$\begin{aligned} f_{p_1,p_k}(x) &= \frac{(p_1p_k - p_1 - p_k + 1)x - 1}{(p_1p_k - p_1 - p_k + 1)x - p_1p_k} \\ &= \frac{(p_1p_j - p_1 - p_j + 1)x - 1}{(p_1p_j + p_1\theta - p_1 - p_j - \theta + 1)x - p_1(p_j + \theta)} \\ &+ \frac{\theta(p_1 - 1)x}{(p_1p_j + p_1\theta - p_1 - p_j - \theta + 1)x - p_1(p_j + \theta)} \end{aligned}$$

Evidentemente, $\theta(p_1-1)x > 0$ e note que $(p_1p_j+p_1\theta-p_1-p_j-\theta+1)x-p_1(p_j+\theta) = [(p_1p_j - p_1 - p_j + 1)x - p_1p_j] + [\theta(p_1 - 1)x - \theta p_1]$.

Também note que $\theta(p_1 - 1)x - \theta p_1 = \theta[p_1(x - 1) - x]$ e que $p_1(x - 1) - x > 0$, pois $p_1(x-1)-x = p_1(x-1)-(x-1)-1 = (x-1)(p_1-1)-1 > 0$ uma vez que $2 \leq x$ e $3 \leq p_1$.

Portanto, $\dfrac{\theta(p_1 - 1)x}{(p_1p_j + p_1\theta - p_1 - p_j - \theta + 1)x - p_1(p_j + \theta)} > 0$ e segue que

$$\begin{aligned} f_{p_1,p_k}(x) &< \frac{(p_1p_j - p_1 - p_j + 1)x - 1}{(p_1p_j + p_1\theta - p_1 - p_j - \theta + 1)x - p_1(p_j + \theta)} \\ &< \frac{(p_1p_j - p_1 - p_j + 1)x - 1}{(p_1p_j - p_1 - p_j + 1)x - p_1p_j} = f_{p_1,p_j}(x) \end{aligned}$$

Agora, vamos mostrar que qualquer curva de uma dada família sempre está acima ou abaixo do que qualquer curva de outra família, ou seja, que não há intersecção entre as curvas de famílias distintas.

Mais precisamente, vamos mostrar que $f_{p_i,p_j} > f_{p_k,p_l}$ para primos p_i, p_j, p_k, p_l com $p_i < p_k < p_l$ e p_j qualquer.

Já sabemos que dentro de uma mesma família as curvas são decrescentes, portanto a curva "mais baixa" ocorre quando $p_j \to \infty$. Sendo assim, basta comparar essa curva limite com as curvas da próxima família.

Vamos encontrar uma curva limite para cada família de funções.

Considere $f_{p_i,p_j}(x)$ com p_i fixo. Calculando $f_{p_i,p_j}(x)$ para $p_j \to \infty$ temos

$$\begin{aligned} \lim_{p_j\to\infty} f_{p_i,p_j}(x) &= \lim_{p_j\to\infty} \left(1 + \frac{1}{\dfrac{(p_i - 1)(p_j - 1)x}{p_ip_j - 1} - \dfrac{p_ip_j}{p_ip_j - 1}} \right) \\ &= \frac{(p_i - 1)x}{(p_i - 1)x - p_i} \end{aligned}$$

Chamando $f_{p_i}(x) = \lim_{p_j \to \infty} f_{p_i,p_j}(x)$ temos $f_{p_i}(x) = \dfrac{(p_i-1)x}{(p_i-1)x - p_i}$.

Agora, suponha que existam duas curvas de famílias distintas que se toquem, ou seja, que existam primos p_i, p_k, p_l com $p_i < p_k < p_l$ e $x \geq 2$ tais que $f_{p_k,p_l}(x) = f_{p_i}(x)$. Então para estes valores de p_i, p_k, p_l, x ocorre $\dfrac{(p_k-1)(p_l-1)x-1}{(p_k-1)(p_l-1)x - p_k p_l} = \dfrac{(p_i-1)x}{(p_i-1)x-p_i}$.

Esta expressão é equivalente a $[p_i(p_k+p_l-2) - p_k p_l + 1]x + p_i = 0$ e conclui-se que, se há interseção, então esta ocorre uma única vez (um único ponto) e para o valor de x dado por $x = \dfrac{-p_i}{p_i(p_k+p_l-2) - p_k p_l + 1}$.

Agora, note que

$$\begin{aligned} p_i(p_k+p_l-2) - p_k p_l + 1 &> p_i(p_k+p_l-2) - p_k p_l \\ &\geq p_i[p_k + (p_k+2) - 2] - p_k p_l \\ &> p_i(2p_i - p_l). \end{aligned}$$

Portanto, conclui-se que $|x| < \dfrac{p_i}{p_i|2p_i - p_l|} < 1$ e, consequentemente, $x < 1$, gerando uma contradição pois tínhamos assumido $x \geq 2$.

Isto prova que não há interseção entre as famílias de curvas, e sendo estas contínuas, uma família sempre estará acima da outra. Como esta afirmação vale para quaisquer valores de primos $p_i < p_k < p_l$ e qualquer $x \geq 2$, então $f_{p_i}(x) > f_{p_k,p_l}(x)$ ou $f_{p_i}(x) < f_{p_k,p_l}(x)$ para qualquer $x \geq 2$.

Para saber qual das duas desigualdades é verdadeira basta comparar duas famílias quaisquer para uma dado valor de x com $x \geq 2$, por exemplo, vamos comparar $f_{5,7}(2)$ com $f_3(2)$.

Por um cálculo simples obtemos $f_3(2) = 4$ e $f_{5,7}(2) = \dfrac{47}{13} < 4$.

Portanto, para primos $p_i < p_k < p_l$ e qualquer $x \geq 2$, tem-se $f_{p_i}(x) > f_{p_k,p_l}(x)$, isto é, uma família de curvas sempre está acima da outra para qualquer valor de $x \geq 2$.

Voltando à conjectura de Lehmer para $n = p_1p_2p_3$ com $2 < p_1 < p_2 < p_3$ e considerando $f_{p_1,p_2}(x) = \dfrac{(p_1p_2 - p_1 - p_2 + 1)x - 1}{(p_1p_2 - p_1 - p_2 + 1)x - p_1p_2}$ tem-se que para $p_1 = 3$ e $p_2 = 5$, $f_{3,5}(x) = \dfrac{8x-1}{8x-15}$ e nota-se facilmente que $f_{3,5}(4) = \dfrac{31}{17} < 2$. Portanto, se algum primo estiver na imagem de $f_{3,5}$ isto deve ocorrer para $x = 2$ ou $x = 3$. Calculando, obtem-se $f_{3,5}(2) = 15$ e $f_{3,5}(3) = \dfrac{23}{8}$ logo não há primos na imagem de $f_{3,5}$.

Do exposto sobre as famílias de funções $f_{p_k,p_l}(x)$ segue que, se algum primo estiver na imagem da família $f_{3,q}$ com $q > 5$, então isto deve ocorrer para $x = 2$ ou

$x = 3$.

Calculando $f_3(x) = \lim_{q\to\infty} f_{3,q}(x)$ obtemos $f_3(x) = \dfrac{2x}{2x-3}$, e nota-se que $f_3(3) = 2$. Portanto nenhum dos números $f_{3,q}(3)$ será primo, pois $2 < f_{3,5}(3) < 3$ e $f_3(x)$ é a curva mais baixa da família $f_{3,q}$.

Calculando, obtém-se $f_{3,7}(2) = \dfrac{23}{3}$, $f_{3,11}(2) = \dfrac{39}{7}$,$f_{3,13}(2) = \dfrac{47}{9}$ e $f_{3,17}(2) = \dfrac{63}{13}$. Como $f_{3,17}(2) < 5$ e $f_3(2) = 4$ conclui-se que não há nenhum primo na imagem da família $f_{3,q}$.

Vamos analisar a família $f_{5,p}$.

Um cálculo rápido mostra que $f_{5,7}(3) = \dfrac{71}{37} < 2$ portanto não haverá primo na imagem das curvas $f_{p_1,p}(x)$ para nenhum $p_1 > 5$ e $x \geq 3$, e consequentemente se houver algum primo na imagem da família $f_{5,p}(x)$ este deve ocorrer para $f_{5,p}(2)$.

Um cálculo rápido mostra que $3 < f_{5,7}(2) = \dfrac{47}{13} < 4$, $3 < f_{5,11}(2) = \dfrac{79}{25} < 4$, $3 < f_{5,13}(2) = \dfrac{95}{31} < 4$ e $f_{5,17}(2) = \dfrac{127}{43} < 3$. Além disso, $f_5(x) = \dfrac{4x}{4x-5}$ e $2 < f_5(2) = \dfrac{8}{3} < 3$. Segue destes cálculos que não há primo na imagem da família $f_{5,p}(x)$ para $p > 7$.

Vamos analisar a família $f_{7,p}$.

Como $f_{5,7}(3) = \dfrac{71}{37} < 2$ segue que se houver algum primo na imagem da família $f_{7,p}$, este ocorrerá para $x = 2$. Note que $f_{7,11}(2) = \dfrac{119}{43} < 3$.

Note também que $f_{p_i}(x) = \dfrac{(p_i-1)x}{(p_i-1)x - p_i}$ e se chamarmos $f(x) = \lim_{p_i\to\infty} f_{p_i}(x)$, então $f(x) = \dfrac{x}{x-1}$ e $f(2) = 2$.

Segue, das análises acima, que não há primo em nenhuma imagem de nenhuma das funções $f_{p_1,p_2}(x)$ com $2 < p_1 < p_2$ e $x \geq 2$.

3.3.3 Desenvolvimentos futuros

Os métodos utilizados até aqui são diferentes dos métodos usados por Lehmer. Em [12], Lehmer utilizou aritmética modular e desigualdades para obter os resultados. Contas preliminares apontam que não é possível utilizar uma indução finita para concluir a validade da conjectura para o produto de um número qualquer de primos. Num momento futuro pretende-se estender a demonstração para o caso $n = p_1p_2\ldots p_k$ utilizando algumas das ideias apresentadas neste trabalho juntamente com algumas ferramentas mais sofisticadas de Teoria de Números, encerrando o problema.

Referências Bibliográficas

[1] Barata, João. Notas de aula. Disponível em: $< http://denebola.if.usp.br/ >$. Acesso em 05 de novembro de 2015.

[2] Bertlmann, R. A.; Krammer, P. Bloch vectors for qudits. (2008) Disponível em: $< https://arxiv.org/abs/0806.1174 >$. Acessado em 12 de dezembro de 2017.

[3] Botelho, Geraldo; Pellegrino, Daniel; Teixeira, Eduardo. Fundamentos de Análise Funcional. (2015) Editora SBM.

[4] Chamon, Claudio; Hamma, Alioscia; Mucciolo, Eduardo R. Emergent Irreversibility and Entanglement Spectrum Statistics. Physical Review Letters. 2014.

[5] Cohen, Graeme L.; Hagis, Peter, jun. (1980). "On the number of prime factors of n if $\varphi(n)$ divides $n-1$. Nieuw Arch. Wiskd., III. Ser. 28: 177–185.

[6] Chen, Jianxin; Duan, Runyao; Ji, Zhengfeng; Ying, Mingsheng; Yu, Jun. Existence of Universal Entangler. Journal of Mathematical Physics 49. 2008.

[7] Duistermaat, J. J.; Kolk, J. A.C. Lie Groups. Springer. 2000.

[8] Feng, Wang; MingXing, Luo; XiuBo, Chen; YiXian Yang; XiaoJun, Wang. Typical universal entanglers. Science China. October 2014. Vol 57, No 10, 1913-1917.

[9] Hognas, Goran; Mukherjea, Arunava. Probability Measures on Semigroups. Second Edition. Springer. 2011.

[10] Kimura, Gen. The Bloch Vector for N-Level Systems. Disponível em: $< https://arxiv.org/abs/quant-ph/0301152 >$. Acesso em 15 de outubro de 2017.

[11] Kimura, Gen; Kossakowski, Andrzej. The Bloch-vector space for N-level systems. Disponível em: $< https://arxiv.org/abs/quant-ph/0408014 >$. Acesso em 29 de setembro de 2017.

[12] Lehmer, D. H. "On Euler's totient function". Bulletin of the American Mathematical Society (1932).

[13] Loomis, Lynn. An Introduction to Abstract Harmonic Analysis. D. van Nostrand and Co. 2013.

[14] Mendaš, Istok P. Classification and time evolution of density matrices for a N-state system. Journal of Mathematical Physics. 2008.

[15] Mendes, F. V.; Ramos, R. V. Numerical search for universal entanglers in $C^3 \otimes C^4$ and $C^4 \otimes C^4$. Physics Letters A, 379, 2015, 289-292.

[16] Milies, Cesar Polcino. Números: uma introdução à Matemática. EDUSP. 2013.

[17] Munkres, James R. Topology. Pearson. Second Edition. 2000.

[18] Nielsen, Michael A.; Chuang, Issac. L. Quantum Computation and Quantum Information. Cambridge University Press. 2010.

[19] Ozols, Maris; Mancinska, Laura. Generalized Bloch Vector and the Eigenvalues of a Density Matrix. Disponível em: $< http : //home.lu.lv/ \sim sd20008/papers/Bloch\%20Vectors\%20and\%20Eigenvalues.pdf >$. Acessado em 11 de setembro de 2017.

[20] Viana, Marcelo; Krerley, Oliveira. Fundamentos da Teoria Ergodica. Coleção Fronteiras da Matemática. Editora SBM. 2014.

[21] Yan, Song Y. Number Theory for Computing. Second Edition. Springer. 2002.