



Douglas Soares Gonçalves

# Métodos Matemáticos em Tomografia de Estados Quânticos

CAMPINAS  
2013





UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA  
E COMPUTAÇÃO CIENTÍFICA

Douglas Soares Gonçalves

Métodos Matemáticos em  
Tomografia de Estados Quânticos

Orientador(a): Profa. Dra. Márcia Aparecida Gomes Ruggiero

Coorientador(a): Prof. Dr. Carlile Campos Lavor

Tese de doutorado apresentada ao Instituto de Matemática,  
Estatística e Computação Científica da UNICAMP para  
obtenção do título de **Doutor em Matemática Aplicada**.

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE  
DEFENDIDA PELO ALUNO **Douglas Soares Gonçalves**  
E ORIENTADA PELA PROFA. DRA. **Márcia Aparecida Gomes Ruggiero**.

  
Márcia Aparecida Gomes Ruggiero

  
Carlile Campos Lavor

CAMPINAS  
2013

FICHA CATALOGRÁFICA ELABORADA POR  
MARIA FABIANA BEZERRA MULLER - CRB8/6162  
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E  
COMPUTAÇÃO CIENTÍFICA - UNICAMP

Gonçalves, Douglas Soares, 1982-  
G586m Métodos matemáticos em tomografia de estados quânticos /  
Douglas Soares Gonçalves. – Campinas, SP : [s.n.], 2013.

Orientador: Márcia Aparecida Gomes Ruggiero.  
Coorientador: Carlile Campos Lavor.  
Tese (doutorado) – Universidade Estadual de Campinas,  
Instituto de Matemática, Estatística e Computação Científica.

1. Otimização matemática. 2. Métodos numéricos. 3.  
Tomografia de estados quânticos. 4. Informação quântica. I.  
Ruggiero, Márcia Aparecida Gomes, 1956-. II. Lavor, Carlile  
Campos, 1968-. III. Universidade Estadual de Campinas. Instituto de  
Matemática, Estatística e Computação Científica. IV. Título.

Informações para Biblioteca Digital

**Título em inglês:** Mathematical methods in quantum state tomography

**Palavras-chave em inglês:**

Mathematical optimization

Numerical methods

Quantum state tomography

Quantum information

**Área de concentração:** Matemática Aplicada

**Titulação:** Doutor em Matemática Aplicada

**Banca examinadora:**

Márcia Aparecida Gomes Ruggiero [Orientador]

Sandra Augusta Santos

Amir Ordacgi Caldeira

Reinaldo Oliveira Vianna

Renato Portugal

**Data de defesa:** 22-02-2013

**Programa de Pós-Graduação:** Matemática Aplicada

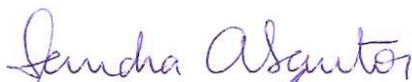
**Tese de Doutorado defendida em 22 de fevereiro de 2013 e aprovada**

**Pela Banca Examinadora composta pelos Profs. Drs.**



---

**Prof(a). Dr(a). MÁRCIA APARECIDA GOMES RUGGIERO**



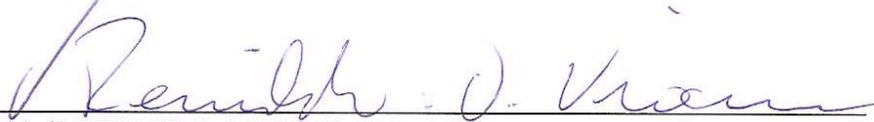
---

**Prof(a). Dr(a). SANDRA AUGUSTA SANTOS**



---

**Prof(a). Dr(a). AMIR ORDACGI CALDEIRA**



---

**Prof(a). Dr(a). REINALDO OLIVEIRA VIANNA**



---

**Prof(a). Dr(a). RENATO PORTUGAL**



*Aos meus pais,  
Carlos e Rosa.*



# Agradecimentos

A Deus por iluminar meu caminho.

À toda minha família pelo suporte e incentivo. Aos meus pais, Carlos e Rosa, pela educação e por me fazer acreditar no trabalho e na perseverança. Aos meus irmãos Diógenes e Danilo pela amizade e o constante apoio.

À Ana Carolina Franciosi Luchetti pela companhia, carinho e compreensão.

À professora Márcia Ruggiero pelos ensinamentos, pela amizade e por acreditar em meu trabalho desde a graduação. Sinto-me honrado em ter sido seu orientando e aprendido muito com ela ao longo dos últimos 7 anos.

Ao professor Carlile Lavor por me propor o projeto para este doutorado. Agradeço pelo desafio proposto, pela confiança e pelo otimismo para me fazer seguir em frente, frente a águas desconhecidas. Sou grato por contar com sua amizade e seu apoio.

À professora Sandra Santos pela colaboração e amizade.

Ao professor Caio Azevedo pela parceria na parte de Inferência Bayesiana e estatística.

Ao professor Reinaldo Oliveira Vianna, por ter possibilitado duas visitas ao Grupo de Informação Quântica da UFMG. Agradeço pela oportunidade, pelas ideias e reflexões que contribuíram para melhorar este trabalho. Também ao Thiago Maciel e ao André Cesário, orientandos do professor Reinaldo, pela amizade e por me ajudarem tanto nos aspectos teóricos quanto computacionais do problema.

Ao professor Paulo Henrique Souto Ribeiro, por me proporcionar um estágio junto ao Grupo de Ótica Quântica da UFRJ. Sem dúvida, sua colaboração foi fundamental para o bom desenvolvimento desta tese. Agradeço também ao seu orientando, agora doutor, Osvaldo Jimenez Farias, por toda ajuda em tomografia de estados quânticos durante minha estadia em terras cariocas.

Por falar em carioca, também agradeço ao Celso F. Araújo, pela hospitalidade, pela amizade e por ter sido meu guia na cidade maravilhosa.

Aos meus amigos da pós-graduação e da vida, em especial a Leandro Prudente, Thadeu Alves Senne, José Araújo Neto, Marcus Nascimento, Juliana Sartori,

---

pela força, motivação, discussões matemáticas e de buteco. Também aos amigos e colegas do Laboratório de Pesquisa Operacional e Otimização (LPOO), pela amizade e “suporte técnico incondicional”. Em particular, Abel Siqueira, Wanderson Luiz, Luiz Rafael dos Santos, Raniere Gaia e Hector Flores.

Aos meus irmãos de aluguel, da Rep Ponta Firme. Um lugar por vezes sujo, sempre desorganizado, mas que se tornou minha segunda casa graças a vocês: Fabiano Gonçalves Lopes (Compatriota), Rafael Alkmin Reis (Varginha), Gustavo Nogueira (Lixeira), Rodrigo Ferraresso (Rudão), André Celarino (Alemão), Ademar Nakamoto (Tio Dema) e Renato Luchetti.

Agradeço também a todos os companheiros do Ludens S.A.

Aos meus amigos de Itapira, em especial: Guilherme Valdo Faria, Cléverson Pelluzzi, Emílio Rafael Poletto, Atílio Marchesini Júnior, Dude e Kauê Turcati de Freitas.

À UNICAMP e ao IMECC pela qualidade de ensino e o suporte à pesquisa.

A todos os professores do Departamento de Matemática Aplicada que contribuíram para minha formação e aprimoramento, em especial aos professores do Grupo de Otimização.

À Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) pelo apoio financeiro (Processo: 2009/08027-0).

## Resumo

A preparação, manipulação e caracterização de sistemas quânticos são tarefas essenciais para a computação quântica. Em Tomografia de Estados Quânticos, o objetivo é encontrar uma estimativa para a matriz de densidade, associada a um ensemble de estados quânticos identicamente preparados, baseando-se no resultado de medições. Este é um importante procedimento em computação e informação quântica, sendo aplicado, por exemplo, para verificar a fidelidade de um estado preparado ou em tomografia de processos quânticos. Nesta tese, estudamos métodos matemáticos aplicados aos problemas que surgem na reconstrução de estados quânticos. Na estimação por Máxima Verossimilhança, apresentamos dois métodos para a resolução dos problemas de otimização dessa abordagem. O primeiro se baseia em uma reparametrização da matriz de densidade e, neste caso, provamos a equivalência das soluções locais do problema de otimização irrestrita associado. No segundo, relacionado à verossimilhança multinomial, demonstramos a convergência global do método sob hipóteses mais fracas que as da literatura. Apresentamos também duas formulações para o caso de tomografia com um conjunto incompleto de medidas: Máxima Entropia e Tomografia Quântica Variacional. Propusemos uma nova formulação para a segunda, de modo a apresentar propriedades mais parecidas às da Máxima Entropia, mantendo a estrutura de um problema de programação semidefinida linear. Para outros problemas de otimização sobre o espaço de matrizes de densidade além do problema da Tomografia de Estados Quânticos, apresentamos um método de Gradiente Projetado que mostrou-se efetivo em testes numéricos preliminares. Por fim, discutimos sobre a implementação de inferência Bayesiana, através de métodos Monte Carlo via cadeias de Markov, no problema de estimação da matriz de densidade.

**Palavras-chave:** Tomografia de Estados Quânticos, Máxima Verossimilhança, reparametrização, mínimos locais, algoritmo  $R\rho R$ , convergência global, medidas incompletas, Máxima Entropia, Tomografia Quântica Variacional, Programação Semidefinida, Gradiente Projetado, inferência Bayesiana, Monte Carlo via cadeias de Markov.



# Abstract

Preparation, manipulation and characterization of quantum states are essential tasks for quantum computation. In Quantum State Tomography, the aim is to find an estimate for the density matrix associated to an ensemble of identically prepared quantum systems, based on the measurement outcomes. This is an important procedure in quantum information and computation applied for instance, to verify the fidelity of a prepared state or in quantum process tomography. In this thesis we study mathematical methods applied to problems that raise from the reconstruction of quantum states. In the Maximum Likelihood Estimation we present two methods to solve the optimization problems of this approach. The first one is based on a reparameterization of the density matrix and, in this case, we prove the equivalence of local solutions of the related unconstrained optimization problem. In the second one, related to multinomial likelihoods, we prove the global convergence of the method under weaker assumptions than those of literature. We also discuss two formulations to the case of quantum state tomography with incomplete measurements: Maximum Entropy and Variational Quantum Tomography. We propose a new formulation for the second one in order to have a similar behavior to the Maximum Entropy approach, keeping the linear semidefinite positive programming structure. Furthermore, in order to solve other optimization problems over the density matrices space besides the Quantum State Tomography, we present a Projected Gradient method which shows a good performance in preliminary numerical tests. We also briefly talk about the implementation of a Bayesian inference scheme, through Monte Carlo Markov chains methods, to the density matrix estimation problem.

**Keywords:** Quantum State Tomography, Maximum Likelihood, reparameterization, local minimizers,  $R\rho R$  algorithm, global convergence, incomplete measurements, Maximum Entropy, Variational Quantum Tomography, Semidefinite Programming, Projected Gradient, Bayesian inference, Monte Carlo Markov chains.



# Sumário

Agradecimentos	ix
Resumo	xi
<b>1 Introdução</b>	<b>1</b>
<b>2 Fundamentos de Mecânica Quântica</b>	<b>5</b>
2.1 Espaço de Estados . . . . .	6
2.1.1 Exemplo: o q-bit . . . . .	6
2.2 Evolução . . . . .	7
2.3 Medições Quânticas . . . . .	8
2.3.1 Distinguindo estados quânticos . . . . .	9
2.3.2 Medições Projetivas . . . . .	10
2.3.3 Medições POVM . . . . .	11
2.4 Sistemas compostos . . . . .	12
2.4.1 Emaranhamento . . . . .	12
2.5 O operador de densidade . . . . .	12
2.5.1 Ensemble de estados quânticos . . . . .	13
2.5.2 Propriedades do operador de densidade . . . . .	14
2.5.3 Convexidade do espaço de matrizes de densidade . . . . .	15
2.5.4 Traço Parcial e Operador de Densidade Reduzido . . . . .	16
2.6 Quão próximos são dois estados quânticos? . . . . .	17
2.6.1 Distância de traço . . . . .	17
2.6.2 Fidelidade . . . . .	18
<b>3 Tomografia de Estados Quânticos</b>	<b>21</b>
3.1 Método padrão: Inversão Linear . . . . .	21
3.1.1 Tomografia de múltiplos q-bits . . . . .	24
3.1.2 Inversão Linear, caso geral . . . . .	24
3.2 Garantindo uma matriz física . . . . .	26
3.3 Um problema de inferência . . . . .	27
3.4 Quadrados mínimos . . . . .	27
3.4.1 Derivadas parciais em $t$ . . . . .	29

3.5	Máxima Verossimilhança . . . . .	30
3.6	Inferência Bayesiana . . . . .	31
3.7	Máxima Entropia . . . . .	32
3.7.1	Conjunto incompleto de medições . . . . .	32
<b>4</b>	<b>Máxima Verossimilhança</b>	<b>35</b>
4.1	Mudança de Variáveis e Minimizadores locais . . . . .	36
4.1.1	Parametrização da Matriz de Densidade . . . . .	37
4.1.2	A aplicação $\rho(t)$ e o conjunto viável $\mathcal{S}$ . . . . .	40
4.1.3	Resultado principal: os minimizadores locais são globais . . . . .	45
4.1.4	Experimentos Numéricos . . . . .	46
4.1.5	Conclusões desta seção . . . . .	50
4.2	Algoritmo $R\rho R$ e Convergência Global . . . . .	51
4.2.1	Convergência global de algoritmos de subida . . . . .	54
4.2.2	Convergência global do $R\rho R$ Diluído . . . . .	56
4.2.3	Exemplos . . . . .	62
4.2.4	Conclusões desta seção . . . . .	64
4.3	Estimativa de erros e matriz de Fisher . . . . .	64
4.3.1	O Método Delta . . . . .	66
4.4	Resumo do Capítulo 4 . . . . .	68
<b>5</b>	<b>Tomografia com um conjunto incompleto de medidas</b>	<b>69</b>
5.1	Máxima Entropia . . . . .	70
5.2	Tomografia Quântica Variacional . . . . .	72
5.3	VQT, Medições da autobase e MaxEnt . . . . .	73
5.4	Dados com ruído e MaxLik-MaxEnt . . . . .	76
5.5	Simulações Numéricas . . . . .	77
5.6	Máxima Entropia e falso emaranhamento . . . . .	80
5.7	Resumo do Capítulo 5 . . . . .	81
<b>6</b>	<b>Gradiente projetado</b>	<b>83</b>
6.1	Algoritmo de Gradiente Projetado . . . . .	84
6.2	Projeção no espaço de Matrizes de Densidade . . . . .	84
6.2.1	Decomposição Espectral . . . . .	85
6.2.2	Projeção no Simplex de probabilidade . . . . .	86
6.3	Experimentos Numéricos . . . . .	88
6.4	Resumo do Capítulo 6 . . . . .	90
<b>7</b>	<b>Inferência Bayesiana</b>	<b>91</b>
7.1	Tomografia Quântica Bayesiana . . . . .	92
7.2	Monte Carlo via Cadeias de Markov . . . . .	93
7.2.1	Metropolis-Hastings . . . . .	94
7.2.2	Distribuição proposta . . . . .	94

---

7.2.3	Distribuição a priori . . . . .	97
7.3	Burn-in e diagnósticos de convergência . . . . .	97
7.3.1	Burn-in . . . . .	97
7.3.2	Diagnósticos de convergência . . . . .	98
7.4	Um breve exemplo . . . . .	102
7.5	Resumo do Capítulo 7 . . . . .	103
<b>8</b>	<b>Conclusões e Trabalhos Futuros</b>	<b>105</b>
8.1	Contribuições da tese . . . . .	105
8.2	Trabalhos futuros . . . . .	106
8.3	Considerações Finais . . . . .	107



# Notações

$I$	Matriz/Operador identidade
$\text{tr}(A)$	Traço da matriz $A$
$A^\dagger$	Transposta conjugada de $A$
$\ A\ _F$	Norma de Frobenius de $A$ , $\text{tr}(A^\dagger A) = \ A\ _F^2$
$\rho$	Matriz de densidade
$\rho \succeq 0$	$\rho$ é uma matriz semidefinida positiva
$\mathcal{S}$	Espaço das matrizes de densidade, $\mathcal{S} = \{\rho \mid \rho = \rho^\dagger, \text{tr}(\rho) = 1, \rho \succeq 0\}$
$\text{int}(\mathcal{S})$	Interior de $\mathcal{S}$ , $\text{int}(\mathcal{S}) = \{\rho \in \mathcal{S} \mid \rho \succ 0\}$
$n_i$	Número de ocorrências da saída experimental $i$
$E_i$	Elemento POVM, associado ao resultado $i$
$\mathcal{L}(\rho)$	Função de verossimilhança, $\mathcal{L}(\rho) = P(n \rho)$ probabilidade dos dados $n$ dado $\rho$
$\pi_0(\rho)$	Distribuição a priori de $\rho$
$\pi(\rho)$	Distribuição a posteriori de $\rho$
$\propto$	Proporcional a (igual a, a menos de uma constante)
$\langle Z \rangle$	Valor esperado do observável $Z$
$\mathbf{E}(X)$	Valor esperado da variável aleatória $X$
$\mathcal{P}_\Omega(\rho)$	Projeção ortogonal de $\rho$ em $\Omega$
	No Capítulo 2, refere-se ao tempo.
$t$	Nas Seções 3.2, 4.1 representa um vetor de parâmetros. Na Seção 4.2 representa o tamanho de passo.
***	Notações específicas em Mecânica Quântica serão introduzidas no Capítulo 2.



# Capítulo 1

## Introdução

Em Tomografia de Estados Quânticos (TEQ), o objetivo é encontrar uma estimativa para a *matriz de densidade*, associada a um *ensemble* de estados quânticos identicamente preparados, baseando-se no resultado de medições [46, 73]. Este é um importante procedimento em computação e informação quântica [26, 48, 69], sendo aplicado, por exemplo, para verificar a fidelidade de um estado preparado [69] ou em tomografia de processos quânticos [56].

O *estado quântico* de um sistema, seja ele representado por um operador/matriz de densidade, um vetor de estado, ou uma função de quasi-probabilidade no espaço de fases, pode ser interpretado como a descrição matemática do conhecimento que temos sobre um sistema quântico [73]. A questão é que a interpretação física do estado quântico não é tão transparente [15]. De acordo com Peres [74]: “Não há nenhuma evidência física de que todo sistema físico tenha, a todo instante, um estado bem definido... Do ponto de vista da teoria quântica, esses símbolos matemáticos (vetores de estados) representam informações estatísticas que nos permitem calcular probabilidades de ocorrência de certos eventos.” Assim, qualquer procedimento de reconstrução do operador densidade (ou equivalente matemático) nada mais é que uma estimação *a posteriori*, de tal operador associado ao sistema quântico, baseada em dados obtidos após se medir certas propriedades específicas do sistema.

Em sistemas clássicos, o estado do sistema é um conjunto de valores que descrevem certas propriedades do sistema. A princípio, é sempre possível, através de múltiplas medições, recuperar completamente o estado de um sistema clássico. Em sistemas quânticos, tal procedimento não é mais possível, devido aos fundamentos da mecânica quântica, sobretudo sua linearidade e o princípio de incerteza de Heisenberg [40].

Sabe-se que ao realizar uma medição sobre um sistema quântico, o mesmo é projetado em um de seus estados prováveis, sendo portanto impossível realizar uma sequência de medições sem interferir na dinâmica do sistema. Portanto, é impossível, com uma única cópia, determinar o estado do sistema. Além disso, o teorema da não-clonagem [98]

proíbe a produção de várias cópias do sistema quântico desconhecido para posterior determinação de seu estado.

Porém, se houver uma fonte que gere sistemas quânticos em um mesmo estado, é possível reconstruir o estado em questão através da Tomografia de Estados Quânticos (TEQ): um procedimento experimental onde um *ensemble* de estados quânticos desconhecidos, mas identicamente preparados, é caracterizado por uma sequência de medições, em diferentes bases [73].

Além do planejamento do experimento para se obter um conjunto tomograficamente completo de medidas, rotinas de pós processamento são necessárias para recuperar as informações contidas nos resultados de medições. Algumas abordagens se baseiam na inversão direta dos dados [96] enquanto outras se apoiam em métodos estatísticos [12, 15, 47, 48].

O termo *tomografia*, emprestado da medicina, foi primeiramente usado em reconstrução de estados quânticos por Vogel e Risken [96], que trataram o problema de reconstrução de estados quânticos como um caso particular da transformada de Radon usada em tomografia de Raio-X. Observou-se que as distribuições de probabilidade obtidas pela detecção homodina correspondem a transformadas de Radon da função de Wigner.

Desde então o problema de reconstrução de estados quânticos recebeu inúmeras contribuições tanto do ponto de vista experimental quanto teórico, e o resultado disso é uma diversidade de métodos para tomografia em variáveis discretas e contínuas.

Este trabalho tem como objetivo analisar os principais métodos de tomografia, entendendo sua motivação a partir dos fundamentos da Mecânica Quântica. Além disto, pretendemos realizar um estudo de um ponto de vista mais matemático, dando ênfase aos problemas de otimização que aparecem nas diferentes metodologias. Não faz parte do escopo desta tese, a descrição de toda a coletânea de métodos para tomografia de estados quânticos, nem tampouco discutir em profundidade os aspectos físicos de tal problema.

A contribuição desta tese está na aplicação de nosso conhecimento matemático, sobretudo em métodos computacionais de otimização, ao problema de tomografia de estados quânticos. Nosso objetivo é melhorar as abordagens existentes, em termos de eficiência e confiabilidade. Tais abordagens, normalmente, recaem em problemas de quadrados mínimos não lineares [33, 52, 58] ou problemas de programação cônica convexa [9, 14, 100], como programação semidefinida [22, 92].

Os aspectos teóricos de otimização, condições de otimalidade e métodos numéricos contam com uma literatura bem consolidada [8, 14, 54, 59, 70], à qual por vezes nos referimos ao longo do texto e que pode auxiliar na leitura deste trabalho.

---

No Capítulo 2, apresentamos os fundamentos da Mecânica Quântica necessários ao entendimento do problema. O Capítulo 3 é dedicado ao problema de tomografia de estados quânticos e uma breve revisão dos principais métodos.

A primeira abordagem a aparecer na literatura foi a inversão linear [73,96], baseada na inversão da regra de Born, onde as probabilidades preditas pela mecânica quântica são igualadas a frequências experimentais normalizadas. Contudo, devido ao ruído experimental, a matriz reconstruída pode não corresponder a um estado físico. Para garantir que a matriz estimada seja válida, precisamos restringi-la ao espaço de matrizes Hermitianas semidefinidas positivas e de traço um.

Uma das alternativas à inversão linear, que incorpora um modelo estatístico para os ruídos e as restrições para a matriz de densidade, é a Estimção por Máxima Verossimilhança, que é discutida no Capítulo 4. Apresentamos dois métodos para resolução do problema de Máxima Verossimilhança.

O primeiro trata das restrições de positividade e de traço unitário através de uma mudança de variáveis [48]. Tal mudança leva a um problema de otimização irrestrito, porém não convexo. Na literatura [2, 48, 91], considerava-se que os mínimos locais provenientes desta reformulação poderiam ser não-globais, o que representaria uma dificuldade nessa abordagem. Nossa contribuição na Seção 4.1 é mostrar que todos esses mínimos locais são globais [36], validando assim o uso da reparametrização proposta [48].

O segundo, tratado na Seção 4.2, é um método específico [46,47] para quando a verossimilhança advem de uma distribuição multinomial. Este método explora a estrutura particular do problema e garante que a cada iteração as restrições de positividade e traço unitário serão preservadas. No entanto, em [79], os autores provam a convergência global do método com a hipótese de busca linear exata, que em geral é uma hipótese muito forte na prática. Nossa principal contribuição na Seção 4.2 é provar a convergência do método usando busca linear inexata, que é uma hipótese mais fraca, e mais viável na prática.

O Capítulo 5, discute a TEQ quando não temos um conjunto informacionalmente completo de medidas. Neste caso, a estimativa para o estado quântico pode não ser determinada unicamente. Analisamos duas abordagens para tomografia com um conjunto incompleto de medidas: estimação de Máxima Entropia [15] e a Tomografia Quântica Variacional (VQT) [55]. A primeira busca a estimativa compatível com as medidas disponíveis e que maximiza a entropia de von Neumann, enquanto a segunda busca a estimativa que minimiza um certo tipo de energia associada às medidas faltantes. Além de uma comparação entre essas duas abordagens do ponto de vista das probabilidades associadas às medidas faltantes, na Seção 5.3 propomos uma modificação na formulação

VQT para que tenha um comportamento mais parecido com a MaxEnt mas preserve a estrutura de um SDP linear. Simulações numéricas validaram o propósito dessa nova formulação.

No Capítulo 6, apresentamos um método de Gradiente Projetado, para problemas de otimização sobre o espaço de matrizes de densidade. Ao contrário dos capítulos anteriores onde os problemas de otimização surgiam da TEQ, neste capítulo discutimos um método geral para minimizar/maximizar funções restritas às matrizes Hermitianas semidefinidas positivas e de traço um. Em particular, apresentamos alguns testes numéricos, aplicando o Gradiente Projetado no problema tomografia por Máxima Verossimilhança, que mostraram a eficácia desse método em comparação com um método específico para TEQ.

O Capítulo 7 traz um discussão sobre inferência Bayesiana aplicada ao problema de Tomografia de Estados Quânticos. Discutimos aspectos de sua implementação através de uma parametrização da matriz de densidade e técnicas de integração Monte Carlo via Cadeias de Markov (MCMC). Um exemplo prático ilustra que a estimativa Bayesiana média garante estimativas para a matriz de densidade de posto completo e consistente com barras de erro, calculadas a partir das amostras geradas pela cadeia de Markov.

Considerações finais, um resumo das contribuições dessa tese e trabalhos futuros estão no Capítulo 8.

## Capítulo 2

# Fundamentos de Mecânica Quântica

A Mecânica Quântica é a teoria física que descreve a mecânica de partículas microscópicas e suas interações com a radiação eletromagnética. No início do século XX, a física clássica não era capaz de explicar certos fenômenos como a radiação do corpo negro ou a catástrofe ultravioleta [72]. Ao longo das primeiras décadas daquele século, a busca por uma explicação para certos fenômenos a níveis atômicos culminou no desenvolvimento da Mecânica Quântica [69, 74].

A seguir, são apresentados os postulados da mecânica quântica, sob uma perspectiva mais matemática, seguindo a notação de Nielsen e Chuang [69]. Tais postulados estabelecem a conexão entre o mundo físico e o formalismo matemático da mecânica quântica.

A Tabela 2.1 apresenta a notação usada na descrição dos postulados da mecânica quântica.

Notação	Descrição
$z^*$	Complexo conjugado do número complexo $z$
$ \psi\rangle$	Vetor. Também conhecido como <i>ket</i> .
$\langle\psi $	Vetor dual para $ \psi\rangle$ . Também conhecido como <i>bra</i> .
$\langle\varphi \psi\rangle$	Produto interno entre os vetores $ \varphi\rangle$ e $ \psi\rangle$ .
$ \varphi\rangle \otimes  \psi\rangle$	Produto tensorial de $ \varphi\rangle$ e $ \psi\rangle$ .
$ \varphi\rangle \psi\rangle$	Abreviação para o produto tensorial de $ \varphi\rangle$ e $ \psi\rangle$ .
$A^*$	Complexo conjugado da matriz $A$ .
$A^T$	Transposta da matriz $A$ .
$A^\dagger$	Hermitiana conjugada ou adjunta da matriz $A$ , $A^\dagger = (A^T)^*$ .
$\langle\varphi A \psi\rangle$	Produto interno entre $ \varphi\rangle$ e $A \psi\rangle$ , ou equivalentemente entre $A^\dagger \varphi\rangle$ e $ \psi\rangle$ .
$\text{tr}(A)$	Traço de $A$ .

Tabela 2.1: Resumo de algumas notações usadas em mecânica quântica.

## 2.1 Espaço de Estados

O primeiro postulado estabelece a arena onde atua a mecânica quântica [69].

**Postulado 1.** *Associado a todo sistema físico isolado está um espaço vetorial complexo munido de produto interno (espaço de Hilbert), chamado espaço de estados. O estado do sistema é completamente descrito por seu vetor de estado  $|\psi\rangle$ , um vetor unitário ( $\langle\psi|\psi\rangle = 1$ ) no espaço de estados.*

### 2.1.1 Exemplo: o q-bit

Nosso exemplo usual será o *q-bit*. O q-bit tem um espaço de estados bidimensional. Suponha que  $|0\rangle$  e  $|1\rangle$  formam uma base ortonormal para este espaço. Então, um *vetor de estados* arbitrário deste espaço é escrito na forma

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.1)$$

onde  $\alpha$  e  $\beta$  são escalares complexos denominados *amplitudes de probabilidade*.

Em verdade, o q-bit corresponde à representação de um sistema físico de dois níveis, tais como o spin 1/2 de alguma partícula, a polarização de um fóton, um átomo de dois níveis ou estados eletrônicos e vibracionais de um íon, por exemplo.

Diferente de um bit clássico, o qual sempre estará em um estado bem definido, 0 ou 1, o q-bit se encontra em uma *superposição* dos estados  $|0\rangle$  e  $|1\rangle$ . Os valores  $|\alpha|^2$  e  $|\beta|^2$  correspondem às probabilidades de se encontrar o q-bit nos estados  $|0\rangle$  e  $|1\rangle$ , respectivamente. A *condição de normalização*  $\langle\psi|\psi\rangle = 1$  nos leva a  $|\alpha|^2 + |\beta|^2 = 1$ .

O q-bit também difere do bit probabilístico (p-bit) já que (2.1) é definido por amplitudes ao invés de probabilidades. A grosso modo, a diferença é que amplitudes se somam (interferem), mas probabilidades não. [17, 57].

Uma figura que nos auxilia na interpretação de sistemas quânticos de dois níveis (q-bits) é a chamada esfera de Bloch.

Como  $|\alpha|^2 + |\beta|^2 = 1$ , podemos reescrever a equação (2.1) como

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle.$$

Os valores  $\theta$  e  $\varphi$  definem um ponto na esfera unitária tridimensional, como mostra a Figura 2.1.1. Apesar de ser uma interpretação útil, sobretudo para testar ideias sobre operadores atuando sobre um q-bit, não há uma generalização simples da esfera de Bloch para múltiplos q-bits.

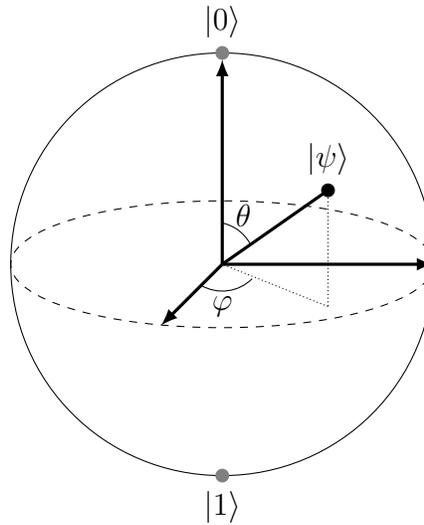


Figura 2.1: Representação de um q-bit na esfera de Bloch

## 2.2 Evolução

O segundo postulado diz respeito à evolução do sistema ao longo do tempo.

**Postulado 2.** *A evolução de um sistema físico fechado é descrita por uma transformação unitária, ou seja, o estado do sistema  $|\psi\rangle$  em um instante  $t_0$  está relacionado com o estado do sistema  $|\psi'\rangle$  em um instante  $t_1$  através de um operador unitário  $U(t_0, t_1)$ , tal que*

$$|\psi'\rangle = U|\psi\rangle.$$

Uma pergunta óbvia é: quais operadores unitários devem ser considerados? No caso de um q-bit, *qualquer* operador unitário pode ser realizado.

Exemplos de tais operadores são as conhecidas *matrizes de Pauli*:

$$\begin{aligned} \sigma_0 = I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \sigma_1 = X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_2 = Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, & \sigma_3 = Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned}$$

Outro operador que aparece com frequência em computação quântica é o *operador de Hadamard*:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

O Postulado 2 descreve a evolução de um sistema físico em dois instantes de tempo distintos. Uma versão mais refinada deste postulado trata da evolução do sistema em

tempo contínuo.

**Postulado 2'.** A evolução de um sistema físico fechado é descrita pela equação de Schrödinger

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle,$$

onde  $\hbar$  é a constante de Planck e  $H$  é um operador Hermitiano conhecido como Hamiltoniano do sistema fechado.

Mas qual a relação entre a equação de Schrödinger e a evolução unitária do Postulado 2?

Basta olhar para a solução da equação de Schrödinger

$$|\psi(t_1)\rangle = \exp\left[\frac{-iH(t_1 - t_0)}{\hbar}\right] |\psi(t_0)\rangle.$$

Assim, temos que

$$|\psi(t_1)\rangle = U(t_0, t_1)|\psi(t_0)\rangle,$$

onde

$$U(t_0, t_1) = \exp\left[\frac{-iH(t_1 - t_0)}{\hbar}\right]$$

é uma *matriz unitária* que depende apenas de  $t_0$  e  $t_1$ .

É fácil ver que  $U = \exp(iK)$  é uma matriz unitária quando  $K$  é Hermitiana. De fato, considerando a decomposição espectral de  $K = Q\Lambda Q^\dagger$ , temos

$$\exp(iK) = \exp(iQ\Lambda Q^\dagger) = Q \exp(i\Lambda) Q^\dagger.$$

Logo,

$$U^\dagger U = Q \exp(i\Lambda)^* Q^\dagger Q \exp(i\Lambda) Q^\dagger = Q \exp(i\Lambda)^* \exp(i\Lambda) Q^\dagger = Q Q^\dagger = I.$$

## 2.3 Medições Quânticas

O postulado anterior diz que um sistema físico *fechado* evolui através de transformações unitárias. Porém, às vezes, o cientista e seu equipamento experimental tem que interferir neste sistema para saber o que se passa lá dentro, e com isso, o sistema deixa de ser fechado e não está mais sujeito a evolução unitária. Os efeitos de medições em sistemas quânticos são tratados pelo Postulado 3.

**Postulado 3.** Medições quânticas são descritas por uma coleção de operadores de medição  $\{M_m\}$  que atuam sobre o espaço de estados do sistema a ser medido. O índice

$m$  representa um dos possíveis resultados do experimento. Se o estado do sistema antes da medição é  $|\psi\rangle$ , então a probabilidade de ocorrer o resultado  $m$  é dada por

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle,$$

e o estado do sistema após a medição é

$$|\psi^m\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}.$$

Os operadores de medição satisfazem a relação de completude:

$$\sum_m M_m^\dagger M_m = I.$$

Um exemplo simples é a medição de um q-bit na base computacional. Tal medição é definida por dois operadores de medição  $M_0 = |0\rangle\langle 0|$  e  $M_1 = |1\rangle\langle 1|$ . Observe que tais operadores satisfazem a relação de completude. Na verdade, a relação de completude expressa o fato de que as probabilidades devem somar um. Suponha que o estado a ser medido é  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Então a probabilidade de se obter o resultado 0 (antes da medição) é

$$p(0) = \langle \psi | M_0^\dagger M_0 | \psi \rangle = \langle \psi | 0 \rangle \langle 0 | \psi \rangle = |\alpha|^2,$$

e sendo este o caso, após a medição o estado do sistema será

$$\frac{M_0 |\psi\rangle}{|\alpha|} = \frac{|0\rangle\langle 0 | \psi \rangle}{|\alpha|} = \frac{\alpha}{|\alpha|} |0\rangle.$$

Note que se o resultado da medição foi 0, então o sistema colapsou no estado  $|0\rangle$ .

### 2.3.1 Distinguindo estados quânticos

Uma importante aplicação do Postulado 3 é o problema de distinguir estados quânticos. No mundo clássico, a distinção de estados de objetos parece trivial, por exemplo, sabemos claramente se uma moeda está virada do lado da cara ou coroa. Porém, na mecânica quântica, as coisas são mais complicadas. Veremos a seguir que estados quânticos não-ortogonais não podem ser distinguidos.

Usaremos a metáfora padrão de um jogo entre os personagens Alice e Bob. Alice escolhe um estado  $|\psi_i\rangle$  ( $1 \geq i \geq n$ ) dentre  $n$  estados possíveis. Então, Alice entrega o estado  $|\psi_i\rangle$  para Bob, cuja tarefa é identificar o índice  $i$  do estado recebido.

Se os estados forem ortogonais, então Bob é capaz de identificá-los da seguinte forma. Primeiro, são definidos os operadores de medição  $M_i = |\psi_i\rangle\langle \psi_i|$ , um para cada possível índice  $i$  e em seguida,  $M_0 = \sqrt{I - \sum_{i \neq 0} |\psi_i\rangle\langle \psi_i|}$ . Tais operadores satisfazem a relação

de completude e, se o estado  $|\psi_i\rangle$  é preparado, então  $p(i) = \langle\psi_i|M_i^\dagger M_i|\psi_i\rangle = \langle\psi_i|M_i|\psi_i\rangle = 1$ , isto é, o resultado  $i$  ocorre com certeza.

Por outro lado, se dois estados  $|\psi_1\rangle$  e  $|\psi_2\rangle$  são não ortogonais, então não existe operadores de medição capazes de distinguir tais estados. Isso ocorre porque  $|\psi_2\rangle$  pode ser decomposto em uma componente paralela e outra ortogonal a  $|\psi_1\rangle$ ,  $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$ , com  $\langle\psi_1|\varphi\rangle = 0$ .

Quando Bob realizar medidas sobre o sistema para discriminar  $|\psi_1\rangle$  de  $|\psi_2\rangle$ , o resultado poderá ser uma projeção sobre o estado ortogonal ou uma projeção sobre o estado paralelo a  $|\psi_1\rangle$ . Se o resultado for uma projeção sobre o estado ortogonal a  $|\psi_1\rangle$ , Bob saberá que trata-se de  $|\psi_2\rangle$ , mas quando o resultado for uma projeção sobre o estado paralelo, a medida pode ter sido realizada tanto sobre  $|\psi_1\rangle$  quanto  $|\psi_2\rangle$ .

### 2.3.2 Medições Projetivas

Como um caso especial do Postulado 3 (medições generalizadas), temos as medições projetivas.

**Definição 2.3.1** (Medições Projetivas). *Um observável  $M$  é um operador Hermitiano que atua sobre o espaço de estados do sistema observado. O observável tem decomposição espectral*

$$M = \sum_m m P_m,$$

onde  $P_m$  é projetor ortogonal sobre o autoespaço de  $M$  associado ao autovalor  $m$ .

Os resultados possíveis da medição correspondem aos autovalores do observável. Ao medir o estado  $|\psi\rangle$ , a probabilidade de se obter o resultado  $m$  é

$$p(m) = \langle\psi|P_m|\psi\rangle,$$

e o estado posterior do sistema será

$$|\psi^m\rangle = \frac{P_m|\psi\rangle}{\sqrt{p(m)}}.$$

Medições projetivas apresentam propriedades interessantes. Por exemplo, é fácil de se obter o valor esperado para medições projetivas:

$$\mathbf{E}(M) = \sum_m m p(m) = \sum_m m \langle\psi|P_m|\psi\rangle = \langle\psi| \sum_m m P_m |\psi\rangle = \langle\psi|M|\psi\rangle.$$

Essa fórmula é muito útil e frequentemente denotada por  $\langle M \rangle = \langle\psi|M|\psi\rangle$ . Com isso, podemos também derivar a expressão para a variância

$$(\Delta M)^2 = \langle(M - \langle M \rangle)^2\rangle = \langle M^2 \rangle - \langle M \rangle^2.$$

### 2.3.3 Medições POVM

A configuração do aparato experimental para uma certa medição pode também ser descrita por um conjunto de elementos POVM (*Positive Operator Value Measure*) ou operadores de medida a valores positivos.

**Definição 2.3.2** (POVM). *Um conjunto de operadores  $\{E_m\}$  tais que*

$$i) E_m \text{ é operador positivo } ( \langle \psi | E_m | \psi \rangle \geq 0, \forall |\psi\rangle )$$

$$ii) \sum_m E_m = I$$

$$iii) p(m) = \langle \psi | E_m | \psi \rangle$$

*é chamado conjunto POVM.*

Note que na definição de medições POVM, não é considerado o estado do sistema após a medição. Exatamente por isso, o POVM é normalmente empregado em situações onde o estado pós-medição não é relevante.

Um exemplo de medição POVM são as medições projetivas ( $E_m = P_m^\dagger P_m = P_m$ ).

Um outro exemplo muito interessante, e relacionado à discriminação de estados quânticos, envolve nossos protagonistas Alice e Bob. Suponha que Alice entregou a Bob um q-bit preparado em um dos estados  $|\psi_1\rangle = |0\rangle$  ou  $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ . Como explicado anteriormente, é impossível para Bob afirmar com certeza qual estado  $|\psi_1\rangle$  ou  $|\psi_2\rangle$  lhe foi dado. Porém, é possível realizar medições que às vezes distinguem os estados, mas nunca havendo um erro de identificação.

Considere o POVM de três elementos

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1 + \sqrt{2}} |1\rangle\langle 1|, \\ E_2 &= \frac{\sqrt{2}}{1 + \sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}, \\ E_3 &= I - E_1 - E_2. \end{aligned}$$

Suponha que Bob esteja com o estado  $|\psi_1\rangle = |0\rangle$ . Neste caso, o resultado não pode ser  $E_1$ , pois  $\langle \psi_1 | E_1 | \psi_1 \rangle = 0$ . Assim, se o resultado da medição foi  $E_1$ , Bob pode seguramente afirmar que está com o estado  $|\psi_2\rangle$ . Um raciocínio análogo pode ser aplicado ao elemento POVM  $E_2$ . No entanto, Bob pode obter algumas vezes o resultado  $E_3$  e, neste caso, ele nada pode afirmar sobre o estado do q-bit.

## 2.4 Sistemas compostos

O quarto postulado nos diz como descrever o estado de um sistema composto.

**Postulado 4.** *O espaço de estados de uma sistema físico composto é o produto tensorial dos espaços de estados dos sistemas componentes. Mais ainda, se enumeramos os sistemas componentes  $1 \leq i \leq n$  e o sistema  $i$  é preparado no estado  $|\psi_i\rangle$ , então o estado geral do sistema composto é  $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ .*

O Postulado 4 nos permite definir uma das mais interessantes e estranhas ideias associadas a sistemas quânticos compostos, o *emaranhamento*.

Considere o estado de dois q-bits

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Este estado, conhecido como estado de Bell, tem uma propriedade notável: ele não pode ser obtido do produto tensorial de nenhum par de q-bits  $|a\rangle$  e  $|b\rangle$ , ou seja,  $|\psi\rangle \neq |a\rangle \otimes |b\rangle = |a\rangle|b\rangle$ ,  $\forall |a\rangle, |b\rangle$ . Dizemos que o estado de um sistema composto com essa propriedade é um *estado emaranhado*.

### 2.4.1 Emaranhamento

Fisicamente falando, o emaranhamento é uma propriedade de um sistema quântico com duas ou mais partes, em que as partes estão ligadas de tal forma que a descrição de uma das partes não pode ser adequadamente realizada sem a completa caracterização das demais, independentemente da distância que as separa.

O assunto iniciou-se com o famoso artigo de Einstein, Podolsky e Rosen [25], conhecido como paradoxo EPR e o termo *emaranhamento* apareceu em uma carta de Schrödinger [82] para descrever a interação entre as partes de um sistema quântico. Embora estes estudos iniciais tenham discutido as propriedades contra-intuitivas dos estados emaranhados, aos poucos, este fenômeno foi reconhecido como uma característica de sistema quânticos e, recentemente, como um dos principais recursos para a computação quântica [69].

## 2.5 O operador de densidade

Podemos descrever a mecânica quântica de forma alternativa usando, no lugar de vetores de estado, o *operador de densidade* ou *matriz de densidade*.

As duas formulações são matematicamente equivalentes. Porém, a abordagem através de matrizes de densidade fornece uma linguagem mais conveniente para descrever os cenários mais comuns em mecânica quântica.

### 2.5.1 Ensemble de estados quânticos

O operador de densidade fornece uma descrição conveniente de sistemas quânticos onde o estado *não é completamente* conhecido. Suponha que um sistema quântico está em um de vários estados  $|\psi_i\rangle$  ( $1 \leq i \leq n$ ), com probabilidade  $p_i$ . Dizemos que  $\{p_i, |\psi_i\rangle\}_{i=1}^n$  é um *ensemble de estados puros*.

O *operador de densidade* para tal sistema é então definido por

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$

Um sistema quântico cujo estado  $|\psi\rangle$  é conhecido *exatamente* é chamado de um *estado puro* e, neste caso, seu operador de densidade é  $\rho = |\psi\rangle \langle \psi|$ . Por outro lado,  $\rho$  estará em um *estado misto* quando seu *ensemble* for uma *mistura* de diferentes estados puros.

Pode-se mostrar que, para um estado puro,  $\text{tr}(\rho^2) = 1$ , enquanto que para estados mistos,  $\text{tr}(\rho^2) < 1$ .

Os postulados da mecânica quântica podem ser reformulados na linguagem do operador de densidade (matriz de densidade).

O Postulado 2 nos diz que a evolução do estado de um sistema quântico se dá através de uma transformação unitária  $U$ . Assim, se um sistema encontra-se no estado  $|\psi_i\rangle$  com probabilidade  $p_i$ , após a evolução, estará no estado  $U|\psi_i\rangle$  com probabilidade  $p_i$ , logo:

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle \langle \psi_i| U^\dagger = U \rho U^\dagger.$$

As medições também podem ser descritas em termos do operador de densidade. Suponha que uma medição é descrita por operadores  $M_m$  e que o estado inicial é  $|\psi_i\rangle$ . Então, a probabilidade de se obter o resultado  $m$  é:

$$p(m|i) = \langle \psi_i | M_m^\dagger M_m | \psi_i \rangle = \text{tr}(M_m^\dagger M_m |\psi_i\rangle \langle \psi_i|),$$

e por resultados de probabilidade

$$p(m) = \sum_i p(m|i) p_i = \sum_i p_i \text{tr}(M_m^\dagger M_m |\psi_i\rangle \langle \psi_i|) = \text{tr}(M_m^\dagger M_m \rho).$$

Se o estado inicial foi  $|\psi_i\rangle$ , então o estado do sistema após obter-se o resultado  $m$  é:

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle}}.$$

Assim, o operador de densidade do sistema após o resultado  $m$  é dado por:

$$\rho_m = \sum_i p(i|m) |\psi_i^m\rangle \langle \psi_i^m| = \sum_i p(i|m) \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle},$$

e como  $p(i|m) = p(m, i)/p(m) = p(m|i)p_i/p(m)$ , temos que

$$\rho_m = \sum_i p_i \frac{M_m |\psi_i\rangle \langle \psi_i| M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)} = \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}.$$

## 2.5.2 Propriedades do operador de densidade

O operador de densidade foi introduzido como um meio de descrever *ensembles* de estados quânticos. O resultado a seguir caracteriza matematicamente os operadores de densidade.

**Teorema 2.5.1** (Caracterização dos operadores de densidade). *Um operador Hermitiano  $\rho$  é um operador de densidade associado a algum ensemble  $\{p_i, |\psi_i\rangle\}_{i=1}^n$  se e somente se satisfaz as condições:*

1.  $\text{tr}(\rho) = 1$  (condição do traço);
2.  $\langle \varphi | \rho | \varphi \rangle \geq 0$ ,  $\forall |\varphi\rangle$ ,  $\rho$  é um operador positivo (condição de positividade).

**Prova.** Seja  $\{p_i, |\psi_i\rangle\}_{i=1}^n$  um *ensemble*. Então, por definição, o operador de densidade associado é dado por

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|.$$

Claramente vemos que  $\rho$  é Hermitiano. Além disso, para qualquer  $|\varphi\rangle$  temos que:

$$\langle \varphi | \rho | \varphi \rangle = \langle \varphi | \left( \sum_i p_i |\psi_i\rangle \langle \psi_i| \right) | \varphi \rangle = \sum_i p_i |\langle \varphi | \psi_i \rangle|^2 \geq 0.$$

Além disso

$$\text{tr}(\rho) = \text{tr} \left( \sum_i p_i |\psi_i\rangle \langle \psi_i| \right) = \sum_i p_i \text{tr}(|\psi_i\rangle \langle \psi_i|) = \sum_i p_i \langle \psi_i | \psi_i \rangle = \sum_i p_i = 1.$$

Por outro lado, seja  $\rho$  um operador Hermitiano positivo semidefinido e de traço um. Sendo  $\rho$  Hermitiano, pelo teorema espectral temos que:

$$\rho = \sum_i \lambda_i |\varphi_i\rangle \langle \varphi_i|,$$

onde  $\lambda_i$ 's são autovalores de  $\rho$  associados aos autovetores ortonormais  $|\varphi_i\rangle$ 's. Como  $\rho$  é positivo, tem-se que  $\lambda_i \geq 0$  para todo  $i$  e, como  $\text{tr}(\rho) = 1$ , então  $\sum_i \lambda_i = 1$ . Portanto,

associado a  $\rho$ , temos um *ensemble* de estados  $\{\lambda_i, |\varphi_i\rangle\}_{i=1}^n$ . ■

Com essa caracterização, podemos agora reformular os postulados da mecânica quântica em termos do operador de densidade:

**Postulado 1.** Associado a todo sistema físico isolado está um espaço vetorial com produto interno (espaço de Hilbert) chamado *espaço de estados*. O estado do sistema é completamente descrito por seu *operador de densidade*, que é um operador  $\rho$  positivo e de traço um. Se um sistema está em um estado  $\rho_i$  com probabilidade  $p_i$ , então seu operador de densidade é  $\sum_i p_i \rho_i$ .

**Postulado 2.** A evolução de um sistema quântico *fechado* é descrita por uma *transformação unitária*. Isto é, o estado  $\rho$  do sistema no tempo  $t_0$  está relacionado com o estado  $\rho'$  do sistema no tempo  $t_1$  por um operador unitário  $U$  que depende apenas de  $t_0$  e  $t_1$ :

$$\rho' = U\rho U^\dagger.$$

**Postulado 3.** Medições quânticas são descritas por uma coleção  $\{M_m\}$  de *operadores de medição*. Tais operadores atuam no espaço de estados do sistema a ser medido. O índice  $m$  diz respeito a um possível resultado do experimento. Se o estado do sistema quântico é  $\rho$ , imediatamente antes da medição, então a probabilidade de ocorrer o resultado  $m$  é

$$p(m) = \text{tr}(M_m^\dagger M_m \rho),$$

e o estado do sistema após a medição será

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\text{tr}(M_m^\dagger M_m \rho)}.$$

Os operadores de medição satisfazem a *relação de completude*

$$\sum_m M_m^\dagger M_m = I.$$

**Postulado 4.** O espaço de estados de um sistema físico composto é o *produto tensorial* dos espaços de estados dos sistemas componentes. Assim, se os sistemas componentes numerados de  $1 \leq i \leq n$  são preparados em estados  $\rho_i$ , então o estado do sistema composto é  $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ .

### 2.5.3 Convexidade do espaço de matrizes de densidade

De agora em diante, denotaremos por  $\mathcal{S}$  o espaço das matrizes de densidade

$$\mathcal{S} = \{ \rho \mid \rho = \rho^\dagger, \text{tr}(\rho) = 1, \rho \succeq 0 \},$$

onde  $\rho \succeq 0$  denota que  $\rho$  pertence ao cone convexo das matrizes Hermitianas semidefinidas positivas [14].

Uma importante propriedade de  $\mathcal{S}$ , e que usaremos com frequência neste texto, é que  $\mathcal{S}$  é um conjunto convexo. De fato, dadas  $A$  e  $B$  matrizes de densidade e  $\alpha \in [0, 1]$ , temos que:

$$\langle \psi | \alpha A + (1 - \alpha) B | \psi \rangle = \alpha \langle \psi | A | \psi \rangle + (1 - \alpha) \langle \psi | B | \psi \rangle \geq 0, \quad \forall |\psi\rangle.$$

Além disso,

$$\text{tr}(\alpha A + (1 - \alpha) B) = \alpha \text{tr}(A) + (1 - \alpha) \text{tr}(B) = \alpha + 1 - \alpha = 1.$$

Logo,  $\alpha A + (1 - \alpha) B$  também é matriz de densidade.

Com isso, mostramos a convexidade do conjunto das matrizes de densidade  $\mathcal{S}$ , propriedade relevante no contexto dos problemas de otimização que surgem em Tomografia de Estados Quânticos, já que a maioria deles consiste em minimizar uma certa distância estatística sobre  $\mathcal{S}$ .

### 2.5.4 Traço Parcial e Operador de Densidade Reduzido

Uma das principais aplicações de operadores de densidade é como uma ferramenta para descrição de subsistemas de sistemas compostos. Tal descrição é fornecida pelo operador de densidade reduzido.

Suponha que tenhamos um sistema físico de duas partes A e B, cujo estado é descrito pelo operador  $\rho^{AB}$ . O operador de densidade reduzido para o sistema A é definido por

$$\rho^A = \text{tr}_B(\rho^{AB}),$$

onde  $\text{tr}_B(\cdot)$  denota o traço parcial, definido por

$$\text{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = (\text{tr}(|b_1\rangle\langle b_2|))|a_1\rangle\langle a_2| = \langle b_1|b_2\rangle|a_1\rangle\langle a_2|.$$

Assim, se temos um sistema com a componente A no estado  $\rho$  e a componente B no estado  $\sigma$ , o estado do sistema é  $\rho^{AB} = \rho \otimes \sigma$  e, então,

$$\rho^A = \text{tr}_B(\rho^{AB}) = \text{tr}_B(\rho \otimes \sigma) = \text{tr}(\sigma) \rho = \rho,$$

como esperado.

Agora, considere um sistema em um estado de Bell  $(|00\rangle + |11\rangle)/\sqrt{2}$ . A matriz de densidade é dada por:

$$\begin{aligned} \rho &= \left( \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) \left( \frac{\langle 00| + \langle 11|}{\sqrt{2}} \right) \\ &= \frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}. \end{aligned}$$

Ao calcular o operador de densidade reduzido para o primeiro componente, obtemos

$$\rho^1 = \text{tr}_2(\rho) = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2}.$$

Note que, apesar do sistema conjunto estar em um estado puro, o qual conhecemos exatamente, a primeira componente está em um estado misto, o qual não temos um conhecimento pleno. Esta estranha propriedade é outra marca do emaranhamento quântico.

## 2.6 Quão próximos são dois estados quânticos?

Nesta seção, são definidos dois conceitos de proximidade (“distância”) entre estados quânticos: *distância de traço* e *fidelidade*. Tais métricas são importantes na prática, pois frequentemente deseja-se saber o quão próximo de um estado teórico conhecido está o estado obtido experimentalmente. Em nosso contexto, servirão também como medida de qualidade da solução do processo de reconstrução de estados quânticos.

### 2.6.1 Distância de traço

**Definição 2.6.1.** A *distância de traço* entre dois estados quânticos  $\rho$  e  $\sigma$  é definida por

$$D(\rho, \sigma) = \frac{1}{2} \text{tr}|\rho - \sigma|,$$

onde  $|A| = \sqrt{A^\dagger A}$ .

Note que se  $\rho$  e  $\sigma$  comutam, então a distância de traço entre  $\rho$  e  $\sigma$  se reduz à distância entre os autovalores de  $\rho$  e  $\sigma$ :

$$\rho = \sum_i r_i |i\rangle\langle i|, \quad \sigma = \sum_i s_i |i\rangle\langle i|,$$

para alguma base ortonormal  $|i\rangle$ . Logo,

$$D(\rho, \sigma) = \frac{1}{2} \text{tr} \left| \sum_i (r_i - s_i) |i\rangle\langle i| \right| = \frac{1}{2} \sum_i |r_i - s_i| = D(r_i, s_i).$$

Uma maneira de entender melhor a distância de traço é pensar no caso de um q-bit e sua representação na esfera de Bloch. Suponha que  $\rho$  e  $\sigma$  tenham os vetores de Bloch  $\vec{r}$  e  $\vec{s}$ :

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \quad \sigma = \frac{I + \vec{s} \cdot \vec{\sigma}}{2},$$

onde  $\vec{r} \cdot \vec{\sigma} = r_1\sigma_1 + r_2\sigma_2 + r_3\sigma_3$ .

Calculando a distância de traço, temos:

$$D(\rho, \sigma) = \frac{1}{2} \text{tr}|\rho - \sigma| = \frac{1}{4} \text{tr}|(\vec{r} - \vec{s}) \cdot \vec{\sigma}| = \frac{|\vec{r} - \vec{s}|}{2}.$$

Isto é, a distância de traço entre dois q-bits corresponde à metade da distância Euclidiana entre eles na esfera de Bloch.

Tal interpretação ajuda a entender (e aceitar) melhor algumas propriedades da distância de traço. Por exemplo, se rotacionarmos a esfera de Bloch, esperamos que a distância entre os q-bits  $\rho$  e  $\sigma$  sejam mantidas, o que nos induz a pensar que a distância de traço é invariante por transformações unitárias (de fato, é).

Outra propriedade muito importante da distância de traço é:

$$D(\rho, \sigma) = \max_P \text{tr}(P(\rho - \sigma)),$$

onde a maximização é sobre todos os operadores de medições projetivas  $P$  ou sobre todos os elementos POVM. Assim, a distância de traço é interpretada como o máximo da diferença entre as probabilidades de que um resultado associado a  $P$  ocorra em  $\rho$  ou em  $\sigma$ .

Portanto, se dois operadores de densidade são próximos na distância de traço, então qualquer medição sobre esses estados quânticos fornecerá distribuições de probabilidade que estarão próximas no sentido clássico de distância. Assim, a distância de traço fornece um limitante superior para a distância entre as distribuições de probabilidade geradas a partir de medições realizadas sobre tais estados quânticos.

## 2.6.2 Fidelidade

Uma segunda medida de distância entre estados quânticos é a *fidelidade*. A fidelidade em si não é uma métrica de operadores densidade, mas possui propriedades interessantes e veremos mais adiante que ela de fato induz uma métrica útil.

**Definição 2.6.2.** A fidelidade entre dois estados quânticos  $\rho$  e  $\sigma$  é definida por

$$F(\rho, \sigma) = \text{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}.$$

Há dois casos especiais em que a fórmula para fidelidade pode ser simplificada. O primeiro é quando  $\rho$  e  $\sigma$  comutam:

$$F(\rho, \sigma) = \text{tr}\sqrt{\sum_i r_i s_i |i\rangle\langle i|} = \text{tr}\left(\sum_i \sqrt{r_i s_i} |i\rangle\langle i|\right) = \sum_i \sqrt{r_i s_i} = F(r_i, s_i).$$

Isto é, quando  $\rho$  e  $\sigma$  comutam, a fidelidade se reduz à fidelidade clássica para as distribuições de autovalores  $r_i$  e  $s_i$  de  $\rho$  e  $\sigma$ .

O segundo caso é quando calculamos a fidelidade entre um estado puro  $|\psi\rangle$  e um estado arbitrário  $\rho$ :

$$F(|\psi\rangle, \rho) = \text{tr} \sqrt{|\psi\rangle\langle\psi| \rho |\psi\rangle\langle\psi|} = \text{tr} \sqrt{\langle\psi|\rho|\psi\rangle} \sqrt{|\psi\rangle\langle\psi|} = \sqrt{\langle\psi|\rho|\psi\rangle}.$$

Neste caso, a fidelidade é igual à raiz quadrada da sobreposição entre  $|\psi\rangle$  e  $\rho$ .

Infelizmente, no caso de um q-bit, não temos uma interpretação na esfera de Bloch para a fidelidade como tínhamos para a distância do traço. No entanto, a fidelidade satisfaz várias das propriedades da distância do traço, entre elas a invariância por transformações unitárias.

Há uma outra caracterização para a fidelidade que é muito útil.

**Teorema 2.6.3** (Teorema de Uhlmann). *Suponha que  $\rho$  e  $\sigma$  são estados de um sistema quântico  $Q$ . Considere um segundo sistema quântico  $R$ , que é uma cópia de  $Q$ . Então:*

$$F(\rho, \sigma) = \max_{|\psi\rangle, |\varphi\rangle} |\langle\psi|\varphi\rangle|,$$

onde o máximo é sobre todas as purificações  $|\psi\rangle$  de  $\rho$  e  $|\varphi\rangle$  de  $\sigma$  em  $RQ$ .

*Demonstração.* Vide [69]. □

A fórmula de Uhlmann não fornece uma ferramenta para o cálculo da fidelidade. Contudo, em várias situações, as propriedades da fidelidade são deduzidas mais facilmente através dessa fórmula. Por exemplo, é fácil ver pela fórmula de Uhlmann que a fidelidade é simétrica em suas entradas e que  $0 \leq F(\rho, \sigma) \leq 1$ . Se  $\rho = \sigma$ , fica claro então que  $F(\rho, \sigma) = 1$  e, se  $\rho \neq \sigma$ , então  $|\psi\rangle \neq |\varphi\rangle$  para alguma purificação de  $\rho$  e  $\sigma$ , logo  $F(\rho, \sigma) < 1$ . Além disso, tem-se que  $F(\rho, \sigma) = 0$  se, e somente se,  $\rho$  e  $\sigma$  tem suporte em subespaços ortogonais. De fato, se  $\rho$  e  $\sigma$  tem suporte em subespaços ortogonais, tais estados são perfeitamente distinguíveis, logo, esperamos que a fidelidade entre eles seja minimizada.

Podemos relacionar a fidelidade com a distância de traço considerando as distribuições de probabilidade induzidas por medições. Pode-se mostrar que:

$$F(\rho, \sigma) = \min_{\{E_m\}} F(p_m, q_m) = \min_{\{E_m\}} \sum_m \sqrt{\text{tr}(E_m \rho) \text{tr}(E_m \sigma)},$$

onde o mínimo é sobre todos os elementos POVM  $\{E_m\}$ .

A fidelidade em si não é uma métrica. Porém, podemos definir uma métrica induzida pela fidelidade. Dizemos que o *ângulo* entre os estados  $\rho$  e  $\sigma$  é dado por

$$A(\rho, \sigma) = \arccos F(\rho, \sigma).$$

Claramente, o ângulo é não negativo, simétrico em suas entradas e igual a zero se, e somente se,  $\rho = \sigma$ . Além disso, pode-se mostrar, através da fórmula de Uhlmann, que o ângulo cumpre a desigualdade triangular e, portanto, define uma métrica.

Qualitativamente falando, a fidelidade se comporta como o inverso da distância do traço, diminui à medida que os estados tornam-se mais distinguíveis e aumenta à medida que tornam-se menos distinguíveis.

A distância de traço e a fidelidade estão fortemente relacionadas, apesar de suas aparências distintas. Elas podem ser consideradas medidas equivalentes de distância entre estados quânticos em várias aplicações e não importa quando uma ou outra é usada, pois resultados obtidos com uma podem ser usados para deduzir resultados equivalentes com a outra. Uma importante relação entre elas é:

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}.$$

Assim, concluímos este capítulo, que apresentou os fundamentos da mecânica quântica necessários ao entendimento do problema de tomografia de estados quânticos. Este será o tema do Capítulo 3.

# Capítulo 3

## Tomografia de Estados Quânticos

A natureza probabilística dos sistemas quânticos é revelada através da realização de experimentos. Ao realizar um experimento repetidas vezes sobre um *ensemble* de sistemas identicamente preparados, o experimentalista não é capaz de descrever deterministicamente os resultados obtidos, mas sim, observar as estatísticas de certos eventos, expressas na forma de probabilidades ou valores esperados. Assim, a teoria quântica responde à pergunta: que estatísticas podem ser esperadas dado que o estado quântico é conhecido? Esse é o papel central do estado quântico. Por outro lado, a determinação do estado quântico em si constitui um *problema inverso*. O problema inverso da determinação do estado quântico, dadas as estatísticas do experimento, é chamado *reconstrução* ou *tomografia de estado quântico*.

Suponha que tenhamos um *ensemble* de  $N$  estados quânticos, identicamente preparados em um estado desconhecido, descrito pelo operador de densidade  $\rho$  e que realizamos sobre cada instância uma medição, podendo obter  $M$  resultados possíveis. Cada medição pode ser descrita por um conjunto  $\{E_j\}$  de elementos POVM, cada  $E_j$  associado a um possível resultado  $j$ . Supondo que cada resultado  $j$  foi registrado  $n_j$  vezes,  $N = \sum_j n_j$ , logo as frequências relativas são dadas por  $f_j = n_j/N$ .

Pelo postulado da medida, sabe-se que ao realizar uma medição, a probabilidade de ocorrência do resultado  $j$  é dada por

$$p_j = \text{tr}(E_j \rho). \quad (3.1)$$

Usando esses ingredientes, é possível inferir o estado  $\rho$  do sistema em questão. Nas seções seguintes deste capítulo, discutiremos as principais características das abordagens mais utilizadas para tomografia de estados quânticos.

### 3.1 Método padrão: Inversão Linear

Se as probabilidades  $p_j$  fossem conhecidas, poderíamos obter  $\rho$  diretamente a partir das equações definidas por (3.1). Essa é a base dos métodos padrão em tomografia de estados quânticos, chamados de *inversão linear*. Porém, experimentalmente

é utilizado apenas um *ensemble* de dimensão finita e a única informação disponível ao experimentalista são as frequências relativas  $f_j$ . Com isso, temos um modelo (realístico) modificado:

$$f_j = \text{tr}(E_j \rho). \quad (3.2)$$

Resolvendo este sistema de equações lineares, podemos obter uma estimativa para o operador de densidade  $\rho$ .

No caso de experimentos com variáveis contínuas, como por exemplo a detecção homodina [83], os índices discretos  $j$  devem ser substituídos pelo par de variáveis contínuas  $x$  e  $\phi$  correspondentes ao valor detectado e à fase de um operador de quadratura. Então, a partir da função de quase-probabilidade de Wigner:

$$W(x, p) = \frac{1}{\pi} \int_{-\infty}^{\infty} \langle x + x' | \rho | x - x' \rangle e^{-2ipx'} dx',$$

podemos obter a distribuição de probabilidade de amplitudes de quadraturas, para diferentes fases  $0 \leq \phi \leq \pi$ :

$$P(x_\phi) = \int_{-\infty}^{\infty} W(x_\phi \cos \phi - p_\phi \sin \phi, x_\phi \sin \phi + p_\phi \cos \phi) dp_\phi.$$

As distribuições  $P(x_\phi)$  são obtidas experimentalmente pela detecção homodina e, aplicando a transformada inversa de Radon para diferentes fases  $\phi$ , podemos reconstruir a matriz de densidade  $\rho$ .

No entanto, sobretudo quando o tamanho do *ensemble*  $N$  é pequeno, as frequências relativas  $f_j$  podem diferir substancialmente das probabilidades verdadeiras  $p_j$ . Com isso, o modelo modificado (3.2) geralmente não possui solução no espaço das matrizes físicas (semidefinidas positivas e de traço um). Essa é a principal desvantagem dessa abordagem. Contudo, a inversão linear é a técnica padrão, a mais popular, porque em muitas aplicações, o *ensemble* de sistemas medidos é tão grande, que as flutuações da ordem de  $1/N$  podem ser ignoradas [73]. Além disso, uma vantagem da inversão linear é sua simplicidade e baixo custo computacional em relação a outras abordagens.

Seja  $d$  a dimensão do espaço de Hilbert associado a um sistema, em um experimento com variáveis discretas. Para que o sistema de equações lineares (3.2) seja invertível, precisamos de um número de equações igual ao número de incógnitas da matriz  $d \times d$ ,  $\rho$ . Em geral, como  $M < d^2$ , são realizadas diferentes medições  $i$ , cada qual associada a uma configuração do aparato experimental e descrita por um conjunto POVM  $\{E_{ij}\}$ . Se cada medição  $i$  é realizada sobre um *ensemble* de tamanho  $N_i$  e o número de ocorrências do resultado  $j$  nesta configuração é  $n_{ij}$ , então

$$\frac{n_{ij}}{N_i} = f_{ij} = \text{tr}(E_{ij} \rho) \quad (3.3)$$

é o sistema de equações lineares a ser resolvido para determinar  $\rho$ . Um conjunto de medições para as quais o sistema linear definido por (3.3) tem solução única é chamado de *conjunto tomograficamente completo* ou *quorum* [27]. Determinar o menor conjunto de medições para as quais um estado  $\rho$  é unicamente determinado é um tópico de pesquisa em atividade [77].

Ao longo dessa tese, por simplicidade na notação, usaremos um único índice  $j$  para indexar o par (medição  $i$ , possível resultado  $j$ ), salvo situações onde o uso de dois índices torna o texto mais claro. Além disso, também é comum usar  $N_i = N$ , isto é, usar o mesmo número de repetições por medição. É claro que se temos, por exemplo, medições distintas  $i = 1, 2, \dots, k$ , cada qual descrita por POVM's  $\{E_{ij}\}_j$  e repetida  $N$  vezes, é possível definir um novo conjunto POVM  $\{E_{j'}\}$  com um índice  $j'$  associado a cada par  $(i, j)$ ,  $E_{j'} = \frac{1}{k}E_{ij}$  e  $n_{j'} = \frac{1}{k}n_{ij}$ .

Para ilustrar o procedimento de inversão linear, vamos nos ater, por enquanto, à tomografia de q-bits e descrever apenas a teoria necessária, sem nos preocuparmos com sua realização física.

### Exemplo: Tomografia de um q-bit

Como já vimos, se dispomos de uma única cópia de um q-bit, cujo estado *desconhecido*  $\rho$  queremos identificar, tal tarefa é impossível. No entanto, se dispomos de várias instâncias identicamente preparadas, é possível estimar tal matriz de densidade.

Suponha que tenhamos uma fonte de q-bits identicamente preparados. O conjunto  $\left\{ \frac{I}{\sqrt{2}}, \frac{X}{\sqrt{2}}, \frac{Y}{\sqrt{2}}, \frac{Z}{\sqrt{2}} \right\}$  forma uma base ortonormal para o espaço de matrizes, com respeito ao produto interno de *Hilbert-Schmidt*:

$$\langle A|B \rangle = \text{tr}(A^\dagger B).$$

Com isso,  $\rho$  pode ser escrita como

$$\begin{aligned} \rho &= \hat{\alpha}_0 \frac{I}{\sqrt{2}} + \hat{\alpha}_1 \frac{X}{\sqrt{2}} + \hat{\alpha}_2 \frac{Y}{\sqrt{2}} + \hat{\alpha}_3 \frac{Z}{\sqrt{2}} \\ &= \alpha_0 \sigma_0 + \alpha_1 \sigma_1 + \alpha_2 \sigma_2 + \alpha_3 \sigma_3, \end{aligned}$$

onde

$$\alpha_i = \frac{\hat{\alpha}_i}{\sqrt{2}} = \frac{1}{\sqrt{2}} \frac{\text{tr}(\sigma_i \rho)}{\sqrt{2}} = \frac{1}{2} \text{tr}(\sigma_i \rho).$$

Na literatura, encontramos também a forma

$$\rho = \frac{1}{2} \sum_{i=0}^3 S_i \sigma_i,$$

onde os parâmetros  $S_i = \text{tr}(\sigma_i \rho)$  são chamados *parâmetros de Stokes*.

O fato é que

$$\rho = \frac{\text{tr}(\rho) I + \text{tr}(X\rho) X + \text{tr}(Y\rho) Y + \text{tr}(Z\rho) Z}{2}, \quad (3.4)$$

e os parâmetros  $\text{tr}(\sigma_i \rho)$  têm a interpretação de *valor esperado* para os *observáveis*:

$$\mathbf{E}(\sigma_j) = \sum_m m p(m) = \sum_m m \text{tr}(P_m \rho) = \text{tr} \left( \left( \sum_m m P_m \right) \rho \right) = \text{tr}(\sigma_j \rho).$$

Assim, ao realizar um *grande número* de medições do observável  $\sigma_i$ , podemos obter uma estimativa para  $\text{tr}(\sigma_i \rho) = \mathbf{E}(\sigma_i) \approx \frac{1}{n} \sum_{i=1}^n z_i$ , onde  $z_i$  são os resultados experimentais e com isso obter uma aproximação para  $\rho$ .

### 3.1.1 Tomografia de múltiplos q-bits

Estendendo a representação da matriz de densidade de um único q-bit, um estado  $\rho$  de  $n$  q-bits pode ser representado por

$$\rho = \frac{1}{2^n} \sum_{i_1, i_2, \dots, i_n=0}^3 S_{i_1, i_2, \dots, i_n} \sigma_{i_1} \otimes \sigma_{i_2} \otimes \dots \otimes \sigma_{i_n}.$$

Normalizando  $S_{0,0,\dots,0} = 1$ , restam  $4^n - 1$  parâmetros a serem determinados, para identificar o estado quântico.

Por exemplo, o estado de um sistema composto por 2 q-bits pode ser representado por

$$\rho = \frac{1}{2^2} \sum_{i,j=0}^3 S_{ij} \sigma_i \otimes \sigma_j,$$

onde  $S_{ij} = \text{tr}(\sigma_i \otimes \sigma_j \rho)$ . Note que  $\sigma_i$  e  $\sigma_j$  são as conhecidas matrizes de Pauli (ou quaisquer outras matrizes que formem uma base ortonormal com respeito ao produto interno de Hilbert-Schmidt). Neste exemplo, devemos determinar 15 parâmetros  $S_{ij}$  para identificar o estado do sistema.

### 3.1.2 Inversão Linear, caso geral

Generalizemos agora a ideia apresentada nas seções anteriores para sistemas quânticos, discretos, com mais de dois níveis.

Seja  $\{\Gamma_i\}$  uma base ortonormal para o espaço das matrizes Hermitianas de ordem  $d$ , isto é:

$$\text{tr}(\Gamma_i \Gamma_j) = \delta_{i,j} \quad ,$$

onde  $\delta_{i,j}$  é o delta de Kronecker, e

$$A = \sum_i \text{tr}(\Gamma_i A) \Gamma_i, \quad \forall A.$$

Usando essa base, podemos escrever  $\rho$  como

$$\rho = \sum_{i=1}^{d^2} S_i \Gamma_i, \quad (3.5)$$

onde os coeficientes  $S_i = \text{tr}(\Gamma_i \rho)$  são os conhecidos parâmetros de Stokes. Considerando a condição de normalização,  $\text{tr}(\rho) = 1$ , precisamos determinar  $d^2 - 1$  coeficientes. Se realizamos medições descritas por um conjunto POVM  $\{E_j\}$ , a mecânica quântica nos diz que

$$f_j \approx p_j = \text{tr}(E_j \rho), \quad (3.6)$$

onde  $f_j = n_j/N$  denota as frequências normalizadas ( $n_j$  e  $N$  denotam respectivamente, o número de contagens e a constante de normalização, e  $j$  indexa o par resultado-configuração do aparato experimental). Tomando o produto interno e usando (3.5) e (3.6), temos:

$$f_j \approx \text{tr}(E_j \rho) = \sum_i S_i \text{tr}(E_j \Gamma_i). \quad (3.7)$$

Definindo a matriz  $d^2 \times d^2$ ,  $B_{ij} = \text{tr}(E_j \Gamma_i)$ , podemos obter os parâmetros  $S_i$  e, consequentemente, a matriz de densidade  $\rho$  resolvendo o *sistema linear*

$$Bs = f, \quad (3.8)$$

onde  $s$  é o vetor com componentes  $S_i$  e  $f$  o vetor com componentes  $f_j$ . É claro que, nesse contexto, assumimos que foram realizadas medições suficientes para  $d^2$  equações lineares independentes, já que temos  $d^2$  incógnitas.

Poderíamos pensar em um número insuficiente de medições de modo a recair em um sistema linear subdeterminado. Porém, nesse caso, a unicidade da solução não pode ser assegurada e teríamos que definir um critério para estabelecer qual é a solução desejada. A seção 3.7 fala sobre o princípio de Máxima Entropia, uma possível abordagem nestes casos.

Se  $\Gamma_i$  e  $\{E_j\}$  forem escolhidos de tal forma que  $B$  seja não singular, um *conjunto completo de medições*, então a solução para o sistema linear (3.8) é unicamente determinada e obtemos de forma analítica a matriz de densidade  $\rho$ .

Como já discutido anteriormente, quando o tamanho do *ensemble*  $N$  é pequeno, as frequências normalizadas  $f_j$  não produzirão boas aproximações para as probabilidades  $\text{tr}(E_j \rho)$ . Mais ainda, a lei dos grandes números diz que as frequências normalizadas

serão boas aproximações para as probabilidades teóricas apenas se as medições forem repetidas um grande número de vezes, o que nem sempre é o caso. Isso geralmente leva à obtenção de uma matriz que pode não ser uma matriz de densidade legítima, apresentando autovalores negativos ou com traço diferente de um.

## 3.2 Garantindo uma matriz física

Uma saída para este problema da inversão linear é buscar pela matriz Hermitiana que melhor ajusta os dados experimentais, restringindo a busca ao espaço das matrizes Hermitianas semidefinidas positivas e de traço um. Em outras palavras, ao invés de resolver o sistema de equações lineares (3.2), poderíamos resolver o seguinte problema de minimização restrito:

$$\begin{aligned} \min_{\rho} \quad & D(f, p(\rho)) \\ \text{s.a} \quad & \text{tr}(\rho) = 1, \\ & \rho \succeq 0, \end{aligned} \tag{3.9}$$

onde  $D(f, p)$  representa uma distância estatística entre as frequências relativas e as probabilidades teóricas. Diferentes distâncias  $D(f, p)$ , obviamente, podem levar a diferentes resultados e esse é o ponto em que diferem as principais abordagens para Tomografia de Estados Quânticos.

As restrições que definem o problema (3.9) são conhecidas como igualdades/desigualdades lineares matriciais [14, 22]. Em verdade, métodos clássicos [54, 70] de minimização não foram desenvolvidos para lidar com restrições desse tipo, o que nos leva a recorrer à programação cônica convexa [14]. No caso em que  $D(f, p)$  é uma função linear de  $\rho$ , temos um problema de *programação semidefinida linear* [14, 22, 92], o qual apresenta uma teoria bem consolidada e métodos eficientes [1, 41, 67, 68, 88] de resolução.

Em geral, apesar de convexa,  $D(f, p)$  não é uma função linear de  $\rho$  e isso requer uma reformulação do problema para o caso de programação semidefinida linear, ou outra maneira de lidar com as restrições que definem o espaço das matrizes de densidade  $\mathcal{S}$ .

Uma alternativa para lidar com as restrições sobre a matriz de densidade, apresentada em James et. al. [48], é utilizar a mudança de variáveis:

$$\rho(t) = \frac{T(t)^\dagger T(t)}{\text{tr}(T(t)^\dagger T(t))}, \tag{3.10}$$

onde  $T(t)$  é uma matriz triangular superior, lembrando o fator de Cholesky [62] e  $t$  é um vetor representando as entradas da matriz  $T$ . Note que com a mudança de variáveis (3.10),  $\rho(t)$  será sempre semidefinida positiva e de traço unitário para todo

$t \neq 0$ . Essa mudança de variáveis resulta em um problema de minimização irrestrito em  $t$ . No entanto, tal mudança de variáveis faz com que a função resultante

$$f(t) = D(f, p(\rho(t)))$$

apresente vários mínimos locais. A possibilidade de existirem minimizadores locais, não-globais, é destacada na literatura [2, 48, 91] e provavelmente desmotivou o uso dessa estratégia. Na Seção 4.1 do Capítulo 4, esclarecemos este ponto, mostrando que todos os mínimos locais de  $f(t)$  são globais, desde que  $D(f, p(\rho))$ , como função de  $\rho$ , seja convexa em  $\mathcal{S}$ .

Note ainda que, na formulação (3.9) acima, não precisamos necessariamente de um conjunto tomograficamente completo de medições, todavia, pagando o preço pela não unicidade de soluções.

### 3.3 Um problema de inferência

Determinar um parâmetro que rege a distribuição de uma população, com base nos dados amostrais, constitui um problema estatístico de inferência [16, 51]. Uma estimativa para tal parâmetro pode ser obtida por vários métodos estatísticos, entre eles, estimativa de Quadrados Mínimos, Máxima Verossimilhança, Máxima Entropia, estimativas baseadas em inferência Bayesiana, dentre outros.

A fim de obter informação sobre um sistema quântico de interesse, precisamos realizar medições e extrair a informação desejada dos dados obtidos. A otimização desses dois processos constitui o problema quântico de inferência estatística [42, 43, 57]. Uma vez fixado o conjunto de medições obtemos um problema de inferência clássica [3, 5]: a Tomografia de Estados Quânticos.

Em Tomografia de Estados Quânticos, à população corresponde a *distribuição conjunta* dos dados experimentais  $\{N_j\}$ , o parâmetro a ser estimado é a matriz de densidade  $\rho$  e os dados amostrais correspondem aos dados experimentais registrados  $\{n_j\}$ . O uso de letras maiúsculas para diferenciar  $N_j$  de  $n_j$  tem por objetivo ressaltar que o “número de vezes que ocorreu o resultado  $j$  em  $N$  repetições” é uma variável aleatória. Novamente, consideramos  $j$  indexando o par (configuração do aparato experimental, resultado).

As próximas seções resumem os principais aspectos de cada abordagem para estimativa da matriz de densidade.

### 3.4 Quadrados mínimos

Já que, em geral, as frequências relativas  $f_j$  não são boas aproximações para as probabilidades verdadeiras  $p_j$ , quando  $N$  não é suficientemente grande, não é razoável

esperar que a inversão linear forneça uma estimativa que satisfaça a positividade e o traço unitário. Assim, a formulação de quadrados mínimos (3.11) parece bastante natural para o problema de encontrar a matriz semidefinida positiva e de traço um que minimiza a soma dos erros ao quadrado, i.e., a soma das distâncias Euclidianas entre  $f_j$  e  $p_j$ :

$$\begin{aligned} \min_{\rho} \quad & \sum_{j=1}^M (\text{tr}(E_j \rho) - f_j)^2 \\ \text{s.a} \quad & \text{tr}(\rho) = 1, \\ & \rho \succeq 0. \end{aligned} \tag{3.11}$$

Apesar da aparente simplicidade em sua formulação, as restrições do problema (3.11) representam um obstáculo a métodos clássicos de minimização. De fato, o conjunto viável  $\mathcal{S}$  para o problema (3.11) é resultado da intersecção do cone convexo  $\rho \succeq 0$  das matrizes semidefinidas positivas com o hiperplano  $\text{tr}(I\rho) = 1$  e trata-se de um conjunto convexo como mostrado na Seção 2.5.3.

Como discutido anteriormente, se a função objetivo fosse linear, teríamos um problema de programação semidefinida linear [14, 22], para o qual há métodos eficientes [41, 67, 68] de resolução. No entanto, a função objetivo de (3.11) é quadrática e convexa e métodos que generalizam as ideias de programação semidefinida [90, 99] para resolução de tal problema ainda estão em desenvolvimento.

Uma alternativa é reformular o problema (3.11) através da introdução de variáveis auxiliares para a forma:

$$\begin{aligned} \min_{\rho, p, t} \quad & t \\ \text{s.a} \quad & \|f - p\|_2 \leq t \\ & \text{tr}(E_j \rho) = p_j \quad j = 1, 2, \dots, M \\ & \text{tr}(\rho) = 1, \\ & \rho \succeq 0, \end{aligned} \tag{3.12}$$

onde  $f$  é vetor de frequências relativas  $f_j$ . A restrição é conhecida como *cone de segunda ordem* e é um caso particular de programação semidefinida. Vários pacotes computacionais [13, 53, 85, 89] são capazes de resolver o problema (3.12).

Por outro lado, usando a mudança de variáveis (3.10), o problema (3.11) torna-se um problema irrestrito em  $t$ :

$$\min_t \sum_{j=1}^M (\text{tr}(E_j \rho(t)) - f_j)^2. \tag{3.13}$$

O problema (3.13) pode apresentar vários mínimos locais, com respeito a  $t$ , em decorrência da mudança de variáveis (3.10). No entanto, como mencionado anteriormente,

todos os mínimos locais são equivalentes, como será mostrado na Seção 4.1 do Capítulo 4, uma vez que a função objetivo de (3.11) é convexa em  $\mathcal{S}$  com respeito a  $\rho$ .

### 3.4.1 Derivadas parciais em $t$

Para resolver o problema (3.13), podemos empregar métodos específicos para quadrados mínimos não lineares [33, 52, 58, 100] e estes geralmente necessitam das derivadas parciais das funções resíduo:

$$r_j(t) = \text{tr}(E_j \rho(t)) - f_j. \quad (3.14)$$

Mais ainda, sempre que usarmos a mudança de variáveis (3.10), será importante conhecer as derivadas parciais de  $\rho(t)$  em relação a  $t_i$ . Assumindo que  $T(t)$  em (3.10) tem a estrutura:

$$T(t) = \begin{pmatrix} t_1 & t_{d+1} + it_{d+2} & \dots & \dots & t_{d^2-1} + it_{d^2} \\ 0 & t_2 & t_{d+3} + it_{d+4} & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & t_{3d-1} + it_{3d-2} \\ 0 & \dots & \dots & 0 & t_d \end{pmatrix}, \quad (3.15)$$

temos que

$$\text{tr}(T(t)^\dagger T(t)) = \sum_{i=1}^{d^2} t_i^2, \quad (3.16)$$

e, além disso:

$$\frac{\partial T(t)^\dagger T(t)}{\partial t_i} = T(t)^\dagger T(e_i) + T(e_i)^\dagger T(t), \quad (3.17)$$

onde  $e_i$  denota o  $i$ -ésimo vetor canônico.

Assim, temos que

$$\frac{\partial \rho(t)}{\partial t_i} = \frac{\partial}{\partial t_i} \frac{T(t)^\dagger T(t)}{\text{tr}(T(t)^\dagger T(t))} = \frac{(T(t)^\dagger T(e_i) + T(e_i)^\dagger T(t)) \text{tr}(T(t)^\dagger T(t)) - 2t_i T(t)^\dagger T(t)}{\text{tr}(T(t)^\dagger T(t))^2}, \quad (3.18)$$

e, portanto,

$$\frac{\partial r_j(t)}{\partial t_i} = \text{tr} \left( E_j \frac{\partial \rho(t)}{\partial t_i} \right). \quad (3.19)$$

Na estimativa de quadrados mínimos, nos preocupamos apenas em minimizar a soma

dos resíduos  $r_j$  ao quadrado, sem levar em conta a distribuição conjunta das variáveis aleatórias  $\{N_j\}$ . Por outro lado, assumindo alguma distribuição sobre os resultados experimentais, podemos aplicar outros métodos de inferência estatística, como por exemplo, a estimação por máxima verossimilhança.

### 3.5 Máxima Verossimilhança

Após realizar as medições e registrar os resultados, o conhecimento sobre o sistema medido é aumentado. Uma vez que a mecânica quântica é “probabilística”, faz pouco sentido perguntar: “Que estado quântico é determinado pelos resultados das medições?”. Talvez uma questão mais apropriada seja: “Que estado quântico torna os resultados das medições mais prováveis?” [47].

Como mencionado anteriormente, em Tomografia de Estados Quânticos, o parâmetro a ser estimado é a matriz de densidade  $\rho$ , a qual define a distribuição conjunta das variáveis aleatórias  $\{N_j\}$ . Essa abordagem, considerada em trabalhos anteriores [2, 46–48], tem como formulação:

$$\begin{aligned} \max_{\rho} \quad & \mathcal{L}(\rho) \equiv P(n_1, \dots, n_M | \rho) \\ \text{s.a} \quad & \text{tr}(\rho) = 1, \\ & \rho \succeq 0, \end{aligned} \tag{3.20}$$

onde  $P(n_1, \dots, n_M | \rho)$  é a probabilidade de ocorrência dos resultados  $\{n_j\}$  dado o parâmetro  $\rho$ . Assim, procura-se no espaço das matrizes de densidade aquela que maximiza a probabilidade de ocorrência dos dados experimentais obtidos.

É claro que hipóteses distintas sobre a distribuição conjunta das variáveis  $\{N_j\}$  levarão a distintas funções de verossimilhança  $\mathcal{L}(\rho)$ .

Por exemplo, em [46, 47], considera-se uma distribuição multinomial. De fato, se temos  $M$  resultados possíveis para um experimento, o qual é repetido  $N$  vezes (tamanho do *ensemble*), então a probabilidade de se obter  $\{n_j\}$  é:

$$\mathcal{L}(\rho) = \frac{N!}{\prod_{i=1}^M n_i} \prod_{j=1}^M p_j(\rho)^{n_j} = \frac{N!}{\prod_{i=1}^M n_i} \prod_{j=1}^M \text{tr}(E_j \rho)^{n_j}. \tag{3.21}$$

Já em [2, 48], onde a tomografia é realizada medindo a polarização de fótons gerados através de conversão paramétrica descendente [50, 97], é usual considerar que cada  $N_j$ , número de vezes que a saída  $j$  foi registrada em um intervalo de tempo, possui uma distribuição Poissoniana de parâmetro  $N \text{tr}(E_j \rho)$ . Para  $N$  razoavelmente grande, essa Poissoniana pode ser aproximada por uma Gaussiana de média e variância iguais a

$N\text{tr}(E_j\rho)$ :

$$P(N_j = n_j) = \frac{1}{\sqrt{2\pi N\text{tr}(E_j\rho)}} \exp\left(-\frac{1}{2} \frac{(N\text{tr}(E_j\rho) - n_j)^2}{N\text{tr}(E_j\rho)}\right). \quad (3.22)$$

Considerando independentes as ocorrências de cada resultado  $j$ , tem-se então como função de verossimilhança:

$$\mathcal{L}(\rho) = \frac{1}{N_{norm}} \prod_{j=1}^M \exp\left(-\frac{1}{2} \frac{(N\text{tr}(E_j\rho) - n_j)^2}{N\text{tr}(E_j\rho)}\right), \quad (3.23)$$

onde  $N_{norm}$  é uma constante de normalização.

Geralmente, é mais fácil maximizar  $\ln \mathcal{L}(\rho)$  ao invés de  $\mathcal{L}(\rho)$  propriamente, mas esta discussão, bem como métodos para resolver o problema (3.20) usando (3.21) e (3.23), serão tratados no Capítulo 4.

A popularidade da estimação por máxima verossimilhança como um método para estimação de parâmetros se deve principalmente às suas boas propriedades assintóticas [16, 51], que serão melhor discutidas no Capítulo 4. Dentre elas, podemos destacar a invariância, isto é, se  $\rho_{ML}$  é a estimativa de máxima verossimilhança para  $\rho$ , então  $\varphi(\rho_{ML})$  será a estimativa de máxima verossimilhança para  $\varphi(\rho)$ . Além disso, se certas hipóteses de regularidade são satisfeitas, o estimador de máxima verossimilhança é assintoticamente eficiente, isto é, quando  $N \rightarrow \infty$ , o estimador de máxima verossimilhança torna-se o estimador não viesado de mínima variância.

## 3.6 Inferência Bayesiana

Uma objeção à estimação por Máxima Verossimilhança é que a estimativa para matriz de densidade pode ter posto deficiente, ou seja, com um ou mais autovalores nulos. Isso implica que a probabilidade de ocorrência de certos eventos (saídas experimentais) é zero, o que não pode ser justificado com uma quantidade finita (e muitas vezes pequena) de dados. Além disso, não há como utilizar barras de erro consistentes com uma probabilidade nula. [12]

Ao contrário da Máxima Verossimilhança, que busca uma única estimativa maximamente plausível, a inferência Bayesiana também considera outras estimativas um pouco menos plausíveis. Em verdade, em inferência Bayesiana o parâmetro a ser estimado  $\rho$  é considerado em si uma variável aleatória e nos interessa descobrir qual a distribuição  $\pi(\rho)$  de tal parâmetro. Tal distribuição, chamada a posteriori, é resultado do produto da verossimilhança, com uma distribuição a priori  $\pi_0(\rho)$  que representa o conhecimento prévio sobre o sistema. A partir da posteriori é que obtemos uma estimativa pontual

$\hat{\rho}$ , tomando por exemplo, a média de tal distribuição, assim como barras de erro consistentes podem ser obtidas a partir da variância e do desvio padrão dessa distribuição.

No Capítulo 7 discutimos sobre inferência Bayesiana aplicada ao problema de Tomografia de Estados Quânticos, e sua implementação através de métodos Monte Carlo via cadeias de Markov [29, 32].

## 3.7 Máxima Entropia

Outra abordagem para a reconstrução de estados quânticos é o princípio de Máxima Entropia, introduzido em mecânica estatística por Jaynes [49], que vê a entropia como uma medida de informação.

A entropia de um sistema quântico é definida como [15, 49]

$$S(\rho) = -\text{tr}(\rho \ln \rho). \quad (3.24)$$

A estimativa de Máxima Entropia  $\rho_{ME}$  é aquela que maximiza (3.24) e satisfaz as equações (3.2) para o conjunto de medidas realizadas. Em verdade, se temos um conjunto tomograficamente completo e pensamos em medições idealizadas, livres de erro, então existe uma única estimativa  $\rho$  que satisfaz todas as equações (3.2). Por outro lado, se não temos um conjunto completo de medições, pode haver mais de uma solução para as equações (3.2). Neste caso, a estimativa de Máxima Entropia busca pela solução menos viesada compatível com os dados observados [15].

### 3.7.1 Conjunto incompleto de medições

No caso de um conjunto incompleto de medições, na inversão linear, o sistema de equações (3.7) não poderá ser resolvido unicamente e normalmente apresentará mais de uma solução de quadrados mínimos (3.11). De fato, com medições incompletas podemos ter mais de um estado minimizando a distância entre as probabilidades teóricas e as frequências experimentais. Consequentemente, também teremos mais de uma solução na estimação por máxima verossimilhança, em verdade, um conjunto convexo de soluções.

Neste caso, alguma medida deve ser empregada para definir qual a solução desejada. Por exemplo, a estimativa de Máxima Entropia busca a estimativa, compatível com as medições realizadas, que maximiza a entropia de von Neumann (3.24). No entanto outras alternativas podem ser consideradas.

Por exemplo, ao invés da estimativa de Máxima Entropia, podemos optar pela estimativa de Mínima Divergência de Kullback-Leibler [71]. Para isso, consideramos a

entropia relativa de Kullback-Leibler:

$$K(\rho, \rho_0) = \text{tr}(\rho(\log \rho - \log \rho_0)), \quad (3.25)$$

da estimativa para o estado  $\rho$ , em relação a uma estimativa a priori  $\rho_0$ . É claro que  $\rho$  que minimiza  $K(\rho, \rho_0)$  e é compatível com os dados experimentais, apresenta um viés em favor de  $\rho_0$ . De fato, essa pode ser a intenção, caso o experimentalista tenha algum conhecimento prévio do estado a ser estimado. Usando  $\rho_0 = (1/d)I$ , então tal solução coincide com a de Máxima Entropia.

Outra estratégia, que recai em um problema de programação semidefinida linear, é a Tomografia Quântica Variacional [55], onde busca-se uma estimativa para  $\rho$ , compatível com as medidas realizadas, e que minimiza um certo tipo de energia associada às medidas faltantes.

O Capítulo 5 é dedicado à tomografia de estados com um conjunto incompleto de medidas, onde discutimos mais a fundo sobre estimação por Máxima Entropia [15] e Tomografia Quântica Variacional [55].



# Capítulo 4

## Máxima Verossimilhança

Em inferência estatística [16, 51], a Estimação por Máxima Verossimilhança (EMV) é um método usado para determinar uma estimativa de um parâmetro desconhecido  $\theta$ , baseado nos dados amostrais  $x$ . A ideia é maximizar a função densidade de probabilidade conjunta  $P(x|\theta)$  como função apenas de  $\theta$ , isto é, a estimativa de máxima verossimilhança  $\hat{\theta}_{emv}$  é o valor que maximiza a probabilidade de se obter os dados observados.

Mediante certas hipóteses [51], a EMV possui várias propriedades interessantes do ponto de vista estatístico. Isso explica porque é amplamente utilizada para estimativa de parâmetros. Dentre outras, podemos destacar:

- **Consistência:**  $\lim_{n \rightarrow \infty} P(|\hat{\theta}_n - \theta| < \varepsilon) = 1, \forall \varepsilon > 0$ , onde  $\hat{\theta}_n$  é a estimativa para uma amostra finita de tamanho  $n$ . Isso significa que o estimador de máxima verossimilhança  $\hat{\theta}$  tende a ser não viesado quando  $n \rightarrow \infty$ .
- **Assintoticamente Normal e Eficiente:** quando  $n \rightarrow \infty$ ,  $\hat{\theta} \sim N(\theta, \mathcal{I}(\theta)^{-1})$ , isto é,  $\hat{\theta}$  tem distribuição normal com média  $\theta$  e matriz de covariância  $\mathcal{I}(\theta)^{-1}$ , onde  $\mathcal{I}(\theta)$  é a matriz de informação de Fisher. Em outras palavras, à medida que o tamanho da amostra aumenta a EMV torna-se um estimador eficiente.
- Em **amostras finitas**, se um estimador não viesado de mínima variância existe, então EMV o escolherá; isto é, EMV se comporta pelo menos tão bem quanto outros métodos em amostras finitas.
- Por fim, a propriedade de **invariância**, isto é, se  $\hat{\theta}$  é a EMV para  $\theta$  então  $\tau(\hat{\theta})$  é a EMV para  $\tau(\theta)$ .

Como vimos na Seção 3.5, em Tomografia de Estados Quânticos [2, 46–48], a estimativa

de máxima verossimilhança pode ser obtida resolvendo o problema:

$$\begin{aligned} \max_{\rho} \quad & \mathcal{L}(\rho) = P(n|\rho) \\ \text{s.a} \quad & \text{tr}(\rho) = 1, \\ & \rho \succeq 0, \end{aligned} \tag{4.1}$$

em que  $P(n|\rho)$  é a probabilidade de ocorrência dos resultados  $n$  dado o parâmetro  $\rho$ . Como discutido na Seção 3.5, a função de verossimilhança  $\mathcal{L}(\rho)$  será definida pela distribuição de probabilidade conjunta das variáveis aleatórias  $\{N_j\}$ , onde  $N_j$  é o número de ocorrências do resultado  $j$  em  $N$  repetições.

Um ponto importante, já mencionado na Seção 3.2, é como lidar com as restrições de (4.1), conhecidas como desigualdades lineares matriciais [14, 22].

Este capítulo apresenta dois métodos para resolução do problema de Máxima Verossimilhança (4.1). A Seção 4.1 trata das restrições de positividade e de traço unitário através da mudança de variáveis (3.10). Tal mudança leva a um problema de otimização irrestrito, porém não convexo. Na literatura [2, 48, 91], considerava-se que os mínimos locais provenientes desta reformulação poderiam ser não-globais, o que representaria uma dificuldade nessa abordagem. Nossa contribuição na Seção 4.1 é mostrar que todos esses mínimos locais são globais [36], validando assim o uso da reparametrização (3.10).

Já na Seção 4.2, estudamos um método específico [46, 47] para quando  $\mathcal{L}(\rho)$  advem de uma distribuição multinomial. Este método explora a estrutura particular do problema e garante que a cada iteração as restrições de (4.1) serão preservadas. No entanto, em [79], os autores provam a convergência global do método com a hipótese de busca linear exata, que em geral é uma hipótese muito forte na prática. Nossa principal contribuição na Seção 4.2 é provar a convergência do método usando uma busca linear inexata que garanta uma melhoria suficiente na verossimilhança a cada iteração.

Além disso, a Seção 4.3 traz uma breve discussão sobre a estimação de erros na EMV usando a matriz de informação de Fisher.

## 4.1 Mudança de Variáveis e Minimizadores locais

Em geral, ao invés de maximizar  $\mathcal{L}(\rho)$ , é mais fácil minimizar a função log-verossimilhança negativa

$$F(\rho) = -\log \mathcal{L}(\rho).$$

Logo, o problema de otimização (4.1) equivale a

$$\begin{aligned} \min_{\rho} \quad & F(\rho) \\ \text{s.a} \quad & \text{tr}(\rho) = 1, \\ & \rho \succeq 0. \end{aligned} \tag{4.2}$$

Do ponto de vista da otimização, se  $F(\rho)$  é uma função convexa, temos um problema de otimização convexa [14] uma vez que o conjunto viável  $\mathcal{S}$  é convexo. Em problemas de otimização convexa, todo minimizador local é global.

As restrições que definem o problema (4.2) são conhecidas como igualdades/desigualdades lineares matriciais [14] e quando a função objetivo  $F(\rho)$  é linear temos um problema de programação semidefinida linear (SDP) [14, 87].

Embora existam eficientes métodos de pontos interiores para programação semidefinida linear [14, 87], a reformulação de (4.2) na forma de um SDP linear requer a introdução de variáveis e restrições auxiliares que aumentam a dimensão, e portanto a dificuldade do problema de otimização.

Nessa seção, consideramos a reparametrização proposta em [2, 48] que converte o problema (4.2) em um problema de otimização irrestrito.

### 4.1.1 Parametrização da Matriz de Densidade

Relembremos que  $\rho$  deve ser Hermitiana semidefinida positiva e de traço um. Para satisfazer a restrição de não negatividade, podemos considerar o produto  $T^\dagger T$ , para qualquer matriz  $T$ , e claramente temos que

$$\langle \psi | T^\dagger T | \psi \rangle = \langle \psi' | \psi' \rangle \geq 0, \quad \forall |\psi\rangle. \tag{4.3}$$

Além disso, a condição de traço unitário pode ser obtida normalizando

$$\frac{T^\dagger T}{\text{tr}(T^\dagger T)}. \tag{4.4}$$

Este tipo de matriz satisfaz as propriedades matemáticas necessárias a uma matriz densidade.

Por exemplo, se o espaço de estados tem dimensão  $d$ , uma escolha natural para a matriz  $T$  em (4.4) é uma matriz triangular superior, como em (3.15). Essa escolha, apresentada em [48], é motivada pelo fato de que em um sistema com  $n$  q-bits, precisamos determinar  $4^n$  parâmetros (os parâmetros de Stokes) para obter uma estimativa da matriz de densidade. Mais ainda, essa escolha lembra o fator de Cholesky [62] se

considerarmos apenas elementos positivos na diagonal. Assim, obtemos a versão parametrizada da matriz  $\rho$ :

$$\rho(t) = \frac{T(t)^\dagger T(t)}{\text{tr}(T(t)^\dagger T(t))}. \quad (4.5)$$

Usando tal parametrização, as restrições sobre uma matriz de densidade são satisfeitas. Note que essa função é uma função contínua e sobrejetiva que vai do espaço de parâmetros  $\mathbb{R}_*^{d^2} = \mathbb{R}^{d^2} \setminus \{0\}$  ao espaço de matrizes densidade  $\mathcal{S}$ . No entanto,  $\rho(t)$  não é injetiva, pois uma mesma matriz pode ser imagem de diferentes parâmetros. Por exemplo, considere a matriz:

$$\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}.$$

Por inspeção de (4.5), é fácil encontrar pelo menos 4 soluções  $t = (\pm 1/\sqrt{2}, \pm 1/\sqrt{2}, 0, 0)^\dagger$ . Além disso, note que qualquer múltiplo não-nulo de  $t$ ,  $\alpha t \quad \forall \alpha \neq 0$ , resulta na mesma matriz.

A parametrização (4.5) assegura a positividade e o traço unitário, mas agora, precisamos minimizar a função  $F(\rho(t))$  com respeito aos novos parâmetros  $t_i$ 's. É claro que a estrutura dessa função depende da distribuição de probabilidade assumida para as incertezas experimentais.

Normalmente,  $F(\rho)$  é uma função convexa em  $\rho$ , para  $\rho \in \mathcal{S}$ . Porém, após a parametrização (4.5), a nova função objetivo  $F(\rho(t))$  se torna uma função não convexa em  $t$  com vários mínimos locais.

Para ilustrar esse fato considere a tomografia de fótons como tratado em [2]. Neste caso o ruído é assumido Gaussiano, como ocorre em vários outros sistemas físicos. Então, a probabilidade de se obter os dados observados  $n$ , dado  $\rho(t)$ , é:

$$P(n | \rho(t)) = \frac{1}{N_0} \prod_j \exp \left[ -\frac{(n_j - \bar{n}_j)^2}{2\bar{\sigma}_j^2} \right], \quad (4.6)$$

onde  $\bar{n}_j$  é o valor esperado,  $\bar{\sigma}_j$  é o desvio padrão (aproximado por  $\sqrt{\bar{n}_j}$ ) para o número de vezes que o  $j$ -ésimo resultado ocorreu, e  $N_0$  é um fator de normalização.

Segundo (3.6),

$$\bar{n}_j = N \text{tr}(\Pi_j \rho(t)), \quad (4.7)$$

onde  $\Pi_j$  é uma medição projetiva, e então, obtemos

$$P(n | \rho(t)) = \frac{1}{N_0} \prod_j \exp \left[ -\frac{(N \text{tr}(\Pi_j \rho(t)) - n_j)^2}{2 N \text{tr}(\Pi_j \rho(t))} \right], \quad (4.8)$$

e para maximizar tal função é suficiente minimizar a log-verossimilhança negativa:

$$F(\rho(t)) = \sum_j \frac{[\text{tr}(\Pi_j \rho(t)) - f_j]^2}{2 \text{tr}(\Pi_j \rho(t))} = \frac{1}{2} \sum_j \left( \frac{\text{tr}(\Pi_j \rho(t)) - f_j}{\sqrt{\text{tr}(\Pi_j \rho(t))}} \right)^2. \quad (4.9)$$

Essa é uma função não-convexa de  $t$ , com vários mínimos locais. Por exemplo, se consideramos a tomografia de um q-bit referente à polarização de um único fóton, a matriz  $\rho(t)$  é:

$$\rho(t) = \frac{1}{t_1^2 + t_2^2 + t_3^2 + t_4^2} \begin{pmatrix} t_1^2 & t_1 t_3 + i t_1 t_4 \\ t_1 t_3 - i t_1 t_4 & t_2^2 + t_3^2 + t_4^2 \end{pmatrix}. \quad (4.10)$$

Realizando medições projetivas com base em  $\{|H\rangle, |V\rangle, |D\rangle, |R\rangle\}$  [2, 48], as quais correspondem respectivamente a estados de polarização horizontal, vertical, diagonal e circular-direita, temos:

$$\begin{aligned} \text{tr}(|H\rangle\langle H|\rho) &= \langle H|\rho(t)|H\rangle = \frac{t_1^2}{t_1^2 + t_2^2 + t_3^2 + t_4^2}, \\ \text{tr}(|V\rangle\langle V|\rho) &= \langle V|\rho(t)|V\rangle = \frac{t_2^2 + t_3^2 + t_4^2}{t_1^2 + t_2^2 + t_3^2 + t_4^2}, \\ \text{tr}(|D\rangle\langle D|\rho) &= \langle D|\rho(t)|D\rangle = \frac{1}{2} \left( 1 + \frac{2t_1 t_3}{t_1^2 + t_2^2 + t_3^2 + t_4^2} \right), \\ \text{tr}(|R\rangle\langle R|\rho) &= \langle R|\rho(t)|R\rangle = \frac{1}{2} \left( 1 - \frac{2t_1 t_4}{t_1^2 + t_2^2 + t_3^2 + t_4^2} \right). \end{aligned} \quad (4.11)$$

Substituindo esses componentes na expressão (4.9), claramente obtemos uma função não-convexa  $F(t)$ . Os exemplos da Seção 4.1.4 ilustram esse fato.

Já que  $F(\rho(t))$  é uma função não convexa de  $t$ , podemos encontrar problemas no processo de otimização. Se minimizadores locais, não-globais existirem, o algoritmo pode encontrar um minimizador local  $t^*$ , que não é global, e a matriz de densidade correspondente  $\rho(t^*)$  pode não ser a EMV  $\hat{\rho}$ .

Alguns trabalhos na área [2, 48, 91] consideram a existência de minimizadores locais que não são globais. Neste caso, um bom chute inicial deve ser fornecido, para que o algoritmo de otimização possa alcançar o minimizador global. Para superar essa dificuldade, alguns autores propuseram pontos iniciais inteligentes para o método de otimização, acreditando que esses pontos pudessem levar a convergência ao minimizador global. Por exemplo, em [48], o chute inicial é baseado em  $\rho_{LM}$  obtido da inversão linear. No entanto, o cálculo desse ponto inicial, requer a solução de um sistema linear, estimar autovalores, e fatoração matricial. Isso representa um alto custo computacional e torna-se proibitivo em sistemas grandes. Além disso, não há garantia de que o minimizador global é alcançado.

Na Seção 4.1.3 provamos que, contrariamente ao que se esperava, todos os minimizadores locais  $t$  de  $F(\rho(t))$  são equivalentes, no sentido de que todos eles são globais e, portanto, levam à mesma estimativa para a matriz de densidade  $\rho(t)$ . Como  $F(\rho)$  consideramos, não apenas a função (4.9) da tomografia de fótons, mas qualquer função convexa de  $\rho$  em  $\mathcal{S}$ . Em verdade, exploramos as propriedades matemáticas da aplicação  $\rho(t)$ , definida por (4.5), para provar que todos os minimizadores  $F(\rho(t))$  são equivalentes.

Primeiro, a Seção 4.1.2 trata da teoria necessária para provar que todos os minimizadores de  $F(\rho(t))$ , para  $t \in \mathbb{R}_{**}^{d^2} = \left\{ t \in \mathbb{R}_*^{d^2} \mid t_i \neq 0, \forall i = 1, \dots, d \right\}$ , são de fato minimizadores globais.

### 4.1.2 A aplicação $\rho(t)$ e o conjunto viável $\mathcal{S}$

Começamos esta seção considerando o problema geral de otimização de uma função convexa  $f(x)$ , tal que  $x \in \Omega$ , com  $\Omega$  também convexo, dada uma parametrização  $x(t)$ . Desenvolvemos condições suficientes para provar a equivalência entre os minimizadores locais. Então, tratamos a otimização de  $F(\rho(t))$  como um caso particular.

Considere o problema de otimização convexa

$$\begin{aligned} \min_x \quad & f(x) \\ \text{s.a.} \quad & x \in \Omega, \end{aligned} \tag{4.12}$$

onde  $f$  é convexa no conjunto convexo  $\Omega \subset \mathbb{R}^n$ .

Seja  $x = x(t)$  uma aplicação *contínua* e *sobrejetiva*  $x : D \rightarrow \Omega$ ,  $D \subset \mathbb{R}^n$  e considere o seguinte problema de otimização irrestrita associado:

$$\min_{t \in D} \quad \phi(t) = f(x(t)). \tag{4.13}$$

É elementar que se  $t^*$  é um minimizador global de (4.13), então  $x^* = x(t^*)$  é também um minimizador global de (4.12). De fato,  $\phi(t^*) \leq \phi(t) \forall t$ , ou seja,  $f(x(t^*)) \leq f(x(t)) \forall t$ , e como  $x(t)$  é sobrejetiva, isso implica que  $f(x^*) \leq f(x)$ ,  $\forall x \in \Omega$ .

Porém, em geral, métodos de otimização podem encontrar apenas minimizadores locais, e alguns minimizadores locais de (4.13) podem não ser globais. De fato, considere o problema de minimizar  $f(x) = x^2$  em  $\mathbb{R}$ , um problema convexo e a seguinte mudança de variáveis  $x(t) = t(t-1)^2 + 1$ . Claramente  $x(t)$  é contínua e sobrejetiva em  $\mathbb{R}$ . Porém, observando o gráfico de  $f(x(t))$ , como função de  $t$ , na Figura 4.1, vemos claramente que tal função apresenta minimizadores locais, não globais. Logo, precisamos de hipóteses mais fortes sobre a aplicação  $x(t)$  para mostrar que todos os minimizadores locais de

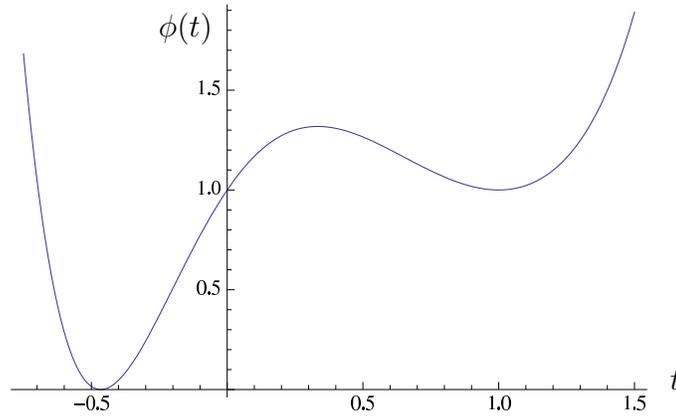


Figura 4.1: Nem todo minimizador local é global

(4.13) são globais.

Se  $x(t)$  é um homeomorfismo, sobre  $\Omega$ , em subconjuntos  $D_\alpha \subset D$  tais que  $D = \cup_\alpha D_\alpha$ , então podemos provar o resultado desejado. Essa condição é mais fraca que pedir que  $x(t)$  seja um homeomorfismo em  $D$ , e é mais facilmente satisfeita por algumas aplicações, em particular a aplicação  $\rho(t)$  em TEQ.

**Hipótese 4.1.1.** *Para a aplicação  $x(t)$ ,  $x : D \rightarrow \Omega$ , existem conjuntos  $D_\alpha \subset D$  tais que  $D = \cup_\alpha D_\alpha$  e, para cada  $D_\alpha$ ,  $x : D_\alpha \rightarrow \Omega$  é um homeomorfismo.*

**Teorema 4.1.1.** *Seja  $x(t)$ ,  $x : D \rightarrow \Omega$  contínua e sobrejetiva. Se a Hipótese 4.1.1 é verificada, então qualquer minimizador local de (4.13) é global.*

*Demonstração.* Seja  $t^*$  um minimizador global de (4.13) e suponha que exista um minimizador local, não-global  $\hat{t}$ . Então,  $f(x(\hat{t})) \leq f(x(t)) \forall t \in B(\hat{t}, \delta) \cap D$ , mas  $f(x(t^*)) < f(x(\hat{t}))$ .

Seja  $x^* = x(t^*)$  e  $\hat{x} = x(\hat{t})$ . Usando a convexidade de  $f$  em  $\Omega$ , e a relação  $f(x^*) < f(\hat{x})$ , temos:

$$f(\lambda x^* + (1 - \lambda)\hat{x}) \leq \lambda f(x^*) + (1 - \lambda)f(\hat{x}) < \lambda f(\hat{x}) + (1 - \lambda)f(\hat{x}) = f(\hat{x}), \quad \forall \lambda \in (0, 1).$$

Note que  $\tilde{x} = \lambda x^* + (1 - \lambda)\hat{x} \in \Omega$ ,  $\forall \lambda \in (0, 1)$ , já que  $\Omega$  é um conjunto convexo, e para  $\lambda$  suficientemente próximo de zero,  $\tilde{x}$  é tão próximo de  $\hat{x}$  quanto necessário, isto é, dado  $\varepsilon > 0$  existe  $\lambda > 0$  tal que  $\tilde{x} \in B(\hat{x}, \varepsilon) \cap \Omega$ .

Como  $x(t)$  satisfaz a Hipótese 4.1.1,  $x(t)$  é um homeomorfismo de  $D_\alpha$  sobre  $\Omega$ , onde  $D_\alpha$  é tal que  $\hat{t} \in D_\alpha$ . Logo, pela continuidade da inversa de  $x(t)$ , dado  $\delta_0 > 0$ , existe  $\varepsilon(\delta_0) > 0$  tal que  $\tilde{x} \in B(\hat{x}, \varepsilon(\delta_0)) \cap \Omega$  implica em  $\tilde{t} \in B(\hat{t}, \delta_0) \cap D_\alpha$ , onde  $\tilde{t} = x^{-1}(\tilde{x})$ . Em particular podemos escolher  $\delta_0 < \delta$ . Portanto, existe  $\tilde{t} \in B(\hat{t}, \delta) \cap D$  tal que  $f(x(\tilde{t})) < f(x(\hat{t}))$ , o que contradiz o fato de  $\hat{t}$  ser minimizador local.  $\square$

Os exemplos a seguir deixam claro o significado do Teorema 4.1.1.

**Exemplo 1.** Considere o problema

$$\begin{aligned} \min_x \quad & (x - 1)^2 \\ \text{s.a} \quad & x \geq 0. \end{aligned} \tag{4.14}$$

Parametrizando  $x = t^2$ , temos que a restrição de positividade estará assegurada  $\forall t \in \mathbb{R}$ . Então temos o seguinte problema irrestrito em  $t$ :

$$\min_t \quad (t^2 - 1)^2, \tag{4.15}$$

cujo gráfico é apresentado na Figura 4.2. Perceba que os minimizadores locais dessa

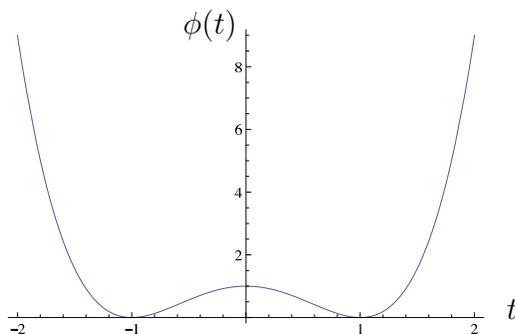


Figura 4.2: Exemplo 1

função  $t = \pm 1$ , correspondem à solução do problema original  $x = 1$ . Note que para  $t \geq 0$  ou  $t \leq 0$ ,  $x(t) = t^2$  cumpre a Hipótese 4.1.1.

**Exemplo 2.** Considere o problema

$$\begin{aligned} \min_{x,y} \quad & (x - 1)^2 + (y - 1)^2 \\ \text{s.a} \quad & x + y = 1, \\ & x, y \geq 0. \end{aligned} \tag{4.16}$$

Parametrizando  $x = \cos^2 \frac{\pi}{4}t$  e  $y = \sin^2 \frac{\pi}{4}t$ , as restrições serão satisfeitas e obtemos o problema irrestrito equivalente

$$\min_t \quad (\cos^2 \frac{\pi}{4}t - 1)^2 + (\sin^2 \frac{\pi}{4}t - 1)^2. \tag{4.17}$$

O gráfico da função objetivo deste problema unidimensional é apresentado na Figura 4.3. Observe que os mínimos locais desta função de  $t$  correspondem à solução do problema original  $(x, y) = (\frac{1}{2}, \frac{1}{2})$ . Perceba que  $(x(t), y(t))$  é um homeomorfismo entre cada um dos intervalos  $[0, 2] + 2n$ , para  $n \in \mathbb{Z}$ , e o conjunto viável de (4.16).

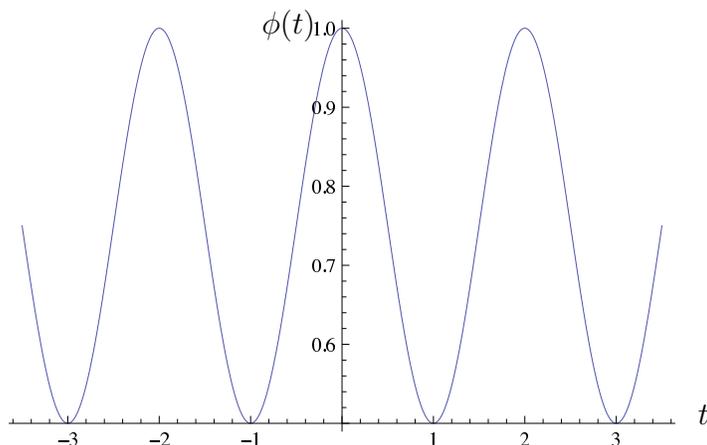


Figura 4.3: Exemplo 2

**Exemplo 3.** Considere o problema

$$\begin{aligned} \min_x \quad & (x + 1)^2 \\ \text{s.a} \quad & x \geq 0. \end{aligned} \tag{4.18}$$

Considerando a parametrização  $x = t^2$ , temos o problema irrestrito

$$\min_t \quad (t^2 + 1)^2, \tag{4.19}$$

cujo gráfico da função é apresentado na Figura 4.4. Note que a solução  $t = 0$  corres-

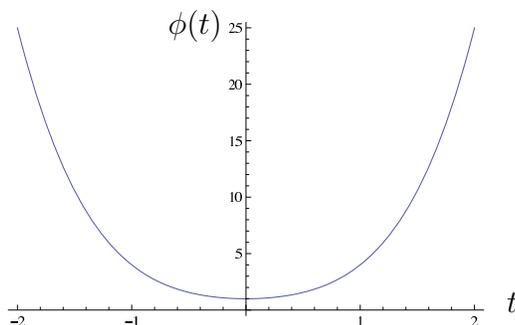


Figura 4.4: Exemplo 3

ponde a  $x = 0$ , solução do problema original, que se encontra na fronteira do conjunto viável.

Agora, como um caso particular dos resultados acima, provamos a equivalência entre os minimizadores locais de  $F(\rho(t))$ . Para isso, precisamos mostrar que a Hipótese 4.1.1 é satisfeita para  $\rho(t)$  definido por (4.5). Em verdade, mostramos que  $\rho : \mathbb{R}_{**}^{d^2} \rightarrow \text{int}(\mathcal{S})$

satisfaz 4.1.1, onde  $\mathbb{R}_{**}^{d^2} = \left\{ t \in \mathbb{R}_*^{d^2} \mid t_i \neq 0, \forall i = 1, \dots, d \right\}$  e  $\text{int}(\mathcal{S})$  é o interior relativo de  $\mathcal{S}$ .

**Proposição 4.1.2.** *A hipótese 4.1.1 é satisfeita pela aplicação  $\rho : \mathbb{R}_{**}^{d^2} \rightarrow \text{int}(\mathcal{S})$ .*

*Demonstração.* Primeiro, precisamos definir os conjuntos  $D_{\alpha,j}$  tais que  $\mathbb{R}_{**}^{d^2} = \cup_{\alpha,j} D_{\alpha,j}$ . O índice  $j$  é um-a-um com as possíveis permutações de sinal dos elementos da diagonal de  $T(t)$  ( $2^d$  permutações de sinal possíveis), ou seja,

$$D_{\alpha,j} = \left\{ t \in \mathbb{R}_{**}^{d^2} \mid \|t\|_2^2 = \alpha \text{ e } t_1, \dots, t_d \text{ cumprindo a } j\text{-ésima configuração de sinal} \right\},$$

que implica em, para  $t \in D_{\alpha,j}$ ,

$$\rho(t) = \frac{1}{\alpha} T(t)^\dagger T(t).$$

A fatoração de Cholesky [35, 62] estabelece que uma matriz Hermitiana  $A$  é definida positiva, se e somente se, existe uma única matriz triangular superior  $T$  com elementos positivos na diagonal, tal que  $A = T^\dagger T$ . É importante destacar que a existência e unicidade do fator triangular superior  $T$  são satisfeitas não apenas sob a condição de que os elementos da diagonal são estritamente positivos, mas também para qualquer ordem fixada de sinais dos elementos da diagonal de  $T$ . Além disso, o fator triangular é contínuo pois cada uma de suas entradas é uma composição de funções contínuas das entradas de  $A$ , [84].

Logo,  $\rho : D_{\alpha,j} \rightarrow \text{int}(\mathcal{S})$  define um homeomorfismo, pois é contínua, bijetiva e tem inversa contínua, a qual é justamente o fator triangular superior com uma escolha fixa de sinais da diagonal. Como  $\mathbb{R}_{**}^{d^2} = \cup_{\alpha,j} D_{\alpha,j}$ , então  $\rho : \mathbb{R}_{**}^{d^2} \rightarrow \text{int}(\mathcal{S})$  cumpre a hipótese 4.1.1.  $\square$

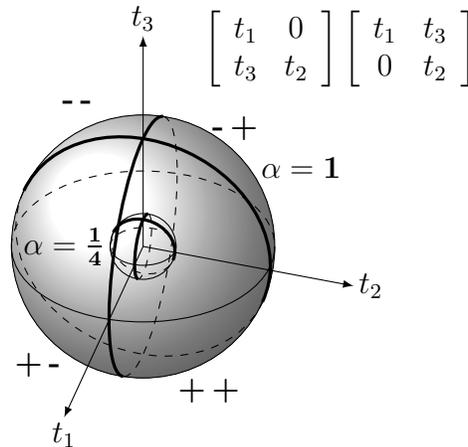


Figura 4.5: Particionando  $\mathbb{R}_{**}^{d^2}$  em conjuntos  $D_{\alpha,j}$

A Figura 4.5 mostra como os conjuntos  $D_{\alpha,j}$  são definidos no caso de uma matriz simétrica (entradas reais)  $2 \times 2$ .

### 4.1.3 Resultado principal: os minimizadores locais são globais

Nessa seção, usando o Teorema 4.1.1 e a Proposição 4.1.2, mostramos que todos os minimizadores locais da função log-verossimilhança negativa  $F(\rho(t))$  são globais. Para qualquer função convexa  $F(\rho)$ , o problema de minimizar  $F(\rho)$  em  $\mathcal{S}$  é um problema de otimização convexa, onde os minimizadores locais  $\rho^*$  são globais. De fato, se temos um conjunto informacionalmente completo de medidas, então o minimizador desse problema de otimização convexa é único.

Como temos um problema de otimização convexo e a aplicação  $\rho(t)$  satisfaz a Hipótese 4.1.1, como um corolário do Teorema 4.1.1 e da Proposição 4.1.2, estabelecemos o principal resultado desta seção.

**Corolário 4.1.3.** *Se  $F(\rho)$  é uma função convexa de  $\rho \in \mathcal{S}$ , então todos os minimizadores locais de  $F(\rho(t))$ , para  $t \in \mathbb{R}_{**}^{d^2}$ , são globais.*

*Demonstração.* Como  $F(\rho)$  é convexa em  $\mathcal{S}$  então também é convexa em  $\text{int}(\mathcal{S})$ . Logo, minimizar  $F(\rho)$  em  $\text{int}(\mathcal{S})$  é um problema de otimização convexa. Segundo a Proposição 4.1.2 a aplicação  $\rho(t)$ ,  $\rho : \mathbb{R}_{**}^{d^2} \rightarrow \text{int}(\mathcal{S})$ , satisfaz a Hipótese 4.1.1, e então o Teorema 4.1.1 pode ser aplicado, o que implica que todos os minimizadores locais de  $F(\rho(t))$  em  $\mathbb{R}_{**}^{d^2}$  são globais.  $\square$

O resultado prático fornecido pelo Corolário 4.1.3 é que não importa qual minimizador local de  $\hat{t} \in \mathbb{R}_{**}^{d^2}$  é encontrado. Todos eles são equivalentes, no sentido de que levam à mesma matriz densidade  $\hat{\rho} = \rho(\hat{t})$  que corresponde à estimativa de máxima verossimilhança. Em verdade, cada minimizador local é a solução única do problema

$$\min_{t \in D_{\alpha,j}} F(\rho(t)), \quad (4.20)$$

para cada  $\alpha$  e  $j$ . Como  $\rho(t)$  é um homeomorfismo de  $D_{\alpha,j}$  em  $\text{int}(\mathcal{S})$ , se minimizar  $F(\rho)$  em  $\text{int}(\mathcal{S})$  tem uma única solução, então (4.20) também terá solução única.

Por exemplo, o problema

$$\begin{aligned} \min_{t \in \mathbb{R}^{d^2}} & F(\rho(t)) \\ \text{s.a} & \quad \|t\|_2^2 = 1, \\ & \quad t_i > 0 \quad i = 1, \dots, d, \end{aligned} \quad (4.21)$$

terá um único minimizador local  $\hat{t}$  e portanto global. Isso corresponde a  $\alpha = 1$  e  $j$  associado aos sinais todos positivos dos elementos da diagonal  $t_1, \dots, t_d$ .

Embora o resultado acima considere  $\rho(t)$  restrito a  $\mathbb{R}_{**}^{d^2}$  sobre  $\text{int}(\mathcal{S})$ , é direto mostrar

que esses conjuntos são densos em  $\mathbb{R}_*^{d^2}$  e  $\mathcal{S}$ , respectivamente. Portanto, pela continuidade de  $F(\rho)$  e  $F(\rho(t))$ , temos

$$\min_{\rho \in \mathcal{S}} F(\rho) = \inf_{\rho \in \text{int}(\mathcal{S})} F(\rho) \quad \text{e} \quad \min_{t \in \mathbb{R}_*^{d^2}} F(\rho(t)) = \inf_{t \in \mathbb{R}_{**}^{d^2}} F(\rho(t)).$$

Portanto, na prática, é suficiente considerar  $\mathbb{R}_{**}^{d^2}$  ao invés de  $\mathbb{R}_*^{d^2}$ . Em verdade, é suficiente considerar apenas um conjunto  $D_{\alpha,j}$ , por exemplo, restringindo  $\|t\|_2^2 = 1$  e  $t_i > 0$  para  $i = 1, \dots, d$ . Mas essas restrições tornam o problema de otimização mais difícil que um problema irrestrito, e o Corolário 4.1.3 nos dá a garantia de que qualquer minimizador local do problema irrestrito em  $\mathbb{R}_{**}^{d^2}$  pode ser usado.

De fato, pontos que pertencem a  $\mathbb{R}_*^{d^2} \setminus \mathbb{R}_{**}^{d^2}$  correspondem a matrizes densidade de posto deficiente que estão na fronteira de  $\mathcal{S}$ . Do ponto de vista de otimização numérica, para métodos de pontos interiores, soluções na fronteira, em geral, são atingidas apenas no limite. Isto é, numericamente, um ponto no interior suficientemente próximo da solução da fronteira é declarado solução dentro de uma certa tolerância. Além disso, a função log-verossimilhança negativa, por exemplo (4.9), pode não estar definida em alguns estados da fronteira, dependendo do conjunto POVM escolhido. Do ponto de vista experimental, matrizes na fronteira de  $\mathcal{S}$  correspondem a estados com autovalores nulos, por exemplo estados puros, que são raramente observados na prática devido a dificuldades tanto na realização quanto a imperfeições no aparato experimental, levando a dados experimentais com ruído.

Finalmente, destacamos que o resultado acima permanece válido para qualquer função convexa  $F(\rho)$  em  $\mathcal{S}$ . Em particular, podemos aplicar o resultado à função log-verossimilhança negativa  $F(\rho) = -\log P(n|\rho)$ , pois quando  $P(n|\rho)$  é Gaussiana ou multinomial, a função  $F(\rho)$  será convexa.

#### 4.1.4 Experimentos Numéricos

Mencionamos que alguns artigos [2, 48, 91] consideram a possibilidade de encontrar minimizadores locais que não são globais, ao minimizar a função (4.9). No entanto, na Seção 4.1.3, mostramos que todos os minimizadores locais de  $F(\rho(t))$  em  $\mathbb{R}_{**}^{d^2}$  são também globais. O que pode ocorrer em alguns casos é a estagnação de certos métodos, os quais não possuem propriedade de convergência global [54, 70] (tal propriedade não deve ser confundida com convergência a minimizadores globais).

**Definição 4.1.4.** *Seja  $F \in \mathcal{C}^1$ . Dizemos que um algoritmo de otimização para resolver*

$$\min_{x \in \mathbb{R}^n} F(x)$$

*tem convergência global a pontos estacionários ( $\nabla F(x) = 0$ ), se todo ponto de acumulação de uma sequência de iterandos  $\{x_k\}_{k=1}^{\infty}$  gerada pelo algoritmo é um ponto estacionário de  $F(x)$ .*

Alguns métodos de otimização irrestrita, por exemplo o conhecido método de Nelder-Mead [19, 66], não possui propriedade de convergência global, isto é, um ponto de estagnação pode não ser estacionário. Além disso, pacotes comerciais implementam alguns métodos que não tem convergência global: por exemplo, a rotina `fminsearch` do `MATLAB`, a qual implementa o método de Nelder-Mead, e a rotina `FindMinimum` do `Mathematica`, a qual implementa o método de Powell [75]. Ambos os métodos, usados em tomografia de estados quânticos, podem parar prematuramente, antes de alcançar um minimizador local ou um ponto estacionário.

Mesmo métodos que tenham propriedade de convergência global podem ainda parar prematuramente por conta de dificuldades numéricas. Desse modo, é importante investigar qual critério de parada foi acionado, a fim de evitar conclusões equivocadas. Na prática, geralmente esperamos que um algoritmo de otimização possa encontrar, ao menos, um ponto  $\varepsilon$ -estacionário  $x^*$ , isto é,  $\|\nabla F(x^*)\| < \varepsilon$ . Entretanto, o problema de otimização pode ser mal escalado, ou tão difícil, que outro critério de parada deve ser empregado para evitar que o algoritmo itere indefinidamente. Normalmente, critérios de estagnação como mudanças muito pequenas nas variáveis  $\|x_{k+1} - x_k\| < \varepsilon_x$  ou na função objetivo  $|F(x_{k+1}) - F(x_k)| < \varepsilon_F$  são usados e, limitantes superiores são fixados para o número máximo de iterações ou avaliações de função. Como é preferível parar com o critério de  $\varepsilon$ -estacionariedade, as demais tolerâncias devem ser menores que  $\varepsilon$ , por exemplo  $\varepsilon_x = \varepsilon_F = \varepsilon^2$  quando  $0 < \varepsilon \ll 1$ .

Uma outra consequência indesejável da parametrização (4.5) é que quando  $\|t\| \rightarrow \infty$ ,  $\|\nabla_t F(\rho(t))\| \rightarrow 0$ . Logo, algoritmos de otimização usando como critério de parada  $\|\nabla F(\rho(t))\| < \varepsilon$ , podem parar em pontos  $t$  com  $\|t\|$  grande, mesmo se  $t$  não é um minimizador de (4.9). Portanto, limitantes artificiais nas variáveis devem ser usados para evitar tal situação.

Os próximos exemplos mostram o que pode resultar em soluções indesejáveis em TEQ ao usar métodos inapropriados, sem propriedade de convergência global ou numericamente instáveis. Para tais exemplos, fixamos as tolerâncias em  $\varepsilon_x = \varepsilon_F = 10^{-8}$  e o número máximo de iterações e avaliações de função como  $M = 2 \times 200 \times n$ , onde  $n$  é o número de variáveis do problema de otimização, e  $200 \times n$  é o limite padrão usado na rotina `fminsearch` do `MATLAB`. Pode-se definir essas tolerâncias usando a rotina `optimset`. Infelizmente, `MATLAB` usa a mesma tolerância na variação da função objetivo e na norma do gradiente,  $\varepsilon_F = \varepsilon$ , e não há opção de usar tolerâncias distintas para estes testes. Nos exemplos 1 e 2, usamos  $\varepsilon = 10^{-8}$ .

**Exemplo 1.** Considere  $\rho = |H\rangle\langle H|$  como o estado verdadeiro que desejamos identificar com a tomografia. Os valores esperados para medições projetivas baseadas em  $\{|H\rangle, |V\rangle, |D\rangle, |R\rangle\}$ , e perturbados por algum tipo de erro (gerados computacionalmente com base em uma distribuição Gaussiana), tem o papel de frequências experimentais normalizadas:  $f_H = 0.9990$ ,  $f_V = 0.0002$ ,  $f_D = 0.4995$ ,  $f_R = 0.4994$ . Usando a rotina

`fminsearch` do MATLAB R2009a, com ponto inicial  $t_0 = (-0.0001, 0.999, 0.001, 0.999)^T$ , recuperamos a seguinte matriz:

$$\rho = \begin{bmatrix} 0.2219 & -0.3634 + 0.0002i \\ -0.3634 - 0.0002i & 0.7781 \end{bmatrix}.$$

A rotina de otimização parou após  $k = 595$  iterações, com valor de função objetivo  $\bar{F} = 2.2316$ , e norma do gradiente  $\|\nabla \bar{F}\| = 0.0013$ . O critério de parada acionado foi  $\|\bar{x} - x_l\|_\infty \leq \varepsilon_x$  e  $|\bar{f} - f_l| \leq \varepsilon_F$ , onde  $\bar{f} = f(\bar{x})$  é o valor de função no melhor ponto  $\bar{x}$  e  $f_l$ 's são os valores de função em outros pontos do simplex  $x_l$ 's.

Por outro lado, usamos também a rotina `lsqnonlin` para problemas de quadrados mínimos não lineares, do MATLAB R2009a, considerando a estrutura especial da função (4.9). Fornecendo as derivadas parciais para construir a matriz Jacobiana, a rotina executa um algoritmo de região de confiança [18]. Usando o mesmo ponto inicial, obtemos:

$$\rho = \begin{bmatrix} 0.9998 & -0.0005 + 0.0006i \\ -0.0005 - 0.0006i & 0.0002 \end{bmatrix},$$

com  $\bar{F} = 3.2 \times 10^{-7}$ ,  $\|\nabla \bar{F}\| = 5.3024 \times 10^{-10}$ , após  $k = 22$  iterações. Perceba a diferença entre as normas dos gradientes nesses dois casos. Claramente, o primeiro não corresponde a um ponto estacionário, tampouco um minimizador local.

Outro aspecto importante é a não unicidade da parametrização  $\rho(t)$ . Considere o mesmo conjunto de dados acima. Usando `lsqnonlin` a partir do ponto inicial  $t_0 = (1, 0.001, 0, 0)^T$ , obtemos a solução

$$\hat{t} = (0.999, 0.0141, -0.0005, 0.0006)^T,$$

a qual fornece a matriz

$$\rho(\hat{t}) = \begin{bmatrix} 0.9998 & -0.0005 + 0.0006i \\ -0.0005 - 0.0006i & 0.0002 \end{bmatrix}.$$

Iniciando de outro ponto  $t'_0 = (-1, -0.001, 0, 0)^T$ , a solução é

$$t' = (-0.999, -0.0141, 0.0005, -0.0006)^T,$$

a qual fornece a matriz

$$\rho(t') = \begin{bmatrix} 0.9998 & -0.0005 + 0.0006i \\ -0.0005 - 0.0006i & 0.0002 \end{bmatrix}.$$

Ambos  $\hat{t}$  e  $t'$  satisfazem o critério numérico de estacionariedade  $\|\nabla F\| < \varepsilon$ . Apesar de minimizadores locais distintos, recuperamos a mesma matriz de densidade, comprovando o que comentamos na Seção 4.1.1.

**Exemplo 2.** Considere os seguintes dados experimentais extraídos de um conjunto completo de medidas sobre os graus de liberdade de polarização de dois fótons gerados pelo processo de conversão paramétrica descendente [2], onde o estado preparado é quase puro:

$$\begin{array}{rcccc} n_1 & = & 3043 & n_5 & = & 1546 & n_9 & = & 1556 & n_{13} & = & 1070 \\ n_2 & = & 32 & n_6 & = & 1283 & n_{10} & = & 122 & n_{14} & = & 1048 \\ n_3 & = & 2159 & n_7 & = & 938 & n_{11} & = & 1271 & n_{15} & = & 1611 \\ n_4 & = & 19 & n_8 & = & 1595 & n_{12} & = & 1621 & n_{16} & = & 114. \end{array}$$

Primeiro, usamos `fminsearch` do MATLAB R2009a, com chute inicial  $t_i = 1/\sqrt{d}$  para  $i \leq d$  e  $t_i = 0$ , para  $i > d$  (correspondendo ao estado maximamente misto,  $I/d$ ). O algoritmo pára porque o número máximo de avaliações de função ( $2 \times 16 \times 200 = 6400$ ) foi atingido. A matriz de densidade recuperada é apresentada na Figura 4.6 e apresenta pureza  $\text{tr}(\rho_1^2) = 0.5298$ .

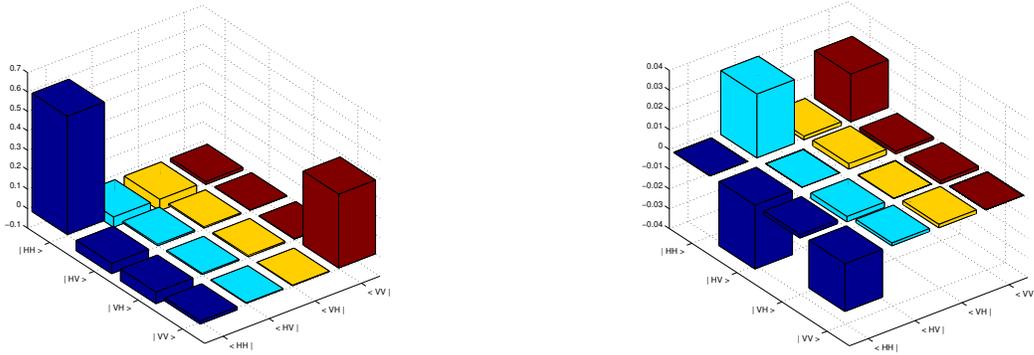


Figura 4.6: Partes real (esquerda) e imaginária (direita) da matriz de densidade do Exemplo 2 usando o *solver* `fminsearch` do MATLAB.

Em seguida, usamos `lsqnonlin` do MATLAB R2009a, com o mesmo ponto inicial, e obtemos a matriz de densidade da Figura 4.7, com pureza  $\text{tr}(\rho_2^2) = 0.9008$ .

**Exemplo 3.** Para concluir os experimentos numéricos e destacar o significado do Corolário 4.1.3, consideramos o estado  $\rho = |R\rangle\langle R|$ , e as frequências normalizadas  $f_H = 0.5$ ,  $f_V = 0.5$ ,  $f_D = 0.5$  e  $f_R = 1$ . A teoria apresentada na Seção 4.1.3 nos diz que a solução do problema de minimizar  $F(\rho(t))$  em  $D_{\alpha,j}$  é única, para cada  $\alpha$  e  $j$ . Logo, se incluirmos a restrição  $\|t\|_2^2 = 1$ , isto é, fixando  $\alpha = 1$  e escolhendo uma ordem de sinais dentre  $++,+-,-+,-,-$ , no caso de matrizes  $2 \times 2$ , então teremos exatamente uma solução. Para testar esse fato numericamente, definimos quatro problemas de minimizar  $F(\rho(t))$  sujeito a  $\|t\|_2^2 = 1$  e para cada problema as restrições:  $t_1 > 0$  e  $t_2 > 0$ ,  $t_1 > 0$  e  $t_2 < 0$ ,  $t_1 < 0$  e  $t_2 > 0$ ,  $t_1 < 0$  e  $t_2 < 0$ . Para cada escolha de sinais, usamos um procedimento multistart [45], gerando 23 pontos iniciais aleatórios com componentes no intervalo  $[-1, 1]$ , que foram usados pela rotina `fmincon` para resolver os problemas

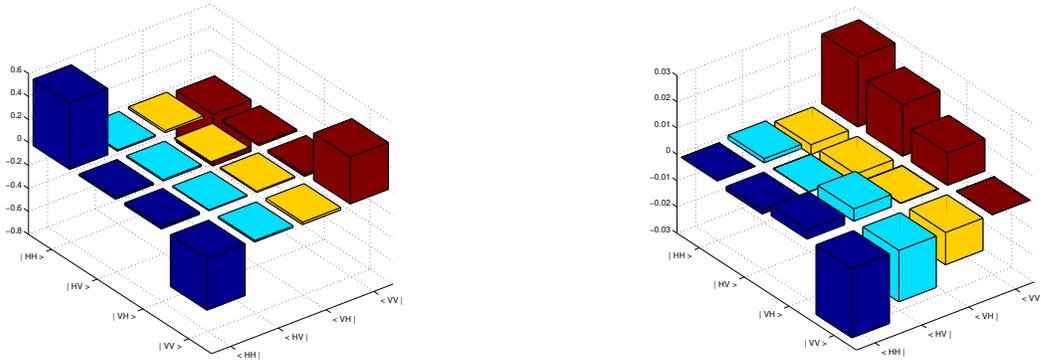


Figura 4.7: Partes real (esquerda) e imaginária (direita) da matriz de densidade do Exemplo 2 usando o solver `lsqnonlin` do MATLAB. Derivadas parciais foram fornecidas.

de otimização restrita. Usamos as tolerâncias  $\varepsilon_x = \varepsilon_F = 10^{-12}$  e consideramos que um problema é resolvido somente se a medida de otimalidade de primeira ordem é menor que  $\varepsilon = 10^{-6}$ , descartando soluções que não cumpram esse critério. Consideramos, para cada escolha de sinais, uma lista de soluções, e assim que uma nova solução candidata  $\hat{t}$  é obtida, a incluímos na lista somente se  $\|\hat{t} - t\|_2 > 10^{-2}$ . Para cada escolha de sinais, cada lista tem apenas um membro como mostra a Tabela 4.1. Este experimento

	++	+-	-+	--
$t_1$	0.7071	0.7071	-0.7071	-0.7071
$t_2$	0.0024	-0.0000	0.0001	-0.0002
$t_3$	0.0000	0.0000	-0.0000	0.0000
$t_4$	-0.7071	-0.7071	0.7071	0.7071

Tabela 4.1: Soluções para cada ordenação de sinais, após 23 pontos iniciais aleatórios.

numérico confirma o esperado pela teoria das Seções 4.1.2 e 4.1.3.

Esses exemplos esclarecem a natureza dos minimizadores locais de  $F(\rho(t))$  e ilustram alguns equívocos que podem ocorrer na minimização da função log-verossimilhança negativa, destacando a importância de métodos de otimização com garantias teóricas de convergência e estáveis numericamente, assim como a análise dos critérios de parada e tolerâncias.

### 4.1.5 Conclusões desta seção

Nesta seção, mostramos que a estimação por máxima verossimilhança através da parametrização (4.5), quando usada com métodos de otimização numérica apropriados, é um procedimento eficaz para estimar a matriz de densidade em Tomografia de Estados Quânticos. Provamos que apesar dessa abordagem implicar em um problema

de otimização irrestrito com possivelmente vários minimizadores, todos eles são globais. Portanto, usando-se um método de otimização numérica globalmente convergente e numericamente estável, uma solução local, que também é global, será encontrada independentemente do ponto inicial.

Isso tem consequências práticas importantes, pois como foi discutido, a utilização de ponto iniciais mais elaborados representa um custo computacional adicional, tornando assim proibitiva para reconstrução de estados quânticos de um número grande de q-bits.

Mais ainda, contrariamente ao que era assumido por trabalhos anteriores, nossos exemplos mostram que falhas na estimação da matriz de densidade ótima estão mais relacionados ao uso de rotinas de otimização inapropriadas que não tem propriedade de convergência global ou sofrem de instabilidade numérica. Esse fato foi provavelmente confundido com a existência de minimizadores locais não-globais no processo de minimização da função log-verossimilhança negativa. Portanto, devemos ser cuidadosos na escolha e análise dos critérios de parada e tolerâncias utilizadas.

Por fim, nossos resultados sobre a parametrização  $\rho(t)$  e os minimizadores locais de  $F(\rho(t))$  permanecem válidos para qualquer função convexa de  $\rho$ ,  $F(\rho)$ .

## 4.2 Algoritmo $R\rho R$ e Convergência Global

Nessa seção, discutimos o algoritmo  $R\rho R$  [46] para resolver o problema de otimização que surge na estimação por Máxima Verossimilhança.

Seguindo [46, 47], consideramos medidas descritas por um conjunto POVM  $\{E_i\}_i$

$$E_i \succeq, 0 \quad \sum_i E_i = I,$$

e uma verossimilhança definida por uma distribuição multinomial, para um conjunto de frequências normalizadas  $\{f_i\}$ :

$$\mathcal{L}(\rho) \propto \prod_i p_i(\rho)^{Nf_i},$$

onde  $p_i(\rho) = \text{tr}(E_i\rho)$ . Como a função log-verossimilhança é mais tratável, nosso objetivo é encontrar  $\rho$  que resolve o problema

$$\begin{aligned} \max_{\rho} \quad & \sum_i f_i \log p_i(\rho) \equiv f(\rho) \\ \text{s.a} \quad & \text{tr}(\rho) = 1 \\ & \rho \succeq 0. \end{aligned} \tag{4.22}$$

Vamos estudar um algoritmo específico para a resolução de (4.22), proposto em [46, 47], que tira proveito da estrutura do problema e, em geral, funciona bem na prática.

Considere o gradiente da função objetivo  $f(\rho)$ , dado por

$$\nabla f(\rho) = \sum_i \frac{f_i}{\text{tr}(E_i \rho)} E_i \equiv R(\rho). \quad (4.23)$$

Aplicando as condições de otimalidade de Karush-Kuhn-Tucker (KKT) [59, 70] ao problema (4.22), temos

$$-R(\rho) + \lambda_0 I - S = 0, \quad (4.24)$$

$$\text{tr}(\rho) = 1, \quad \rho \succeq 0, \quad (4.25)$$

$$S\rho = 0, \quad S \succeq 0, \quad (4.26)$$

ou equivalentemente

$$\text{tr}(\rho) = 1, \quad \rho \succeq 0, \quad (4.27)$$

$$(R(\rho) - \lambda_0 I)\rho = 0, \quad -R(\rho) + \lambda_0 I \succeq 0. \quad (4.28)$$

Tomando o traço na igualdade em (4.28) e usando (4.27) temos que

$$\lambda_0 = \text{tr}(R(\rho)\rho) = 1.$$

Assumindo que na solução  $\rho \succ 0$ , temos que uma matriz de densidade positiva  $\rho$  resolve (4.22) se satisfaz a equação extrema

$$R(\rho)\rho = \rho, \quad (4.29)$$

ou equivalentemente

$$R(\rho)\rho R(\rho) = \rho. \quad (4.30)$$

Se a matriz de densidade  $\rho$  é restrita às matrizes diagonais, a solução de (4.29) pode ser obtida pelo algoritmo Expectation-Maximization (EM) [93]. O algoritmo EM garante que a verossimilhança aumenta a cada iteração e converge a um ponto fixo de (4.29). No entanto, o algoritmo EM não pode ser aplicado ao problema quântico, pois sem a restrição diagonal ele pode não preservar a positividade da matriz. Em [47], foi proposto um método iterativo baseado na equação (4.30), chamado  $R\rho R$ :

$$\rho^{k+1} = \mathcal{N} [R(\rho^k)\rho^k R(\rho^k)],$$

onde  $\mathcal{N}$  é uma constante de normalização que garante traço unitário.

Note que a positividade é preservada explicitamente a cada iteração. Outra propriedade notável do algoritmo  $R\rho R$  é seu custo computacional: a cada iteração é necessário

apenas calcular produtos matriz-matriz. Esta é uma iteração bem barata comparada a uma iteração de um método de pontos-interiores para SDP, por exemplo.

Embora o algoritmo  $R\rho R$  seja uma generalização do algoritmo EM, sua convergência não é garantida em geral. Em [79], é apresentado um contra-exemplo onde o método cicla. Por esse motivo, aquele trabalho propõe uma versão “diluída do algoritmo”  $R\rho R$ , que chamaremos  $R\rho R$  Diluído.

A ideia é controlar o tamanho de passo a cada iteração, através de uma combinação entre o operador  $R(\rho)$  e o operador identidade:

$$\rho^{k+1} = \mathcal{N} \left[ \frac{I + tR(\rho^k)}{1+t} \right] \rho^k \left[ \frac{I + tR(\rho^k)}{1+t} \right], \quad (4.31)$$

controlada pelo parâmetro  $t > 0$ , e onde  $\mathcal{N}$  é uma constante de normalização. É importante notar que à medida que  $t \rightarrow \infty$  a iteração tende à iteração  $R\rho R$ . Além disso, quando  $t > 0$  é suficientemente pequeno, é provado que a função de verossimilhança é estritamente aumentada, sempre que  $R(\rho)\rho \neq \rho$ . Também é demonstrado que o  $R\rho R$  Diluído é convergente à matriz de densidade de máxima verossimilhança se o ponto inicial é o estado maximamente misto  $\rho^0 = (1/d)I$  e se, a cada iteração, o valor ótimo de  $t$  é utilizado

$$t = \arg \max_{t>0} f(\rho^{k+1}(t)). \quad (4.32)$$

Em programação não-linear [8, 59, 70], isto é chamado de busca linear exata. Ainda que a convergência possa ser obtida usando tal estratégia, em geral, resolver (4.32) pode ser caro computacionalmente. Em [79] os autores demonstram a convergência global com busca linear exata. No entanto, sugerem que na prática deve-se usar um esquema *ad hoc* para se determinar o melhor valor fixo para o parâmetro  $t$  a ser usado por todas as iterações.

Aqui, ao invés de impor (4.32), propomos uma busca linear inexata para determinar o tamanho de passo  $t$  a cada iteração (4.31). Não procuramos o valor ótimo de  $t > 0$ , mas qualquer valor que assegure uma melhoria suficiente na log-verossimilhança. Provamos que este procedimento está bem definido e que, empregando-o, e usando como matriz inicial qualquer  $\rho^0 \in \text{int}(\mathcal{S})$ , as iterações (4.31) convergem à solução de (4.22). A implementação da busca linear inexata é direta e apresentamos alguns exemplos mostrando que essa estratégia é superior ao procedimento *ad hoc* de usar um valor fixo para  $t$ .

Na Subseção 4.2.1 revisamos a teoria de convergência global em programação não-linear necessária às nossas demonstrações. A Subseção 4.2.2 apresenta a prova de convergência global do algoritmo  $R\rho R$  Diluído usando busca linear inexata e a condição de Armijo. Exemplos ilustrando as diferenças e similaridades de nossa proposta com a tradicional (tamanho de passo fixo) são apresentados na Subseção 4.2.3. A Subseção 4.2.4 apresenta algumas considerações finais.

### 4.2.1 Convergência global de algoritmos de subida

Esta subsecção está baseada na referência [8].

Considere o seguinte problema de maximização

$$\begin{aligned} \max_x \quad & f(x) \\ \text{s.a.} \quad & x \in \Omega, \end{aligned} \tag{4.33}$$

onde  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  é uma função continuamente diferenciável e  $\Omega \in \mathbb{R}^n$  é um conjunto convexo.

Dada a aproximação  $x^k$  para a solução de (4.33), métodos de direção de subida tentam melhorar o valor atual da função objetivo gerando uma direção de busca  $d^k$  e atualizando o iterando

$$x^{k+1} = x^k + t_k d^k, \tag{4.34}$$

onde  $t_k$  é o tamanho de passo.

Dizemos que a direção  $d^k$  é uma *direção de subida* no iterando  $x^k$  se

$$\nabla f(x^k)^T d^k > 0.$$

Isso assegura que, para um tamanho de passo  $t_k > 0$  suficientemente pequeno, o valor da função objetivo é aumentado. Dizemos que uma direção de subida  $d^k$  é *factível* se  $x^{k+1}$  definido em (4.34) pertence a  $\Omega$  para  $t_k \in (0, \varepsilon)$ , para algum  $\varepsilon > 0$ .

Desse modo, a iteração (4.34) pode ser repetida enquanto houver uma direção factível e de subida. Se em algum ponto  $x^*$  não há direção factível e de subida, dizemos que  $x^*$  é um *ponto estacionário*. Sabemos que todo maximizador local é um ponto estacionário, mas a recíproca não é verdadeira em geral. Se a função  $f$  é côncava no conjunto convexo  $\Omega$ , então todo ponto estacionário é também um maximizador.

Um algoritmo de maximização para (4.33) é dito *globalmente convergente* [8, 70] se todo ponto limite da sequência gerada pelo algoritmo é um ponto estacionário, independentemente do ponto inicial  $x^0$ . Embora direções factíveis e de subida assegurem que, para  $t_k > 0$  suficientemente pequeno, podemos aumentar o valor da função, isso não é suficiente para assegurar a convergência global. A razão é que um acréscimo simples,  $f(x^{k+1}) > f(x^k)$ , na função ao longo de tal direção é um objetivo muito modesto, e contra-exemplos unidimensionais são facilmente construídos [59]. Para atingir maximizadores locais, ou pelo menos pontos estacionários, um aumento *suficiente* a cada iteração se faz necessário.

Uma escolha natural para  $t_k$ , quando pensamos em maximizar a função objetivo na

direção  $d^k$ , é a solução do problema:

$$t_k = \operatorname{argmax}_t f(x^k + td^k), \quad (4.35)$$

o que é chamado de *busca linear exata*. No entanto, encontrar o maximizador global de  $f$  ao longo da direção  $d^k$  é por si só um problema difícil, e a menos que a função  $f$  tenha uma estrutura especial, como uma quadrática por exemplo, o esforço computacional pode ser considerável.

Para evitar o esforço computacional de (4.35), uma busca linear inexata pode ser realizada. Um esquema bastante natural consiste na redução sucessiva do tamanho do passo. Uma vez que a busca é ao longo de uma direção de subida, eventualmente para  $t_k$  pequeno, podemos obter  $f(x^k + t_k d^k) > f(x^k)$ . Mas, esse aumento simples pode não evitar algumas dificuldades de convergência. Uma possível estratégia é usar a regra de *Armijo*, a qual demanda um tamanho de passo  $t$  tal que uma melhoria substancial na função objetivo seja obtida:

$$f(x^k + td^k) > f(x^k) + \gamma t \nabla f(x^k)^T d^k, \quad (4.36)$$

onde  $\gamma \in (0, 1)$ . Podemos diminuir o tamanho de passo  $t$  até que a condição (4.36) seja verificada. Há outras alternativas à redução sucessiva do tamanho do passo, como por exemplo, estratégias baseadas em interpolação quadrática ou cúbica [70].

Além da escolha do tamanho do passo, condições sobre as direções de subida  $d^k$  também são necessárias para se evitar certos problemas. Por exemplo, não é desejável ter direções  $d^k$  com norma pequena quando estamos longe da solução. É também necessário evitar que uma sequência de direções  $\{d^k\}$  torne-se ortogonal ao gradiente de  $f$  pois, neste caso, a derivada direcional é praticamente zero e então pouco ou nenhum progresso na função objetivo pode ser obtido. Uma condição geral que evita tais problemas é denominada *gradient related* [8].

**Definição 4.2.1** (*Gradient related*). Uma sequência de direções  $\{d^k\}$  é *gradient related* se, para qualquer subsequência  $\{x^k\}_{k \in \mathcal{K}}$  que converge a um ponto não estacionário, a correspondente subsequência de direções  $\{d^k\}_{k \in \mathcal{K}}$  é limitada e satisfaz

$$\liminf_{k \rightarrow \infty} \inf_{k \in \mathcal{K}} \nabla f(x^k)^T d^k > 0.$$

Essa condição significa que  $\|d^k\|$  não se torna “tão pequena” ou “tão grande” em relação a  $\|\nabla f(x^k)\|$  e que  $d^k$  e  $\nabla f(x^k)$  não serão ortogonais.

Se um algoritmo gera direções factíveis e de subida que satisfazem a condição *gradient related* e os tamanhos de passo são escolhidos segundo a regra de Armijo, então é possível provar a convergência global [8].

**Teorema 4.2.2** (Convergência global). *Seja  $\{x^k\}$  uma sequência gerada por um método de direções factíveis e de subida  $x^{k+1} = x^k + t_k d^k$ , e assumamos que  $\{d^k\}$  é gradient related e  $t_k$  é escolhido pela regra de Armijo. Então, todo ponto limite de  $\{x^k\}$  é um ponto estacionário.*

*Demonstração.* Veja [8, Proposição 2.2.1]. □

## 4.2.2 Convergência global do $R\rho R$ Diluído

Lembrando que  $R(\rho) \equiv \nabla f(\rho)$ , vamos reescrever a iteração (4.31) como

$$\rho^{k+1} = \frac{(I + t\nabla f(\rho^k)) \rho^k (I + t\nabla f(\rho^k))}{\text{tr}((I + t\nabla f(\rho^k)) \rho^k (I + t\nabla f(\rho^k)))} \equiv G(\rho^k). \quad (4.37)$$

Esta expressão pode ser vista como uma iteração de ponto fixo. Expandindo-a, obtemos

$$G(\rho) = \frac{\rho + t(\nabla f(\rho)\rho + \rho\nabla f(\rho)) + t^2 \nabla f(\rho)\rho\nabla f(\rho)}{1 + 2t + t^2 \text{tr}(\nabla f(\rho)\rho\nabla f(\rho))}. \quad (4.38)$$

Note que  $\rho^*$  é um ponto fixo de  $G(\rho)$ ,  $G(\rho^*) = \rho^*$ , para  $t > 0$ , se as seguintes condições são satisfeitas

$$\rho^* = \nabla f(\rho^*)\rho^*\nabla f(\rho^*) = \nabla f(\rho^*)\rho^*. \quad (4.39)$$

Se as condições acima são verificadas para uma matriz definida positiva e de traço um  $\rho^*$ , então as *condições de otimalidade*, (4.24)-(4.26), para o problema (4.22) são satisfeitas e  $\rho^*$  é a estimativa de máxima verossimilhança.

**Lema 4.2.3.** *Para qualquer  $\rho \in \text{int}(\mathcal{S})$  temos que*

$$\text{tr}(\nabla f(\rho)\rho) = 1.$$

*Demonstração.* Consequência direta de (4.23). □

**Lema 4.2.4.** *Para  $\rho \in \text{int}(\mathcal{S})$ , temos que*

$$\text{tr}(\nabla f(\rho)\rho\nabla f(\rho)) \geq 1,$$

*com igualdade se e somente se  $\rho = \nabla f(\rho)\rho$ .*

*Demonstração.* Pelo Lema 4.2.3

$$1 = \text{tr}(\nabla f(\rho)\rho) = \text{tr}(\nabla f(\rho)\rho^{1/2}\rho^{1/2}),$$

e aplicando Cauchy-Schwarz, obtemos

$$1 = |\text{tr}(\nabla f(\rho)\rho^{1/2}\rho^{1/2})|^2 \leq \text{tr}(\nabla f(\rho)\rho\nabla f(\rho)) \text{tr}(\rho) = \text{tr}(\nabla f(\rho)\rho\nabla f(\rho)).$$

A igualdade na desigualdade de Cauchy-Schwarz ocorre quando  $\nabla f(\rho)\rho^{1/2} = \alpha\rho^{1/2}$ , ou equivalentemente, quando  $\nabla(\rho)\rho = \rho$ . □

Vamos simplificar a expressão (4.38), definindo, para algum  $\rho$ ,

$$q(t) = 1 + 2t + t^2 \text{tr}(\nabla f(\rho)\rho\nabla f(\rho)).$$

Como  $\text{tr}(\nabla f(\rho)\rho\nabla f(\rho)) \geq 1$ , pelo Lema 4.2.4, temos que  $q(t) \geq 1$  para todo  $t \geq 0$ . Além disso, se  $\rho \in \mathcal{S}$ , então  $G(\rho) \in \mathcal{S}$ , para qualquer  $t \geq 0$ , consequência de (4.37). Assim,  $G(\rho)$  define um caminho no espaço de matrizes de densidade  $\mathcal{S}$ , parametrizado por  $t$  tal que, quando  $t \rightarrow 0$ ,  $G(\rho) \rightarrow \rho$ , e quando  $t \rightarrow \infty$ ,  $G(\rho) \rightarrow \tilde{\rho}$ , onde

$$\tilde{\rho} = \frac{\nabla f(\rho)\rho\nabla f(\rho)}{\text{tr}(\nabla f(\rho)\rho\nabla f(\rho))},$$

como no algoritmo  $R\rho R$  original [46].

Além disso, definimos a matriz

$$\bar{\rho} = \frac{\nabla f(\rho)\rho + \rho\nabla f(\rho)}{2}. \quad (4.40)$$

Ao contrário de  $\tilde{\rho}$ , a matriz  $\bar{\rho}$ , em geral, não está no conjunto  $\mathcal{S}$ .

Agora, reescrevendo a expressão (4.38), obtemos

$$G(\rho) = \frac{1}{q(t)}\rho + \frac{2t}{q(t)}\bar{\rho} + \frac{t^2 \text{tr}(\nabla f(\rho)\rho\nabla f(\rho))}{q(t)}\tilde{\rho}. \quad (4.41)$$

Portanto, temos uma combinação convexa das matrizes  $\rho$ ,  $\bar{\rho}$  e  $\tilde{\rho}$  e o caminho definido por  $t$  está no interior do conjunto convexo cujos pontos extremos são  $\rho$ ,  $\bar{\rho}$  e  $\tilde{\rho}$ , como mostra a Figura 4.8.

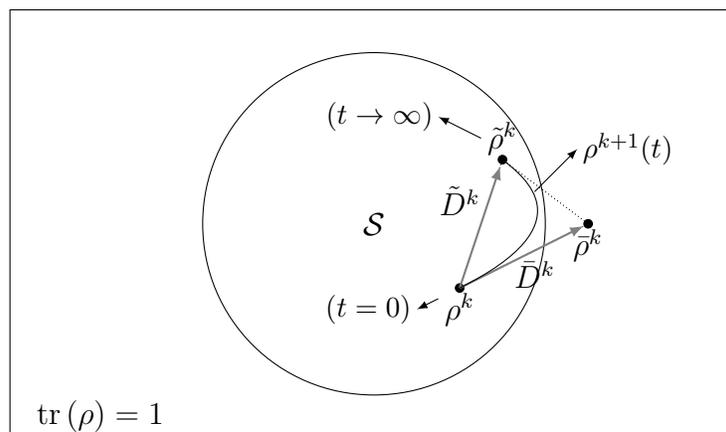


Figura 4.8: Interpretação geométrica de  $G(\rho^k)$  como um caminho (curva) em  $\mathcal{S}$ , parametrizado por  $t$ .

Por fim, definindo as direções

$$\bar{D} = \bar{\rho} - \rho, \quad (4.42)$$

$$\tilde{D} = \tilde{\rho} - \rho, \quad (4.43)$$

e usando (4.41), obtemos

$$G(\rho) = \rho + \frac{2t}{q(t)}\bar{D} + \frac{t^2 \text{tr}(\nabla f(\rho)\rho\nabla f(\rho))}{q(t)}\tilde{D},$$

que fornece uma iteração como (4.34)

$$\hat{\rho} = G(\rho) = \rho + tD,$$

onde

$$D = \frac{2}{q(t)}\bar{D} + \frac{t \text{tr}(\nabla f(\rho)\rho\nabla f(\rho))}{q(t)}\tilde{D}. \quad (4.44)$$

A direção de busca  $D$  é uma combinação cônica das direções  $\bar{D}$  e  $\tilde{D}$  (Figura 4.8). É importante provar que essas direções são factíveis e de subida.

**Proposição 4.2.5.** *As direções  $\bar{D}$  e  $\tilde{D}$  são direções factíveis e de subida para qualquer ponto não estacionário  $\rho$ .*

*Demonstração.* Para provar que  $\bar{D}$  é uma direção de subida precisamos mostrar que

$$\text{tr}(\nabla f(\rho)\bar{D}) > 0.$$

Usando a definição de  $\bar{D}$ , temos

$$\bar{D} = \bar{\rho} - \rho = \frac{\nabla f(\rho)\rho + \rho\nabla f(\rho)}{2} - \rho.$$

Para um ponto não estacionário  $\rho$ , isto é,  $\nabla f(\rho)\rho \neq \rho$ , temos pelo Lema 4.2.4 que

$$\text{tr}(\nabla f(\rho)\bar{D}) = \text{tr}(\nabla f(\rho)\rho\nabla f(\rho)) - \text{tr}(\nabla f(\rho)\rho) = \text{tr}(\nabla f(\rho)\rho\nabla f(\rho)) - 1 > 0,$$

implicando que  $\bar{D}$  é uma direção de subida. Se  $\rho \succ 0$ , então existe  $t > 0$  tal que  $\rho + t\bar{D} \in \mathcal{S}$ , logo a direção é factível.

De forma similar para  $\tilde{D}$

$$\text{tr}(\nabla f(\rho)\tilde{D}) = \frac{\text{tr}(\nabla f(\rho)\nabla f(\rho)\rho\nabla f(\rho))}{\text{tr}(\nabla f(\rho)\rho\nabla f(\rho))} - 1 > 0.$$

Como  $\tilde{\rho} \in \mathcal{S}$ , para  $t \in (0, 1]$ , temos também  $\rho + t\tilde{D} \in \mathcal{S}$ . □

Como a direção  $D$  é uma combinação positiva de direções factíveis e de subida, ela é também uma direção factível e de subida. Para provar que a sequência de direções  $\{D^k\}$  é *gradient related*, precisamos dos lemas a seguir.

**Lema 4.2.6.** *Para  $\rho^k \succ 0$  e  $\text{tr}(\rho^k) = 1$ , a matriz  $\bar{\rho}^k$  definida em (4.40), é solução do seguinte problema*

$$\begin{aligned} \max_{\rho} \quad & \text{tr}(\nabla f(\rho^k)(\rho - \rho^k)) - \frac{1}{2} \text{tr}\left((\rho - \rho^k)\rho^{k-1}(\rho - \rho^k)\right) \\ \text{s.a.} \quad & \text{tr}(\rho) = 1 \end{aligned} \quad (4.45)$$

*Demonstração.* Escrevendo as condições de otimalidade

$$-\nabla f(\rho^k) + \frac{1}{2} \left[ (\rho - \rho^k)\rho^{k-1} + \rho^{k-1}(\rho - \rho^k) \right] + \lambda_0 I = 0, \quad (4.46)$$

$$\text{tr}(\rho) = 1. \quad (4.47)$$

Na equação (4.46), multiplicando a direita por  $\rho^k$  e tomando o traço, temos

$$-\text{tr}(\nabla f(\rho^k)\rho^k) + \text{tr}(\rho - \rho^k) + \lambda_0 \text{tr}(\rho^k) = 0,$$

que implica em  $\lambda_0 = 1$ . Assim, de

$$-\nabla f(\rho^k) + \frac{1}{2} \left[ (\rho - \rho^k)\rho^{k-1} + \rho^{k-1}(\rho - \rho^k) \right] + I = 0,$$

obtemos que

$$\rho\rho^{k-1} + \rho^{k-1}\rho = \nabla f(\rho^k).$$

Impondo a simetria na solução  $\rho$ , e usando a simetria de  $\rho^k$  e  $\nabla f(\rho^k)$ , concluímos que

$$\rho = \nabla f(\rho^k)\rho^k = \rho^k \nabla f(\rho^k) = \frac{\nabla f(\rho^k)\rho^k + \rho^k \nabla f(\rho^k)}{2} = \bar{\rho}^k.$$

□

**Lema 4.2.7.** *A sequência de direções  $\{\bar{D}^k\}$ , associada à sequência  $\{\rho^k\}$ , definida por*

$$\rho^{k+1} = \rho^k + t \bar{D}^k,$$

*satisfaz*

$$\liminf_{k \rightarrow \infty} \inf_{k \in \mathcal{K}} \text{tr}(\nabla f(\rho^k)(\bar{\rho}^k - \rho^k)) > 0.$$

*para toda subsequência  $\{\rho^k\}_{k \in \mathcal{K}}$  convergindo a um ponto não estacionário  $\rho'$ .*

*Demonstração.* Suponha que há uma subsequência  $\{\rho^k\}_{k \in \mathcal{K}}$  convergindo a um ponto não estacionário  $\rho'$ . O Lema 4.2.6 nos diz que  $\bar{\rho}^k$  é solução de (4.45). Logo, em  $\bar{\rho}^k$ , o gradiente da função objetivo de (4.45) é ortogonal ao hiperplano  $\text{tr}(\rho) = 1$ , ou seja

$$\text{tr} \left( \left[ \nabla f(\rho^k) - \frac{1}{2} ((\bar{\rho}^k - \rho^k)(\rho^k)^{-1} + (\rho^k)^{-1}(\bar{\rho}^k - \rho^k)) \right] (\rho - \bar{\rho}^k) \right) = 0,$$

$\forall \rho$  tal que  $\text{tr}(\rho) = 1$ . Como o conjunto viável de (4.45) contem  $\mathcal{S}$ , temos que

$$\text{tr} \left( \left[ \nabla f(\rho^k) - \frac{1}{2} ((\bar{\rho}^k - \rho^k)(\rho^k)^{-1} + (\rho^k)^{-1}(\bar{\rho}^k - \rho^k)) \right] (\rho - \bar{\rho}^k) \right) = 0, \quad \forall \rho \in \mathcal{S}.$$

Expandindo a expressão acima, obtemos

$$\text{tr}(\nabla f(\rho^k)(\rho - \bar{\rho}^k)) = -\frac{1}{2} [\text{tr}((\rho^k - \bar{\rho}^k)(\rho^k)^{-1}(\rho - \bar{\rho}^k)) + \text{tr}((\rho - \bar{\rho}^k)(\rho^k)^{-1}(\rho^k - \bar{\rho}^k))],$$

$\forall \rho \in \mathcal{S}$ . Em particular, para  $\rho = \rho^k$ ,

$$\text{tr}(\nabla f(\rho^k)(\bar{\rho}^k - \rho^k)) = \text{tr}((\rho^k - \bar{\rho}^k)(\rho^k)^{-1}(\rho^k - \bar{\rho}^k)) = \|\rho^k - \bar{\rho}^k\|_{(\rho^k)^{-1}}^2. \quad (4.48)$$

Pela continuidade da solução do problema no Lema (4.2.6), temos

$$\lim_{k \rightarrow \infty, k \in \mathcal{K}} \bar{\rho}^k = \bar{\rho} = \frac{\nabla f(\rho')\rho' + \rho'\nabla f(\rho')}{2}.$$

Tomando limite em (4.48), obtemos

$$\lim_{k \rightarrow \infty} \inf_{k \in \mathcal{K}} \text{tr}(\nabla f(\rho^k)(\bar{\rho}^k - \rho^k)) = \|\rho' - \bar{\rho}\|_{(\rho')^{-1}}^2 > 0.$$

Como  $\rho'$  é não estacionário, o lado direito da desigualdade acima é positivo, completando a prova.  $\square$

Usando os lemas anteriores, podemos mostrar que a sequência de direções  $\{D^k\}$  é *gradient related*. Assim, escolhendo o tamanho de passo  $t_k$  a cada iteração de modo a satisfazer a condição de Armijo, (4.36), podemos obter um algoritmo globalmente convergente segundo o Teorema 4.2.2.

**Proposição 4.2.8.** *A sequência de direções  $\{D^k\}$  é gradient related.*

*Demonstração.* Primeiro, vamos mostrar que  $\{D^k\}$  é limitada. De fato,  $\rho^{k+1}(t_k) = \rho^k + t_k D^k = G(\rho^k)$  está em  $\mathcal{S}$ , uma vez que  $\rho^k \succ 0$  e  $t_k \geq 0$  por definição. Em particular, para  $t_k = 1$ , temos  $\rho^{k+1}(1) = \rho^k + D^k \in \mathcal{S}$ , e como  $\mathcal{S}$  é limitado, então  $\{D^k\}$  é também limitado.

Agora, seja  $\{\rho^k\}_{k \in \mathcal{K}}$  uma subsequência da sequência  $\{\rho^k\}$  definida por  $\rho^{k+1} = \rho^k + t_k D^k$ .

Suponha que  $\{\rho^k\}_{k \in \mathcal{K}}$  converge a um ponto não estacionário  $\rho'$ . Usando a definição de  $D^k$ , obtemos

$$\operatorname{tr}(\nabla f(\rho^k)D^k) = \frac{2}{q(t_k)} \operatorname{tr}(\nabla f(\rho^k)\bar{D}^k) + \frac{t_k \operatorname{tr}(\nabla f(\rho^k)\rho^k \nabla f(\rho^k))}{q(t_k)} \operatorname{tr}(\nabla f(\rho^k)\tilde{D}^k).$$

O segundo termo do lado direito é não negativo, então

$$\operatorname{tr}(\nabla f(\rho^k)D^k) \geq \frac{2}{q(t_k)} \operatorname{tr}(\nabla f(\rho^k)\bar{D}^k).$$

Considerando  $t_k \in (0, t_{max}]$ , temos

$$\operatorname{tr}(\nabla f(\rho^k)D^k) \geq \frac{2}{q(t_{max})} \operatorname{tr}(\nabla f(\rho^k)\bar{D}^k).$$

Tomando limite na subsequência convergindo ao ponto não estacionário,

$$\liminf_{k \rightarrow \infty} \operatorname{tr}(\nabla f(\rho^k)D^k) \geq \frac{2}{q(t_{max})} \liminf_{k \rightarrow \infty} \operatorname{tr}(\nabla f(\rho^k)\bar{D}^k),$$

e usando o Lema 4.2.7,

$$\liminf_{k \rightarrow \infty} \operatorname{tr}(\nabla f(\rho^k)D^k) > 0,$$

que implica que  $\{D^k\}$  é *gradient related*. □

Usando o fato de  $\{D^k\}$  ser *gradient related*, ao invés de um esquema de busca linear exata para determinar o tamanho de passo  $t_k$ , podemos usar um esquema de busca linear inexata e atribuir a  $t_k$  qualquer valor positivo que satisfaça a condição de Armijo:

$$f(\rho^k + tD^k) \geq f(\rho^k) + \gamma t \operatorname{tr}(\nabla f(\rho^k)D^k). \quad (4.49)$$

Dessa forma, os passos do algoritmo que usa busca linear inexata são os seguintes:

**Algoritmo 4.2.1.**

**Passo 0.** Dados  $\rho^0 \succ 0$  tal que  $\operatorname{tr}(\rho^0) = 1$ ,  $t_{max} > 0$  e  $0 < \alpha_0 < \alpha_1 < 1$ , defina  $k = 0$  e  $t_0 = t_{max}$ .

**Passo 1.** Se algum critério de parada foi verificado, pare. Caso contrário, calcule as direções  $\bar{D}^k$  e  $\tilde{D}^k$ .

**Passo 2.** Faça  $t = \max\{1, t_{k-1}\}$ . Enquanto

$$f(\rho^k + tD^k) < f(\rho^k) + \gamma t \operatorname{tr}\left(\nabla f(\rho^k) \left(\frac{2}{q(t)}\bar{D}^k + \frac{t \operatorname{tr}(\nabla f(\rho^k)\rho^k \nabla f(\rho^k))}{q(t)}\tilde{D}^k\right)\right),$$

faça  $t \in [\alpha_0 t, \alpha_1 t]$ .

**Passo 3.** Faça  $t_k = t$  e  $\rho^{k+1} = \rho^k + t_k D^k$ . Vá para o passo 1.

**Teorema 4.2.9.** *Todo ponto limite  $\rho^*$  da sequência  $\{\rho^k\}$  gerada pelo Algoritmo 4.2.1 é um ponto estacionário, isto é,  $\nabla f(\rho^*)\rho^* = \rho^* = \rho^*\nabla f(\rho^*)$ .*

*Demonstração.* Aplicação direta do Teorema 4.2.2, substituindo  $x^k$  por  $\rho^k$  e  $d^k$  por  $D^k$ .  $\square$

No Passo 2, ao invés de sucessivas reduções do tamanho de passo  $t$ , pode-se usar, por exemplo, interpolação quadrática ou cúbica [70] para estimar o tamanho de passo  $t$  que minimiza  $f(\rho^k + tD^k)$ , a fim de tornar a busca linear mais efetiva.

### 4.2.3 Exemplos

Primeiro, consideramos o contra-exemplo onde o  $R\rho R$  puro cicla [79]. Suponha que fizemos três medições em um q-bit com o aparato descrito por  $\Pi_0 = |0\rangle\langle 0|$  e  $\Pi_1 = |1\rangle\langle 1|$ , detectando  $|0\rangle$  uma vez e  $|1\rangle$  duas. Usando o estado maximamente misto,  $(1/d)I$ , como ponto inicial e considerando a convergência quando a distância entre dois iterandos consecutivos é pequena o suficiente (menor que  $10^{-7}$ ). Para cada  $t$  fixado no algoritmo  $R\rho R$  Diluído definimos  $t_{max} = t$  em nosso algoritmo que usa busca linear inexata. Usamos  $\gamma = 10^{-4}$  e  $\alpha_0 = \alpha_1 = 0.5$  no Algoritmo 4.2.1.

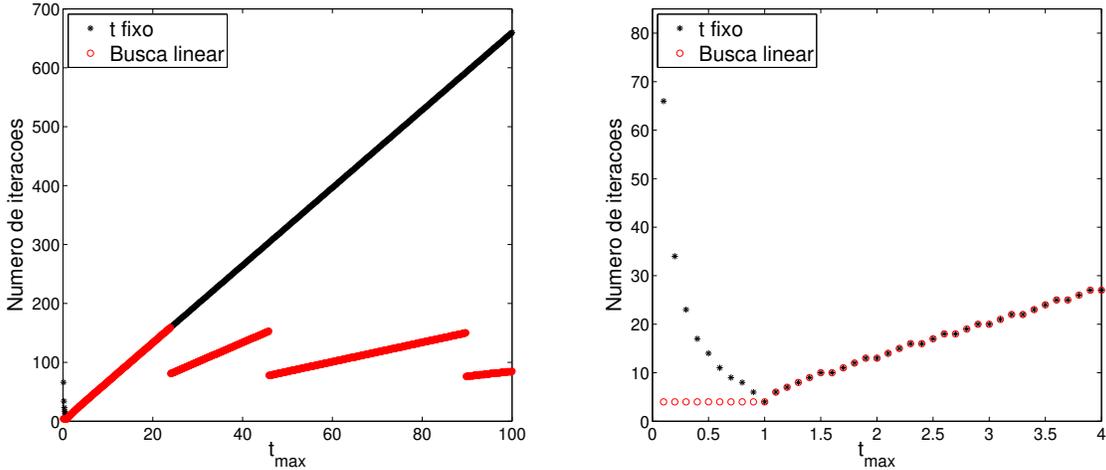


Figura 4.9: Número de iterações em função de  $t_{max}$ .

A Figura 4.9 apresenta a comparação entre a versão com tamanho de passo fixo,  $t = t_{max}$ , em preto, contra a que usa busca linear inexata, em vermelho, descrita na seção anterior. À esquerda podemos ver que o número de iterações cresce conforme o passo  $t$  aumenta, para a versão que usa  $t$  fixo. Isso era esperado pois a medida que  $t \rightarrow \infty$  as iterações tendem a iterações do  $R\rho R$  puro, que sabemos que não converge. Por outro lado, a versão que emprega busca linear mantém o número de iterações limitado, independentemente do valor de  $t_{max}$ .

O painel à direita é a versão ampliada do intervalo  $[0, 4]$  do esquerdo, para mostrar o comportamento para valores pequenos de  $t$ . Como esperado, embora o  $R\rho R$  Diluído garanta o crescimento monótono da verossimilhança para passos suficientemente pequenos, a repetição de passos pequenos leva a um maior número de iterações. O Algoritmo 4.2.1 garante um acréscimo substancial na verossimilhança através do procedimento de busca linear. Para evitar passos extremamente pequenos, a cada iteração do Algoritmo 4.2.1, a primeira tentativa para o tamanho de passo  $t_k$  é pelo menos 1.

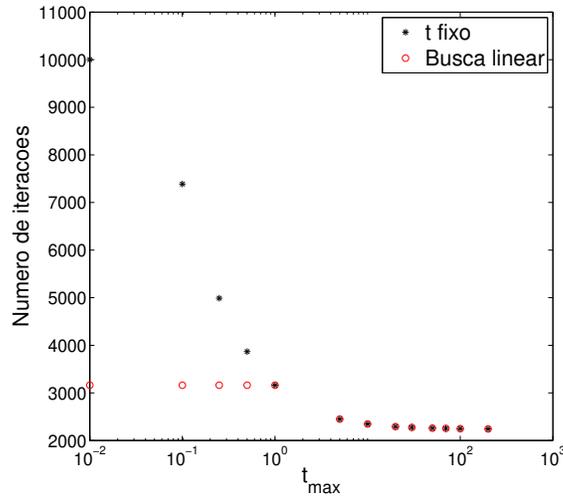


Figura 4.10: Número de iterações em função de  $t_{max}$ .

A seguir, consideramos como dados as probabilidades teóricas associadas a um estado  $W$ . A Figura 4.10 apresenta o número de iterações para diferentes valores de  $t$  (escala logarítmica). Novamente, valores (fixos) pequenos de  $t$  produzem um número elevado de iterações. É importante notar também que, nesse exemplo, o comportamento da versão com busca linear é o mesmo que o da versão com “ $t$  fixo” à medida que o valor  $t_{max}$  aumenta. Isso significa que no Algoritmo 4.2.1, o passo completo  $t_k = t_{max}$  foi aceito (cumpriu a condição de Armijo) em toda iteração.

Em [79], os autores afirmam que deve-se tentar primeiro um valor grande para o tamanho de passo  $t$  e realizar iterações  $R\rho R$  diluídas com o mesmo valor de  $t$ . Se as iterações não convergirem então deve-se tentar novamente com um valor menor de  $t$ . Esse procedimento *ad hoc* é motivado pois o padrão da Figura 4.10 ocorre frequentemente na prática, e então quanto maior  $t$  menor o número de iterações. No entanto, qual é um bom palpite para um valor grande de  $t$  a fim de assegurar poucas iterações? E se a convergência não ocorrer, como escolher um valor menor de  $t$  de modo a garantir a convergência? Essas decisões podem resultar em uma série de re-execuções do algoritmo até que um bom valor de  $t$  seja encontrado e, isso pode mudar de um conjunto de dados para outro.

Portanto, o uso de uma busca linear com Armijo representa uma melhoria no algoritmo  $R\rho R$  diluído, ajustando o tamanho de passo  $t$  apenas quando necessário e com convergência que não depende de uma escolha específica de tal parâmetro nem do ponto inicial.

#### 4.2.4 Conclusões desta seção

Demonstramos a convergência global do algoritmo  $R\rho R$  Diluído usando busca linear com a condição de Armijo. A busca linear inexata é uma hipótese mais fraca que a busca linear exata usada na prova de convergência em trabalhos anteriores [79]. Além disso, a globalização proposta através de busca linear, não depende de um palpite para o tamanho de passo fixo ao longo de todas as iterações. Ao invés disso, como é usual em otimização não-linear, o tamanho do passo é ajustado apenas quando necessário a fim de assegurar um aumento suficiente na função de verossimilhança a cada iteração. Portanto, o procedimento de busca linear com Armijo é uma globalização eficaz para o algoritmo  $R\rho R$  Diluído e representa uma melhoria prática para este algoritmo usado na Tomografia de Estados Quânticos.

### 4.3 Estimativa de erros e matriz de Fisher

Dentre as propriedades da estimativa de máxima verossimilhança, talvez a mais relevante seja a eficiência. O erro em tal estimativa está relacionado com uma interessante medida de informação: a informação de Fisher [28]. A informação de Fisher  $\mathcal{I}(\theta)$  é uma medida da quantidade de informação que um observável de uma variável aleatória  $x$  carrega sobre o parâmetro desconhecido  $\theta$ . Formalmente tal medida é definida como a variância do *score*:

$$\frac{\partial \ln P(x | \theta)}{\partial \theta},$$

onde  $P(x|\theta)$  é a função de verossimilhança. Sob certas condições de regularidade [51], pode-se mostrar que o primeiro momento do *score* é zero, e então

$$\mathcal{I}(\theta) = \mathbf{E} \left( \left( \frac{\partial}{\partial \theta} \ln P(x | \theta) \right)^2 \right). \quad (4.50)$$

Além disso, se  $\ln P(x|\theta)$  é duas vezes continuamente diferenciável com respeito a  $\theta$ , então é possível reescrever a informação de Fisher como:

$$\mathcal{I}(\theta) = -\mathbf{E} \left( \frac{\partial^2}{\partial \theta^2} \ln P(x|\theta) \right),$$

ou seja, podemos interpretá-la como a curvatura da função de máxima verossimilhança em uma vizinhança do maximizador. Para uma curvatura elevada, teremos um maximizador forte e informação elevada, enquanto para um maximizador fraco, curvatura quase plana, temos pouca informação.

Outro resultado importante, obtido por Cramér e Rao [21, 76], é que a variância de qualquer estimador não viesado  $\hat{\theta}$ , é limitada inferiormente pela inversa da informação de Fisher:

$$\mathbf{Var}(\hat{\theta}) \geq \frac{1}{\mathcal{I}(\theta)}.$$

No caso em que  $\theta$  é um vetor de parâmetros a ser estimado, o conceito de informação de Fisher é estendido através da matriz de Fisher  $F$ , com entradas:

$$F_{kl} = \mathbf{E} \left( \frac{\partial \ln \mathcal{L}}{\partial \theta_k} \frac{\partial \ln \mathcal{L}}{\partial \theta_l} \right). \quad (4.51)$$

Como assintoticamente o estimador de máxima verossimilhança tem distribuição normal de média  $\theta$  e matriz de co-variância  $F^{-1}$ , podemos usar a matriz de Fisher para deduzir os erros em valores esperados para observáveis, como proposto em [80].

Considere uma base  $\{\Gamma_k\}$  para o espaço de matrizes Hermitianas, onde  $\Gamma_0 = I$ ,  $\text{tr}(\Gamma_k \Gamma_l) = 0$  para  $k \neq l$  e  $\text{tr}(\Gamma_k \Gamma_l) = 1$  para  $k = l > 0$ . Assim para uma matriz de densidade  $\rho$  de ordem  $d$  podemos escrever

$$\rho = \frac{1}{d} I + \sum_k r_k \Gamma_k. \quad (4.52)$$

Uma vez conhecida a estimativa de máxima verossimilhança  $\rho_{ML}$ , é fácil determinar o vetor  $r_{ML}$  de coeficientes de sua combinação linear na base  $\{\Gamma_k\}$ . Assintoticamente o estimador  $\hat{r} \sim N(r, F^{-1})$ , onde  $F$  é a matriz de Fisher associada à função log-verossimilhança com respeito a  $r$ .

No caso da função (3.21) proveniente de uma distribuição multinomial, temos que as entradas da matriz de Fisher são definidas por

$$F_{kl} = N \sum_j \frac{\text{tr}(\Gamma_k E_j) \text{tr}(\Gamma_l E_j)}{p_j}, \quad (4.53)$$

onde  $p_j = \text{tr}(E_j \rho_{ML})$ .

Já para a função (3.23) proveniente de uma distribuição Gaussiana, temos que as entradas da matriz de Fisher são

$$F_{kl} = \sum_j \frac{\text{tr}(\Gamma_k E_j) \text{tr}(\Gamma_l E_j) (1 + N p_j)}{p_j^2}. \quad (4.54)$$

Seja  $Z$  um observável e  $z$  o vetor de coeficientes da combinação linear na base  $\{\Gamma_k\}$ . Pela teoria quântica, temos que

$$\langle Z \rangle = \text{tr}(Z\rho),$$

onde  $\rho$  é o estado (parâmetro) que queremos estimar. Logo, a estimativa para o valor esperado de  $Z$  é

$$\langle Z \rangle = \langle \langle Z \rangle \rangle = \text{tr}(Z\langle \rho \rangle) = \text{tr}\left(Z \mathbf{E}\left(\frac{1}{d} + \sum_k r_k \Gamma_k\right)\right) = \text{tr}(Z\rho_{ML})$$

e a estimativa para a variância é dada por

$$(\Delta Z)^2 = \mathbf{Var}(\text{tr}(Z\rho)) = \mathbf{Var}\left(\frac{z_0}{d} + \sum_k z_k r_k\right) = z^\dagger F^{-1} z. \quad (4.55)$$

A expressão acima permite colocar barras de erro no valor esperado de qualquer observável  $Z$ , sendo portanto uma importante ferramenta na análise de experimentos com sistemas quânticos [80].

### 4.3.1 O Método Delta

É possível generalizar o resultado (4.55) para funções não lineares de  $\rho$ , através de um resultado muito utilizado em inferência, conhecido como o Método Delta [51].

**Teorema 4.3.1** (Método Delta). *Seja  $X_n$  uma sequência de variáveis aleatórias que satisfazem*

$$\sqrt{n}(X_n - \theta) \rightarrow N(0, \sigma^2), \quad (4.56)$$

*em distribuição. Para uma dada função  $g$  e um valor específico de  $\theta$ , suponha que  $g'(\theta)$  existe e é não nulo. Então,*

$$\sqrt{n}(g(X_n) - g(\theta)) \rightarrow N(0, \sigma^2[g'(\theta)]^2),$$

*em distribuição.*

*Demonstração.* Considere a expansão de Taylor de  $g(X_n)$  em  $\theta$

$$g(X_n) = g(\theta) + g'(\theta)(X_n - \theta) + R_n,$$

onde  $R_n \rightarrow 0$  quando  $X_n \rightarrow \theta$ . De (4.56) segue que  $X_n \rightarrow \theta$  em probabilidade e portanto  $R_n \rightarrow 0$  em probabilidade. Aplicando-se então uma extensão do Teorema do Limite Central [51] obtemos o resultado desejado.  $\square$

A versão multivariada deste resultado é a seguinte.

**Teorema 4.3.2.** *Seja  $(X_1^{(n)}, \dots, X_N^{(n)})$  uma sequência de vetores aleatórios independentes que satisfazem*

$$\sqrt{n} \left[ (X_1^{(n)}, \dots, X_N^{(n)}) - (\theta_1, \dots, \theta_N) \right] \rightarrow N(0, \Sigma),$$

*em distribuição. Seja  $g$  uma função real de  $N$  argumentos com derivadas parciais de primeira ordem contínuas. Então,*

$$\sqrt{n}[g(X_1^{(n)}, \dots, X_N^{(n)}) - g(\theta_1, \dots, \theta_n)] \rightarrow N(0, \nu^2), \quad \nu^2 = \nabla g(\theta)^\dagger \Sigma \nabla g(\theta),$$

*dado que  $\nu^2 > 0$ .*

*Demonstração.* Veja [51]. □

Considerando-se a representação de  $\rho$  pela equação (4.52) e a normalidade assintótica do estimador de máxima verossimilhança  $\hat{r}$ , a aplicação do método Delta é imediata para qualquer função  $g(r)$ , tal que  $\nabla g(r) \neq 0$ . Isto é

$$\nu^2 = \text{Var}(g(r)) = \nabla g(r)^\dagger F^{-1} \nabla g(r), \quad (4.57)$$

onde  $F^{-1}$  é a inversa da matriz de Fisher. Note que  $\nu^2 > 0$ , desde que  $F^{-1}$  seja definida positiva. Isto ocorre quando a solução de máxima verossimilhança corresponde a um maximizador estrito.

Por exemplo, considere a pureza  $\text{tr}(\rho^2)$ . Expressando-a em função de  $r$ , temos

$$g(r) = \text{tr}(\rho^2) = \text{tr} \left( \left( \frac{1}{d} I + \sum_k r_k \Gamma_k \right) \left( \frac{1}{d} I + \sum_l r_l \Gamma_l \right) \right) = \frac{1}{d} + \sum_i r_i^2.$$

Neste caso, temos que  $\nabla g(r) = (2r_1, 2r_2, \dots, 2r_{d^2-1})^t$  e

$$\nu^2 = \text{Var}(g(r)) = 4r^\dagger F^{-1} r.$$

É claro que, como um caso particular, recuperamos a variância de um observável. Seja

$$g(r) = \text{tr}(Z\rho) = \frac{z_0}{d} + \sum_i z_i r_i.$$

Como  $\nabla g(r)_i = z_i$ , temos que

$$\text{Var}(g(r)) = \nabla g(r)^\dagger F^{-1} \nabla g(r) = z^\dagger F^{-1} z,$$

que coincide com a expressão (4.55).

## 4.4 Resumo do Capítulo 4

Neste capítulo, estudamos a estimação da matriz de densidade através de Máxima Verossimilhança. Foram discutidos dois métodos de resolução para o problema de otimização associado.

O primeiro, baseado em uma reparametrização da matriz de densidade [48], foi tratado na Seção 4.1. Nossa principal contribuição foi mostrar que os mínimos locais do problema de minimização irrestrita, que surgem após a reparametrização, são todos globais. Esse resultado foi publicado na revista *Quantum Information and Computation* [36].

O segundo, específico para medidas descritas por um conjunto POVM e para verossimilhança multinomial [46, 47], foi abordado na Seção 4.2. Este método tira proveito da estrutura do problema e garante a positividade e traço unitário através de uma iteração computacionalmente barata. A convergência global do método foi provada em [79], mas com a hipótese de busca linear exata. Nossa contribuição na Seção 4.2 foi demonstrar a convergência do método usando busca linear inexata e uma condição tipo Armijo, o que é mais viável na prática. Este resultado foi submetido à revista *Physical Review A*.

Além disso, na Seção 4.3, tratamos da estimação de erros, em quantidades calculadas a partir da estimativa de máxima verossimilhança, através da matriz de Fisher. Usando um resultado estatístico conhecido como método Delta [16, 51], generalizamos o resultado de [80] para funções não-lineares da matriz de densidade.

# Capítulo 5

## Tomografia com um conjunto incompleto de medidas

Quando não temos um conjunto informacionalmente completo de medições, a estimativa para o estado quântico não pode ser determinada unicamente. Neste caso, dentre as matrizes de densidade compatíveis com os dados disponíveis, geralmente é preferida aquela que é menos comprometida com as informações faltantes.

Neste capítulo, estudamos duas abordagens para tomografia com um conjunto incompleto de medidas: estimação de Máxima Entropia [15] e a Tomografia Quântica Variacional (VQT) [55]. A primeira busca a estimativa compatível com as medidas disponíveis e que maximiza a entropia de von Neumann, enquanto a segunda busca a estimativa que minimiza um certo tipo de energia associada às medidas faltantes.

Na Seção 5.1, discutimos sobre a estimativa de Máxima Entropia e os métodos utilizados para a resolução de tal problema. Na Seção 5.2, apresentamos a formulação VQT que consiste em um problema de programação semidefinida linear [14, 22]. A Seção 5.3 traz uma comparação entre essas duas abordagens do ponto de vista das probabilidades associadas às medidas faltantes. Na mesma seção, propomos uma modificação na formulação VQT para que tenha um comportamento mais parecido com a MaxEnt, mas preserve a estrutura de um SDP linear. A Seção 5.4 trata do caso de medidas com ruído e apresenta a estimativa de Máxima Verossimilhança assistida por Máxima Entropia (MaxLik-MaxEnt). Simulações numéricas comparando as abordagens anteriores são apresentadas na Seção 5.5. A Seção 5.6 traz uma breve discussão sobre a estimação de Máxima Entropia e emaranhamento. Considerações finais desse capítulo estão na Seção 5.7.

## 5.1 Máxima Entropia

A tarefa de estimar a matriz de densidade com base nos resultados de medições, ou simplesmente Tomografia de Estados Quânticos, é essencial em computação quântica [26,56,69]. Além da tomografia de estados ser um assunto importante por si só, ela é também empregada em tomografia de processos quânticos e na validação de portas quânticas. No entanto, é conhecido que o número de medições necessárias cresce exponencialmente com o número de q-bits. Neste caso, tomar um conjunto informacionalmente completo de medições pode se tornar impraticável. Desse modo, é importante o estudo de métodos que saibam lidar com informação incompleta.

A abordagem de Máxima Entropia (MaxEnt) foi introduzida por Buzek et al. [15], no contexto de tomografia de estados quânticos com dados incompletos, seguindo o princípio de Jaynes [49]: não podemos tirar nenhuma conclusão que não seja garantida pelos dados experimentais.

A ideia é tomar como estimativa para  $\rho$  a matriz de densidade que maximiza a entropia de von Neumann

$$S(\rho) = -\text{tr}(\rho \ln \rho),$$

e é compatível com os dados disponíveis. Tal estimativa é obtida resolvendo-se o seguinte problema de otimização

$$\begin{aligned} \max_{\rho} \quad & -\text{tr}(\rho \ln \rho) \\ \text{s.a} \quad & \text{tr}(E_i \rho) = f_i, \quad i \in \mathcal{I} \\ & \text{tr}(\rho) = 1, \\ & (\rho \succeq 0), \end{aligned} \tag{5.1}$$

onde  $\{E_i\}$  é o conjunto POVM associado às frequências  $\{f_i\}$  e  $\mathcal{I}$  denota o conjunto de índices das medidas disponíveis. Embora tenhamos que lidar com restrições no espaço das matrizes semidefinidas positivas, é possível obter uma solução explícita para (5.1), usando as condições de otimalidade de primeira ordem [14, 70].

Aplicando as condições de primeira ordem, obtemos

$$\begin{aligned} \ln \rho + I + \lambda_0 I + \sum_{i \in \mathcal{I}} \lambda_i E_i &= Z, \\ \text{tr}(E_i \rho) &= f_i, \quad i \in \mathcal{I} \\ \text{tr}(\rho) &= 1, \\ \rho \succeq 0, \quad Z \succeq 0 & \\ \rho Z &= 0. \end{aligned} \tag{5.2}$$

Assumindo que  $\rho \succ 0$ , temos

$$\begin{aligned} \ln \rho + I + \lambda_0 I + \sum_{i \in \mathcal{I}} \lambda_i E_i &= 0, \\ \text{tr}(E_i \rho) &= f_i, \quad i \in \mathcal{I} \end{aligned} \quad (5.4)$$

$$\begin{aligned} \text{tr}(\rho) &= 1, \end{aligned} \quad (5.5)$$

onde  $\lambda_i$  são os multiplicadores de Lagrange associados às restrições de igualdade. Da primeira equação de (5.4), obtemos

$$\rho = \exp \left( - \sum_{i \in \mathcal{I}} \lambda_i E_i - \lambda_0 I - I \right) \succ 0,$$

e definindo  $1/\exp(-\lambda_0 - 1) = \mathcal{N} = \text{tr}(\exp \sum_i -\lambda_i E_i)$ , temos

$$\rho_{ME} = \frac{1}{\mathcal{N}} \exp \sum_{i \in \mathcal{I}} -\lambda_i E_i. \quad (5.6)$$

Claramente,  $\rho_{ME} \succ 0$  e  $\text{tr}(\rho_{ME}) = 1$  devido à constante de normalização  $\mathcal{N}$ . Os multiplicadores de Lagrange podem ser determinados resolvendo o sistema de equações não lineares

$$\text{tr}(E_j \rho_{ME}) = f_j, \quad j \in \mathcal{I},$$

ou seja,

$$\text{tr} \left( E_j \exp \sum_{i \in \mathcal{I}} -\lambda_i E_i \right) = \mathcal{N} f_j, \quad j \in \mathcal{I}. \quad (5.7)$$

Em geral, como os dados tem ruído  $\{f_i\}$ , resolvemos o seguinte problema de quadrados mínimos não-lineares

$$\min_{\lambda} \sum_{j \in \mathcal{I}} \left[ \text{tr} \left( E_j \exp \sum_{i \in \mathcal{I}} -\lambda_i E_i \right) - \mathcal{N} f_j \right]^2, \quad (5.8)$$

no lugar do sistema de equações (5.7).

Porém, podemos encontrar problemas numéricos ao resolver o sistema de equações não lineares (5.7) ou o problema de quadrados mínimos não lineares (5.8), principalmente quando a solução está próxima de ter posto deficiente.

Uma estratégia numericamente mais estável é estimar os multiplicadores de Lagrange resolvendo o dual de (5.1), definido por

$$\min_{\lambda, \lambda_0} \sum_{i \in \mathcal{I}} f_i \lambda_i + \lambda_0 + \text{tr} \left( \exp(-\lambda_0 - 1) \exp \left( \sum_{i \in \mathcal{I}} -\lambda_i E_i \right) \right). \quad (5.9)$$

É possível determinar  $\lambda_0$  analiticamente,

$$\lambda_0 = \log \operatorname{tr} \left( \exp \left( \sum_i -\lambda_i E_i \right) \right) - 1.$$

Logo, o problema dual se reduz a

$$\min_{\lambda} \sum_{i \in \mathcal{I}} f_i \lambda_i + \log \operatorname{tr} \left( \exp \left( \sum_i -\lambda_i E_i \right) \right). \quad (5.10)$$

A hipótese de que existe um ponto viável tal que  $\rho \succ 0$  é necessária para garantir que o gap de dualidade seja zero [14]. Uma maneira de checar tal condição é resolver o seguinte problema de factibilidade:

$$\begin{aligned} \min_{\rho, t} \quad & t \\ \text{s.a} \quad & \operatorname{tr}(E_i \rho) = f_i, \quad i \in \mathcal{I} \\ & \operatorname{tr}(\rho) = 1, \\ & \rho + tI \succeq 0. \end{aligned} \quad (5.11)$$

Note que esse é um SDP linear que tenta encontrar a  $\rho$  mais próxima de  $I/d$  e compatível com os dados disponíveis.

## 5.2 Tomografia Quântica Variacional

Em [55], Maciel et al. introduziram a Tomografia Quântica Variacional (VQT) para tomografia com um conjunto incompleto de medidas. A formulação VQT é

$$\begin{aligned} \min_{\rho, \Delta} \quad & \sum_{i \in \mathcal{I}} \Delta_i + \sum_{i \notin \mathcal{I}} \operatorname{tr}(E_i \rho) \\ \text{s.a} \quad & |\operatorname{tr}(E_i \rho) - f_i| \leq \Delta_i f_i \quad i \in \mathcal{I} \\ & \operatorname{tr}(\rho) = 1, \\ & \rho \succeq 0, \end{aligned} \quad (5.12)$$

onde  $\{E_i\}$  é o conjunto POVM,  $f_i$  as frequências,  $\Delta_i$  as tolerâncias e  $\mathcal{I}$  o índice das frequências *medidas*. As duas últimas restrições são as restrições usuais do espaço de matrizes de densidade. As demais restrições são fáceis de se entender. No caso de um experimento ideal (livre de ruído), pedimos que a estimativa para  $\rho$  seja compatível com as frequências medidas, isto é,

$$\operatorname{tr}(E_i \rho) = f_i, \quad \forall i \in \mathcal{I}. \quad (5.13)$$

Porém, na prática, o ruído perturba as frequências e então permitimos que as restrições acima sejam violadas por uma pequena tolerância tal que

$$|\text{tr}(E_i\rho) - f_i| \leq \Delta_i f_i, \quad \forall i \in \mathcal{I}. \quad (5.14)$$

É claro que queremos que tais tolerâncias sejam as menores possíveis, o que explica o primeiro termo na função objetivo. No entanto, como discutido anteriormente, no cenário com dados incompletos, pode existir mais de uma estimativa que minimiza tais tolerâncias e satisfaz as demais restrições. Portanto, o VQT também tenta minimizar um tipo de energia, dado por

$$E = \text{tr}(H\rho) = \text{tr}\left(\sum_{i \notin \mathcal{I}} E_i \rho\right) = \sum_{i \notin \mathcal{I}} \text{tr}(E_i \rho), \quad (5.15)$$

onde  $H$  desempenha o papel de um Hamiltoniano.

Uma das principais virtudes do VQT é que a formulação (5.12) é um SDP linear (problema de programação semidefinida [14, 22]) para o qual existe uma série de métodos eficientes [41, 67] e alguns deles com complexidade polinomial [67], que é uma característica importante para a escalabilidade.

Outra vantagem prática, além de possibilitar a tomografia com dados incompletos, é que podemos definir um limitante superior para as variáveis  $\Delta_i$ . Isso permite controlar a qualidade do ajuste e, além disso, permite identificar dados incompatíveis através da infactibilidade do problema (5.12).

### 5.3 VQT, Medições da autobase e MaxEnt

Como estamos considerando tomografia com um conjunto incompleto de medidas, uma questão importante é: como os métodos atribuem as probabilidades associadas a elementos POVM não medidos? Para simplificar nossa análise, consideremos o caso de medições da autobase em um experimento livre de ruído. Suponha que o estado verdadeiro seja  $\rho$  e que sua decomposição espectral é dada por

$$\rho = \sum_{i \in \mathcal{I}} c_i P_i + \sum_{i \notin \mathcal{I}} c_i P_i,$$

onde  $P_i$ 's são  $d$  projetores ortonormais nos autoespaços de  $\rho$ . Assim, a tarefa de tomografia se reduz a determinar os coeficientes  $c_i$ 's (autovalores) com base nos dados observados. Assumindo que foram medidos  $m < d$  projetores ( $d$  é a dimensão do espaço de Hilbert), temos que

$$c_i = \text{tr}(P_i \rho), \quad \forall i, \quad (5.16)$$

e como assumimos um experimento ideal, obtemos

$$\text{tr}(P_i \rho) = f_i, \quad \forall i \in \mathcal{I}, \quad (5.17)$$

onde  $f_i$ 's são as frequências medidas. Devido à restrição de normalização, temos que

$$\sum_{i \notin \mathcal{I}} c_i = 1 - \sum_{i \in \mathcal{I}} c_i = 1 - \sum_{i \in \mathcal{I}} f_i, \quad (5.18)$$

e a restrição  $\rho \succeq 0$  implica que  $c_i \geq 0, \forall i$ .

Agora, consideremos a solução de MaxEnt, dada por (5.6):

$$\rho_{ME} = \frac{1}{\mathcal{N}} \exp \sum_{i \in \mathcal{I}} -\lambda_i P_i = \frac{1}{\mathcal{N}} \exp \left( \sum_{i \in \mathcal{I}} -\lambda_i P_i - \sum_{i \notin \mathcal{I}} 0 P_i \right) = \sum_{i \in \mathcal{I}} \frac{e^{-\lambda_i}}{\mathcal{N}} P_i + \frac{1}{\mathcal{N}} \sum_{i \notin \mathcal{I}} P_i,$$

onde  $\lambda_i$  são os multiplicadores de Lagrange associados às restrições (5.17). Como  $\rho_{ME}$  deve satisfazer tais restrições, temos

$$f_j = \text{tr}(P_j \rho_{ME}) = \text{tr} \left( P_j \left( \sum_{i \in \mathcal{I}} \frac{e^{-\lambda_i}}{\mathcal{N}} P_i + \frac{1}{\mathcal{N}} \sum_{i \notin \mathcal{I}} P_i \right) \right) = \frac{e^{-\lambda_j}}{\mathcal{N}}.$$

Assim,  $e^{-\lambda_i}/\mathcal{N} = f_i = c_i, \forall i \in \mathcal{I}$ , como esperado. Além disso, como  $\text{tr}(\rho_{ME}) = 1$ , obtemos

$$\sum_{i \in \mathcal{I}} f_i + \frac{d-m}{\mathcal{N}} = 1,$$

que implica que, para os coeficientes não medidos,

$$c_i = \frac{1}{\mathcal{N}} = \frac{1 - \sum_{j \in \mathcal{I}} f_j}{d-m}, \quad \forall i \notin \mathcal{I}. \quad (5.19)$$

Em outras palavras, a solução de MaxEnt

$$\rho_{ME} = \sum_{i \in \mathcal{I}} f_i P_i + \sum_{i \notin \mathcal{I}} \left( \frac{1 - \sum_{j \in \mathcal{I}} f_j}{d-m} \right) P_i \quad (5.20)$$

distribui uniformemente o restante  $1 - \sum_{j \in \mathcal{I}} f_j$  dentre os demais coeficientes  $c_i, \forall i \notin \mathcal{I}$ .

Agora vamos analisar a solução de VQT. Considerando a formulação (5.12) e aplicando as equações (5.16),(5.17),(5.18), obtemos

$$\begin{aligned} & \min_{c_i, \forall i \notin \mathcal{I}} \sum_{i \notin \mathcal{I}} c_i \\ & \text{s.a} \quad \sum_{i \notin \mathcal{I}} c_i = 1 - \sum_{i \in \mathcal{I}} f_i, \\ & \quad \quad c_i \geq 0, \forall i \notin \mathcal{I}. \end{aligned} \quad (5.21)$$

Como estamos supondo um experimento ideal,  $c_i = \text{tr}(P_i \rho) = f_i, \forall i \in \mathcal{I}$ , temos  $\Delta_i = 0, \forall i \in \mathcal{I}$ . Mais ainda, as variáveis do problema (5.21) são  $c_i, \forall i \notin \mathcal{I}$ , e qualquer solução

viável de (5.21) é também ótima, pois a função objetivo coincide com o lado esquerdo da primeira restrição. Logo, podemos concluir que a solução de VQT é expressa por

$$\rho_{VQT} = \sum_{i \in \mathcal{I}} f_i P_i + \sum_{i \notin \mathcal{I}} c_i P_i.$$

Assim, não há restrição ou termo de penalidade na função objetivo que force  $c_i, i \notin \mathcal{I}$ , a concordar com a solução de Máxima Entropia, no sentido de distribuir uniformemente as probabilidades não medidas.

Para garantir que a solução de VQT coincida com a solução de MaxEnt, ao menos no caso ideal de medidas da autobase, propomos uma mudança na formulação (5.12). Vamos definir o vetor  $\tilde{c}$ , de tamanho  $d^2 - m$ , com componentes

$$\tilde{c}_i = \text{tr}(E_i \rho), \quad \forall i \notin \mathcal{I}.$$

Considerando que  $E_i$  são normalmente POVMs (ou projetores), iremos assumir que  $\tilde{c}_i \geq 0$ . Então, temos que

$$\|\tilde{c}\|_1 = \sum_{i \notin \mathcal{I}} |\text{tr}(E_i \rho)| = \sum_{i \notin \mathcal{I}} \text{tr}(E_i \rho) = \text{tr}(H \rho) = E.$$

Nossa proposta consiste em usar

$$\|\tilde{c}\|_\infty = \max_{i \notin \mathcal{I}} |\text{tr}(E_i \rho)| = \max_{i \notin \mathcal{I}} \text{tr}(E_i \rho),$$

no lugar de  $\|\tilde{c}\|_1$  na função objetivo do problema (5.12). Quando a soma das componentes de  $\tilde{c}$  é fixada, minimizar  $\|\tilde{c}\|_\infty$  promove uma distribuição mais uniforme desses coeficientes.

Neste caso, a formulação VQT $_\infty$  (VQT com  $\|\cdot\|_\infty$ ) é

$$\begin{aligned} \min_{\rho, \Delta} \quad & \sum_{i \in \mathcal{I}} \Delta_i + \max_{i \notin \mathcal{I}} \text{tr}(E_i \rho) \\ \text{s.a} \quad & |\text{tr}(E_i \rho) - f_i| \leq \Delta_i f_i \quad i \in \mathcal{I} \\ & \text{tr}(\rho) = 1, \\ & \rho \succeq 0, \end{aligned} \tag{5.22}$$

e para o caso de medições da autobase, o equivalente de (5.21) é

$$\begin{aligned} \min_{c_i, \forall i \notin \mathcal{I}} \quad & \max_{i \notin \mathcal{I}} c_i \\ \text{s.a} \quad & \sum_{i \notin \mathcal{I}} c_i = 1 - \sum_{i \in \mathcal{I}} f_i, \\ & c_i \geq 0, \quad \forall i \notin \mathcal{I}. \end{aligned} \tag{5.23}$$

Note que o problema (5.23) tem uma única solução que corresponde a distribuir uniformemente o restante  $1 - \sum_{i \in \mathcal{I}} f_i$  dentre os coeficientes  $c_i, \forall i \notin \mathcal{I}$ , e que, portanto, coincide com a solução de MaxEnt neste caso.

Além de concordar com a solução de MaxEnt no caso da autobase, a modificação proposta não torna o problema (5.22) mais difícil que (5.12). Isso porque minimizar  $\|\tilde{c}\|_\infty$  equivale a minimizar uma variável auxiliar  $\delta$  sujeita a  $|\tilde{c}_i| \leq \delta, \forall i \notin \mathcal{I}$ . Logo, temos novamente um SDP linear

$$\begin{aligned}
 \min_{\rho, \Delta, \delta} \quad & \sum_{i \in \mathcal{I}} \Delta_i + \delta \\
 \text{s.a.} \quad & |\text{tr}(E_i \rho) - f_i| \leq \Delta_i f_i \quad i \in \mathcal{I} \\
 & \text{tr}(E_i \rho) \leq \delta \quad i \notin \mathcal{I} \\
 & \text{tr}(\rho) = 1, \\
 & \rho \succeq 0.
 \end{aligned} \tag{5.24}$$

Embora a equivalência entre a nova formulação VQT (5.24) e MaxEnt seja verdadeira apenas na autobase, a relação entre essas duas abordagens é clara: ambas, cada qual da sua maneira, tentam definir as probabilidades não medidas o mais uniformemente possível.

## 5.4 Dados com ruído e MaxLik-MaxEnt

Quando consideramos dados com ruído, as restrições (5.13) podem não ser satisfeitas por nenhuma matriz de densidade. Considerando algum modelo estatístico para os ruídos, podemos aplicar a estimação por Máxima Verossimilhança, discutida no Capítulo 4.

No entanto, quando não temos um conjunto tomograficamente completo de medidas ou dados faltantes, pode existir um conjunto convexo de maximizadores da verossimilhança, isto é, um conjunto convexo de matrizes para as quais a verossimilhança atinge seu valor máximo. Então, a intersecção desse conjunto com o conjunto de matrizes de densidade pode ser um conjunto convexo não-vazio e, neste caso, teremos mais de uma solução de máxima verossimilhança. Cada uma dessas soluções é compatível com os dados disponíveis, no sentido de que minimiza alguma distância relativa entre as frequências observadas  $f_j$  e as probabilidades previstas pela mecânica quântica  $\text{tr}(E_j \rho)$ . Porém, essas soluções diferem em como ajustar as probabilidades não medidas.

Uma maneira de escolher uma solução dentre as soluções de máxima verossimilhança neste caso é aplicar o método MaxEnt restrito às soluções de verossimilhança. Para tal, após obter uma das soluções de MaxLik, digamos  $\rho_{ML}$ , sabemos que

$$\text{tr}(E_i \rho) = \bar{p}_i \equiv \text{tr}(E_i \rho_{ML}), \quad \forall i \in \mathcal{I}, \quad \forall \rho \in \mathcal{S}_{ML},$$

onde  $\mathcal{S}_{ML}$  é o conjunto solução de MaxLik. Então, podemos obter a solução de MaxEnt dentre as soluções de MaxLik resolvendo o problema (5.1) e substituindo  $f_i$  por  $\bar{p}_i$  para todo  $i \in \mathcal{I}$ . Esse é o método de Máxima Verossimilhança assistida por Máxima Entropia (MaxLik-MaxEnt) [78]. Uma outra possibilidade é considerar a maximização conjunta da verossimilhança e da entropia através de uma função Lagrangiana [86].

## 5.5 Simulações Numéricas

A fim de comparar as abordagens  $VQT_\infty$  e MaxEnt, para cada posto, geramos 100 matrizes de densidade distribuídas uniformemente segundo medida de Haar [101], representando estados de 4 q-bits. As simulações foram feitas em um computador Intel Core 2 Duo, 2 GB RAM, em MATLAB, usando Yalmip/SEDUMI [53, 85] para modelar e resolver os problemas de SDP linear. Fixamos uma base SIC-POVM [81] e para cada posto, a Figura 5.1 apresenta o melhor, o pior e a média do número de medidas necessárias para que um dado método convirja ao estado de referência. Consideramos que um método convergiu se a distância do traço em relação ao estado de referência for menor que  $10^{-4}$ . Primeiramente, consideramos dados sem ruído. Como

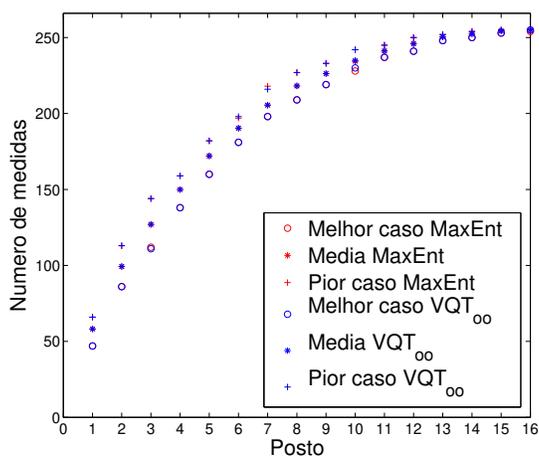


Figura 5.1: Convergência de  $VQT_\infty$  e MaxEnt conforme aumentamos o número de medidas

podemos ver, o número de medidas necessárias para a convergência é quase a mesma para os métodos MaxEnt e  $VQT_\infty$ . A Figura 5.1 também mostra que o pior caso de cada método não excede um número  $\mathcal{O}(rd \log d)$  de medidas ( $r$  é posto) mencionado em trabalhos de *compressed sensing* [38] em tomografia quântica.

Agora, comparamos a convergência dos métodos em termos de distância de traço média e entropia média para estados de posto 1 conforme o número de medidas aumenta, que está ilustrado na Figura 5.2. Novamente, podemos notar um comportamento similar

entre MaxEnt e  $VQT_{\infty}$ , o primeiro com uma distância de traço um pouco menor e entropia maior que o segundo.

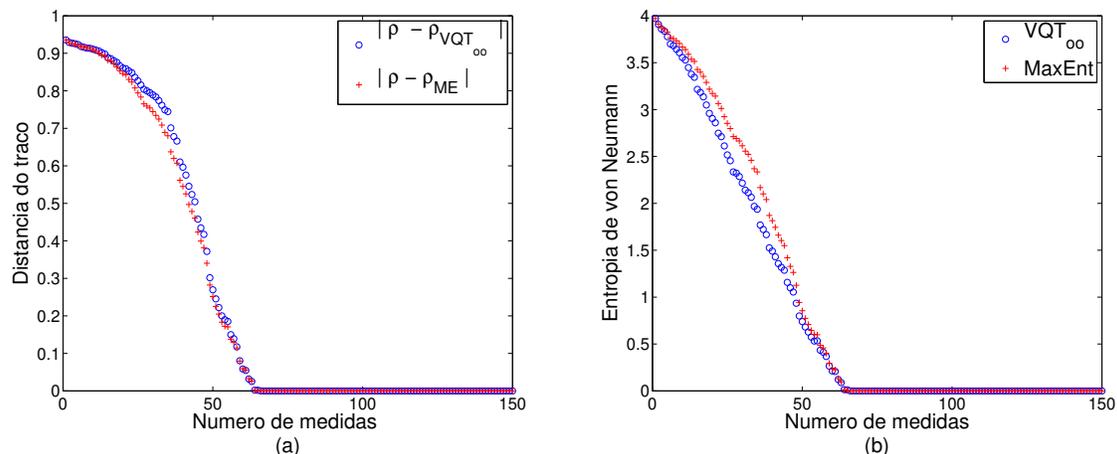


Figura 5.2: Esquerda: Distância de traço média para o estado verdadeiro de posto 1,  $VQT_{\infty}$  e MaxEnt. Direita: Entropia de von Neumann de  $VQT_{\infty}$  e MaxEnt.

O impacto da modificação proposta (5.24) aparece quando comparamos a distância de  $\tilde{c}$ , o vetor de probabilidades não medidas, ao vetor uniforme cujas entradas estão definidas em (5.19). A Figura 5.3 mostra, para postos 1 e 6, a divergência de Kullback-Leibler média de  $\tilde{c}$  à distribuição uniforme. Como podemos ver, o  $VQT_{\infty}$  está mais próximo do MaxEnt que a formulação VQT original. Quando o número de medidas é suficiente para determinar unicamente o estado, observamos então a concordância dos métodos.

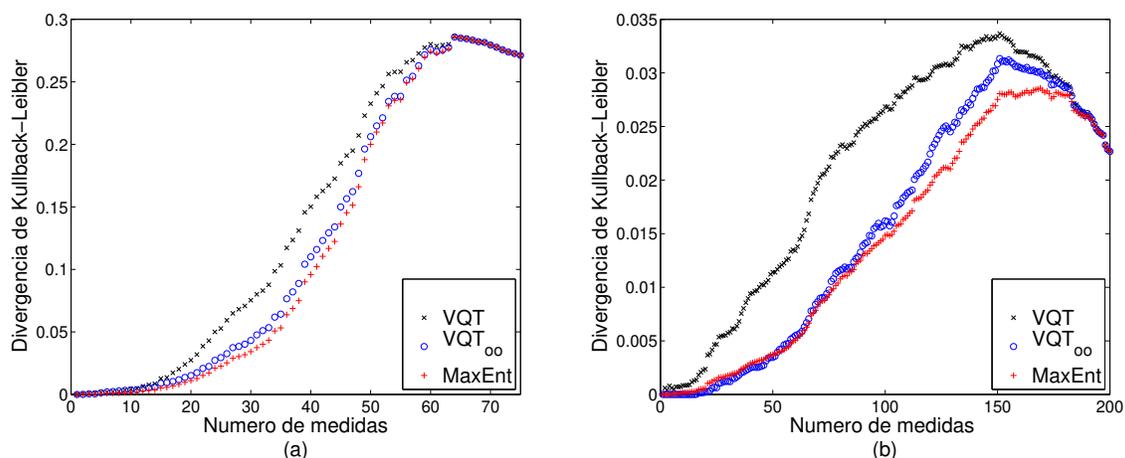


Figura 5.3: Divergência de Kullback-Leibler média de  $\tilde{c}$  para a distribuição uniforme.

Para estudar as propriedades de convergência dos métodos em um cenário mais realístico,

introduzimos dois tipos de erro nas probabilidades verdadeiras: um usando uma perturbação Gaussiana com média zero e variância  $10^{-6}$  e outro considerando valores uniformemente distribuídos em um intervalo de 5% de desvio das probabilidades verdadeiras. Como as equações (5.13) podem não ser satisfeitas para dados com ruído, utilizamos o método MaxLik-MaxEnt na comparação com  $VQT_{\infty}$ . Como função de verossimilhança, utilizamos uma variante de (3.23). A Figura 5.4 plota a distância do traço em função do número de medidas para estados de posto um e para os dois tipos de erro.

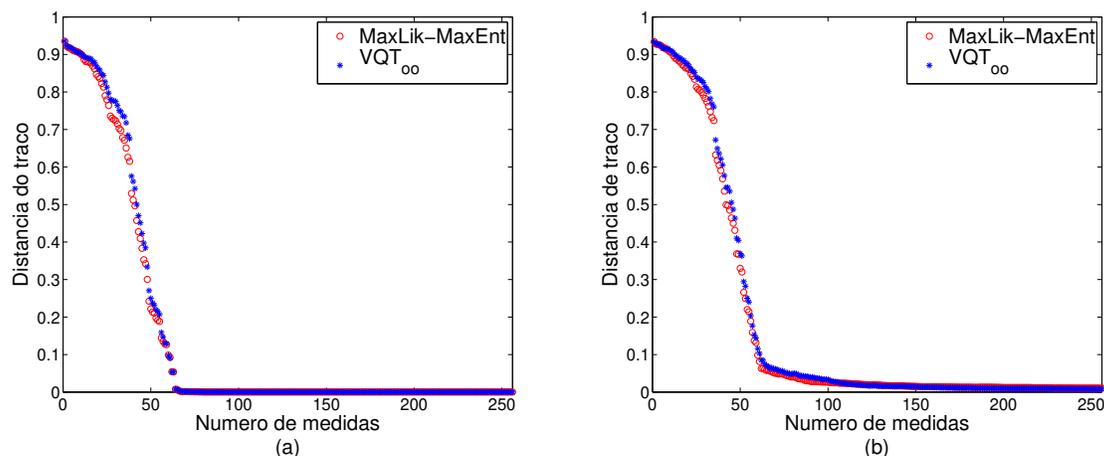


Figura 5.4: Esquerda: Distância do traço média ao estado de referência com probabilidades perturbadas por um ruído Gaussiano. Direita: Distância do traço média com 5% de ruído uniforme.

Essas simulações numéricas corroboram a relação entre os métodos  $VQT_{\infty}$  e MaxEnt já provada na Seção 5.3 para medidas na autobase. A nova formulação proposta (5.22), assim como a abordagem MaxEnt, tenta ajustar as probabilidades não medidas o mais uniforme possível. Vimos que os resultados para estes dois métodos são bem parecidos e o  $VQT_{\infty}$  tem a vantagem de ser um SDP linear, evitando assim os problemas de otimização não-linear do MaxEnt.

A Figura 5.5 apresenta o tempo médio de CPU gasto por Maxlik-MaxEnt, VQT e  $VQT_{\infty}$  para postos 1 e 6. Embora o  $VQT_{\infty}$  tenha um tempo maior que os outros para poucas medidas, ele se apresenta estável conforme o número de medidas aumenta. É importante destacar os “picos” de MaxEnt, que são uma consequência dos problemas de otimização não-lineares, pontos iniciais, etc. Cada tomografia usando  $VQT_{\infty}$  não leva mais que 5 segundos, enquanto MaxLik-MaxEnt gasta por volta de 12 segundos no pior caso.

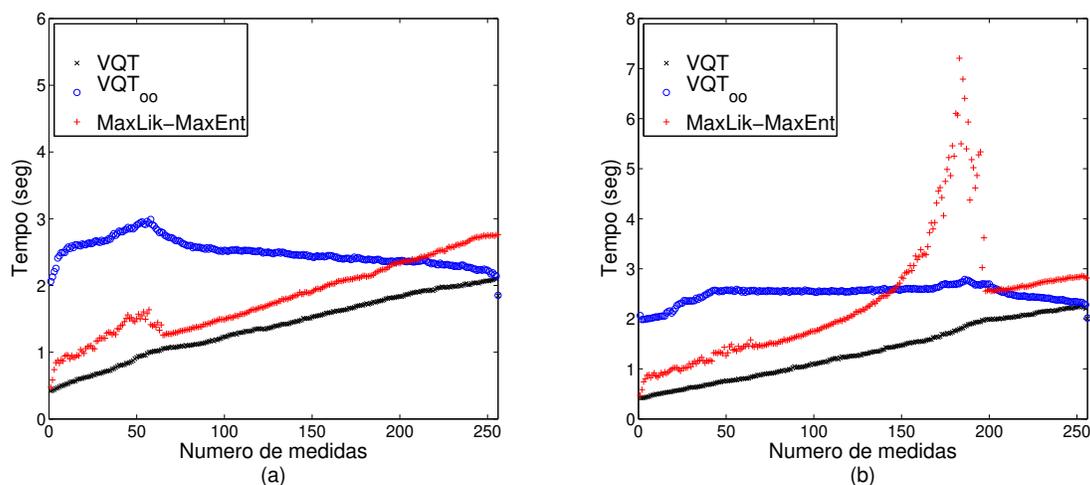


Figura 5.5: Tempo médio de CPU gasto conforme o número de medidas aumenta. (a) Posto 1, (b) Posto 6.

## 5.6 Máxima Entropia e falso emaranhamento

Segundo o princípio de Jaynes [49], não podemos tirar nenhuma conclusão que não seja garantida pelos dados experimentais. A motivação da Máxima Entropia [15] é obter a estimativa compatível com as observações e que seja menos comprometida com os dados faltantes.

Entretanto, em [44], Horodecki et al. apresentam um exemplo onde a estimativa de Máxima Entropia superestima o emaranhamento do sistema. É apresentado um conjunto incompleto de medidas para as quais existem estados separáveis compatíveis, que satisfazem (5.13). Porém, a solução que maximiza a entropia de von Neumann é um estado emaranhado. Neste sentido, a estimação por Máxima Entropia pode gerar falso emaranhamento, uma vez que o estado verdadeiro poderia ser separável.

Portanto, a solução mais entrópica não corresponde a de mínimo emaranhamento. Uma alternativa para não superestimar o emaranhamento é buscar dentre as soluções compatíveis com as medidas, aquela que minimiza alguma medida de emaranhamento, como por exemplo a entropia relativa de emaranhamento [94], o emaranhamento de formação [7], ou a negatividade [95].

A questão é que tais medidas, em geral, não são estritamente convexas, e como consequência, a estimativa de mínimo emaranhamento e compatível com as medidas pode não ser única. Ainda em [44], é sugerido calcular a estimativa de máxima entropia dentre as soluções de mínimo emaranhamento a fim de recuperar a unicidade.

## 5.7 Resumo do Capítulo 5

Neste capítulo, estudamos métodos para tomografia com um conjunto incompleto de medidas. Analisamos a abordagem de Máxima Entropia (MaxEnt) e a Tomografia Quântica Variacional (VQT). O comportamento desses métodos foi estudado teoricamente e através de simulações numéricas. Em particular, estudamos como cada um deles atribui as probabilidades associadas a elementos POVM não medidos.

Propusemos também uma variação do método VQT para tomografia quântica com dados incompletos, denominado  $VQT_\infty$ , que tenta ajustar as probabilidades não medidas o mais uniforme possível. Como consequência, mostramos que  $VQT_\infty$  tem um comportamento similar com o já conhecido método de MaxEnt e com MaxLik-MaxEnt na presença de ruído. Essa afirmação foi confirmada por simulações numéricas e demonstrada teoricamente para o caso de medições da autobase.

Portanto, com a formulação  $VQT_\infty$ , obtemos uma estimativa para a matriz de densidade tão pouco tendenciosa quanto a de MaxEnt e com a vantagem de trabalhar com problemas de SDP linear, que podem ser resolvidos eficientemente por métodos que possuem complexidade polinomial, uma propriedade importante em tomografia de sistemas quânticos cada vez maiores.

Além disso, na Seção 5.6, discutimos brevemente o problema de falso emaranhamento que pode surgir ao se utilizar a estimação por Máxima Entropia.



# Capítulo 6

## Gradiente projetado

Nos capítulos anteriores, nos deparamos com diferentes problemas de otimização restritos ao espaço de matrizes de densidade  $\mathcal{S}$ . No Capítulo 4, foram apresentados dois métodos para obter a estimativa de máxima verossimilhança: um utilizando uma reparametrização da variável  $\rho$ , detalhado na Seção 4.1, e outro específico para verossimilhança multinomial, apresentado na Seção 4.2. No Capítulo 5, estudamos algumas formulações baseadas em programação semidefinida linear.

Neste capítulo, propomos um método de Gradiente Projetado [8, 54, 70] aplicado ao problema:

$$\begin{aligned} \min_{\rho} \quad & F(\rho) \\ \text{s.a} \quad & \text{tr}(\rho) = 1, \\ & \rho \succeq 0. \end{aligned} \tag{6.1}$$

Ao contrário dos métodos anteriores que supõem alguma estrutura específica de  $F(\rho)$ , tais como convexidade ou linearidade, aqui pedimos apenas que  $F : \Omega \rightarrow \mathbb{R}$  seja uma função continuamente diferenciável em  $\rho$ , em um aberto  $\Omega$  contendo  $\mathcal{S}$ .

Esse método tem aplicação não só no problema de tomografia de estados, mas pode ser empregado para minimizar qualquer função de  $\rho$  em  $\mathcal{S}$ .

A Seção 6.1 apresenta o algoritmo básico de gradiente projetado. O subproblema de projeção em  $\mathcal{S}$  é tratado na Seção 6.2. A Seção 6.3 traz resultados numéricos de uma comparação entre Gradiente Projetado e o algoritmo  $R\rho R$ , descrito na Seção 4.2. Considerações finais e possíveis extensões das ideias apresentadas neste capítulo estão na Seção 6.4.

## 6.1 Algoritmo de Gradiente Projetado

A seguir apresentamos um algoritmo de Gradiente Projetado com estratégia de convergência global baseada em busca linear e critério de Armijo [8, 70]. Empregamos a notação,  $\mathcal{P}_{\mathcal{S}}(\cdot)$ , para denotar a projeção ortogonal (com respeito ao produto interno do traço) em  $\mathcal{S}$ .

**Algoritmo 6.1.1** (Gradiente Projetado).

**Inicialização.** Dado  $\rho^0 \in \mathcal{S}$ ,  $\varepsilon > 0$  e  $\gamma \in (0, 1)$ .

**Passo 1.** Calcule  $\mathcal{P}_{\mathcal{S}}(\rho^k - \nabla F(\rho^k))$ .

**Passo 2.** Faça  $D^k = \mathcal{P}_{\mathcal{S}}(\rho^k - \nabla F(\rho^k)) - \rho^k$ . Se  $\|D^k\| < \varepsilon$ , pare. Caso contrário faça  $\alpha = 1$ .

**Passo 3.** Enquanto  $F(\rho^k + \alpha D^k) \geq F(\rho^k) + \gamma\alpha(\text{tr}(D^k \nabla F(\rho^k)))$ , faça  $\alpha = 0.5\alpha$ .

**Passo 4.** Faça  $\rho^{k+1} = \rho^k + \alpha D^k$  e  $k = k + 1$ . Volte ao **Passo 1**.

No Passo 3, empregamos uma busca linear (backtracking) até que a condição de Armijo seja satisfeita. Desse modo, temos a convergência a um ponto estacionário, independentemente da estimativa inicial  $\rho^0$ , como foi discutido na Seção 4.2.1. Além disso, trabalhos recentes [10] mostram que um melhor desempenho pode ser obtido usando-se um tamanho de passo espectral [6] para a direção do gradiente juntamente com busca linear não-monótona [37].

No Passo 1 do Algoritmo 6.1.1, temos que encontrar a projeção da matriz Hermitiana  $\rho^k - \nabla F(\rho^k)$  em  $\mathcal{S}$ . Neste trabalho, descreveremos na Seção 6.2 como calcular a projeção através da decomposição espectral. Outras alternativas existem, como por exemplo, usar projeções inexatas [11], resolvendo o subproblema de projeção por programação semidefinida.

## 6.2 Projeção no espaço de Matrizes de Densidade

A projeção de uma matriz Hermitiana  $\hat{\rho}$  no espaço das matrizes de densidade, com respeito ao produto interno de Hilbert-Schmidt, é a solução do problema:

$$\begin{aligned} \min_{\rho} \quad & \frac{1}{2} \|\rho - \hat{\rho}\|_F^2 \\ \text{s.a} \quad & \text{tr}(\rho) = 1, \\ & \rho \succeq 0. \end{aligned} \tag{6.2}$$

Note que (6.2) é um problema de programação semidefinida não-linear e podemos resolvê-lo, por exemplo, através de métodos de pontos-interiores [90, 99].

Outra forma de encontrar a projeção é usar o fato de que a norma de Frobenius é invariante por transformações unitárias. Considere a decomposição espectral de  $\hat{\rho}$ :

$$\hat{\rho} = U\hat{\Lambda}U^\dagger.$$

Então,

$$\|\rho - \hat{\rho}\|_F^2 = \left\| \rho - U\hat{\Lambda}U^\dagger \right\|_F^2 = \left\| U^\dagger \rho U - \hat{\Lambda} \right\|_F^2.$$

Definindo  $Y = U^\dagger \rho U$ , temos que para  $\rho \in \mathcal{S}$ ,

$$\text{tr}(Y) = \text{tr}(U^\dagger \rho U) = \text{tr}(\rho U^\dagger U) = \text{tr}(\rho) = 1$$

e  $Y \succeq 0$ . Daí, temos que

$$\|\rho - \hat{\rho}\|_F^2 = \left\| Y - \hat{\Lambda} \right\|_F^2 = \sum_i (Y_{ii} - \hat{\Lambda}_{ii})^2 + \sum_{i,j} Y_{ij}^2.$$

Devido às restrições que definem  $\rho$ , e portanto  $Y$ , temos que  $Y_{ii} \geq 0$ ,  $\forall i$  e  $\sum_i Y_{ii} = 1$ . Assim, a matriz que minimiza as duas somatórias acima, respeitando as restrições, é dada por

$$\rho^* = U\Lambda^*U^\dagger,$$

onde  $\Lambda^*$  é solução do problema quadrático

$$\begin{aligned} \min_{\Lambda} \quad & \left\| \Lambda - \hat{\Lambda} \right\|_2^2 \\ \text{s.a} \quad & \sum_i \Lambda_{ii} = 1, \\ & \Lambda \succeq 0. \end{aligned} \tag{6.3}$$

### 6.2.1 Decomposição Espectral

Em geral, quando precisamos calcular todos os autovalores e autovetores de uma matriz Hermitiana  $A$ , a estratégia padrão é primeiro reduzir a matriz à forma de Hessenberg e em seguida aplicar o algoritmo QR com deslocamentos [35, 62].

No caso de matrizes simétricas, a forma de Hessenberg corresponde a uma matriz tri-diagonal  $T$ :

$$A = VTV^\dagger,$$

onde  $V$  é uma matriz unitária. A redução à forma tridiagonal através de  $n - 2$  reflexões de Householder custa  $\frac{4}{3}n^3$  flops (operações de ponto flutuante: adições e multiplicações). Se os autovetores são necessários, a reconstrução de  $V$  custa mais  $2n^3$  flops.

Como  $T$  é semelhante a  $A$ , os autovalores são os mesmos. A segunda etapa consiste em aplicar o algoritmo QR para encontrar os autovalores de  $T$ . Iniciando com  $T_0 = T$ , as iterações são definidas como:

$$\begin{aligned} T_k - \sigma_k I &= Q_k R_k, \\ T_{k+1} &= R_k Q_k + \sigma_k I, \end{aligned}$$

onde  $\sigma_k$  corresponde ao deslocamento utilizado para acelerar a convergência. É importante notar que o algoritmo QR preserva a estrutura de Hessenberg, tridiagonal no caso simétrico. Aproveitando essa estrutura tridiagonal, cada fatoração QR pode ser realizada com  $n - 1$  rotações de Givens. As matrizes tridiagonais  $T_k$  convergem a uma matriz diagonal contendo os autovalores de  $T$ . A matriz de autovetores de  $T$  é obtida do produto  $Q_1 Q_2 Q_3 \dots Q_{n-1}$ .

Quando apenas os autovalores são necessários, é possível reorganizar o algoritmo para encontrar todos eles em  $\mathcal{O}(n^2)$  flops. No entanto, se precisamos também dos autovetores, esse custo aumenta para aproximadamente  $6n^3$  flops (considerando duas iterações por autovalor). Com isso, o custo total de redução a forma tridiagonal mais o algoritmo QR é de aproximadamente  $9n^3$  [35].

De posse dos autovetores e autovalores, para encontrar a projeção de  $\hat{\rho}$  em  $\mathcal{S}$  devemos agora obter a projeção dos autovalores no simplex unitário.

### 6.2.2 Projeção no Simplex de probabilidade

Por conveniência, representaremos as matrizes diagonais  $\Lambda$  e  $\hat{\Lambda}$  de (6.3) como vetores  $x$  e  $\hat{x}$ . Assim, ficamos com o problema

$$\begin{aligned} \min_x \quad & \frac{1}{2} \|x - \hat{x}\|_2^2 \\ \text{s.a} \quad & \sum_i x_i = 1, \\ & x \geq 0, \end{aligned} \tag{6.4}$$

onde  $x \in \mathbb{R}^n$ , com  $x_i = \Lambda_{ii}$ ,  $\forall i$ . A solução de (6.4) corresponde à projeção do vetor  $\hat{x}$  (autovalores de  $\hat{\rho}$ ) no simplex unitário (ou simplex de probabilidades)

$$\Delta^n = \left\{ x \in \mathbb{R}^n \mid \sum_i x_i = 1, x \geq 0 \right\}.$$

Embora (6.4) seja um problema de programação quadrática, existem métodos diretos para calcular tal projeção [14,24,64]. Aqui, consideramos a alternativa proposta em [64].

Começamos com um algoritmo de projeções alternadas, já que a projeção em  $V = \{x \mid e^T x = 1\}$  e a projeção em  $\mathbb{R}_+^n$  possuem fórmulas fechadas:

$$\mathcal{P}_V(x) = x + \left( \frac{1 - e^T x}{n} \right) e,$$

$$\mathcal{P}_+(x) = \max \{x, 0\}.$$

É possível obter um algoritmo que converge em um número finito de passos, notando que as componentes negativas de  $\mathcal{P}_V(x)$  permanecerão nulas na solução.

**Teorema 6.2.1.** *Seja  $V$  um subespaço afim de  $\mathbb{R}^n$  e  $K \subset V$  um conjunto não-vazio, fechado e convexo. Se  $c \notin V$ , então*

$$\mathcal{P}_K(c) = \mathcal{P}_K(\mathcal{P}_V(c)).$$

*Demonstração.* Vide [64]. □

Para o próximo teorema, considere  $K = \Delta^n$ , e as seguintes notações:

$$I_n = \{1, 2, \dots, n\},$$

$$X_I = \{x \in \mathbb{R}^n \mid x_i = 0, \forall i \in I \subset I_n\},$$

$$n_i = \dim(X_I),$$

$$V_I = X_I \cap V,$$

$$K_I = X_I \cap K.$$

**Teorema 6.2.2.** *Seja  $I \subset I_n$ ,  $c \in V_I$  e defina  $\tilde{I} = \{i \notin I \mid c_i < 0\}$ . Então, se  $\tilde{I} \neq \emptyset$ , tem-se que  $p_{K_I}(c) \in K_{I \cup \tilde{I}}$ .*

*Demonstração.* Vide [64]. □

Este teorema nos diz que se  $c \in V_I$  possui alguma componente negativa, então a projeção  $p_{K_I}(c)$  se encontra em um simplex menor  $K_J = X_J \cap K$ , tal que  $I \subset J$ .

Os teoremas 6.2.1 e 6.2.2 fornecem um procedimento (recursivo) simples para encontrar a projeção de  $c$  em  $K = \Delta^n$ , apresentado a seguir.

**Algoritmo 6.2.1** (Projeção no simplex unitário).

**Inicialização.** Dado  $c \in \mathbb{R}^n$ , faça  $x = c$ ,  $I = \emptyset$ .

**Passo 1.** Calcule  $\tilde{x} = \mathcal{P}_{V_I}(x)$ . Se  $\tilde{x} \geq 0$ , pare ( $\tilde{x} = \mathcal{P}_K(c)$ ).

**Passo 2.** Faça  $I \leftarrow I \cup \{i \mid \tilde{x}_i < 0\}$  e substitua  $x$  por  $\mathcal{P}_{X_I}(\tilde{x})$ . Vá para o Passo 1.

A projeção de  $x$  em  $V_I$  é dada explicitamente por

$$\tilde{x}_i = x_i + \frac{(1 - \sum_i x_i)}{n_I}, \quad \forall i \notin I$$

$$\tilde{x}_i = 0, \quad \forall i \in I$$

e a projeção em  $X_I$  é dada por

$$\mathcal{P}_{X_I}(\tilde{x}) = \max\{\tilde{x}, 0\}.$$

O algoritmo termina em um número finito de passos pois a cada iteração, trabalhamos em subespaços  $X_I$  de dimensão cada vez menor (A cada iteração estamos resolvendo problemas de projeção em conjuntos com dimensão cada vez menor  $K_I \subset K_J \subset \dots$ ).

Seja  $x^*$  a solução de 6.4. Definindo  $\Lambda^* = \text{Diag}(x^*)$ , temos que a projeção de  $\hat{\rho}$  em  $\mathcal{S}$  é dada por

$$\mathcal{P}_{\mathcal{S}}(\hat{\rho}) = U\Lambda^*U^\dagger.$$

### 6.3 Experimentos Numéricos

Os testes numéricos desta seção têm por objetivo mostrar que o método de Gradiente Projetado é uma alternativa eficaz para problemas de minimização sobre o espaço de matrizes de densidade.

Consideremos o caso particular de tomografia de 2, 3 e 4 q-bits, assumindo uma estatística multinomial e o problema de Máxima Verossimilhança (4.22). Como o algoritmo  $R\rho R$  [46, 47, 79], descrito na Seção 4.2, foi desenvolvido especificamente para tal problema, esta foi nossa escolha para as comparações.

A Tabela 6.1 traz os resultados de nossa simulação. Consideramos 10 matrizes de densidade de posto completo, geradas aleatoriamente, associadas a 2, 3 e 4 q-bits. Para cada instância, fixamos um conjunto SIC-POVM e fornecemos as probabilidades associadas. Como ponto inicial, utilizamos o estado maximamente misto  $\rho^0 = (1/d)I$  para os dois métodos e consideramos que o algoritmo convergiu quando a distância entre a aproximação corrente e o estado de referência é menor que  $10^{-4}$ . Na Tabela 6.1, podemos ver para cada método e instância, o número de iterações, o tempo de execução e o tempo por iteração. Os dois métodos foram implementados em MATLAB.

Uma das principais características da iteração  $R\rho R$  é sua facilidade de implementação e baixo custo computacional, já que envolve apenas o produto de matrizes (além da avaliação de  $R(\rho) = \nabla F(\rho)$ ). Por outro lado, no método de Gradiente Projetado, temos uma iteração mais cara, já que temos que calcular a projeção de  $\rho - \nabla F(\rho)$  em  $\mathcal{S}$ . Isso fica evidente observando o tempo por iteração na Tabela 6.1.

	$R\rho R$			Gradiente Projetado			
	Iter.	Tempo(s)	Tempo/Iter.	Iter.	Tempo(s)	Tempo/Iter.	
2 q-bits	1	80	0.0508	0.0006	39	0.0444	0.0011
	2	57	0.0206	0.0004	15	0.0129	0.0009
	3	27	0.0103	0.0004	11	0.0108	0.0010
	4	22	0.0080	0.0004	9	0.0087	0.0010
	5	39	0.0140	0.0004	10	0.0087	0.0009
	6	97	0.0353	0.0004	58	0.0475	0.0008
	7	55	0.0209	0.0004	25	0.0252	0.0010
	8	115	0.0413	0.0004	20	0.0186	0.0009
	9	220	0.0760	0.0003	67	0.0753	0.0011
	10	247	0.0862	0.0003	20	0.0174	0.0009
3 q-bits	1	129	0.1799	0.0014	33	0.0925	0.0028
	2	220	0.3025	0.0014	23	0.0753	0.0033
	3	620	0.8464	0.0014	175	0.4639	0.0027
	4	448	0.6124	0.0014	21	0.0683	0.0033
	5	362	0.4956	0.0014	13	0.0389	0.0030
	6	132	0.1839	0.0014	33	0.0924	0.0028
	7	404	0.5541	0.0014	20	0.0585	0.0029
	8	99	0.1381	0.0014	15	0.0451	0.0030
	9	122	0.1696	0.0014	16	0.0481	0.0030
	10	1005	1.3647	0.0014	41	0.1140	0.0028
4 q-bits	1	329	2.5169	0.0077	20	0.2878	0.0144
	2	2117	16.1622	0.0076	24	0.3513	0.0146
	3	1262	9.6684	0.0077	78	1.0960	0.0141
	4	702	5.3685	0.0076	19	0.2989	0.0157
	5	587	4.5237	0.0077	19	0.2746	0.0145
	6	588	4.5028	0.0077	27	0.4227	0.0157
	7	1869	14.2499	0.0076	355	4.8916	0.0138
	8	1169	8.9678	0.0077	69	0.9645	0.0140
	9	1089	8.3183	0.0076	67	0.9396	0.0140
	10	375	2.8741	0.0077	16	0.2327	0.0145

Tabela 6.1: Comparativo  $R\rho R \times$  Gradiente Projetado.

No entanto, apesar de um custo por iteração maior, o Gradiente Projetado, em geral, realiza bem menos iterações, e demanda um tempo menor para convergir. Dos 30 problemas teste, ele convergiu em menor tempo em 26, apresentando sempre um menor número de iterações.

Estes estudos preliminares mostram o Gradiente Projetado como um método promissor para a minimização de funções no espaço de matrizes de densidade. É claro que os resultados apresentados trataram de problemas de pequeno porte, envolvendo matrizes de no máximo ordem 16. Devemos estar cientes de que o custo no cálculo da projeção em  $\mathcal{S}$  via decomposição espectral pode ser proibitivo para dimensões muito grandes e,

neste caso, determinar inexatamente a projeção [11] pode ser mais viável. Já o algoritmo  $R\rho R$ , que faz uso apenas de produto de matrizes, pode tirar proveito de estrutura de esparsidade, e apesar de ter mais iterações, talvez apresente um tempo total menor em problemas de larga escala.

## 6.4 Resumo do Capítulo 6

Neste capítulo, apresentamos um método de gradiente projetado para resolver o problema de minimizar  $F(\rho)$  em  $\mathcal{S}$ . A contribuição foi descrever um método que possa ser aplicado não só na Tomografia de Estados Quânticos, em particular na estimação de Máxima Verossimilhança, mas também na minimização/maximização de outras funções restritas ao espaço de matrizes densidade.

A Seção 6.3 apresentou alguns resultados numéricos, onde o Gradiente Projetado mostrou-se mais eficiente em relação ao algoritmo  $R\rho R$  utilizado em tomografia de estados quânticos. Em geral, mesmo com um custo por iteração maior, o número de iterações apresentadas pelo Gradiente Projetado foi bem menor que o de  $R\rho R$ , resolvendo em menor tempo a maioria dos problemas.

Além da aplicabilidade na minimização de outras funções restritas a  $\mathcal{S}$ , uma possível extensão é considerar restrições lineares adicionais, do tipo

$$\text{tr}(A_i\rho) = a_i,$$

no problema (6.1). Neste caso, a projeção de  $\rho - \nabla F(\rho)$  seria na intersecção do subespaço afim, definido pelas restrições lineares, com  $\mathcal{S}$ . Podemos considerar a própria restrição do traço  $\text{tr}(\rho) = 1$  como parte das restrições lineares, e toda a discussão da Seção 6.2 pode ser generalizada considerando-se a projeção no subespaço afim

$$\mathcal{V} = \{\rho \mid \text{tr}(A_i\rho) = a_i, \text{tr}(\rho) = 1\},$$

no lugar de  $\{\rho \mid \text{tr}(\rho) = 1\}$ , que também possui uma fórmula fechada.

# Capítulo 7

## Inferência Bayesiana

Como vimos no Capítulo 4, a estimação por Máxima Verossimilhança (EMV) considera como melhor estimativa para a matriz de densidade, a matriz  $\hat{\rho}$  que maximiza a probabilidade dos dados observados. Um questionamento importante sobre essa abordagem é que dados reais, em geral, contêm erros e podem implicar no máximo (irrestrito) da verossimilhança fora do espaço de matrizes de densidade. Esse é o motivo pelo qual a inversão linear pode gerar matrizes inválidas. Neste caso, a EMV se encontra na fronteira de  $\mathcal{S}$  e, assim, corresponde a uma matriz de posto deficiente, ou seja, com um ou mais autovalores nulos. Isso implica que a probabilidade de ocorrência de certos eventos (saídas experimentais) é zero, o que não pode ser justificado com uma quantidade finita (e muitas vezes pequena) de dados. Além disso, não há como utilizar barras de erro consistentes com uma probabilidade nula [12].

Ao contrário da EMV, que busca uma única estimativa maximamente plausível, a inferência Bayesiana também considera outras estimativas um pouco menos plausíveis. Em verdade, em inferência Bayesiana, o parâmetro a ser estimado  $\rho$  é considerado em si uma variável aleatória e nos interessa descobrir qual a distribuição  $\pi(\rho)$ . Tal distribuição, chamada a posteriori, é resultado do produto da verossimilhança, com uma distribuição a priori  $\pi_0(\rho)$ . A partir da posteriori é que obtemos uma estimativa pontual  $\hat{\rho}$ , tomando por exemplo, a média de tal distribuição, assim como barras de erro consistentes podem ser obtidas a partir da variância e do desvio padrão dessa distribuição.

Na Seção 7.1, descrevemos como a inferência Bayesiana pode ser aplicada na Tomografia de Estados Quânticos. A Seção 7.2 traz uma implementação prática através de simulações Monte Carlo via cadeias de Markov (MCMC). A Seção 7.3 discute alguns aspectos de convergência. Um exemplo ilustrando a abordagem Bayesiana, em contraste com a EMV e a inversão linear, é apresentado na Seção 7.4. A Seção 7.5 traz algumas considerações finais.

## 7.1 Tomografia Quântica Bayesiana

A Inferência Bayesiana [29, 32], como o próprio nome sugere, é baseada na regra de Bayes:

$$P(H|D) = \frac{P(D|H)P(H)}{P(D)},$$

onde  $P(D|H)$  é a probabilidade de se obter os dados  $D$  dada a hipótese  $H$  (isto é, a função de verossimilhança),  $P(H)$  é a distribuição *a priori* de  $H$  e  $P(H|D)$  é a distribuição *a posteriori* de  $H$  mediante os dados  $D$ .  $P(D)$  é a probabilidade marginal dos dados  $D$ :

$$P(D) = \sum_H P(D|H)P(H),$$

onde o somatório é sobre todas as hipóteses plausíveis. Isso significa que os dados observados  $D$  atualizam o conhecimento a priori:  $P(H) \rightarrow P(H|D)$ .

A extensão dessa ideia à Tomografia de Estados Quânticos [4, 12, 23] é direta se substituirmos  $H$  por  $\rho$  e  $D$  pelos dados experimentais. Então, em TEQ, da atualização de Bayes temos que

$$\pi(\rho) \propto \mathcal{L}(\rho)\pi_0(\rho), \quad (7.1)$$

onde  $\mathcal{L}(\rho)$  é a função de verossimilhança,  $\pi_0(\rho)$  é a distribuição a priori e  $\pi(\rho)$  a distribuição a posteriori.

A distribuição a priori  $\pi_0(\rho)$  claramente afeta a posteriori e representa o conhecimento prévio do experimentalista sobre o estado do sistema. Quando tal informação prévia não está disponível, é usual tomar uma distribuição uniforme ou uma priori não-informativa a fim de reduzir o viés.

A verossimilhança  $\mathcal{L}(\rho) = P(n | \rho)$  é a probabilidade de se obter os dados observados  $n$  dada a matriz de densidade  $\rho$ . Ela representa a informação contida nos dados e atualiza o conhecimento a priori.

Uma vez que em Inferência Bayesiana (IB) o parâmetro  $\rho$  a ser estimado é considerado ele próprio uma variável aleatória, o objetivo é calcular a distribuição a posteriori  $\pi(\rho)$  de tal parâmetro. A partir da posteriori, podemos inferir o valor esperado de qualquer função  $g(\rho)$ :

$$\mathbf{E}(g(\rho)) = \int_{\mathcal{S}} g(\rho) \pi(\rho) d\rho, \quad (7.2)$$

onde a integração é sobre o espaço de matrizes de densidade  $\mathcal{S}$ . Em particular, como estimativa pontual para  $\rho$  podemos utilizar, por exemplo, a média

$$\rho_B = \int_{\mathcal{S}} \rho \pi(\rho) d\rho. \quad (7.3)$$

Há dois grandes desafios no cálculo das expressões (7.2) e (7.3). O primeiro é como calcular as integrais sobre os espaço de matrizes de densidade  $\mathcal{S}$ . Mesmo quando  $\pi(\rho)$  tem uma expressão analítica, a integração é difícil por conta da geometria de  $\mathcal{S}$ : a intersecção de um hiperplano, definido por  $\text{tr}(\rho) = 1$ , com o cone das matrizes Hermitianas semidefinidas positivas,  $\rho \succeq 0$ . Podemos usar técnicas de integração Monte Carlo [32] para aproximar os valores esperados por médias amostrais:

$$\mathbf{E}(g(\rho)) \approx \frac{1}{n} \sum_{t=1}^n g(\rho_t),$$

onde  $\{\rho_t\}_t$  são amostras de  $\pi(\cdot)$ .

No entanto, aqui aparece o segundo desafio: como amostrar de  $\pi(\cdot)$ ? Amostrar diretamente de  $\pi(\rho)$  pode ser difícil principalmente por seu suporte em  $\mathcal{S}$ . Na literatura, existem poucas distribuições sobre o espaço das matrizes de densidade e a maior parte das existentes é formada por distribuições uniformes  $\mathcal{S}$  segundo alguma medida apropriada [101]. Por exemplo, para gerar matrizes de densidade  $W$  aleatórias, uniformemente distribuídas segundo a medida de Hilbert-Schmidt, basta tomar uma matriz  $X$  do ensemble de Ginibre [34, 60, 63] (com entradas normais padrão independentes) e tomar

$$W = \frac{X^\dagger X}{\text{tr}(X^\dagger X)}. \quad (7.4)$$

Felizmente, mesmo quando  $\pi(\cdot)$  tem uma expressão complicada ou desconhecida, ou ainda, não sabemos como amostrar diretamente de tal distribuição, podemos ainda realizar inferência Bayesiana usando métodos Monte Carlo via Cadeias de Markov (MCMC) [29, 32].

## 7.2 Monte Carlo via Cadeias de Markov

Suponha que desejamos obter amostras  $\{\theta_t\}$  de uma distribuição  $\pi(\theta)$ . As amostras  $\{\theta_t\}$  podem ser geradas por um processo que obtem amostras no suporte de  $\pi(\cdot)$  espalhadas em proporções corretas. Uma maneira de se fazer isso é através de uma cadeia de Markov que tem  $\pi(\cdot)$  como distribuição estacionária. Este processo é chamado Monte Carlo via Cadeias de Markov (MCMC) [29, 32].

Uma cadeia de Markov é uma sequência de variáveis aleatórias  $\{\theta_0, \theta_1, \theta_2, \dots\}$  tal que o próximo estado da cadeia  $\theta_{t+1}$  é amostrado de uma distribuição  $P(\theta_{t+1} | \theta_t)$  que depende apenas do estado atual. Sob certas condições de regularidade [32], a cadeia gradualmente esquece seu estado inicial  $\theta_0$  e,  $P^{(t)}(\cdot | \theta_0)$  eventualmente converge para uma única distribuição estacionária  $\phi(\cdot)$ . Assim, conforme  $t$  cresce, as amostras  $\{\theta_t\}$  parecem mais e mais com amostras de  $\phi(\cdot)$ .

Então, se a distribuição estacionária  $\phi(\cdot)$  é a distribuição alvo  $\pi(\cdot)$ , após um longo *burn-in* (descarte) de  $m$  iterações, os pontos  $\{\theta_t\}$  serão aproximadamente amostras dependentes de  $\pi(\cdot)$ , permitindo estimar  $\mathbf{E}(g(\theta))$  pela média ergódica [32]:

$$\bar{g} = \frac{1}{n - m} \sum_{t=m+1}^n g(\theta_t). \quad (7.5)$$

Além da média Bayesiana para  $g(\theta)$ , podemos também obter intervalos de credibilidade para  $g(\theta)$  através das amostras  $\{\theta_t\}$  geradas via MCMC. Por exemplo, se temos 1000 amostras  $\theta_t$ , um intervalo de credibilidade de 95% para  $g(\theta)$ , pode ser obtido ordenando os 1000 valores  $g(\theta_t)$ , em ordem crescente, e definindo o intervalo  $(g(\theta)_{25}, g(\theta)_{975})$ .

Mas ainda fica a questão: como gerar uma cadeia de Markov que tem  $\pi(\cdot)$  como distribuição estacionária?

### 7.2.1 Metropolis-Hastings

Para construir uma cadeia de Markov com distribuição estacionária  $\pi(\cdot)$ , podemos usar o algoritmo de Metropolis-Hastings [39, 61]. A cada tempo  $t$ , para escolher o próximo estado  $\theta_{t+1}$ , primeiro amostramos um candidato  $y$  de uma distribuição proposta  $q(\cdot | \theta_t)$ . O candidato  $y$  é aceito com probabilidade  $\alpha(\theta_t, y)$ :

$$\alpha(\theta_t, y) = \min \left( 1, \frac{\pi(y)q(\theta_t | y)}{\pi(\theta_t)q(y | \theta_t)} \right). \quad (7.6)$$

Se o candidato é aceito, o próximo estado da cadeia passa a ser  $\theta_{t+1} = y$ . Caso contrário, a cadeia não se move:  $\theta_{t+1} = \theta_t$ .

Notavelmente, é possível mostrar que independentemente da distribuição proposta, a distribuição estacionária será  $\pi(\cdot)$  [32]. No entanto, a velocidade de convergência depende de quanto a distribuição proposta  $q(\cdot | \cdot)$  se parece com a distribuição desejada  $\pi(\cdot)$ .

### 7.2.2 Distribuição proposta

A partir da distribuição proposta é que serão gerados os candidatos no algoritmo Metropolis-Hastings, que serão aceitos, ou não, segundo o critério (7.6). Apesar da teoria garantir a convergência da cadeia de Markov gerada, independentemente da distribuição proposta, a velocidade de convergência depende fortemente de tal escolha.

O suporte de nossa distribuição a posteriori  $\pi(\rho)$  é o espaço das matrizes de densidade  $\mathcal{S}$ . Assim, é razoável pedir que os candidatos gerados da distribuição proposta  $q(\rho | \cdot)$  também estejam em  $\mathcal{S}$ .

A questão é que a distribuição em  $\mathcal{S}$  mais discutida na literatura é a distribuição uniforme [101]. Sem dúvida, gerar matrizes de densidade uniformemente distribuídas, segundo alguma medida apropriada, é de grande utilidade para gerar estados mistos de forma aleatória, que podem ser usados, por exemplo, em simulações numéricas. No entanto, a distribuição uniforme não é uma boa escolha para a distribuição proposta em MCMC, pois a maior parte dos candidatos gerados podem ser rejeitados e a cadeia de Markov pode ficar estagnada por muito tempo.

O ideal é que a densidade proposta esteja centrada no estado atual da cadeia  $\rho_t$  e que possamos controlar a variância de modo a garantir uma taxa de aceitação (número de candidatos aceitos pelo número de candidatos gerados) razoável [29], entre 30% e 60%, por exemplo.

Em [12], onde é proposta a Inferência Bayesiana em TEQ, é sugerido que os candidatos sejam gerados de um passeio aleatório no espaço de matrizes de densidade. Associado ao passeio aleatório, temos uma distribuição proposta simétrica  $q(\rho|\sigma) = q(\sigma|\rho) = q(|\rho - \sigma|)$ , e o critério (7.6) é simplificado. Neste mesmo trabalho, é apresentado um procedimento para gerar estados mistos aleatórios inspirado em passeio aleatório, mas não é mostrado que  $q(\rho|\sigma) = q(|\rho - \sigma|)$ . Já em [23], é utilizado MCMC em inferência Bayesiana para tomografia de estados comprimidos com difusão de fase, onde a matriz de densidade fica em função de apenas 3 parâmetros: compressão, anti-compressão e ruído de fase. A distribuição proposta utilizada é uma Normal, centrada no valor atual da cadeia e com variância fixada, para cada um dos parâmetros.

Aqui, seguimos a ideia de [23] de parametrizar a matriz  $\rho(\theta)$ , mas damos um passo além, no sentido de usar uma parametrização aplicável a qualquer estado misto. Tal parametrização da matriz de densidade foi apresentada em (3.10) e as questões relacionadas a máximos locais da verossimilhança foram tratadas na Seção 4.1. Como discutido na Subseção 4.1.3, se os parâmetros  $t$  que definem (3.15) são restritos a  $\|t\|_2^2 = 1$  e  $t_i > 0$  para  $i = 1, 2, \dots, d$ , onde  $d$  é a ordem de  $\rho$  (não confundir o vetor de parâmetros  $t$  com o índice das cadeias), então a verossimilhança será unimodal.

Para atender esses requisitos, podemos redefinir os  $d^2$  parâmetros  $t$  como produtos de senos e cossenos de  $d^2 - 1$  ângulos  $\theta_i$ :

$$\begin{aligned}
 t_1 &= \sin \theta_{d^2-1} \sin \theta_{d^2-2} \dots \sin \theta_2 \sin \theta_1, \\
 t_2 &= \sin \theta_{d^2-1} \sin \theta_{d^2-2} \dots \sin \theta_2 \cos \theta_1, \\
 &\vdots \\
 t_{d^2-1} &= \sin \theta_{d^2-1} \cos \theta_{d^2-2}, \\
 t_{d^2} &= \cos \theta_{d^2-1},
 \end{aligned} \tag{7.7}$$

ou equivalentemente, definindo  $\cos \theta_0 = \sin \theta_{d^2} = 1$ , temos

$$t_i = \cos \theta_{i-1} \prod_{j=i}^{d^2} \sin \theta_j.$$

É elementar mostrar que  $\|t(\theta)\|_2^2 = 1$  e, para que  $t_i(\theta) > 0$  para  $i = 1, 2, \dots, d$ , basta definir o espaço paramétrico de  $\theta$  como

$$\Theta = \{0 < \theta_i < \pi/2, \text{ para } i = 1, 2, \dots, d-1, \text{ e } 0 < \theta_i < \pi, \text{ para } i \geq d\}.$$

Uma parametrização similar é usada em [65], para gerar amostras uniformes no espaço de matrizes definidas positivas e de traço constante. Desse modo, mudamos nosso espaço paramétrico do espaço de matrizes de densidade  $\rho$  para o espaço de parâmetros  $\theta$ , e agora estamos interessados na distribuição a posteriori dos parâmetros  $\theta$ :

$$\pi(\theta) \propto \mathcal{L}(\rho(\theta))\pi_0(\theta), \quad (7.8)$$

onde  $\pi_0(\theta)$  é a distribuição a priori de  $\theta$ . Note que a verossimilhança  $\mathcal{L}(\rho(\theta))$  continua dependendo de  $\rho$  e dos resultados de medições observados, só que agora como função de  $\theta$ . Neste caso, como  $\rho$  é função de  $\theta$ , a estimativa pontual para  $\rho$  passa a ser:

$$\rho_B = \int_{\Theta} \rho(\theta)\pi(\theta)d\theta.$$

Em verdade, a integral acima é aproximada pela média ergódica (7.5) calculada a partir das amostras  $\{\theta_t\}$  geradas via MCMC. Como a relação entre  $\Theta$  e  $\text{int}(\mathcal{S})$  é um-a-um pela parametrização (7.7), quando geramos amostras  $\{\theta_t\}$  de  $\pi(\theta)$ , implicitamente geramos amostras  $\{\rho_t\}$  de  $\pi(\rho)$ , tais que  $\rho_t = \rho(\theta_t)$ .

Para gerar candidatos  $y$  no algoritmo de Metropolis-Hastings, consideramos  $y_i$ 's amostrados independentemente de Normais truncadas no intervalo de cada parâmetro, centradas em  $\theta_{i,t}$  e com desvio padrão  $\Delta_i$ . Como resultado, a densidade proposta  $q(y | \theta_t)$  é definida como um produto de densidades Normais truncadas.

Assim, usando a simetria da distribuição Normal, temos que a razão entre as densidades propostas no critério (7.6) é dada por

$$\frac{q(\theta_t | y)}{q(y | \theta_t)} = \prod_{i=1}^{d^2-1} \frac{\Phi(\frac{b_i - \theta_{i,t}}{\sigma}) - \Phi(\frac{a_i - \theta_{i,t}}{\sigma})}{\Phi(\frac{b_i - y_i}{\sigma}) - \Phi(\frac{a_i - y_i}{\sigma})},$$

onde  $[a_i, b_i]$  é o intervalo onde  $\theta_i$  está definido e  $\Phi(\cdot)$  é a função de densidade acumulada da Normal padrão.

### 7.2.3 Distribuição a priori

Como já mencionamos anteriormente, a distribuição a priori  $\pi_0(\theta)$  contém informação prévia sobre o parâmetro  $\theta$  e influi na posteriori  $\pi(\theta)$ , segundo a equação (7.8). Quando alguma informação sobre o parâmetro de interesse  $\theta$  é conhecida, esta deve ser incorporada através de  $\pi_0(\theta)$ .

Por exemplo, suponha que o experimentalista tenha boas razões para acreditar que os estados mais plausíveis devem estar próximos de  $|0\rangle\langle 0|$ . Neste caso, pela parametrização (7.7), teremos três ângulos  $\theta_1$ ,  $\theta_2$  e  $\theta_3$ , e obtemos o estado  $|0\rangle\langle 0|$  quando  $\theta_3 = \pi/2$ ,  $\theta_2 = \pi/2$  e  $\theta_1 = \pi/2$ . Assim, podemos utilizar como distribuições a priori para esses parâmetros, distribuições Normais truncadas (no intervalo de cada  $\theta_i$ ) centradas em  $\pi/2$ , e controlar através da variância o quanto acredita-se ou não nesses valores.

Quando tal informação a priori não está disponível, devemos utilizar uma priori uniforme ou não-informativa.

## 7.3 Burn-in e diagnósticos de convergência

Como a teoria garante que a cadeia de Markov produzida pelo Metropolis-Hastings eventualmente converge à distribuição desejada  $\pi(\cdot)$ , dado um número suficientemente grande de iterações, surgem duas questões: quão longo deve ser o *burn-in* e quantas iterações são necessárias? As próximas subseções tentam responder essas perguntas.

### 7.3.1 Burn-in

Normalmente, os elementos das primeiras iterações da cadeia de Markov podem estar longe de amostras da distribuição alvo  $\pi(\cdot)$ . Geralmente, descartamos as primeiras, digamos  $m$ , iterações e consideramos os elementos restantes da cadeia como amostras de  $\pi(\cdot)$ .

Um tipo de análise para determinar o tamanho do *burn-in* é rodar  $N \geq 2$  cadeias em paralelo, iniciando de pontos suficientemente dispersos no espaço paramétrico e verificar quando elas se misturam.

Ilustramos essa análise na Figura 7.1, para o caso de uma matriz de densidade real representada na forma

$$\begin{bmatrix} x & z \\ z & y \end{bmatrix} = \begin{bmatrix} t_1 & \\ & t_2 \end{bmatrix} \begin{bmatrix} t_1 & t_3 \\ & t_2 \end{bmatrix}, \quad (7.9)$$

onde

$$\begin{aligned} t_1 &= \sin \theta_2 \sin \theta_1 \\ t_2 &= \sin \theta_2 \cos \theta_1 \\ t_3 &= \cos \theta_2. \end{aligned}$$

Simulamos 3 cadeias em paralelo para cada um dos parâmetros  $\theta_1$ ,  $\theta_2$ . A Figura 7.1 revela que as cadeias misturam-se rápido, antes de 500 iterações.

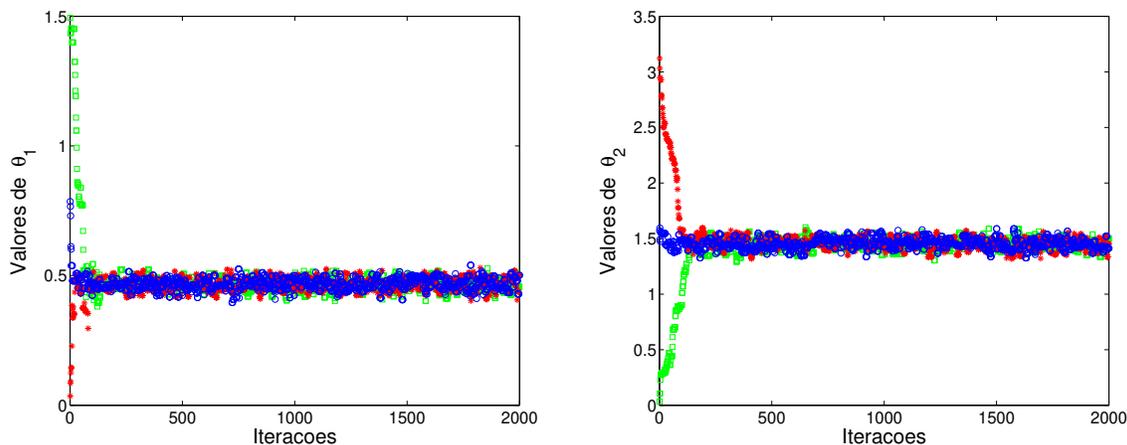


Figura 7.1: A mistura de 3 cadeias em paralelo para cada parâmetro  $\theta_1$ ,  $\theta_2$ .

Outra maneira de estudar a mistura das cadeias é monitorar as autocorrelações. É esperado que a cadeia gradualmente esqueça as iterações iniciais, e então as autocorrelações devem decrescer conforme a cadeia evolui. A Figura 7.2 mostra as autocorrelações das cadeias de cada parâmetro.

### 7.3.2 Diagnósticos de convergência

No fim das contas, como saber que a cadeia já convergiu? Como saber se o número de iterações é suficiente?

Podemos usar, por exemplo, os *traceplots* (gráficos dos valores simulados) e monitorar o comportamento da cadeia. A Figura 7.3 mostra o comportamento das cadeias em nosso pequeno exemplo  $2 \times 2$ , para os parâmetros  $\theta_1$  e  $\theta_2$ . Podemos ver que as cadeias se estabilizam em torno de um determinado valor, o que indica a convergência.

Associada à cadeia  $\{\theta_t\}$ , temos também a cadeia  $\{\rho_t\}$ . A Figura 7.4 apresenta as cadeias para as componentes  $x$ ,  $y$ ,  $z$  de  $\rho$ . Vemos que as cadeias se estabilizam em torno dos valores verdadeiros, indicados pelas linhas vermelhas, que correspondem à matriz

$$\rho_* = \begin{bmatrix} 0.2 & 0.05 \\ 0.05 & 0.8 \end{bmatrix},$$

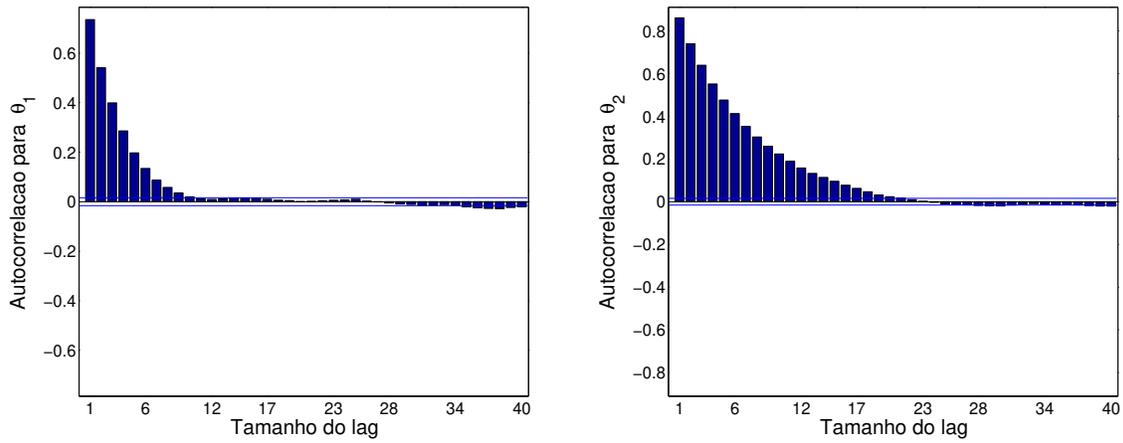


Figura 7.2: Gráficos de autocorrelação

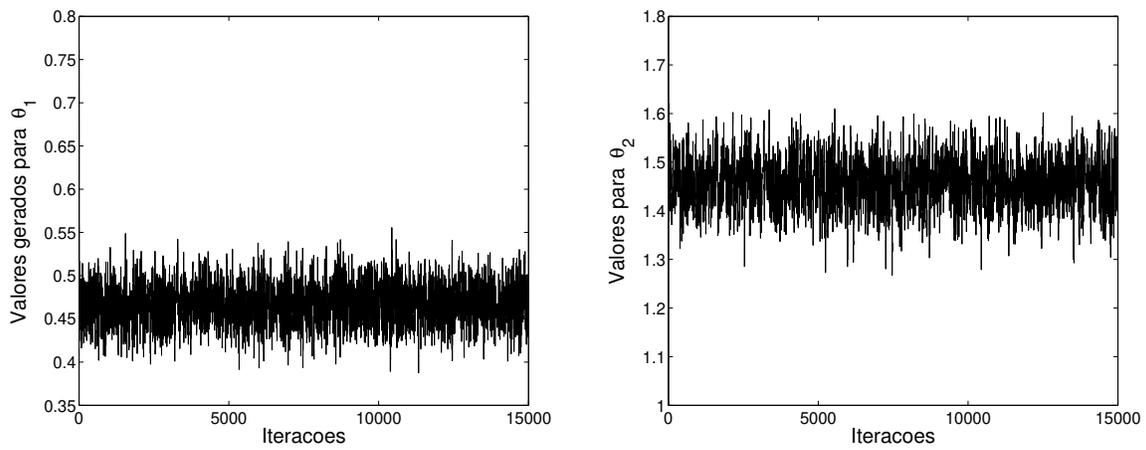


Figura 7.3: Traceplots para as cadeias  $\theta_1$  e  $\theta_2$ .

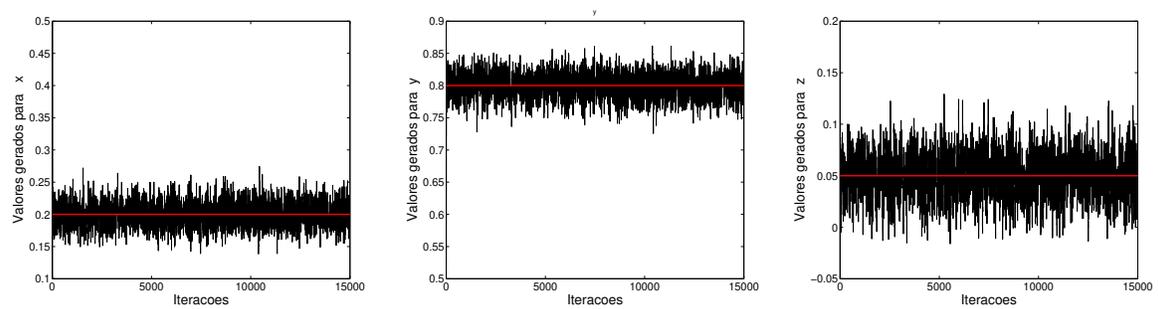


Figura 7.4: Traceplots para as cadeias x, y e z.

a partir da qual geramos os dados desta simulação. Nesta simulação consideramos uma verossimilhança multinomial e um conjunto POVM definindo as probabilidades. Como priori, adotamos distribuições uniformes para cada parâmetro  $\theta_1, \theta_2$ . Em verdade, quando utilizamos apenas  $t_1, t_2$  e  $t_3$  na parametrização de uma matriz de densidade de um q-bit, estamos implicitamente adotando que  $t_4 = 0$ , ou seja, que teremos uma matriz real, o que também é uma informação a priori.

No entanto, para instâncias maiores, não é fácil monitorar  $d^2 - 1$  cadeias. Logo, precisamos de critérios mais algébricos e computacionais para verificar se as cadeias estão convergindo. Com esse propósito, uma série de *diagnósticos de convergência* foram desenvolvidos [20]. Aqui, discutiremos apenas dois deles: o diagnóstico de Gelman-Rubin [30] e o de Geweke [31].

O diagnóstico de Gelman-Rubin [30] consiste em comparar as variâncias “entre” e “dentre” as cadeias em paralelo. É suposto que temos  $N \geq 2$  cadeias, iniciadas em pontos suficientemente espaçados.

Primeiro, calculamos a variância “dentre” ( $W$ ) e “entre” ( $B$ ) as cadeias:

$$W = \frac{1}{m} \sum_{j=1}^m s_j^2, \quad B = \frac{n}{m-1} \sum_{j=1}^m (\bar{\theta}_j - \bar{\bar{\theta}})^2,$$

onde  $\theta$  representa o parâmetro a ser estimado,  $\bar{\theta}_j$  e  $s_j^2$  são a média e a variância da cadeia  $j$ , e  $\bar{\bar{\theta}} = \frac{1}{N} \sum_j \bar{\theta}_j$ . Então, estimamos a variância do estimador  $\hat{\theta}$  pela média ponderada

$$\text{Var}(\hat{\theta}) = \left(1 - \frac{1}{n}\right)W + \frac{1}{n}B,$$

e obtemos o fator de encolhimento

$$\hat{R} = \sqrt{\frac{\text{Var}(\hat{\theta})}{W}}.$$

A variância  $W$  é subestimada pela variância verdadeira de  $\hat{\theta}$ , logo,  $\hat{R} \geq 1$  e valores  $\hat{R} < 1.1$  indicam convergência. A Figura 7.5 apresenta o fator de encolhimento para os três parâmetros considerados anteriormente. Consideramos 3 cadeias em paralelo para cada parâmetro. O fator de encolhimento é próximo de um para os três parâmetros e permanece menor que 1.025 após 4000 iterações.

O diagnóstico de convergência de Geweke [31] pode ser aplicado a uma longa cadeia. Ele é um teste de igualdade de médias entre as primeiras e as últimas amostras da cadeia, descartado o *burn-in*. Tipicamente, comparamos a média amostral dos primeiros 10% da cadeia (após o *burn-in*) com a média amostral dos últimos 50%. Ao normalizar pelo desvio padrão da cadeia, obtemos um teste do tipo Z-score, e então, valores

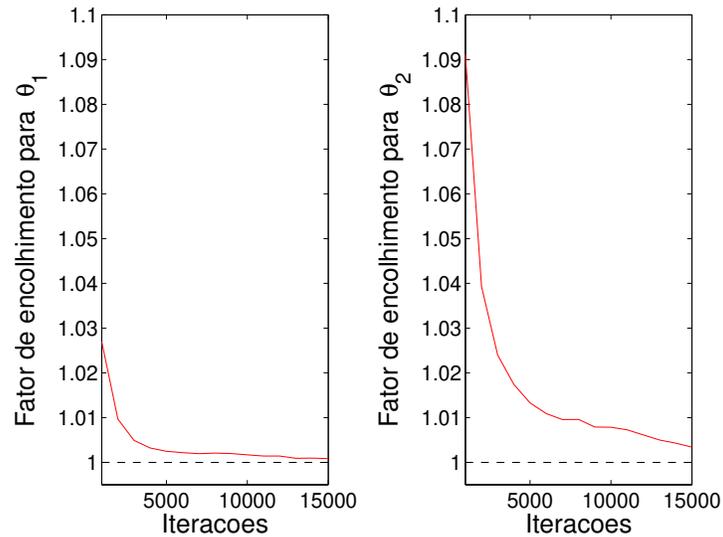


Figura 7.5: Fatores de encolhimento no diagnóstico de Gelman-Rubin.

próximos das caudas de uma distribuição Normal padrão indicam que a cadeia ainda não convergiu.

A Figura 7.6 apresenta os Z-scores para os três parâmetros. Como os valores permanecem afastados das caudas e próximos a zero, a convergência não pode ser rejeitada.

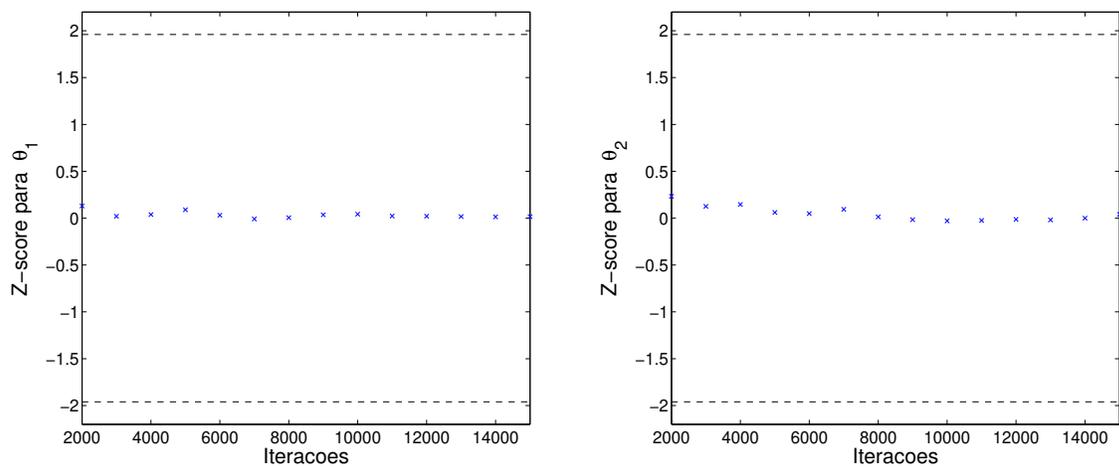


Figura 7.6: Diagnóstico de convergência de Geweke.

## 7.4 Um breve exemplo

Neste exemplo, cujos dados foram extraídos de [12], comparamos as estimativas fornecidas pela inversão linear, Máxima Verossimilhança e inferência Bayesiana. Considere a tomografia de um q-bit com observáveis  $\sigma_x$ ,  $\sigma_y$  e  $\sigma_z$ . Por simplicidade, consideramos  $\langle \sigma_y \rangle = 0$ . Suponha que realizamos 16 medidas de  $\sigma_x$  e  $\sigma_z$ , contendo 14  $|0\rangle$  e 2  $|1\rangle$ , 14  $|+\rangle$  e 2  $|-\rangle$ .

A partir desses dados, pode-se mostrar analiticamente que a inversão linear fornece como estimativa:

$$\rho_{LI} = \frac{1}{2} \left( \mathbb{I} + \frac{3}{4}\sigma_x + \frac{3}{4}\sigma_z \right) = \begin{bmatrix} 0.8750 & 0.3750 \\ 0.3750 & 0.1250 \end{bmatrix}.$$

Essa matriz tem uma autovalor negativo e as estimativas  $\langle \sigma_x \rangle = \text{tr}(\sigma_x \rho_{LI})$  e  $\langle \sigma_z \rangle = \text{tr}(\sigma_z \rho_{LI})$  caem fora dos valores físicos possíveis como mostrado na Figura 7.7 por uma estrela vermelha.

Usando a verossimilhança (3.21), obtemos de forma analítica a EMV:

$$\rho_{ML} = \frac{1}{2} \left( \mathbb{I} + \frac{1}{\sqrt{2}}\sigma_x + \frac{1}{\sqrt{2}}\sigma_z \right) = \begin{bmatrix} 0.8536 & 0.3536 \\ 0.3536 & 0.1464 \end{bmatrix}.$$

Essa matriz tem um autovalor nulo e o ponto que representa as estimativas  $\langle \sigma_x \rangle$  e  $\langle \sigma_z \rangle$  fica na fronteira da região admissível, representada na Figura 7.7 por um círculo. Tal estimativa não é compatível com barras de erros bem fundadas e atribui probabilidade zero a certos eventos, o que não pode ser justificado por essa pequena quantidade de dados.

Por outro lado, usando a abordagem Bayesiana descrita na Seção 7.2, tendo como verossimilhança (3.21) e com priori uniforme (segundo medida de Hilbert-Schmidt [101]), a estimativa Bayesiana média é

$$\rho_B^1 = \begin{bmatrix} 0.8284 & 0.3307 \\ 0.3307 & 0.1716 \end{bmatrix}.$$

A média Bayesiana para as estimativas  $\langle \sigma_x \rangle$  e  $\langle \sigma_z \rangle$  é representada por um ponto vermelho na Figura 7.7. Na Figura 7.7, os pontos amarelos correspondem aos valores de  $\langle \sigma_x \rangle$  e  $\langle \sigma_z \rangle$  calculados em cada amostra da matriz de densidade gerada pela cadeia de Markov (após o *burn-in*). Também mostramos na Figura 7.7 o erro padrão da média.

Como consideramos uma priori vaga ou uniforme e a quantidade de dados é pequena, a estimativa média Bayesiana se encontra entre o centro e a EMV (na borda). Assim, a estimativa Bayesiana média está longe o suficiente da borda para ser compatível com barras de erro, representadas aqui pelas elipses de erro padrão.

Suponha que aumentamos a quantidade de dados, por exemplo, multiplicando os dados acima por 10. A inversão linear e a EMV permanecem as mesmas pois as frequências relativas são as mesmas. Mas agora, o peso da verossimilhança é maior e pode mudar nosso conhecimento a priori uniforme rumo a EMV, como podemos ver no segundo quadro da Figura 7.7. A BME correspondente é

$$\rho_B^{10} = \begin{bmatrix} 0.8491 & 0.3496 \\ 0.3496 & 0.1509 \end{bmatrix}.$$

Esta estimativa ainda está afastada o suficiente da borda e é compatível com barras de erro. Multiplicando os dados iniciais por 100, obtemos como BME:

$$\rho_B^{100} = \begin{bmatrix} 0.8530 & 0.3529 \\ 0.3529 & 0.1470 \end{bmatrix},$$

e essa situação é ilustrada no terceiro quadro da Figura 7.7. Em resumo, começando com uma priori não-informativa, nossa estimativa vai em direção a EMV (na fronteira), à medida que o tamanho da amostra aumenta. Isso é esperado do ponto de vista Bayesiano, pois probabilidades nulas só podem ser atribuídas assintoticamente, e então, temos barras de erro bem fundadas ao utilizar inferência Bayesiana, já que os erros padrão também decrescem de forma apropriada.

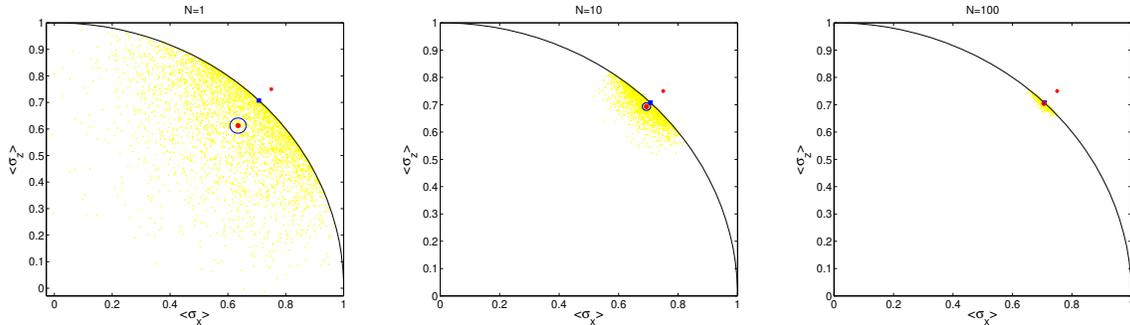


Figura 7.7: Solução da inversão linear apresentada como uma estrela vermelha fora dos possíveis valores esperados para os observáveis  $\sigma_x$  e  $\sigma_z$ . EMV em azul, na borda. Pontos amostrados em amarelo e a estimativa Bayesiana média, representada por um ponto vermelho, para tamanhos de amostra cada vez maiores. Os erros padrão para  $\langle \sigma_x \rangle$  e  $\langle \sigma_z \rangle$  são representados por elipses em azul.

## 7.5 Resumo do Capítulo 7

Neste capítulo, descrevemos a aplicação de inferência Bayesiana ao problema de Tomografia de Estados Quânticos através de simulações Monte Carlo via cadeias de

Markov. Na Seção, 7.2 propusemos uma possível parametrização para matrizes de densidade que permite a implementação de um algoritmo Metropolis-Hastings e questões de convergência desse algoritmo foram tratadas na Seção 7.3.

Diferente da estimação por verossimilhança, onde busca-se a estimativa mais provável para o estado, na abordagem Bayesiana, estados um pouco menos prováveis também são considerados através da distribuição a posteriori. Como consequência, ao utilizar prioris não-informativas, temos a garantia de que a estimativa Bayesiana média será sempre uma matriz de posto completo (sem autovalores nulos) e compatível com barras de erro consistentes. Essas propriedades foram ilustradas com o exemplo da Seção 7.4.

No entanto, é importante comentar sobre o custo computacional mais elevado da abordagem Bayesiana em relação aos problemas de otimização que aparecem na EMV. Esse custo mais alto é o preço pago por se obter uma amostra de tamanho relevante da posteriori  $\pi(\rho)$ , com a qual podemos caracterizar os estados mais plausíveis.

Temos ciência de que os estudos apresentados neste capítulo ainda são preliminares, os testes apresentados pequenos, e de maneira alguma, defendemos que as ideias aqui apresentadas para inferência Bayesiana, via MCMC, no problema TEQ, sejam ótimas. O intuito foi apenas mostrar que, de fato, é viável (e implementável) aplicar métodos Bayesianos no problema de TEQ e obter estimativas mais razoáveis.

É importante mencionar também que, em certas situações experimentais, é sabido que o estado do sistema pertence a uma determinada família a qual define uma própria parametrização para a matriz de densidade. Neste caso, é intuitivo que tal parametrização deva ser usada no lugar de (7.7) e que as distribuições propostas e prioris para os novos parâmetros devem mudar também.

Outro ponto importante e que merece estudos futuros é como definir distribuições (diferentes da uniforme) no espaço de matrizes densidade  $\mathcal{S}$ , nas quais possamos controlar a centralidade e a dispersão.

# Capítulo 8

## Conclusões e Trabalhos Futuros

Neste capítulo, resumimos as principais contribuições ao longo dessa tese, comentamos sobre possibilidades para trabalhos futuros e encerramos com algumas considerações finais sobre o problema de Tomografia de Estados Quânticos.

### 8.1 Contribuições da tese

Nossa primeira contribuição foi detalhada no Capítulo 4, onde analisamos a reparametrização da matriz de densidade, proposta em [48]. Na Seção 4.1, provamos que os mínimos locais do problema de minimização irrestrita que surgem após tal reparametrização, são todos globais. Este resultado, apesar de teórico, tem implicações práticas e valida o procedimento proposto em [48] para encontrar a estimativa de Máxima Verossimilhança. Esse trabalho foi publicado na revista *Quantum Information and Computation* [36].

Ainda no Capítulo 4, na Seção 4.2, discutimos sobre a convergência global do algoritmo  $R\rho R$  [47] para tomografia por Máxima Verossimilhança. Em [79], foi demonstrada a convergência global do algoritmo, mas com a hipótese de busca linear exata. Nossa contribuição foi demonstrar a convergência do método usando busca linear inexata e uma condição tipo Armijo, o que é mais viável na prática. Este trabalho está sendo preparado para a submissão.

No Capítulo 5, propusemos uma variação do método VQT para tomografia quântica com dados incompletos, denominado  $VQT_\infty$ . Esse método tenta ajustar as probabilidades não medidas o mais uniforme possível. Como consequência, mostramos que  $VQT_\infty$  tem um comportamento similar com o já conhecido método de Máxima Entropia, o que foi corroborado por simulações numéricas e demonstrado teoricamente para o caso de medições da autobase. Com isso, obtemos uma método que fornece uma estimativa tão pouco tendenciosa quanto a estimativa de Máxima Entropia, com a vantagem de uma formulação SDP linear. Este trabalho foi submetido para a *Physical Review A*.

Visando uma aplicação em outros problemas de otimização sobre o espaço de matrizes de densidade, além da Tomografia de Estados Quânticos, no Capítulo 6 apresentamos um método de gradiente projetado. Em testes preliminares, aplicados ao problema de EMV em TEQ, para o caso particular de uma verossimilhança multinomial, o método mostrou-se mais eficiente que a versão globalizada do algoritmo  $R\rho R$ , específico para tal problema.

Por fim, no Capítulo 7, descrevemos a aplicação de inferência Bayesiana ao problema de Tomografia de Estados Quânticos, através de simulações Monte Carlo via cadeias de Markov. A motivação para o estudo dessa abordagem é que a EMV, às vezes, pode retornar como estimativa mais provável, uma matriz de densidade contendo autovalores nulos. Isso atribui probabilidade nula a certos eventos, o que não pode ser justificado com uma quantidade finita de dados. Já na abordagem Bayesiana, estimativas um pouco menos prováveis também são consideradas através da distribuição a posteriori. Assim, temos a garantia de que a estimativa Bayesiana média será sempre uma matriz de posto completo (sem autovalores nulos) e compatível com barras de erro consistentes.

## 8.2 Trabalhos futuros

Uma questão importante na EMV é como propagar os erros em quantidades calculadas a partir da estimativa da matriz de densidade. Na Seção 4.3, discutimos brevemente sobre estimação de erros através da matriz de Fisher. Na prática, não utilizamos realmente a matriz de Fisher, mas sim a Hessiana da função log-verossimilhança avaliada em seu maximizador. Esta é uma boa aproximação para a matriz de Fisher apenas assintoticamente, para uma amostra suficientemente grande. Neste sentido, vale a pena investigar em quais situações tal procedimento é válido e em que outras vale mais a pena empregar simulações Monte Carlo.

Na Seção 5.6, comentamos brevemente o problema de falso emaranhamento que pode surgir ao se utilizar a estimação por Máxima Entropia. Sem sombra de dúvidas, sendo o emaranhamento um recurso básico em computação e comunicação quântica, é importante obter estimativas que não nos digam que o estado é mais emaranhado do que ele realmente é. Uma ideia natural é procurar pela estimativa para a matriz de densidade, compatível com os resultados de medições disponíveis e que minimize alguma medida de emaranhamento.

Quanto ao método de Gradiente Projetado, apresentado no Capítulo 6, devemos realizar mais testes numéricos em outros problemas de otimização sobre o espaço de matrizes densidade, e estendê-lo para restrições lineares gerais.

Os resultados do Capítulo 7 sobre inferência Bayesiana, via MCMC, no problema TEQ,

ainda são incipientes, e serviram apenas para mostrar que, de fato, é viável (e implementável) aplicar métodos Bayesianos no problema de TEQ e obter estimativas mais razoáveis. Uma pesquisa mais direcionada em distribuições sobre o espaço de matrizes de densidade é certamente um tópico interessante e com aplicação não só em inferência Bayesiana, mas também em simulações e no estudo de propriedades de estados quânticos. Outro ponto importante é especializar a metodologia do Capítulo 7 para problemas de estimação de estados, onde se conhece uma parametrização particular do estado em questão.

## 8.3 Considerações Finais

A motivação inicial dessa tese foi o estudo das soluções locais do problema de otimização na estimação por Máxima Verossimilhança, mediante a reparametrização discutida na Seção 4.1. A necessidade de se entender essa abordagem estatística e a teoria física associada ao problema de Tomografia de Estados Quânticos nos levou a estudar outras formulações: Máxima Verossimilhança, inferência Bayesiana, Máxima Entropia, Tomografia Quântica Variacional, e métodos numéricos para resolução das mesmas.

Em relação a cada formulação, pudemos, ainda que de forma modesta, dar nossa contribuição, seja do ponto de vista teórico ou computacional. Após estudar todas essas formulações, fica a pergunta: qual delas é a melhor? Qual a solução definitiva, o melhor modelo/método matemático, para o problema de Tomografia de Estados Quânticos?

De fato, não temos uma resposta definitiva. Não tivemos por objetivo comparar as diversas abordagens. Além disso, é difícil definir critérios e estabelecer condições homogêneas a todas as formulações/métodos. Cada uma tem sua inspiração, e sua aplicação, diferente das demais, apesar de todas serem empregadas em Tomografia de Estados Quânticos. Portanto, cada uma tem sua aplicabilidade, sua vantagem, dependendo do cenário em questão.

Por exemplo, se tivéssemos um experimento ideal, se nosso aparato experimental fosse perfeito, então bastaria aplicar a inversão linear dos dados para obter a matriz associada ao estado verdadeiro.

Flutuações, imperfeições e ruídos experimentais pedem algum modelo estatístico para tratar os dados. Neste caso, parece sensato aplicar a estimação por Máxima Verossimilhança. Mas, ainda resta a escolha da verossimilhança que melhor descreve os dados do experimento e do método para resolver o problema de otimização. Métodos gerais funcionam, mas métodos específicos podem ser mais eficientes.

Uma objeção à EMV é que a estimativa pode estar na borda de  $\mathcal{S}$  e, então, pos-

suir autovalores nulos, atribuindo probabilidades nulas a certos resultados de medidas. A estimativa Bayesiana média aparece como uma alternativa. Ao se utilizar uma priori não-informativa, temos a garantia de que a estimativa será de posto completo. É claro que, quando disponível, a priori deve incorporar o conhecimento do experimentalista sobre o sistema. No entanto, dentre as abordagens apresentadas, a Bayesiana é a que apresenta o maior custo computacional (o extremo oposto da inversão linear).

Por falar em informação a priori, em alguns casos, a questão de autovalores nulos podem não representar um problema. Pelo contrário, se o experimentalista tem boas razões para acreditar que o estado preparado é próximo de puro, é desejável uma estimativa com o maior número possível de autovalores nulos.

Não discutimos nessa tese a abordagem de *compressed sensing* [38] para tomografia de estados, onde a hipótese é de que o estado verdadeiro tem muitos autovalores nulos, ou seja, é de posto pequeno. Isso permite estabelecer garantias probabilísticas de reconstrução do estado com um número de medidas bem inferior a  $d^2$ .

A questão de tomografia com um conjunto incompleto de medidas se torna cada vez mais importante, uma vez que o número de medidas necessárias para caracterizar unicamente a matriz de densidade cresce exponencialmente com o tamanho do sistema. Para 10 q-bits, em geral, precisamos de  $2^{10} = 1024$  medidas! Nesse cenário, a formulação de Máxima Entropia e a Tomografia Quântica Variacional vem auxiliar na estimação com dados incompletos, a segunda com a vantagem de problemas SDP lineares contra problemas de otimização não linear da primeira.

Portanto, cada abordagem apresenta certas propriedades que a tornam mais adequada a um ou outro determinado tipo de situação.

Por fim, há um crescente interesse em escalabilidade na tomografia de estados quânticos, já que realizar  $d^2$  medidas torna-se impraticável em sistemas de tamanho moderado. Logo, é importante a determinação de um subconjunto de medidas mais representativas, mais informativas, para um dado experimento e métodos numéricos eficientes para o pós-processamento, a fim de tornar possível a tomografia de sistemas quânticos de dimensão cada vez maior, necessários ao desenvolvimento da computação quântica.

# Referências Bibliográficas

- [1] F. Alizadeh. Interior point methods in semidefinite programming with applications to combinatorial optimization. *SIAM Journal on Optimization*, 5(1):13–51, 1995.
- [2] J. Altepeter, E. Jeffrey, and P. Kwiat. Photonic state tomography. volume 52 of *Advances In Atomic, Molecular, and Optical Physics*, pages 105–159. Academic Press, 2005.
- [3] L. Artiles, R. Gill, and M. Guta. An invitation to quantum tomography. *Journal of the Royal Statistical Society B*, 67:109–134, 2005.
- [4] K. Audenaert and S. Scheel. Quantum tomographic reconstruction with error bars: a Kalman filter approach. *New Journal of Physics*, 11(2):023028, 2009.
- [5] O. E. Barndorff-Nielsen, R. Gill, and P. E. Jupp. On quantum statistical inference. *Journal of the Royal Statistical Society B*, 65:775–816, 2003.
- [6] J. Barzilai and J. Borwein. Two-point step size gradient methods. *IMA Journal of Numerical Analysis*, 8(1):141–148, 1988.
- [7] C. H. Bennett, D. P. D. Vincenzo, J. Smolin, and W. K. Wothers. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3814, 1996.
- [8] D. Bertsekas. *Nonlinear programming*. Athena Scientific, 2nd edition, 1999.
- [9] D. Bertsekas, A. Nedic, and A. E. Ozdaglar. *Convex Analysis and Optimization*. Athena Scientific, 2003.
- [10] E. G. Birgin, J. M. Martínez, and M. Raydan. Nonmonotone spectral projected gradient methods on convex sets. *SIAM Journal on Optimization*, 10:1196–1211, 2000.
- [11] E. G. Birgin, J. M. Martínez, and M. Raydan. Inexact spectral projected gradient methods on convex sets. *IMA Journal of Numerical Analysis*, 23:539–559, 2003.
- [12] R. Blume-Kohout. Optimal, reliable estimation of quantum states. *New Journal of Physics*, 12:043034, 2010.

- [13] B. Borchers. A C library for semidefinite programming. *Optimization Methods and Software*, 11(1):613–623, 1999.
- [14] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.
- [15] V. Buzek, G. Drobny, R. Derka, G. Adam, and H. Wiedemann. Quantum state reconstruction from incomplete data. *Chaos, Solitons & Fractals*, 10(6):981–1074, 1999.
- [16] G. Casella and R. L. Berger. *Statistical Inference*. Duxbury Press, 2001.
- [17] A. T. Cesário. An essay on the foundations of classical and quantum information theory. Master’s thesis, Universidade Federal de Minas Gerais, 2011.
- [18] T. F. Coleman and Y. Li. An interior trust region approach for nonlinear minimization subject to bounds. *SIAM Journal on Optimization*, 6(2):418–445, 1996.
- [19] A. Conn, K. Scheinberg, and L. Vicente. *Introduction to Derivative-Free Optimization*. Society for Industrial and Applied Mathematics, 2009.
- [20] M. K. Cowles and B. P. Carlin. Markov chain Monte Carlo convergence diagnostics: A comparative review. *Journal of the American Statistical Association*, 91(434):883–904, 1996.
- [21] H. Cramér. *Mathematical Methods of Statistics*. Princeton University Press, 1946.
- [22] E. de Klerk. *Aspects of Semidefinite Programming: Interior Point Algorithms and Selected Applications*. Kluwer Academic Publishers, 2002.
- [23] J. DiGuglielmo, C. Messenger, J. Fiurášek, B. Hage, A. Sambrowski, T. Schmidt, and R. Schnabel. Markov chain Monte Carlo estimation of quantum states. *Physical Review A*, 79:032114, 2009.
- [24] J. Duchi, S. Shalev-Shwartz, Y. Singer, and T. Chandra. Efficient projections onto the  $l_1$ -ball for learning in high dimensions. In *Proceedings of the 25th international conference on Machine learning*, ICML ’08, pages 272–279. ACM, 2008.
- [25] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.
- [26] T. Evangelista, C. Lavor, and W. R. M. Rabelo. A new method to calculate the inconclusive coefficients in the quantum state discrimination. *International Journal of Modern Physics C*, 22(2):95–105, 2011.
- [27] U. Fano. Description of states in quantum mechanics by density matrix and operator techniques. *Reviews of Modern Physics*, 29(1):74–93, 1957.

- 
- [28] R. A. Fisher. Theory of statistical estimation. *Mathematical Proceedings of the Cambridge Philosophical Society*, 22(05):700–725, 1925.
- [29] D. Gamerman and H. F. Lopes. *Markov Chain Monte Carlo: Stochastic Simulation for Bayesian Inference*. London: Taylor and Francis, 2nd edition, 2006.
- [30] A. Gelman and D. B. Rubin. Inference from iterative simulation using multiple sequences. *Statistical Science*, 7:457–511, 1992.
- [31] J. Geweke. Evaluating the accuracy of sampling-based approaches to the calculation of posterior moments. In J. M. Bernardo, J. Berger, A. P. Dawid, and A. F. M. Smith, editors, *Bayesian Statistics 4*, pages 169–193. Oxford University Press, 1992.
- [32] W. Gilks, S. Richardson, and D. Spiegelhalter. *Markov chain Monte Carlo in practice*. Chapman and Hall, 1996.
- [33] P. E. Gill and W. Murray. Algorithms for the solution of the nonlinear least-squares problem. *SIAM Journal on Numerical Analysis*, 15(5):977–992, 1978.
- [34] J. Ginibre. Statistical ensembles of complex, quaternion, and real matrices. *Journal of Mathematical Physics*, 6(3):440–449, 1965.
- [35] G. Golub and C. Van Loan. *Matrix computations*. Johns Hopkins University Press, 3 edition, 1996.
- [36] D. S. Gonçalves, M. A. Gomes-Ruggiero, C. Lavor, O. J. Fariás, and P. H. S. Ribeiro. Local solutions of maximum likelihood estimation in quantum state tomography. *Quantum Information and Computation*, 12(9):775–790, 2012.
- [37] L. Grippo, F. Lampariello, and S. Lucidi. A nonmonotone line search technique for Newton’s method. *SIAM Journal on Numerical Analysis*, 23(4):707–716, 1986.
- [38] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert. Quantum state tomography via compressed sensing. *Physical Review Letters*, 105:150401, 2010.
- [39] W. K. Hastings. Monte Carlo sampling methods using Markov Chains and their applications. *Biometrika*, 57(1):97–109, 1970.
- [40] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik A Hadrons and Nuclei*, 43:172–198, 1927.
- [41] C. Helmberg, F. Rendl, R. Vanderbei, and H. Wolkowicz. An interior-point method for semidefinite programming. *SIAM Journal on Optimization*, 6:342–361, 1996.

- [42] C. W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, 1976.
- [43] A. S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory*. North-Holland, 1982.
- [44] R. Horodecki, M. Horodecki, and P. Horodecki. Entanglement processing and statistical inference: The Jaynes principle can produce fake entanglement. *Physical Review A*, 59(3):1799–1803, 1999.
- [45] R. Horst, P. M. Pardalos, and N. V. Thoai. *Introduction to Global Optimization*. Nonconvex Optimization and Its Applications. Kluwer Academic Publishers, 2nd edition, 2000.
- [46] Z. Hradil. Quantum-state estimation. *Physical Review A*, 55(3):R1561–R1564, 1997.
- [47] Z. Hradil, J. Řeháček, J. Fiurášek, and M. Ježek. Maximum-likelihood methods in quantum mechanics. In *Quantum State Estimation*, volume 649 of *Lecture Notes in Physics*, pages 163–172. Springer, 2004.
- [48] D. F. James, P. G. Kwiat, W. J. Munro, and A. G. White. Measurement of qubits. *Physical Review A*, 64(5):052312, 2001.
- [49] E. Jaynes. Information theory and statistical mechanics. *Physical Review Online Archive (Prola)*, 106(4):620–630, 1957.
- [50] P. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard. Ultrabright source of polarization-entangled photons. *Physical Review A*, 60(2):R773–R776, 1999.
- [51] E. L. Lehman and G. Casella. *Theory of Point Estimation*. Springer, 1998.
- [52] K. Levenberg. A method for the solution of certain non-linear problems in least squares. *The Quarterly of Applied Mathematics*, 2:164–168, 1944.
- [53] J. Löfberg. Yalmip : A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, 2004.
- [54] D. Luenberger. *Linear and Nonlinear Programming*. Springer, 2nd edition, 2003.
- [55] T. O. Maciel, A. T. Cesário, and R. O. Vianna. Variational quantum tomography with incomplete information by means of semidefinite programs. *International Journal of Modern Physics C*, 22(12):1361–1372, 2011.
- [56] T. O. Maciel and R. O. Vianna. Optimal estimation of quantum processes using incomplete information: variational quantum process tomography. *Quantum Information and Computation*, 12(5):0442–0447, 2012.

- 
- [57] J. D. Malley and J. Hornstein. Quantum statistical inference. *Statistical Science*, 8(4):433–457, 1993.
- [58] D. Marquardt. An algorithm for least-squares estimation of nonlinear parameters. *SIAM Journal on Applied Mathematics*, 11(2):431–441, 1963.
- [59] J. M. Martínez and S. A. Santos. *Métodos Computacionais de Otimização*. IMPA, 20º Colóquio Brasileiro de Matemática. SBM, 1995.
- [60] M. L. Mehta. *Random Matrices*. Academic Press, 3rd edition, 2004.
- [61] N. Metropolis, A. W. Rosenbluth, M. N. Rosenbluth, A. H. Teller, and E. Teller. Equation of state calculations by fast computing machines. *Journal of Chemical Physics*, 21:1087–1092, 1953.
- [62] C. Meyer. *Matrix Analysis and Applied Linear Algebra*. Society for Industrial and Applied Mathematics, 2001.
- [63] F. Mezzadri. How to generate random matrices from the classical compact groups. *Notices of the American Mathematical Society*, 54:592, 2007.
- [64] C. Michelot. A finite algorithm for finding the projection of a point onto the canonical simplex of  $\mathbb{R}^n$ . *Journal of Optimization Theory and Applications*, 50(1):195–200, 1986.
- [65] M. Mittelbach, B. Matthiesen, and E. A. Jorswieck. Sampling uniformly from the set of positive definite matrices with trace constraint. *IEEE Transactions on Signal Processing*, 60(5):2167–2179, 2012.
- [66] J. Nelder and R. Mead. A simplex method for function minimization. *The Computer Journal*, 7(4):308–313, 1965.
- [67] A. Nemirovski and M. Todd. Interior-point methods for optimization. *Acta Numerica*, 17:191–234, 2008.
- [68] Y. Nesterov and M. J. Todd. Primal-dual interior-point methods for self-scaled cones. *SIAM Journal on Optimization*, 8(2):324–364, 1998.
- [69] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2004.
- [70] J. Nocedal and S. J. Wright. *Numerical Optimization*. Springer, 1999.
- [71] S. Olivares and M. G. A. Paris. Quantum estimation via the minimum Kullback entropy principle. *Physical Review A*, 76(4):042120, 2007.

- [72] A. Pais. *Inward Bound: Of Matter and Forces in the Physical World*. Oxford University Press, 1986.
- [73] M. Paris and J. Reháček, editors. *Quantum State Estimation*, volume 649 of *Lecture Notes in Physics*. Springer, 2004.
- [74] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 1993.
- [75] M. Powell. An efficient method for finding the minimum of a function of several variables without calculating derivatives. *The Computer Journal*, 7(2):155–162, 1964.
- [76] C. R. Rao. Information and the accuracy attainable in the estimation of statistical parameters. *Bulletin of the Calcutta Mathematical Society*, 37:81–89, 1945.
- [77] J. Řeháček. Minimal qubit tomography. *Physical Review A*, 70(5):052321, 2004.
- [78] J. Rehacek and Z. Hradil. Maximum entropy assisted maximum likelihood inversion. In *Lasers and Electro-Optics Europe, 2005. CLEO/Europe. 2005 Conference on*, page 466, 2005.
- [79] J. Řeháček, Z. Hradil, E. Knill, and A. Lvovsky. Diluted maximum-likelihood algorithm for quantum tomography. *Physical Review A*, 75(4):042108, 2007.
- [80] J. Řeháček, D. Mogilevtsev, and Z. Hradil. Tomography for quantum diagnostics. *New Journal of Physics*, 10(4):043022, 2008.
- [81] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6):2171–2180, 2004.
- [82] E. Schrödinger and M. Born. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(04):555–563, 1935.
- [83] D. Smithey. Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum. *Physical Review Letters*, 70(9):1244–1247, 1993.
- [84] G. W. Stewart. On the perturbation of  $LU$  and Cholesky factors. *IMA Journal on Numerical Analysis*, 17(1):1–6, 1997.
- [85] J. F. Sturm. Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones. [http://www.optimization-online.org/DB\\_HTML/2001/10/395.html](http://www.optimization-online.org/DB_HTML/2001/10/395.html), 1998.

- 
- [86] Y. S. Teo, B. Stoklasa, B.-G. Englert, J. Rehacek, and Z. Hradil. Incomplete quantum state estimation: A comprehensive study. *Physical Review A*, 85:042317, 2012.
- [87] M. Todd. Semidefinite optimization. *Acta Numerica*, 10:515–560, 2001.
- [88] M. Todd, K. Toh, and R. Tütüncü. On the Nesterov-Todd direction in semidefinite programming. *SIAM Journal on Optimization*, 8:769–796, 1996.
- [89] K. Toh, M. Todd, and R. Tutunc. SDPT3 - a Matlab software package for semidefinite programming. *Optimization Methods and Software*, (11):545–581, 1999.
- [90] K.-C. Toh. An inexact primal–dual path following algorithm for convex quadratic sdp. *Mathematical Programming*, 112(1):221–254.
- [91] K. Usami. Accuracy of quantum-state estimation utilizing Akaike’s information criterion. *Physical Review A*, 68(2):022314, 2003.
- [92] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.
- [93] Y. Vardi and D. Lee. From image deblurring to optimal investments: Maximum likelihood solutions for positive linear inverse problems. *Journal of the Royal Statistical Society. Series B (Methodological)*, 55(3):569–612, 1993.
- [94] V. Vedral, M. B. Plenio, K. Jacobs, and P. L. Knight. Quantifying entanglement. *Physical Review Letters*, 78:2275, 1997.
- [95] G. Vidal and R. F. Werner. Computable measure of entanglement. *Physical Review A*, 65:032314, 2002.
- [96] K. Vogel and H. Risken. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. *Physical Review A*, 40(5):2847–2849, 1989.
- [97] A. White, D. F. James, P. H. Eberhard, and P. G. Kwiat. Nonmaximally entangled states: Production, characterization, and utilization. *Physical Review Letters*, 83(16):3103–3107, 1999.
- [98] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.
- [99] H. Yamashita, H. Yabe, and K. Harada. A primal–dual interior point method for nonlinear semidefinite programming. *Mathematical Programming*, 135:89–121, 2012.

- [100] Y.-X. Yuan. Recent advances in numerical methods for nonlinear equations and nonlinear least squares. *Numerical Algebra, Control and Optimization*, 1(1):15–34, 2011.
- [101] K. Zyczkowski, K. A. Penson, I. Nechita, and B. Collins. Generating random density matrices. *Journal of Mathematical Physics*, 52(6):062201, 2011.