Estratégias Para a Realização do Protocolo de Codificação Superdensa Via Canais Quânticos Puros e Parcialmente Emaranhados

Roger Alfredo Kögler

Julho de 2016

Universidade Federal de Minas Gerais

Instituto de Ciências Exatas – Departamento de Física

Estratégias Para a Realização do Protocolo de Codificação Superdensa Via Canais Quânticos Puros e Parcialmente Emaranhados

Roger Alfredo Kögler

Orientador: Leonardo Teixeira Neves

Dissertação apresentada ao departamento de Física da Universidade Federal de Minas Gerais, para a obtenção do título de Mestre em Física.

Agradecimentos

Aos meus pais Alfredo Kögler e Cristiane Loechelt Stuker, à mestre Mayara Santana Pinto, ao doutor Miguel Ángel Solís Prosser, ao doutor Henri Stuker, ao professor doutor Leonardo Teixeira Neves, aos profissionais do departamento de Física da Universidade Federal de Minas Gerais e à instituição de fomento FAPEMIG.

Resumo

O protocolo de codificação superdensa via canais quânticos puros e parcialmente emaranhados é estudado no contexto de discriminação ótima de estados não-ortogonais. Estratégias de discriminação com mínimo erro (EM), confiança máxima (CM) e estratégias que interpolam entre elas serão utilizadas para a realização do protocolo. Primeiramente, mostra-se que a estratégia EM realiza a codificação superdensa com probabilidade de falha nula e informação mútua máxima entre as partes comunicantes. Em seguida, admitindo-se uma probabilidade não nula de falha no processo, é mostrado que a estratégia CM é aquela que, com maior chance de sucesso, permite que o protocolo seja realizado com a informação mútua máxima alcançável pelo canal, a qual é maior que no caso determinístico e depende apenas do número de Schmidt do estado emaranhado. Além disso, considera-se a iteração da estratégia CM em caso de falha e mostra-se que existem canais para os quais é possível aumentar a probabilidade de sucesso de se realizar o protocolo com a informação mútua maior que no caso determinístico. Finalmente, analisa-se a aplicação de estratégias intermediárias entre EM e CM com as quais se mostra possível a realização da codificação superdensa com probabilidade de sucesso superior à permitida pela estratégia CM e informação mútua maior que a alcançada via EM. Expressões analíticas para a informação mútua são derivadas para todos os protocolos estudados.

Palavras chave: protocolos de informação quântica, codificação superdensa, discriminação de estados quânticos, estados simétricos.

Abstract

The superdense coding protocol via partially entangled pure quantum channels is studied in the context of optimal discrimination among nonorthogonal states. Discrimination strategies with minimum error (ME), maximum confidense (MC) and strategies that interpolate them will be used to perform the protocol. First, it is shown that the superdence coding with null failure probability and maximum mutual information between the communicating parts is related to the ME strategy. Then, admitting a nonzero failure probability in the process, it is shown that the MC strategy enables the protocol to be performed with the maximum achievable mutual information for the channel with greater chance of success, which is higher than the deterministic case and depends only on the Schmidt rank of the entangled state. Furthermore, it is considered the iteration of the MC strategy in the case of failure and it is shown that there are channels for which it is possible to increase the success probability of performing the protocol with higher mutual information than the deterministic case. Lastly, it is analyzed the application of intermediate strategies between ME and CM in which it is shown to be possible to execute superdense coding with higher probability of success than allowed by the CM strategy and greater mutual information than provided by EM strategy. Analytical expressions for the mutual information are derived for all the studied protocols.

Keywords: quantum information protocols, superdense coding, quantum state discrimination, symmetric states.

Sumário

Introdução

Codificação superdensa [1] é um protocolo de informação quântica que utiliza emaranhamento [2–7] como recurso para aumentar a capacidade de transmissão de informação clássica através de um canal quântico. Um remetente, Alice, e um destinatário, Bob, compartilham um sistema quântico bipartido. Alice codifica a mensagem que deseja enviar a Bob aplicando uma operação unitária apropriada sobre sua parte. Em seguida, ela envia-lhe seu sistema e ele decodifica a mensagem através de uma medição no sistema composto. Como exemplo, considere que os sistemas quânticos de ambos pertençam a espaços de Hilbert bidimensionais. Nesse caso, se não há emaranhamento, Alice pode transmitir uma de duas mensagens perfeitamente distinguíveis para Bob. Entretanto, se houver emaranhamento, e ele for máximo, ela poderá transmitir uma de quatro mensagens possíveis, aumentando, assim, a capacidade do canal.

Quando o emaranhamento compartilhado por Alice e Bob não é máximo, a codificação superdensa pode ser abordada de duas maneiras: i) Busca-se o número máximo de mensagens perfeitamente distinguíveis que podem ser transmitidas através do canal quântico [8–11]. Para dimensões maiores que 2, esse número será intermediário ao obtido pelo canal maximamente emaranhado e o de um canal sem emaranhamento [8].[1] ii) Tenta-se transmitir tanta informação quanto seria possível por um canal maximamente emaranhado. Nesse caso, as mensagens não serão perfeitamente distinguíveis, uma vez que são codificadas em estados quânticos não-ortogonais. Consequentemente, o protocolo apresentará erros ou resultados inconclusivos no processo de decodificação realizado através da medição de Bob. Então, o objetivo é minimizar essas imperfeições com a aplicação de estratégias de medição otimizadas que identifiquem, da melhor maneira possível, o estado do sistema que carrega a mensagem de Alice [12–14]. Nesta dissertação apenas a segunda abordagem será estudada.

[1] Para sistemas bidimensionais, como do exemplo acima, é impossível codificar três mensagens perfeitamente distinguíveis [8].

Existem diversas estratégias que permitem a discriminação ótima de estados quânticos não-ortogonais, as quais podem ser divididas em determinísticas [15–18] e probabilísticas [19–24]. Estratégias determinísticas sempre inferem um estado, dado um resultado de medição, com certa probabilidade de erro. Estratégias probabilísticas permitem a identificação dos estados com maior confiança que as estratégias determinísticas, ao custo de admitirem resultados inconclusivos com probabilidade não nula. Diferentes tipos de protocolos de codificação superdensa podem ser realizados de acordo com a estratégia de discriminação adotada.

No presente trabalho, será mostrado que a realização da codificação superdensa via canais quânticos puros e parcialmente emaranhados depende da capacidade de discriminação entre estados simétricos não-ortogonais e igualmente prováveis. Para essa classe de estados, a medição que otimiza o processo de discriminação é conhecida para as principais estratégias. Será mostrado, então, que protocolos realizados através da aplicação dessas estratégias são ótimos tanto de forma determinística quanto probabilística.

A dissertação está organizada da seguinte maneira: no capítulo 1 serão apresentados alguns fundamentos de informação e computação quântica necessários para a compreensão do trabalho. Além disso, juntamente com a codificação superdensa, serão apresentados os protocolos de teleportação quântica e troca de emaranhamento, também importantes em informação quântica. No capítulo 2 serão estudadas as medições quânticas generalizadas e as principais estratégias de discriminação de estados não-ortogonais. Essas estratégias, aplicadas a conjuntos de estados simétricos equiprováveis, serão revisadas no capítulo 3. O capítulo 4 traz a revisão de resultados da aplicação de discriminação de estados simétricos para a realização ótima dos protocolos de teleportação quântica e troca de emaranhamento via canais parcialmente emaranhados. Os resultados desta dissertação serão apresentados no capítulo 5, onde se utilizam as ferramentas descritas nos capítulos anteriores para o estudo do protocolo de codificação superdensa realizado com emaranhamento parcial. Por fim, as conclusões são apresentadas no capítulo 6.

1

Conceitos Básicos de Informação Quântica e Computação Quântica

A informação e a computação quântica se originaram da combinação de mecânica quântica, ciências da computação e teoria de informação. No início da década de 1980, um simulador quântico foi proposto por Feynman [25]. Ao simular efeitos quânticos, sua máquina apresentou um ganho exponencial em comparação a uma máquina de Turing clássica[1] executando a mesma tarefa. Pouco depois, a computação quântica foi formalmente definida por Deutsch através de sua descrição de um computador quântico universal [26]. Foi evidenciado, ainda, que a execução de algoritmos em computadores quânticos pode apresentar vantagens de processamento, como no caso do algoritmo de Deutsch-Jozsa [27]. Este exibe um ganho exponencial na tarefa de determinar se uma função é constante ou balanceada. Desde então, esta é uma área em constante avanço teórico e experimental, embora o desenvolvimento tecnológico do computador quântico ainda não tenha sido alcançado [3, 5].

Inspirado pela teoria clássica de informação, se observou que sistemas quânticos poderiam ser utilizados para armazenamento, processamento e transmissão de informação. Isso origina a área de informação quântica [3–7], onde propriedades da mecânica quântica, como superposição e emaranhamento, permitem não só que tarefas análogas às clássicas apresentem um ganho em eficiência, mas também que produza novos protocolos de comunicação impossíveis de serem realizados classicamente. Alguns exemplos destes protocolos serão apresentados aqui.

Neste capítulo serão introduzidos os conceitos básicos de informação quântica e computação quântica necessários para o entendimento do restante do trabalho. Primeiramente será feita a quantização da unidade fundamental de informação clássica, o bit.[2] O emaranhamento de estados quânticos será estudado para o caso de estados puros de sistemas

[1] Uma máquina de Turing descreve o processamento binário de informação, o equivalente a um computador clássico.

[2] Contração do termo em inglês *binary digit*.

bipartidos. Será feita, ainda, uma breve descrição de portas lógicas quânticas e a representação da computação quântica em forma de circuitos. Por fim, serão mostrados três protocolos de informação quântica: codificação superdensa [1], teleportação quântica [28] e troca de emaranhamento [29], onde o primeiro é o foco principal do presente trabalho.

1.1 Do Bit ao *Qubit*

Classicamente, bits de informação são codificados em sistemas físicos binários [3], ou seja, sistemas que possuem apenas duas possibilidades de estado (sim ou não, ligado ou desligado, verdadeiro ou falso, 0 ou 1, etc.). Como exemplo prático, no caso de computadores, a informação binária pode ser codificada na passagem ou não de corrente elétrica em componentes chamados transistores. Mensagens mais complexas, que exigem mais do que apenas duas possibilidades, são codificadas em sequências de bits. Por exemplo, se 4 mensagens diferentes são necessárias, precisa-se de no mínimo dois bits por mensagem. A tabela 1.1 mostra quatro mensagens binárias diferentes, onde foi adotada a notação em termos de 0 e 1.

Tabela 1.1: Exemplo de 4 mensagens em codificação binária.

Mensagem	**Código Binário**
0	00
1	01
2	10
3	11

O primeiro passo para o tratamento quântico do processamento de informação é tratar quanticamente a unidade de registro de informação, o bit. Para isso, tornar-se-á quântico o sistema físico binário, sendo o elemento de informação chamado agora de *qubit*[3] [3–5]. *Qubits* são sistemas quânticos em um espaço de Hilbert ($\mathcal{H}$) bidimensional cujos estados puros são descritos por vetores unitários que possuem a forma geral

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

onde $|0\rangle$ e $|1\rangle$ denotam uma base conhecida como base computacional. Os coeficientes complexos α e β são as amplitudes de probabilidade e respeitam a condição de normalização $|\alpha|^2 + |\beta|^2 = 1$, onde $|\alpha|^2$ e $|\beta|^2$ são as probabilidades de projetar o estado $|\psi\rangle$ em um dos

[3]Contração do termo em inglês *quantum bit*.

respectivos estados da base, $|0\rangle$ ou $|1\rangle$. Exemplos de sistemas físicos desse tipo são átomos de dois níveis, partículas de *spin*-$\frac{1}{2}$ e a polarização de um fóton.

Como os coeficiente α e β são variáveis contínuas, existem infinitas possibilidades para o estado $|\psi\rangle$. Mas, a medição do estado fornece apenas duas possibilidades perfeitamente distinguíveis, dadas por projetores ortogonais no espaço bidimensional.[4] Portanto, a informação extraída do estado $|\psi\rangle$ é equivalente a um bit. Com isso em mente, é possível se deixar pensar que não existem vantagens na utilização de *qubits* para o registro de informação. Porém, vantagens surgem quando o processamento da informação é levado em conta, algumas das quais serão vistas nos protocolos de informação quântica descritos na seção 1.6.

Assim como no caso clássico, conjuntos de *qubits* podem ser necessários para a codificação de mensagens. Estes são denotados pelo produto tensorial dos estados individuais dos *qubits*. Por exemplo, sejam dois estados quaisquer $|\psi\rangle_1$ e $|\psi\rangle_2$, o estado composto, escrito na base computacional, é dado por

$$\begin{aligned} |\psi\rangle &= |\psi\rangle_1 \otimes |\psi\rangle_2 \\ &= |\psi\rangle_1 |\psi\rangle_2 \\ &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle, \end{aligned} \tag{1.2}$$

onde a notação foi simplificada de modo que $|0\rangle_1 \otimes |0\rangle_2 = |0\rangle_1|0\rangle_2 = |00\rangle$. A esse tipo de estado se dá o nome de estado produto. Note que o número de mensagens que podem ser perfeitamente extraídas desse sistema é igual ao número de elementos que formam uma base completa no seu espaço total. Ou, simplesmente, é igual a dimensão do espaço de Hilbert do sistema composto, que neste caso é 4.

Sistemas de dimensões maiores também possuem um papel importante na computação quântica [1,28]. Um sistema físico com dimensões extras gera um espaço de Hilbert acessível maior. Por exemplo, sistemas quânticos tridimensionais podem ser utilizados como unidade de informação ternária, chamada de *qutrit*. Chama-se a unidade de informação d-dimensional de *qudit*, o qual pode ser representado por

$$|\psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle. \tag{1.3}$$

Os coeficientes complexos c_j respeitam a condição de normalização $\sum_j |c_j|^2 = 1$ e o conjunto $\{|j\rangle\}$ forma uma base ortonormal no espaço d-dimensional, isto é, $\sum_j |j\rangle\langle j| = \mathbb{1}$, onde $\mathbb{1}$ é o operador identidade nesse espaço. É possível, então, codificar d mensagens perfeitamente distinguíveis em um *qudit*.

Além de sua representação vetorial $|\psi\rangle$, um estado puro pode ser descrito por um projetor $|\psi\rangle\langle\psi|$. Isso possibilita a consideração de estados mais gerais. Por exemplo, quando não é

[4] Medições serão discutidas em detalhes no capítulo 2

possível especificar precisamente o estado de um sistema quântico, este será descrito por uma mistura estatística de estados puros [3–5]. Essa situação é representada por um operador densidade,

$$\hat{\rho} = \sum_j \eta_j |\psi_j\rangle\langle\psi_j|, \tag{1.4}$$

onde η_j é a probabilidade do vetor de estado do sistema ser $|\psi_j\rangle$, a qual é normalizada, $\sum_j \eta_j = 1$. Quando operadores desse tipo não podem ser reduzidos a projetores, o sistema é dito estar em um estado misto.

1.2 Estados Emaranhados Bipartidos

Estados puros emaranhados[5] são estados compostos que não podem ser escritos na forma de produto tensorial [2]. Ou seja, existem estados $|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_N$ tal que

$$|\psi\rangle \neq |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \ldots \otimes |\psi\rangle_N, \tag{1.5}$$

onde $|\psi\rangle_j \in \mathcal{H}_j$, $j = 1, \ldots, N$. Neste caso, o estado de cada sistema individual não pode ser descrito independentemente, o que implica que os sistemas estão emaranhados. A medição de uma das partes do estado emaranhado pode afetar o estado da parte que não foi observada [2]. Como exemplo tome o estado de dois *qubits* dado por

$$|\Psi\rangle = \frac{|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2}{\sqrt{2}}. \tag{1.6}$$

Uma identificação do sistema 1 no estado $|0\rangle_1$ implica que o sistema 2 se encontra no estado $|0\rangle_2$. Por outro lado, se o estado do sistema 1 for $|1\rangle_1$, o estado do sistema 2 será $|1\rangle_2$. Estados emaranhados são vastamente explorados em protocolos quânticos de computação e comunicação [1, 3, 28, 29] e de particular interesse são os estados bipartidos ($N = 2$), que serão exclusivamente considerados nas discussões a seguir.

Uma das vantagens dos estados puros bipartidos é que estes podem ser representados como uma soma de termos bi-ortogonais, conhecida por decomposição de Schmidt [3–7]. Sejam os sistemas 1 e 2 com dimensões d_1 e d_2, respectivamente. Existem bases ortonormais $\{|a_j\rangle_1\}$ em $\mathcal{H}_1$ e $\{|a_j\rangle_2\}$ em $\mathcal{H}_2$, tais que

$$|\Psi\rangle = \sum_{j=0}^{N_S-1} \lambda_j |a_j\rangle_1 |a_j\rangle_2, \tag{1.7}$$

onde os termos λ_j são conhecidos como coeficientes de Schmidt e são números reais não-negativos que respeitam a condição de normalização $\sum_j \lambda_j^2 = 1$. O número de termos da

[5] Estados mistos podem apresentar correlações clássicas. No presente trabalho o emaranhamento será considerado apenas para estados puros.

soma, que é igual ao número de coeficientes de Schmidt não nulos, é chamado de número de Schmidt e respeita a relação $N_S \leq \min(d_1, d_2)$. Qualquer estado cujo número de Schmidt seja maior do que 1 é emaranhado pois não pode ser escrito como um estado produto $|\psi\rangle_1 \otimes |\psi\rangle_2$.

O número de Schmidt em (1.7) fornece um critério para a presença de emaranhamento em um estado puro qualquer. Estados maximamente emaranhados são facilmente identificados quando representados pela decomposição de Schmidt. Para isso o número de Schmidt deve ser máximo, ou seja $N_S = \min(d_1, d_2)$, e todos os seus coeficientes de Schmidt iguais, $\lambda_j = 1/\sqrt{N_S}$. Para verificar essa afirmação é necessário um quantificador de emaranhamento [4, 30]. Tome, por exemplo, a entropia linear [31], definida como

$$\mathcal{E} = \frac{d_1}{d_1 - 1}[1 - \mathrm{Tr}(\hat{\rho}_1^2)] = \frac{d_2}{d_2 - 1}[1 - \mathrm{Tr}(\hat{\rho}_2^2)], \tag{1.8}$$

onde $\hat{\rho}_1 = \mathrm{Tr}_2(\hat{\rho})$ e $\hat{\rho}_2 = \mathrm{Tr}_1(\hat{\rho})$ são operadores densidade reduzidos associados ao estado bipartido $\hat{\rho} = |\Psi\rangle\langle\Psi|$. O limite inferior $\mathcal{E} = 0$ indica que o estado $|\Psi\rangle$ não é emaranhado, portanto é um estado produto. Já o limite superior, onde $\mathcal{E} = 1$, indica que o estado é maximamente emaranhado [31]. Suponha um estado escrito em na decomposição de Schmidt com $d_1 \leq d_2$ e $\lambda_j = 1/\sqrt{d_1}, \forall\, l$. O operador densidade correspondente a esse estado é

$$\hat{\rho} = |\Psi\rangle\langle\Psi| = \frac{1}{d_1} \sum_{j,k=0}^{d_1-1} \Big(|a_j\rangle\langle a_k|\Big)_1 \otimes \Big(|a_j\rangle\langle a_k|\Big)_2, \tag{1.9}$$

e o estado reduzido do subsistema 1

$$\begin{aligned} \hat{\rho}_1 &= \mathrm{Tr}_2(\hat{\rho}) \\ &= \frac{1}{d_1} \sum_{j,k=0}^{d_1-1} \Big(|a_j\rangle\langle a_k|\Big)_1 \delta_{jk} \\ &= \frac{1}{d_1} \sum_{j=0}^{d_1-1} \Big(|a_j\rangle\langle a_j|\Big)_1. \end{aligned} \tag{1.10}$$

Como $\hat{\rho}_1$ está escrito em sua decomposição espectral, $\hat{\rho}_1^2$ é simplesmente

$$\hat{\rho}_1^2 = \frac{1}{d_1^2} \mathbb{1}_{d_1}, \tag{1.11}$$

e, portanto, a entropia linear desse estado é dada por

$$\begin{aligned} \mathcal{E}(\hat{\rho}) &= \frac{d_1}{d_1 - 1}[1 - \mathrm{Tr}(\hat{\rho}_1^2)] \\ &= \frac{d_1}{d_1 - 1}\left[1 - \frac{1}{d_1}\right] \\ &= 1. \end{aligned} \tag{1.12}$$

Esse resultado indica que o estado da equação (1.9) é, de fato, maximamente emaranhado.

Por suas, a decomposição de Schmidt e a entropia linear se mostram ferramentas úteis ao se tratar de estados emaranhados puros bipartidos. É evidente que o emaranhamento depende explicitamente da distribuição dos coeficientes da decomposição de Schmidt e a entropia linear fornece um meio simples para a quantificação deste.

1.3 Fidelidade

A fidelidade de estados quânticos é uma forma de quantificar a semelhança entre eles. Considere os dois estados $\hat{\rho}$ e $\hat{\sigma}$. A fidelidade entre eles é definida como

$$F(\hat{\rho},\hat{\sigma}) = \left(\mathrm{Tr}\sqrt{\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}}\right)^2. \tag{1.13}$$

Se um dos estados for puro, tome $\hat{\sigma} = |\psi\rangle\langle\psi|$ como exemplo, a fidelidade pode ser escrita como

$$F(\hat{\rho},|\psi\rangle) = \langle\psi|\hat{\rho}|\psi\rangle. \tag{1.14}$$

Caso os dois estados sejam puros, com $\hat{\rho} = |\phi\rangle\langle\phi|$, a fidelidade se reduz a

$$F(|\phi\rangle,|\psi\rangle) = |\langle\phi|\psi\rangle|^2. \tag{1.15}$$

Assim, quando dois estados são idênticos a fidelidade possui valor 1, caso contrário $0 \leq F < 1$.

1.4 Entropia de Shannon e Entropia Condicional

A entropia de Shannon, definida primeiramente em [32], é uma grandeza que mede a incerteza associada à uma variável aleatória. De mesmo modo, a entropia é uma medida da quantidade de informação necessária, em média, para descrever uma variável aleatória. Seja X uma variável discreta e aleatória, a qual assume o valor x com probabilidade $p(x)$, a entropia de Shannon, $H(X)$, é definida como [32, 33]

$$H(X) = -\sum_x p(x)\log_2 p(x), \tag{1.16}$$

onde o logaritmo foi tomado com base 2 afim de expressar a entropia em bits. Por exemplo, a entropia do lançamento de uma moeda (M) (assumindo que ela não seja tendenciosa por meio algum) é

$$H(M) = -2\frac{1}{2}\log_2\frac{1}{2} = 1 \text{ bit}, \tag{1.17}$$

ou seja, existe 1 bit assoado ao estado da moeda.

Além da entropia de Shannon, a entropia condicional apresentará um papel importante nesta dissertação. Esta e mensura a quantidade média de informação necessária para descrever o resultado de uma variável aleatória Y dado que o valor da variável X é conhecido, e é definida por [32, 33]

$$H(Y|X) = \sum_{x,y} p(x)p(y|x)\log_2 p(y|x), \tag{1.18}$$

onde a probabilidade condicional $p(y|x)$ dita a probabilidade de ocorrência do resultado y, dado que é conhecido o valor x.

1.5 Portas Lógicas Quânticas

Para realizar o processamento da informação codificada em *qubits*/*qudits* é necessária a manipulação destes. Uma maneira simples de se realizar essas manipulações é através de transformações unitárias, ferramentas que serão exclusivamente consideradas aqui. Embora qualquer transformação possa ser considerada uma porta lógica, algumas delas são mais comumente utilizadas, tendo nomes específicos atribuídos a elas [3, 5]. A tabela 1.2 mostra as portas lógicas bidimensionais mais relevantes para o presente trabalho.

Tabela 1.2: Lista de portas lógicas bidimensionais e suas atuações em *qubits*, onde $j, k = 0, 1$ e $\oplus$ denota soma módulo 2.

Porta Lógica	**Forma Explícita**	**Atuação**
NÃO	$\hat{X} = \|1\rangle\langle 0\| + \|0\rangle\langle 1\|$	$\hat{X}\|j\rangle = \|j \oplus 1\rangle$
Deslocamento de Fase	$\hat{Z} = \|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\hat{Z}\|j\rangle = e^{i\pi j}\|j\rangle$
Hadamard	$\hat{H} = \frac{1}{\sqrt{2}}\left[(\|0\rangle + \|1\rangle)\langle 0\| + (\|0\rangle - \|1\rangle)\langle 1\|\right]$	$\hat{H}\|j\rangle = \frac{1}{\sqrt{2}}\sum_j e^{i\pi j}\|j\rangle$
NÃO-controlado	$\hat{C}^{\text{NOT}} = \|0\rangle\langle 0\| \otimes \mathbb{1} + \|1\rangle\langle 1\| \otimes \hat{X}$	$\hat{C}^{\text{NOT}}\|j\rangle\|k\rangle = \|j\rangle\|j \oplus k\rangle$

A operação $\hat{X}$ muda o estado da base computacional para o estado ortogonal a este, sendo identificado como a negação do *qubit*. A porta $\hat{Z}$ é responsável por mudar a fase da amplitude de probabilidade do estado $|1\rangle$. Esses operadores, $\hat{X}$ e $\hat{Z}$, são matrizes que representam dois dos operadores de Pauli. A terceira matriz de Pauli fornece uma atuação idêntica à da operação $\hat{X}\hat{Z}$ e, portanto, foi omitida da tabela. A porta Hadamard faz o papel de superpor os estados da base computacional de modo a manter a distribuição de probabilidade uniforme, com mesmo módulo para todos os estados superpostos. A fase que aparece com a atuação dessa porta é responsável por manter a ortogonalidade dos estados, garantindo a unitariedade da operação. Essa porta é utilizada para realizar processamento

paralelo, sendo sua aplicação mais famosa o algoritmo de Deutsch-Jozsa [27]. Operações controladas, como a $\hat{C}^{\text{NOT}}$, atuam em mais do que um estado simultaneamente. Nesse caso, a atuação no sistema bipartido deixa um deles intacto (controle) e realiza uma operação unitária no outro (alvo). A porta NÃO-controlado recebe esse nome pois a unitária aplicada ao alvo, caso o controle permita, é a porta NÃO. A nomenclatura $\hat{U}^{\text{XOR}}$ também é utilizada, onde o termo XOR indica a expressão em inglês *exclusive or*, que significa "ou exclusivo" em tradução livre.

Essas portas específicas são utilizadas nas descrições de circuitos de diversos protocolos de informação quântica [1, 28, 29]. Entretanto, da forma como foram apresentadas, elas se limitam ao caso bidimensional, sendo de interesse as suas extensões para maiores dimensões. Para isso será tomada como prioridade a similaridade de atuação das portas. Dado que $\{|j\rangle \mid j = 0, \ldots, d-1\}$ denota a base computacional d-dimensional, as generalizações das portas $\hat{X}$ e $\hat{Z}$ são, respectivamente

$$\hat{X} = \sum_{k=0}^{d-1} |k \oplus 1\rangle\langle k|, \tag{1.19}$$

$$\hat{Z} = \sum_{k=0}^{d-1} e^{\frac{2i\pi k}{d}} |k\rangle\langle k|, \tag{1.20}$$

onde o símbolo $\oplus$ agora significa soma módulo d. Esses operadores de fato generalizam o grupo de Pauli [34]. Evidentemente, se $d = 2$ os operadores recaem naqueles mostrados na tabela 1.2. Ainda, é interessante destacar que

$$\hat{X}^n|j\rangle = |j \oplus n\rangle, \tag{1.21}$$

$$\hat{Z}^n|j\rangle = e^{\frac{2i\pi jn}{d}}|j\rangle, \tag{1.22}$$

e

$$\hat{X}^d = \hat{Z}^d = \mathbb{1}. \tag{1.23}$$

A extensão da porta Hadamard é dada pela transformada discreta de Fourier [3–7], que é dada por

$$\hat{\mathcal{F}} = \frac{1}{\sqrt{d}} \sum_{k,l=0}^{d-1} \hat{Z}^l |k\rangle\langle l|. \tag{1.24}$$

A transformada inversa de Fourier satisfaz $\hat{\mathcal{F}}^{-1} = \hat{\mathcal{F}}^\dagger$, e, portanto, $\hat{\mathcal{F}}$ é uma operação unitária. Mas, para quaisquer dimensões maiores do que 2 essa transformação não é hermitiana e terá de ser explicitamente apresentada em circuitos quânticos (veja seção 1.6). Da unitariedade de $\hat{\mathcal{F}}$, a transformada inversa de Fourier é dada por

$$\hat{\mathcal{F}}^{-1} = \frac{1}{\sqrt{d}} \sum_{k,l=0}^{d-1} \hat{Z}^{-l} |k\rangle\langle l|. \tag{1.25}$$

Para o caso bidimensional $\hat{\mathcal{F}} = \hat{H}$.

A última porta a ser generalizada é a $\hat{C}^{\text{NOT}}$. Como esta foi definida em função da porta $\hat{X}$, é intuitivo que sua generalização também o seja, de modo que

$$\hat{G}^{\text{XOR}} = \sum_{j,k=0}^{d-1} \left(|j\rangle\langle j|\right)_1 \otimes \left(|j \oplus k\rangle\langle k|\right)_2 . \tag{1.26}$$

Como apontado em [35], existe uma maneira alternativa mais conveniente de se expressar essa porta. A porta $\hat{G}^{\text{XOR}}$ definida por (1.26) não é um operador hermitiano para dimensões maiores do que 2:

$$\begin{aligned} \hat{G}^{\text{XOR}\dagger} &= \sum_{j,k=0}^{d-1} \left(|j\rangle\langle j|\right)_1 \otimes \left(|k\rangle\langle j \oplus k|\right)_2 \\ &= \sum_{j,l=0}^{d-1} \left(|j\rangle\langle j|\right)_1 \otimes \left(|l \ominus j\rangle\langle l|\right)_2 \\ &\neq \hat{G}^{\text{XOR}}, \end{aligned} \tag{1.27}$$

onde o símbolo $\ominus$ representa subtração módulo d e usou-se a definição $l \equiv j \oplus k$. Mudando a definição da porta para

$$\hat{G}^{\text{XOR}} = \sum_{j,k=0}^{d-1} \left(|j\rangle\langle j|\right)_1 \otimes \left(|j \ominus k\rangle\langle k|\right)_2 , \tag{1.28}$$

a condição de operador hermitiano é respeitada:

$$\begin{aligned} \hat{G}^{\text{XOR}\dagger} &= \sum_{j,k=0}^{d-1} \left(|j\rangle\langle j|\right)_1 \otimes \left(|k\rangle\langle j \ominus k|\right)_2 \\ &= \sum_{j,l=0}^{d-1} \left(|j\rangle\langle j|\right)_1 \otimes \left(|j \ominus l\rangle\langle l|\right)_2 \\ &= \hat{G}^{\text{XOR}}, \end{aligned} \tag{1.29}$$

onde a definição $l \equiv j \ominus k$ foi utilizada. Para o caso bidimensional $j \oplus k = j \ominus k$, portanto essa operação continua sendo equivalente à mostrada na tabela 1.2. Embora não é necessário que a porta $\hat{G}^{\text{XOR}}$ seja hermitiana para os fins do presente trabalho, esse aspecto é conveniente para a representação de circuitos e facilita as discussões futuras envolvendo a operação $\hat{G}^{\text{XOR}}$. Portanto, a definição da equação (1.28) será adotada.

A tabela 1.3 resume as generalizações das portas bidimensionais apresentadas na tabela 1.2 para dimensões finitas quaisquer e mostra a atuação destas em um estado arbitrário da base computacional. Portas lógicas são as ferramentas necessárias para para o processamento de informação codificada em *qudits*. A combinação de portas é uma forma conveniente de

apresentar protocolos de informação quântica e algoritmos de computação quântica, pois fornece uma descrição semelhante à utilizada na computação clássica [3–5, 36]. A seguir será mostrado como essas portas se encaixam nesse contexto.

Tabela 1.3: Lista de portas lógicas d-dimensionais e suas atuações em *qudits*, onde $j, k = 0, \ldots, d-1$, $\oplus$ denota soma módulo d e $\ominus$ denota subtração módulo d.

Porta Lógica	**Forma Explícita**	**Atuação**
$\hat{X}$	$\hat{X} = \sum_{k=0}^{d-1} \lvert k \oplus 1\rangle\langle k\rvert$	$\hat{X}\lvert j\rangle = \lvert j \oplus 1\rangle$
$\hat{Z}$	$\hat{Z} = \sum_{k=0}^{d-1} e^{\frac{2i\pi k}{d}} \lvert k\rangle\langle k\rvert$	$\hat{Z}\lvert j\rangle = e^{\frac{2i\pi j}{d}} \lvert j\rangle$
$\hat{\mathcal{F}}$	$\hat{\mathcal{F}} = \frac{1}{\sqrt{d}} \sum_{k,l}^{d-1} \hat{Z}^l \lvert k\rangle\langle l\rvert$	$\hat{\mathcal{F}}\lvert j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2i\pi jk}{d}} \lvert k\rangle$
$\hat{G}^{\text{XOR}}$	$\hat{G}^{\text{XOR}} = \sum_{j,k=0}^{d-1} (\lvert j\rangle\langle j\rvert)_1 \otimes (\lvert j \ominus k\rangle\langle k\rvert)_2$	$\hat{G}^{\text{XOR}}\lvert j\rangle_1\lvert k\rangle_2 = \lvert j\rangle_1\lvert j \ominus k\rangle_2$

1.6 Circuitos Quânticos

Os protocolos de informação quântica que serão abordados nesta dissertação são combinações de três elementos. O primeiro é o registrador, um sistema quântico onde se armazena, em seu estado, a informação a ser computada. As transformações unitárias, que realizam o processamento da informação são o segundo, sendo estas representadas pelas portas lógicas quânticas. Por último, a extração da informação é feita por meio de medições, as quais serão discutidas em detalhes no capítulo 2. A representação de circuitos quânticos ilustra este processo como um todo de forma clara [3, 5]. Os diferentes registradores são representados por linhas horizontais. É conveniente rotular cada registrador para facilitar a correspondência entre o circuito e as equações que o descrevem. A combinação desses registradores é chamada de canal quântico. Portas de um *qudit* são representadas por caixas com uma indicação da porta em questão. A figura 1.1 exemplifica este tipo de atuação seguida de uma medição na base computacional, também indicada por uma caixa e um símbolo. Portas quânticas que atuam em dois ou mais *qudits* são representadas por caixas que englobam linhas de mais de um registrador, como ilustrado na figura 1.2. O operador $\hat{\mathcal{U}}_{123}$ representa um operador unitário atuando simultaneamente nos sistemas 1, 2 e 3. A porta $\hat{G}^{\text{XOR}}$, apresentada na figura 1.3, é uma exceção à representação por caixas. Em sua representação ficam especificados o

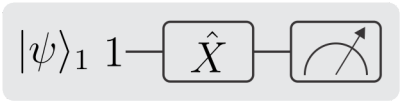

Figura 1.1: Circuito quântico representando a operação $\hat{X}_1|\psi\rangle_1$ seguido de uma medição na base computacional, representada pela última caixa.

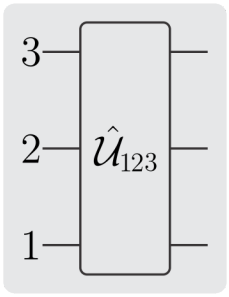

Figura 1.2: Representação da porta quântica $\hat{\mathcal{U}}_{123}$, a qual atua simultaneamente em três sistemas.

qudit de controle, o qual fica inalterado após a atuação da porta, e o *qudit* alvo, que sofrerá modificações condicionais ao estado do controle.

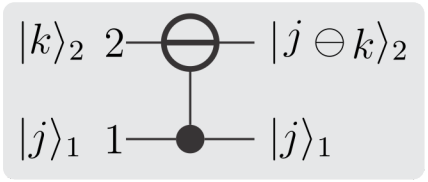

Figura 1.3: Representação da porta $\hat{G}^{\text{XOR}}$, onde $\bullet$ indica o *qudit* de controle. O símbolo $\ominus$ indica a ação da subtração em módulo sobre o *qudit* alvo.

Outra necessidade que pode surgir em meio a protocolos de informação quântica são canais de comunicação clássica. Estes são representados por duas linhas paralelas que saem de uma caixa de medição e se conectam a outras portas do circuito. A seguir serão apresentados alguns protocolos quânticos em forma de circuitos.

1.6.1 Canal de Emaranhamento

Um circuito quântico importante é o canal de emaranhamento, ilustrado na figura 1.4. Este gera um estado bipartido maximamente emaranhado se os estados de entrada forem ortogonais ou idênticos entre si. Por simplicidade, considere os estados de entrada, indicados na figura 1.4, pertencentes à base computacional e que possuam a mesma dimensão d. A

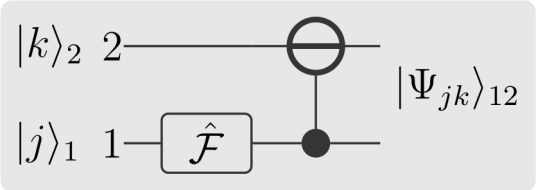

Figura 1.4: Canal de emaranhamento.

equação que descreve esse circuito é dada por

$$\begin{aligned} |\Psi_{jk}\rangle_{12} &= \hat{G}_{12}^{\text{XOR}}[\hat{\mathcal{F}}_1 \otimes \mathbb{1}_2]|j\rangle_1|k\rangle_2 \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} e^{\frac{2i\pi lj}{d}}|l\rangle_1|l \ominus k\rangle_2, \end{aligned} \tag{1.30}$$

onde $\hat{\mathcal{F}}_1$ e $\hat{G}_{12}^{\text{XOR}}$ estão definidas na tabela 1.3. Esse estado é maximamente emaranhado, já que sua entropia linear, definida na equação (1.8), é $\mathcal{E}(|\Psi_{jk}\rangle_{12}) = 1$. Os estados $|\Psi_{jk}\rangle_{12}$ podem ser representados por transformações unitárias em um estado definido como fiducial, dado por

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}|l\rangle|l\rangle. \tag{1.31}$$

Com a atuação das portas $\hat{X}$ e $\hat{Z}$, definidas na tabela 1.3, pode-se escrever os estados $|\Psi_{jk}\rangle_{12}$ como

$$|\Psi_{jk}\rangle_{12} = \hat{X}_2^{-k}\hat{Z}_2^{j}|\Psi_{00}\rangle_{12}. \tag{1.32}$$

O conjunto desses estados forma uma base ortonormal no espaço de Hilbert d^2-dimensional e sua ortogonalidade é verificada na equação

$$\begin{aligned} (\langle\Psi_{j'k'}|\Psi_{jk}\rangle)_{12} &= \frac{1}{d}\sum_{l,l'=0}^{d-1} e^{\frac{2i\pi(jl-j'l')}{d}}(\langle l'|l\rangle)_1(\langle l' \ominus k'|l \ominus k\rangle)_2 \\ &= \frac{1}{d}\sum_{l=0}^{d-1} e^{\frac{2i\pi l(j-j')}{d}}\delta_{kk'} \\ &= \delta_{jj'}\delta_{kk'}, \end{aligned} \tag{1.33}$$

onde foi utilizada a propriedade dada por

$$\sum_{j=0}^{d-1} e^{\frac{2i\pi j(m-n)}{d}} = d\delta_{mn}, \tag{1.34}$$

a qual surge por conta da soma de todas as raízes da unidade ser zero para um dado grau d.

Em diversos protocolos de informação são necessárias medições em uma base de estados maximamente emaranhados. A descrição desse tipo de procedimento também pode ser traduzida para a linguagem de circuitos de modo que o estado passará por um canal inverso ao de emaranhamento, seguido de medições na base computacional, conforme mostrado na figura 1.5. Esse circuito é descrito pela equação

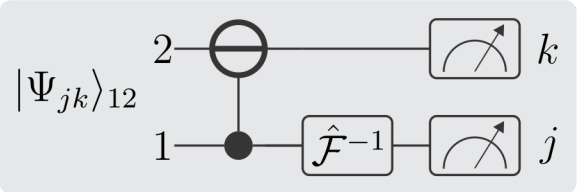

Figura 1.5: Medição do estado maximamente emaranhado $|\Psi_{jk}\rangle_{12}$.

$$\begin{aligned}[\hat{\mathcal{F}}_1^{-1}\otimes\mathbb{1}_2]\hat{G}_{12}^{\text{XOR}}|\Psi_{jk}\rangle_{12} &= [\hat{\mathcal{F}}_1^{-1}\otimes\mathbb{1}_2]\hat{G}_{12}^{\text{XOR}}\hat{G}_{12}^{\text{XOR}}[\hat{\mathcal{F}}_1\otimes\mathbb{1}_2]|j\rangle_1|k\rangle_2 \\ &= |j\rangle_1|k\rangle_2,\end{aligned} \tag{1.35}$$

onde a definição do estado $|\Psi_{jk}\rangle_{12}$, dada pela equação (1.30), foi utilizada juntamente com as propriedades do operador $\hat{G}^{\text{XOR}}$, o qual é unitário e hermitiano, $\hat{G}_{12}^{\text{XOR}}\hat{G}_{12}^{\text{XOR}} = \mathbb{1}_1\otimes\mathbb{1}_2$ e a unitariedade de $\hat{\mathcal{F}}$, $\hat{\mathcal{F}}_1^{-1}\hat{\mathcal{F}}_1 = \mathbb{1}_1$. Uma projeção nos estados $|j\rangle_1$ e $|k\rangle_2$ indicará o estado de entrada do canal, uma vez que a cada estado da base computacional $\{|j\rangle_1|k\rangle_2\}$ está associado um estado da equação (1.30).

1.6.2 Teleportação Quântica

Proposto em 1993, o protocolo de teleportação quântica [28] possibilita que um remetente, Alice, transmita o estado desconhecido de um sistema quântico para um receptor, Bob, sem que seja necessário o envio do sistema quântico em si. Para a realização dessa tarefa Alice e Bob precisam compartilhar um sistema bipartido em um estado maximamente emaranhado e terem acesso a um canal clássico de comunicação. O processo se resume nos seguintes passos: i) Alice realiza uma medição conjunta em uma base maximamente emaranhada na sua parte do sistema compartilhado e no sistema do estado a ser teleportado. ii) Alice comunica o resultado da medição através do canal de comunicação clássica. iii) Bob realiza operações unitárias, condicionais ao resultado de Alice, que deixa sua parte do sistema compartilhado no estado do sistema que ela desejava lhe enviar.

Considere, então, que Alice deseja teleportar um estado desconhecido $|\phi\rangle_3$, dado por

$$|\phi\rangle_3 = \sum_{m=0}^{d-1} c_m|m\rangle_3, \tag{1.36}$$

o qual pertence a um espaço de Hilbert d-dimensional $\mathcal{H}_3$. Alice e Bob compartilham o estado maximamente emaranhado, dado, na decomposição de Schmidt, por

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |n\rangle_1 |n\rangle_2, \tag{1.37}$$

onde os sistemas 1 e 2, pertencentes aos respectivos espaços $\mathcal{H}_1$ e $\mathcal{H}_2$, também são d-dimensionais. Considerou-se as bases de Schmidt $\{|n\rangle_1\}$ e $\{|n\rangle_2\}$ coincidentes com a base computacional de seus respectivos espaços.

Observação 1. Se esse não for inicialmente o caso, Alice e Bob podem realizar operações unitárias para alinhar as bases dos sistemas 1 e 2 com as bases computacionais dos seus respectivos espaços.

O processo de teleportação, mostrado em forma de circuito na figura 1.6, é mais facilmente compreendido utilizando a identidade

$$|\Psi_{00}\rangle_{12} |\phi\rangle_3 = \frac{1}{d} \sum_{j,k=0}^{d-1} \hat{Z}_1^{-j} \hat{X}_1^k |\phi\rangle_1 \hat{G}_{23}^{\text{XOR}} \hat{\mathcal{F}}_2 |j\rangle_2 |k\rangle_3, \tag{1.38}$$

a qual está demonstrada no apêndice A.1. Os operadores $\hat{G}_{23}^{\text{XOR}}$, $\hat{Z}_1$ e $\hat{X}_1$ estão definidos na tabela 1.3 e a transformada inversa de Fourier, $\hat{\mathcal{F}}_2^{-1}$ é dada pela equação (1.25). Seguindo os passos dados no início da seção, Alice deve realizar uma medição em uma base maximamente emaranhada nos sistemas 2 e 3, a qual pode ser feita com a atuação da porta $\hat{G}_{23}^{\text{XOR}}$ seguida de uma transformada inversa de Fourier e de medições na base computacional, conforme discutido na seção 1.6.1. A atuação dessas portas no sistema total é dada por

$$\hat{\mathcal{F}}^{-1} \hat{G}_{12}^{\text{XOR}} |\Psi_{00}\rangle_{12} |\phi\rangle_3 = \hat{Z}_1^{-j} \hat{X}_1^k |\phi\rangle_1 \left(\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_2 \right) \left(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_3 \right). \tag{1.39}$$

Suponha que a medição de Alice nos sistemas 2 e 3 forneça os respectivos resultados j' e k', ambos com probabilidade $1/d$. Isso deixará o sistema 1 no estado $\hat{Z}_1^{-j'} \hat{X}_1^{k'} |\phi\rangle_1$. Para concluir a teleportação, Bob deve realizar a operação $\hat{X}_1^{-k'} \hat{Z}_1^{j'}$, a qual depende dos resultados j' e k'. Então, Alice informa esses resultados através de um canal de comunicação clássica com capacidade de $2 \log_2 d$ bits, deixando Bob ciente das operações que ele deve realizar para finalizar a teleportação do estado $|\phi\rangle_3$. Por fim, após a realização das operações unitárias de Bob, o estado do sistema 1 será exatamente $|\phi\rangle_1$, o que conclui o processo.

Esse protocolo possibilitou, então, a transformação remota do estado do sistema 1, com fidelidade 1, no estado que Alice desejava enviar. Para tanto, não foi necessário nenhum conhecimento do estado $|\phi\rangle_3$ e nenhum sistema quântico foi trocado entre Alice e Bob. Além

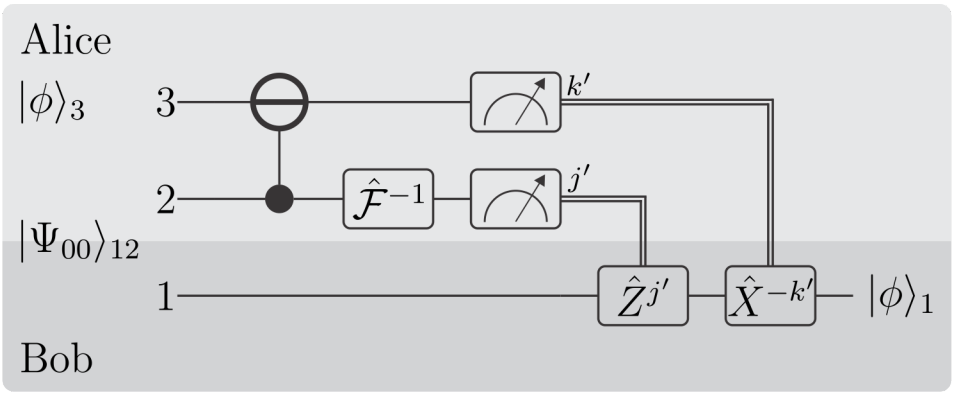

Figura 1.6: Circuito correspondente ao processo de teleportação quântica de *qudits*.

de um estado maximamente emaranhado compartilhado entre eles, a presença de um canal clássico é imprescindível para a conclusão do teleporte, garantindo assim que não há comunicação superluminal no protocolo. Outro ponto importante é que Alice destrói o estado em que o sistema 3 se encontrava ao realizar as medições nos sistemas 2 e 3, portanto não há clonagem presente.

1.6.3 Troca de Emaranhamento

O protocolo de troca de emaranhamento[6], inicialmente sugerido como um teste de desigualdade de Bell [29], consiste em emaranhar dois sistemas quânticos que nunca interagiram entre si. O procedimento é feito com dois estados bipartidos maximamente emaranhados, um compartilhado por Charlie e Alice e o outro por Charlie e Bob. Charlie realiza uma medição na base de estados maximamente emaranhados e comunica seu resultado para Alice e Bob através de canais clássicos, o que transforma o estado dos sistemas deles em um estado maximamente emaranhado. Se Alice e Bob desejam compartilhar um estado previamente especificado, eles realizam transformações unitárias em seus respectivos sistemas, condicionais ao resultado de Charlie.

A figura 1.7 mostra o protocolo de troca de emaranhamento através de um circuito quântico, o qual especifica o estado compartilhado por Charlie e Bob, $|\Psi_{00}\rangle_{12}$, e por Charlie e Alice, $|\Psi_{00}\rangle_{34}$, dados por

$$|\Psi_{00}\rangle_{12} = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} |m\rangle_1 |m\rangle_2, \tag{1.40}$$

$$|\Psi_{00}\rangle_{34} = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |n\rangle_3 |n\rangle_4, \tag{1.41}$$

[6]Tradução livre do nome em inglês, *entanglement swapping*.

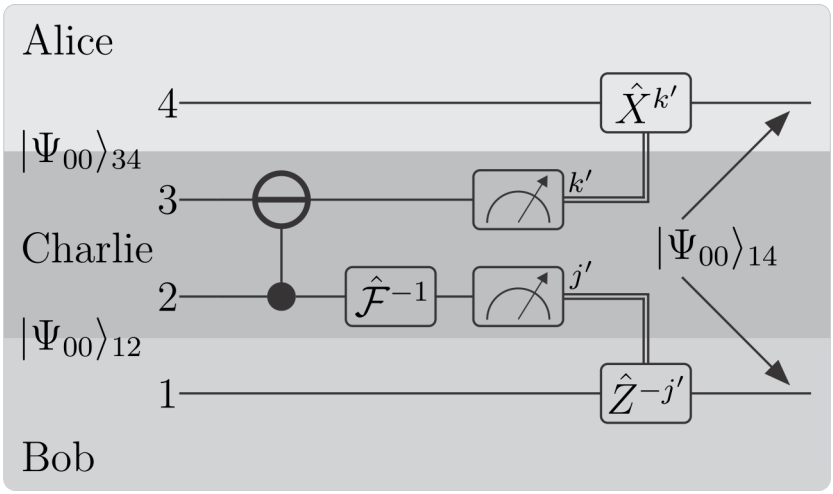

Figura 1.7: Troca de emaranhamento de *qudits* em forma de circuito.

onde os sistemas 1, 2, 3 e 4 pertencem a espaços de Hilbert d-dimensionais e suas bases de Schmidt $\{|m\rangle_1\}$, $\{|m\rangle_2\}$, $\{|n\rangle_3\}$ e $\{|n\rangle_4\}$ são assumidas como coincidentes às bases computacionais de seus respectivos espaços.[7] O estado total pode ser descrito conforme a equação

$$|\Psi_{00}\rangle_{12}|\Psi_{00}\rangle_{34} = \frac{1}{d}\sum_{j,k=0}^{d-1}|\Psi_{jk}\rangle_{14}\hat{G}_{23}^{\text{XOR}}\hat{\mathcal{F}}_2|j\rangle_2|k\rangle_3, \tag{1.42}$$

a qual está demonstrada no apêndice A.2 e o estado $|\Psi_{jk}\rangle_{14}$ é dado pela equação (1.30). Conforme o circuito da figura 1.7 e o que foi discutido na seção 1.6.1, Charlie realiza uma medição em uma base de estados maximamente emaranhados atuando com as portas $\hat{G}_{23}^{\text{XOR}}$, definida na tabela 1.3, e $\hat{\mathcal{F}}_2^{-1}$, dada na equação (1.25), seguidas de medições na base computacional. Após as atuações dos operadores, o estado total dos sistemas 1, 2, 3 e 4 é dado por

$$\hat{G}_{23}^{\text{XOR}}\hat{\mathcal{F}}_2^{-1}|\Psi_{00}\rangle_{12}|\Psi_{00}\rangle_{34} = |\Psi_{jk}\rangle_{14}\left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_2\right)\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|k\rangle_3\right). \tag{1.43}$$

Charlie, então, realiza medições na base computacional nos sistemas 2 e 3, as quais fornecem os respectivos resultados j' e k', ambos com probabilidade $1/d$. Ele comunica seus resultados através de dois canais clássicos com $\log d$ bits de capacidade cada, fazendo com que Alice e Bob compartilhem o estado maximamente emaranhado $|\Psi_{j'k'}\rangle_{14}$. Supondo que eles desejem compartilhar o estado fiducial $|\Psi_{00}\rangle_{14}$, dado pela equação (1.31), eles devem realizar as operações unitárias apontadas na figura 1.7. Da equação (1.32)

$$|\Psi_{00}\rangle_{14} = \hat{Z}_1^{j'}\hat{X}_4^{-k'}|\Psi_{j'k'}\rangle_{14}. \tag{1.44}$$

[7] Se esse não for inicialmente o caso, Alice, Bob e Charlie podem realizar rotações unitárias para alinhar as bases dos sistemas 1, 2, 3 e 4 com as bases computacionais dos seus respectivos espaços de Hilbert.

Como o emaranhamento não é alterado por operações unitárias locais, Alice e Bob podem compartilhar inúmeros outros estados maximamente emaranhados aplicando diferentes operações unitárias condicionais ao resultado de Charlie.

1.6.4 Codificação Superdensa

Codificação superdensa é um protocolo de informação quântica que utiliza estados emaranhados para aumentar a quantidade de informação clássica que pode ser transmitida com o envio de um *qudit*. O protocolo original, proposto por Bennett e Wiesner [1], se resume a um codificador, Alice, que compartilha um par de sistemas d-dimensionais em um estado maximamente emaranhado com um decodificar, Bob. Alice atua com operações unitárias em sua parte do sistema, preparando uma de d^2 mensagens perfeitamente distinguíveis codificadas no estado bipartido. Após a codificação, Alice envia seu sistema para Bob, o qual identifica a mensagem com a realização de uma medição no sistema conjunto. Assim, Alice pode transmitir $2\log_2 d$ bits de informação clássica com o envio de apenas um *qudit*. Esse resultado é contrastante com situações semelhantes que utilizam sistemas clássicos com d estados distinguíveis (ou sistemas quânticos descorrelacionados), onde apenas $\log_2 d$ bits podem ser transmitidos.

Para ilustrar o protocolo, considere que Alice e Bob compartilham um sistema bipartido maximamente emaranhado no estado fiducial, equação (1.31), onde os sistemas 1 e 2 pertencem a espaços d-dimensionais. Utilizando a identidade da equação (1.32), Alice codifica a mensagem jk com a atuação das portas $\hat{Z}_2^j$ e $\hat{X}_2^{-k}$, definidas na tabela 1.3, de modo que o estado compartilhado será dado por

$$\begin{aligned} \hat{X}_2^{-k}\hat{Z}_2^j|\Psi_{00}\rangle_{12} &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} e^{\frac{2i\pi j}{d}}|l\rangle_1|l\ominus k\rangle_2 \\ &= |\Psi_{jk}\rangle_{12}. \end{aligned} \tag{1.45}$$

Como $j,k=0,\ldots,d-1$, existem d^2 estados ortonormais $|\Psi_{jk}\rangle_{12}$, cuja ortogonalidade está demonstrada na equação (1.33). Cada mensagem de Alice corresponde a um desses estados, o que possibilita o envio de $2\log_2 d$ bits de informação. A porta $\hat{X}^{-k}$ $(k=0,\ldots,d-1)$ permuta entre estados ortogonais do sistema 2. Isso pode ser considerado como a parte "clássica" da codificação, uma vez que essa operação possibilita codificar d mensagens em um único *qudit*. A introdução de fases relativas no estado emaranhado através da porta $\hat{Z}^j$ $(j=0,\ldots,d-1)$ é o que possibilita a produção local de d^2 estados ortogonais no sistema bipartido, podendo ser atribuído à esta operação o ganho quântico do protocolo. Dessa maneira, as mensagens são codificadas em estados ortogonais que geram o espaço de Hilbert total $\mathcal{H}_1\otimes\mathcal{H}_2$ do sistema conjunto. Alice envia seu *qudit* para Bob que decodifica a mensagem com uma medição conjunta, a qual pode ser realizada com a atuação das portas $\hat{G}_{12}^{\text{XOR}}$ e $\hat{\mathcal{F}}_1^{-1}$

seguidas de medições na base computacional, conforme mostrado na seção 1.6.1. Isso pode ser visto atuando as portas $\hat{G}_{12}^{\text{XOR}}$ e $\hat{\mathcal{F}}_1^{-1}$ no estado $|\Psi_{jk}\rangle_{12}$, dado pela equação (1.30)

$$\begin{aligned}\hat{\mathcal{F}}^{-1}\hat{G}_{12}^{\text{XOR}}|\Psi_{jk}\rangle_{12} &= \hat{\mathcal{F}}_1^{-1}\hat{G}_{12}^{\text{XOR}}\hat{G}_{12}^{\text{XOR}}\hat{\mathcal{F}}_1|j\rangle_1|k\rangle_2 \\ &= |j\rangle_1|k\rangle_2.\end{aligned} \tag{1.46}$$

A figura 1.8 ilustra o protocolo de codificação superdensa descrito em forma de circuito.

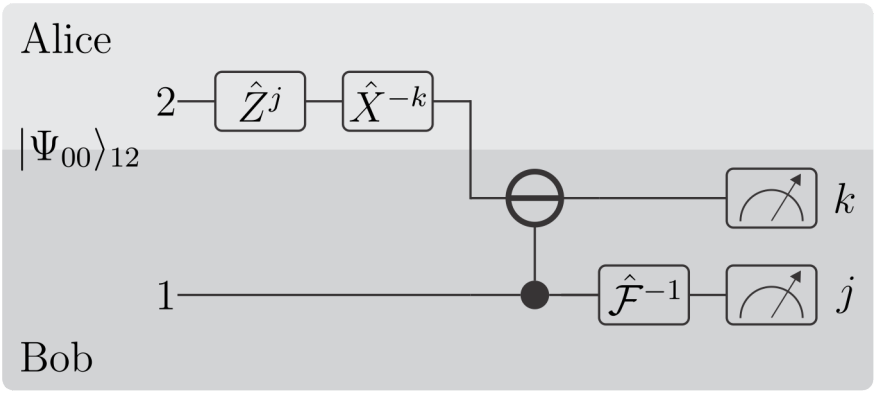

Figura 1.8: Codificação superdensa realizada com estado bipartido maximamente emaranhado de *qudits*.

Codificação superdensa via canais de dimensões distintas

Se os sistemas 1 e 2 possuírem dimensões distintas, nem sempre será possível codificar um número de mensagens equivalente à dimensão do sistema conjunto. Para mostrar isso, considere o sistema 1 pertencente a um espaço d_1-dimensional e o sistema 2 a um espaço d_2-dimensional, com $d_1 \neq d_2$. O estado maximamente emaranhado do sistema conjunto, segundo a decomposição de Schmidt, é dado por

$$|\Psi\rangle_{12} = \frac{1}{\sqrt{D}}\sum_{l=0}^{D-1}|l\rangle_1|l\rangle_2, \tag{1.47}$$

onde $D \equiv \min(d_1, d_2)$. O número de mensagens codificáveis, $\mathcal{N}$, será analisado para ambos os casos, $d_1 > d_2$ e $d_2 > d_1$, recuperando os resultados das referências [10, 12].

Primeiramente assuma $d_1 > d_2$, sendo $D = d_2$. De modo análogo ao caso anterior, Alice atua com as operações unitárias $\hat{Z}_2^j$ e $\hat{X}_2^{-k}$, obtendo

$$\begin{aligned}\hat{X}_2^{-k}\hat{Z}_2^j|\Psi\rangle_{12} &= \frac{1}{\sqrt{d_2}}\sum_{l=0}^{d_2-1}|l\rangle_1\hat{X}_2^{-k}\hat{Z}_2^j|l\rangle_2 \\ &= \frac{1}{\sqrt{d_2}}\sum_{l=0}^{d_2-1}e^{\frac{2i\pi lj}{d_2}}|l\rangle_1|l\ominus k\rangle_2 \\ &= \hat{G}_{12}^{\text{XOR}}\hat{\mathcal{F}}_{1,D}|j\rangle_1|k\rangle_2,\end{aligned} \tag{1.48}$$

onde $j, k = 0, \ldots, d_2 - 1$ e $\hat{\mathcal{F}}_{1,D}$ atua em um subespaço d_2-dimensional. Portanto, é possível codificar d_2^2 mensagens distinguíveis. Alice envia seu sistema para Bob que realiza uma medição segundo o procedimento da figura (1.8). A medição de Bob é feita da mesma forma que no caso onde $d_1 = d_2$, mas com a porta $\hat{G}_{12}^{\text{XOR}}$ atuando em sistemas de dimensões diferentes. Essa particularidade não acarreta diferenças para o protocolo, uma vez que, conforme discutido em [34], é possível definir portas híbridas que mantêm suas definições de atuação. Nesse caso, o número de mensagens codificáveis é menor do que o espaço total do sistema, $d_1 d_2$. Algo que se poderia tentar é a atuação de uma operação que gerasse um número maior de fases para explorar todo o espaço $\mathcal{H}_1$, como, por exemplo,

$$\hat{Z}' \equiv \sum_{m=0}^{d_1-1} e^{\frac{2i\pi m}{d_1}} |m\rangle\langle m|. \tag{1.49}$$

Mas, esse procedimento geraria um conjunto de estados $|\Psi'_{jk}\rangle_{12}$ não-ortogonais e, portanto não perfeitamente distinguíveis, como será discutido no próximo capítulo.

Para o caso inverso, onde $d_1 < d_2$, pode ser intuitivo pensar que serão codificadas d_1^2 mensagens, mas, como o espaço de Hilbert maior está nas mãos de Alice, ela pode explorá-lo para codificar d_2 mensagens, como no caso clássico. Essa operação corresponde à atuação da porta X_2^{-k} $(k = 0, \ldots, d_2 - 1)$. Se a parte quântica da codificação fosse realizada, como nos casos anteriores, pela porta $\hat{Z}_2^j$ $(j = 0, \ldots, d_2 - 1)$, seria gerado um conjunto de estados não-ortogonais no sistema bipartido. Para evitar esse problema, é definida uma nova operação, $\hat{\mathcal{Z}}$, cuja atuação na base computacional é dada por

$$\hat{\mathcal{Z}}_2^j |l\rangle_2 = e^{\frac{2i\pi lj}{D}} |l\rangle_2, \tag{1.50}$$

e é definida como[8]

$$\hat{\mathcal{Z}} \equiv \sum_{m=0}^{D-1} e^{\frac{2i\pi m}{D}} |m\rangle\langle m|. \tag{1.51}$$

Essa definição generaliza o caso anterior, onde $d_1 > d_2$ e $\hat{\mathcal{Z}}_2^j = \hat{Z}_2^j$, e será utilizada como porta quântica padrão para os protocolos de codificação superdensa do capítulo 5. A atuação das portas $\hat{X}_2^{-k}$ $(k = 0, \ldots, d_2 - 1)$ e $\hat{\mathcal{Z}}_2^j$ $(j = 0, \ldots, D - 1)$, permite a codificação de $\mathcal{N} = d_1 d_2$

[8] A porta quântica $\hat{\mathcal{Z}}$ não é necessariamente uma operação unitária. Essa operação atua em um espaço D-dimensional. Sempre que $d_2 > D$, ela pode ser vista como um mapa de $\mathcal{H}_D \to \mathcal{H}_{d_2}$. Operações deste tipo são conhecidas como isometrias, as quais possuem como propriedade a preservação da norma do estado em que atuam. Se $D = d_2$, a isometria é um operador unitário [10].

mensagens. A codificação de Alice é dada por

$$\begin{aligned}\hat{X}_2^{-k}\hat{\mathcal{Z}}_2^{j}|\Psi\rangle_{12} &= \frac{1}{\sqrt{d_1}}\sum_{l=0}^{d_1-1}|l\rangle_1\hat{X}_2^{-k}\hat{\mathcal{Z}}_2^{j}|l\rangle_2 \\ &= \frac{1}{\sqrt{d_1}}\sum_{l=0}^{d_1-1}e^{\frac{2i\pi lj}{d_1}}|l\rangle_1|l\ominus k\rangle_2 \\ &= \hat{G}_{12}^{\text{XOR}}\hat{\mathcal{F}}_1|j\rangle_1|k\rangle_2,\end{aligned} \tag{1.52}$$

a qual explicita os d_1d_2 estados ortogonais. Como nas situações anteriores, Bob conclui o protocolo atuando com as portas $\hat{G}_{12}^{\text{XOR}}$ e $\hat{\mathcal{F}}^{-1}$, seguidas de medições na base computacional. Essa descrição do protocolo de codificação superdensa utiliza as dimensões acessíveis dos sistemas 1 e 2 de modo a codificar o maior número de mensagens possível.

De modo geral, o número de mensagens codificadas por Alice é dado por

$$\mathcal{N} = d_2D, \tag{1.53}$$

onde $D = \min(d_1, d_2)$. $\mathcal{N}$ é o número máximo de mensagens perfeitamente distinguíveis enviadas através de protocolos de codificação superdensa com estados maximamente emaranhados. A figura 1.9 representa o protocolo padrão de codificação superdensa que engloba as três situações apresentadas nessa seção.

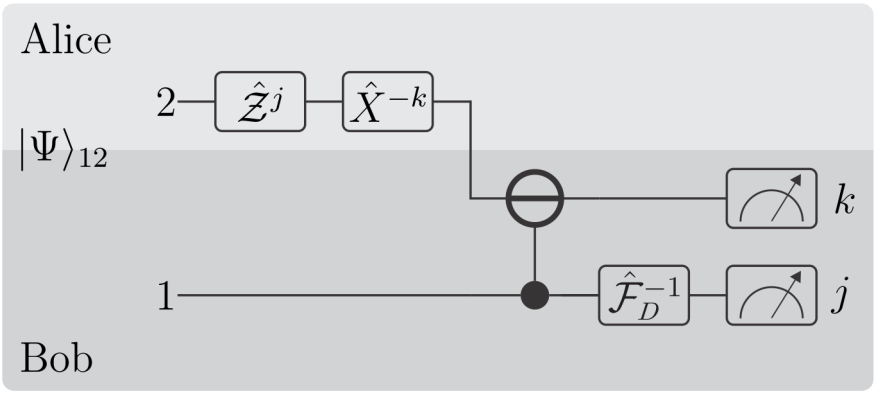

Figura 1.9: Codificação superdensa realizada com estado bipartido maximamente emaranhado de *qudits* com dimensões arbitrárias. A operação $\hat{\mathcal{Z}}$, definida na equação (1.51), substitui a porta quântica $\hat{Z}$ para garantir que sejam gerados estados bipartidos ortogonais.

2

Discriminação de Estados Quânticos

Em diversos protocolos de informação quântica, como codificação superdensa [1], teleportação quântica [28] e troca de emaranhamento [29], é necessária a determinação de estados de sistemas quânticos. Isso pode ser realizado através de uma medição sobre esses sistemas, a qual somente será capaz de determinar o seu estado de forma inequívoca se ele pertencer a um conjunto conhecido de estados mutuamente ortogonais. Caso contrário, se o conjunto for constituído por estados não-ortogonais[1], nenhuma medição irá identificar, de maneira determinística e sem erros, em qual deles o sistema se encontra. Essa limitação pode afetar a eficiência da transmissão de informação em diversos protocolos, como codificação superdensa [12], teleportação quântica [37] e troca de emaranhamento [38] supracitados. Para diminuir seus efeitos, se torna importante o estudo de estratégias de medição que otimizem a distinção de estados não-ortogonais segundo alguma figura de mérito previamente estabelecida.

Este capítulo será dividido em duas partes. Primeiramente será feita uma breve revisão dos postulados referentes às medições em mecânica quântica, tanto para as medições projetivas quanto para as generalizadas. A implementação das medições generalizadas será descrita posteriormente através do teorema de Naimark. Na segunda parte, utilizando as ferramentas apresentadas na primeira, serão discutidas diversas estratégias de discriminação de estados não-ortogonais, as quais serão ilustradas com exemplo simples para o caso de um *qubit*.

2.1 Medições Quânticas

Como visto no capítulo 1, informação pode ser codificada no próprio estado de um sistema quântico. Desse modo a capacidade de identificar o estado é fundamental no processamento de informação quântica. Medições quânticas projetivas e generalizadas são abordadas em diversos textos introdutórios de mecânica quântica [3–7] e serão apresentadas aqui na forma

[1] A existência de estados não-ortogonais é uma consequência do princípio de superposição de estados da mecânica quântica.

de postulados. A implementação de medições generalizadas será descrita com o teorema de Naimark.

2.1.1 Medições Projetivas

Para qualquer observável, O, associado a um sistema quântico, existe um operador hermitiano correspondente, $\hat{O}$, que atua no espaço de Hilbert do sistema, $\mathcal{H}$. Dado que esse operador seja escrito na forma de sua decomposição espectral, $\hat{O} = \sum_j \lambda_j |j\rangle\langle j|$, podem-se listar propriedades que caracterizam uma medição projetiva ao atuá-lo em um estado arbitrário $\hat{\rho}$. Por simplicidade assume-se que não há autovalores degenerados.

1a. Em decorrência do operador $\hat{O}$ ser hermitiano, todos os seus autovalores λ_j são reais.

2a. Os projetores $\hat{P}_j = |j\rangle\langle j|$ geram o espaço de Hilbert total, ou seja, $\sum_j \hat{P}_j = \mathbb{1}$, onde $\mathbb{1}$ é o operador identidade atuando nesse espaço.

3a. Da ortogonalidade dos autovetores de $\hat{O}$, tem-se $\hat{P}_i\hat{P}_j = \hat{P}_i\delta_{ij}$, o que implica diretamente que $\hat{P}_j^2 = \hat{P}_j$ e, portanto, que os autovalores de qualquer projetor são iguais a 0 ou 1.

4a. A medição de O fornece um dos autovalores λ_j.

5a. A probabilidade de se obter o resultado de medição λ_j é $p_j = \mathrm{Tr}(\hat{P}_j\hat{\rho}\hat{P}_j) = \mathrm{Tr}(\hat{P}_j^2\hat{\rho}) = \mathrm{Tr}(\hat{P}_j\hat{\rho})$, onde foi utilizada a propriedade cíclica do traço.[2]

6a. Dado que o resultado da medição é λ_j, o estado do sistema imediatamente após esta é $\hat{\rho}_j = \dfrac{\hat{P}_j\hat{\rho}\hat{P}_j}{\mathrm{Tr}(\hat{P}_j\hat{\rho}\hat{P}_j)} = \dfrac{\hat{P}_j\hat{\rho}\hat{P}_j}{p_j} = |j\rangle\langle j|$.

7a. Se é realizada uma medição e seu resultado não é registrado, o estado do sistema após a medição é a mistura estatística de todos os possíveis resultados, dado pelo operador densidade $\hat{\rho}' = \sum_j p_j\hat{\rho}_j$.

Os itens 1a–3a apresentam propriedades matemáticas, enquanto os itens 4a–7a são postulados da teoria quântica. Essas propriedades mostram a aleatoriedade do processo de medição, já que não é possível prever seu resultado deterministicamente. Apenas quando é garantido que o estado de um sistema quântico coincide com um dos autovetores de um observável, é possível determiná-lo precisamente com uma medição projetiva.

[2] A propriedade cíclica do traço, que afirma a invariância do traço sob permutações cíclicas dos seus argumentos, continuará sendo utilizada posteriormente sem mais menções.

2.1.2 Medições Generalizadas

O número de resultados possíveis ao se realizar uma medição projetiva é limitado ao número de termos ortogonais da decomposição do operador identidade do espaço de Hilbert preenchido pelo estado medido. Assim, medições projetivas restringem o número de resultados possíveis à dimensão do espaço de Hilbert associado ao estado. Entretanto, pode ser desejável um número maior de resultados de medição que preservem a positividade e normalização das probabilidades. Abandonando os projetores $\hat{P}_j$ e substituindo-os por novos operadores de medição $\hat{A}_j$ é possível reformular os postulados da seção anterior a fim de cumprir esses objetivos.

Do postulado 5a nota-se que o que garante a positividade das probabilidades é a positividade do operador $\hat{P}_j^2$. De maneira análoga, para que as probabilidade sejam positivas, introduz-se os operadores $\hat{\Pi}_j = \hat{A}_j^\dagger \hat{A}_j \succeq 0$. A normalização é uma consequência direta do postulado 2a, portanto os operadores positivos $\hat{\Pi}_j$ devem ser uma decomposição da identidade, $\sum_j \hat{\Pi}_j = \mathbb{1}$. Essa decomposição da identidade em termos de operadores positivos é chamada de medida com valores em operadores positivos (POVM)[3] e seus operadores $\hat{\Pi}_j$ são chamados de elementos de POVM.

Como os elementos de POVM são positivos, a existência de $\hat{\Pi}_j^{1/2}$ é garantida. Esse operador pode ser usado na construção dos operadores de detecção $\hat{A}_j$:

$$\hat{A}_j = \hat{U}_j \hat{\Pi}_j^{1/2}, \tag{2.1}$$

onde $\hat{U}_j$ é um operador unitário qualquer. Essa é a forma mais geral possível desses operadores de detecção, e a liberdade no operador unitário será explorada posteriormente. A condição de ortogonalidade dos projetores, postulado 3a, não precisa ser satisfeita pelos operadores de detecção. O abandono desse postulado exclui a restrição no número máximo de resultados de medição, cumprindo assim os requisitos desejados para medições mais gerais.

Novas propriedades, semelhantes às da seção anterior, definem o POVM:

1b. Elementos de POVM são operadores positivos (mais precisamente não-negativos), $\hat{\Pi}_j \succeq 0$.

2b. Um POVM é formado por elementos de POVM que satisfazem a relação de completeza, $\sum_j \hat{\Pi}_j = \mathbb{1}$.

3b. Os elementos de POVM $\hat{\Pi}_j$ podem ser representados por operadores de detecção $\hat{A}_j$ como $\hat{\Pi}_j = \hat{A}_j^\dagger \hat{A}_j$.

4b. Cada resultado de medição j é associado ao elemento de POVM $\hat{\Pi}_j$.

[3] A sigla é originada do nome em inglês *Positive Operator Valued Measure*.

5b. A probabilidade total de se obter um resultado particular ao ser efetuada uma medição é $p_j = \mathrm{Tr}(\hat{A}_j\hat{\rho}\hat{A}_j^\dagger) = \mathrm{Tr}(\hat{A}_j^\dagger\hat{A}_j\hat{\rho}) = \mathrm{Tr}(\hat{\Pi}_j\hat{\rho})$.

6b. O estado do sistema imediatamente após uma medição é $\hat{\rho}_j = \dfrac{\hat{A}_j\hat{\rho}\hat{A}_j^\dagger}{\mathrm{Tr}(\hat{\Pi}_j\hat{\rho})} = \dfrac{\hat{A}_j\hat{\rho}\hat{A}_j^\dagger}{p_j}$.

7b. Se uma medição é realizada e seu resultado não for registrado, o estado do sistema após a medição é descrito pelo operador densidade $\hat{\rho}' = \sum_j p_j\hat{\rho}_j = \sum_j \hat{A}_j\hat{\rho}\hat{A}_j^\dagger$.

A partir desses postulados nota-se que não há necessidade de ortogonalidade entre os operadores $\hat{\Pi}_j$ e, portanto, o número de elementos de POVM não é mais limitado pelo tamanho do espaço de Hilbert do sistema a ser medido. Se os $\hat{\Pi}_j$ forem projetores ortogonais e a soma dos subespaços que atuam for o espaço de Hilbert do sistema a ser medido, recai-se em medições projetivas. Portanto, o POVM representa uma generalização das medições projetivas.

Embora os postulados 1b–7b forneçam uma descrição matemática do POVM, nada foi dito sobre a implementação física desse tipo de medição. Na próxima seção, uma forma de implementar POVMs será mostrada por meio do teorema de Naimark.

2.1.3 Implementação de Medições Generalizadas via Teorema de Naimark

Um POVM pode ser descrito em termos de medições projetivas, possibilitando assim uma implementação física de medições generalizadas [4]. O teorema de Naimark [4,39,40] fornece a reciprocidade de POVMs com transformações unitárias e medições projetivas em um espaço de Hilbert estendido, o que torna possível a implementação de POVMs.

Teorema de Naimark.[4] Dado um POVM, existe uma medição projetiva atuando em um espaço de Hilbert estendido a qual o realiza. Reciprocamente, cada medição projetiva atuando em um espaço de Hilbert estendido fornece um POVM.

Para a realização de um POVM segundo o teorema de Naimark é necessária, então, a extensão do espaço de Hilbert do sistema a ser medido, $\mathcal{H}_\mathcal{S}$. Isto pode ser feito de duas formas distintas, soma direta ou produto tensorial.

No caso de soma direta são utilizadas dimensões extras do próprio sistema, caso existam e sejam acessíveis. O espaço de Hilbert total é dado por $\mathcal{H} = \mathcal{H}_\mathcal{S} \oplus \mathcal{H}_a$, onde $\mathcal{H}_a$ é o subespaço das dimensões extras e o símbolo "$\oplus$" denota a soma direta entre os espaços. A implementação física do POVM se dá por uma transformação unitária, $\hat{U}_{Sa} \in \mathcal{H}_\mathcal{S} \oplus \mathcal{H}_a$,

[4] O teorema de Naimark é, na verdade, mais geral do que sua aplicação na teoria de medições quânticas [7]. No entanto, sua forma restrita apresentada neste capítulo é comumente referida como Teorema de Naimark.

seguida de uma medição projetiva no espaço estendido. Para mostrar essa equivalência considere a decomposição da identidade neste espaço, dada por

$$\mathbb{1}_{\mathcal{H}} = \sum_{j=0}^{d_{\mathcal{H}}-1} (|j\rangle\langle j|)_{\mathcal{H}}, \tag{2.2}$$

onde $d_{\mathcal{H}}$ é a dimensão de $\mathcal{H}$ e $\{|j\rangle\}$ uma base ortonormal nesse espaço. A aplicação da operação unitária $\hat{U}_{Sa}$ fornece

$$\begin{aligned} \hat{U}_{Sa}\mathbb{1}_{\mathcal{H}}\hat{U}_{Sa}^{\dagger} &= \sum_{j=0}^{d_{\mathcal{H}}-1} (\hat{U}_{Sa}|j\rangle\langle j|\hat{U}_{Sa}^{\dagger})_{\mathcal{H}} \\ &= \sum_{j=0}^{d_{\mathcal{H}}-1} (|u_j\rangle\langle u_j|)_{\mathcal{H}} \\ &= \mathbb{1}_{\mathcal{H}}, \end{aligned} \tag{2.3}$$

no qual $\{|u_j\rangle = \hat{U}_{Sa}|j\rangle\}$ é outra base ortonormal em $\mathcal{H}$. Reduzindo essa operação ao subespaço $\mathcal{H}_S$ se obtém

$$\begin{aligned} \mathbb{1}_{\mathcal{H}_S} &= \mathbb{1}_{\mathcal{H}_S}\mathbb{1}_{\mathcal{H}}\mathbb{1}_{\mathcal{H}_S} \\ &= \sum_{j=0}^{d_{\mathcal{H}}-1} \mathbb{1}_{\mathcal{H}_S}(|u_j\rangle\langle u_j|)_{\mathcal{H}}\mathbb{1}_{\mathcal{H}_S} \\ &= \sum_{j=0}^{d_{\mathcal{H}}-1} \hat{\Pi}_j, \end{aligned} \tag{2.4}$$

onde $\hat{\Pi}_j = \mathbb{1}_{\mathcal{H}_S}\hat{U}_{Sa}(|j\rangle\langle j|)_{\mathcal{H}}\hat{U}_{Sa}^{\dagger}\mathbb{1}_{\mathcal{H}_S}$ é um de $d_{\mathcal{H}}$ operadores positivos que somam à identidade em $\mathcal{H}_S$ ($d_{\mathcal{H}_S} < d_{\mathcal{H}}$), sendo assim identificado como um elemento de POVM nesse espaço.

A outra forma de estender o espaço de Hilbert do sistema é por produto tensorial. Para isso, agrega-se um sistema auxiliar, chamado de *ancilla*, ao sistema principal. Considere que $|\psi\rangle_S$ é o estado do sistema no espaço de Hilbert $\mathcal{H}_S$. A realização física de um POVM segundo teorema de Naimark, nesse caso, é equivalente ao processo descrito pelos passos: i) o espaço de Hilbert $\mathcal{H}_S$ é estendido sendo agregado a uma *ancilla*. Esse novo espaço é denotado por $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_a$, onde $\mathcal{H}_a$ é o espaço de Hilbert associado à *ancilla* e o símbolo "$\otimes$" denota o produto tensorial entre os espaços. ii) Uma transformação unitária U_{Sa} é realizada sobre estado do sistema conjunto. iii) Por fim, são realizadas medições projetivas no espaço $\mathcal{H}_a$. Para mostrar a correspondência entre esse procedimento e um POVM, considere que o estado da *ancilla* é denotado por $|\phi\rangle_a$, e que $\{|j\rangle_a\}$ é uma base ortonormal de $\mathcal{H}_a$. O estado conjunto é dado por $|\Psi\rangle_{Sa} = |\psi\rangle_S|\phi\rangle_a$. Define-se a operação unitária $\hat{U}_{Sa}$ de forma a satisfazer a equação

$$\hat{U}_{Sa}(|\psi\rangle_S|\phi\rangle_a) = \sum_j \hat{A}_j|\psi\rangle_S|j\rangle_a. \tag{2.5}$$

Uma medição projetiva $\left[\mathbb{1}_S \otimes (|j^{'}\rangle\langle j^{'}|)_a\right]$ na *ancilla* fornece a atuação individual de um operador $\hat{A}_j$ no estado $|\psi\rangle_S$

$$\begin{aligned}\left[\mathbb{1}_S \otimes (|j^{'}\rangle\langle j^{'}|)_a\right] \hat{U}_{Sa} \left[|\psi\rangle_S|\phi\rangle_a\right] &= \sum_j \hat{A}_j|\psi\rangle_S|j^{'}\rangle_a\langle j^{'}|j\rangle \\ &= \hat{A}_j|\psi\rangle_S|j\rangle_a\end{aligned} \tag{2.6}$$

com probabilidade

$$\begin{aligned}p_j &= \|_a\langle j|\hat{U}_{1a}(|\psi\rangle_S|\phi\rangle_a)\|^2 \\ &= \|\hat{A}_j|\psi\rangle_S\|^2.\end{aligned} \tag{2.7}$$

Como as probabilidades devem ser positivas e somar à unidade, tem-se

$$\begin{aligned}\sum_j p_j &= \sum_j \|\hat{A}_j|\psi\rangle_S\|^2 \\ &= \sum_j {}_S\langle\psi|\hat{A}_j^\dagger\hat{A}_j|\psi\rangle_S \\ &= 1,\end{aligned} \tag{2.8}$$

e, como isso deve se manter para qualquer $|\psi\rangle_S$,

$$\sum_j \hat{A}_j^\dagger\hat{A}_j = \mathbb{1}_S. \tag{2.9}$$

Portanto, o conjunto $\{\hat{A}_j^\dagger\hat{A}_j = \hat{\Pi}_j\}$ é uma decomposição da identidade em termos de operadores positivos e os operadores $\hat{A}_j$ são identificados como operadores de detecção, o que conclui a demonstração do procedimento.

Foi mostrado que o teorema de Naimark é válido independentemente da forma com que espaço de Hilbert é estendido. O uso do método com soma direta ou produto tensorial dependerá do contexto experimental, do sistema que se está utilizando, etc [41–43]. Estratégias de discriminação de estados não-ortogonais, apresentadas a seguir, utilizam medições generalizadas, as quais serão implementadas via teorema de Naimark.

2.2 Discriminação de Estados Quânticos Não-Ortogonais

O problema de discriminação de estados quânticos abordado nesta seção (e ao longo da dissertação) pode ser ilustrado da seguinte maneira. Suponha que Alice envie para Bob um sistema preparado em um dos estados do conjunto $\{\hat{\rho}_j\}$, com probabilidades *a priori* η_j. O trabalho de Bob é identificar o estado enviado a ele através de uma única medição, sendo que

ele conhece todos os estados do conjunto e suas respectivas probabilidades. Se os estados enviados por Alice formarem um conjunto ortogonal, estes podem ser perfeitamente discriminados por medições projetivas. Caso contrário, quando o conjunto de estados é não-ortogonal, é inevitável a presença de incertezas associadas aos resultados das medições [4, 44, 45]. O desenvolvimento de estratégias eficazes para a tarefa de discriminação de estados se torna importante no contexto de informação quântica, onde informação é codificada no próprio estado do sistema. Portanto, a qualidade da discriminação de estados dita a qualidade da informação extraída do sistema, influenciando assim a performance de protocolos de informação quântica, como os que serão estudados nos capítulos 4 e 5.

Na seção anterior foram apresentados os conceitos de medições projetivas e medições generalizadas. A liberdade na construção de POVMs possibilitou a criação de diversas estratégias de discriminação de estados quânticos, cada qual com o objetivo de otimizar uma figura de mérito previamente estabelecida. A seguir serão apresentadas as estratégias de discriminação de estados quânticos com erro mínimo (EM), sem ambiguidade (SA), com confiança máxima (CM) e estratégias intermediárias entre EM e CM.

2.2.1 Discriminação com Erro Mínimo

Considere um conjunto de N estados $\{\hat{\rho}_j \mid j = 0, \ldots, N-1\}$ com probabilidades *a priori* de preparação $\{\eta_j\}$. Se quer realizar uma medição com N resultados possíveis, cada qual identificando um dos estados do conjunto com o menor erro associado possível. Suponha que essa medição seja representada pelo POVM $\{\hat{\Pi}_j \mid j = 0, \ldots, N-1\}$ e que ω_j é o resultado associado ao elemento $\hat{\Pi}_j$ que leva à identificação do estado como $\hat{\rho}_j$. A probabilidade de identificar corretamente será $\mathrm{Tr}(\hat{\Pi}_j\hat{\rho}_j)$, de modo que a probabilidade *média* de que o estado seja identificado erroneamente (P_{erro}) será dada por

$$\begin{aligned} P_{\text{erro}} &= 1 - \sum_j \eta_j \mathrm{Tr}(\hat{\Pi}_j\hat{\rho}_j) \\ &= 1 - P_{\text{corr}}, \end{aligned} \tag{2.10}$$

onde P_{corr} é a probabilidade *média* de identificação correta do estado. Inicialmente tratada por Helstrom [15] no contexto da teoria quântica de detecção, a estratégia EM consiste em encontrar o POVM que minimiza a probabilidade de erro dada pela equação (2.10). As condições suficientes e necessárias para POVMs que satisfaçam as exigências da estratégia foram derivadas independentemente por Holevo [16] e Yuen *et al.* [17] e são dadas por

$$\hat{\Pi}_j(\eta_j\hat{\rho}_j - \eta_k\hat{\rho}_k)\hat{\Pi}_k = 0, \ \forall\ j,k, \tag{2.11}$$

$$\hat{\Gamma} - \eta_k\hat{\rho}_k \geq 0, \ \forall\ k, \tag{2.12}$$

onde

$$\hat{\Gamma} \equiv \sum_{j=0}^{N-1} \eta_j\hat{\rho}_j\hat{\Pi}_j \tag{2.13}$$

é conhecido como operador de Lagrange. As provas de que essas condições são suficientes e necessárias foram recentemente reelaboradas de forma mais simples do que a original nas referências [6, 18].

Exemplo: discriminação de dois estados puros equiprováveis de um *qubit*

A aplicação mais simples da estratégia EM é na discriminação de dois estados puros bidimensionais. Considere que Alice prepare um *qubit* em um dos estados

$$|\psi_0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \tag{2.14}$$

$$|\psi_1\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle, \tag{2.15}$$

com a mesma probabilidade, $\eta_0 = \eta_1 = \frac{1}{2}$, onde $0 \leq \theta \leq \pi/4$. Após a preparação, Alice envia seu estado para Bob, que deve realizar uma medição que forneça o resultado correto com o mínimo de erro possível. Aproveitando a simetria do problema, um bom "chute" para a formulação do POVM é colocar detectores de forma simétrica em relação aos estados, conforme a figura 2.1.

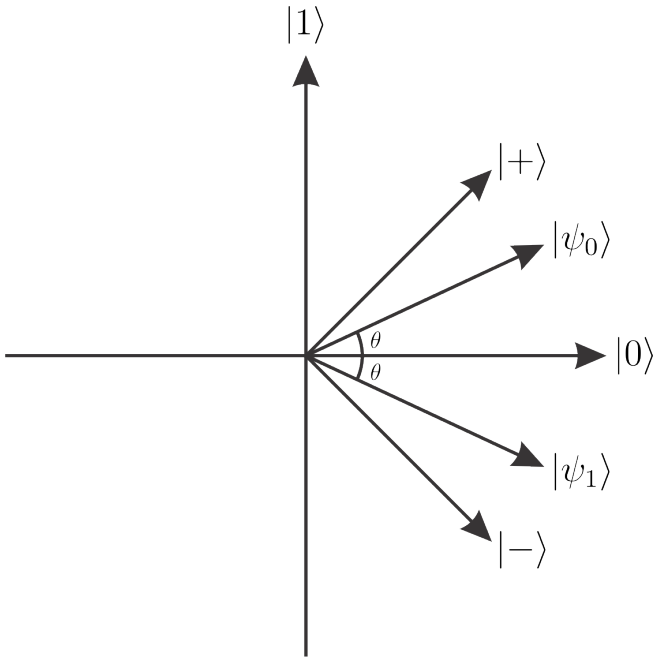

Figura 2.1: Estados equiprováveis preparados por Alice, $|\psi_0\rangle$ e $|\psi_1\rangle$, separados pelo ângulo de 2θ e a posição dos possíveis detectores, $|+\rangle$ e $|-\rangle$.

Os estados, $|+\rangle$ e $|-\rangle$ são dados por

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{2.16}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{2.17}$$

gerando os operadores de medição

$$\begin{aligned}\hat{\Pi}_0 &= |+\rangle\langle+| \\ &= \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|\right),\end{aligned} \tag{2.18}$$

$$\begin{aligned}\hat{\Pi}_1 &= |-\rangle\langle-| \\ &= \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| - |0\rangle\langle 1| - |1\rangle\langle 0|\right).\end{aligned} \tag{2.19}$$

Note que estes operadores satisfazem as condições de medições projetivas dadas na seção 2.1.1, já que são projetores ortogonais no espaço de Hilbert bidimensional. É claro que a inferência destes projetores foi formalmente deduzida [15, 46]. No presente contexto será demonstrado que eles satisfazem as condições (2.11) e (2.12), sendo assim realizadores da estratégia de erro mínimo.

Os operadores densidade $\hat{\rho}_0$ e $\hat{\rho}_1$ serão necessários para os cálculos, e são dados por

$$\begin{aligned}\hat{\rho}_0 &= |\psi_0\rangle\langle\psi_0| \\ &= \cos^2\theta|0\rangle\langle 0| + \sin^2\theta|1\rangle\langle 1| + \sin\theta\cos\theta\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right),\end{aligned} \tag{2.20}$$

$$\begin{aligned}\hat{\rho}_1 &= |\psi_1\rangle\langle\psi_1| \\ &= \cos^2\theta|0\rangle\langle 0| + \sin^2\theta|1\rangle\langle 1| - \sin\theta\cos\theta\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right).\end{aligned} \tag{2.21}$$

A primeira condição é facilmente verificada notando que

$$\begin{aligned}\eta_0\hat{\rho}_0 - \eta_1\hat{\rho}_1 &= \sin\theta\cos\theta\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) \\ &= \sin\theta\cos\theta\left(|+\rangle\langle+| - |-\rangle\langle-|\right),\end{aligned} \tag{2.22}$$

$$\begin{aligned}\eta_1\hat{\rho}_1 - \eta_0\hat{\rho}_0 &= -\sin\theta\cos\theta\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) \\ &= -\sin\theta\cos\theta\left(|+\rangle\langle+| - |-\rangle\langle-|\right).\end{aligned} \tag{2.23}$$

Inserindo esses resultados e as definições dos projetores na equação (2.11), tem-se

$$\begin{aligned}\hat{\Pi}_0(\eta_0\hat{\rho}_0 - \eta_1\hat{\rho}_1)\hat{\Pi}_1 &= \sin\theta\cos\theta\left(|+\rangle\langle+|+\rangle\langle+|-\rangle\langle-| - |+\rangle\langle+|-\rangle\langle-|-\rangle\langle-|\right) \\ &= 0,\end{aligned} \tag{2.24}$$

$$\begin{aligned}\hat{\Pi}_1(\eta_1\hat{\rho}_1 - \eta_0\hat{\rho}_0)\hat{\Pi}_0 &= -\sin\theta\cos\theta\left(|+\rangle\langle+|+\rangle\langle+|-\rangle\langle-| - |+\rangle\langle+|-\rangle\langle-|-\rangle\langle-|\right) \\ &= 0,\end{aligned} \tag{2.25}$$

o que explicita a satisfação da equação (2.11).

Os operadores $\hat{\rho}_j\hat{\Pi}_j$ $(j = 0, 1)$ são importantes tanto para a resolução da condição (2.12) quanto para a equação (2.10) e são dados por

$$\hat{\rho}_0\hat{\Pi}_0 = \frac{\cos^2\theta + \sin\theta\cos\theta}{2}(|0\rangle\langle 0| + |0\rangle\langle 1|) + \frac{\sin^2\theta + \sin\theta\cos\theta}{2}(|1\rangle\langle 1| + |1\rangle\langle 0|), \tag{2.26}$$

$$\hat{\rho}_1\hat{\Pi}_1 = \frac{\cos^2\theta + \sin\theta\cos\theta}{2}(|0\rangle\langle 0| - |0\rangle\langle 1|) + \frac{\sin^2\theta + \sin\theta\cos\theta}{2}(|1\rangle\langle 1| - |1\rangle\langle 0|). \tag{2.27}$$

O operador de Lagrange, equação (2.13), assume, então, a forma explícita

$$\hat{\Gamma} = \frac{\cos^2\theta + \sin\theta\cos\theta}{2}|0\rangle\langle 0| + \frac{\sin^2\theta + \sin\theta\cos\theta}{2}|1\rangle\langle 1|. \tag{2.28}$$

Inserindo esse resultado na equação (2.12) em conjunto com as definições de $\eta_k\hat{\rho}_k, k = 0, 1$, se tem

$$\begin{aligned}\hat{\Gamma} - \eta_0\hat{\rho}_0 &= \frac{\sin\theta\cos\theta}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|\right) \\ &= \sin\theta\cos\theta\hat{\Pi}_0 \\ &\geq 0,\end{aligned} \tag{2.29}$$

$$\begin{aligned}\hat{\Gamma} - \eta_1\hat{\rho}_1 &= \frac{\sin\theta\cos\theta}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| - |0\rangle\langle 1| - |1\rangle\langle 0|\right) \\ &= \sin\theta\cos\theta\hat{\Pi}_1 \\ &\geq 0,\end{aligned} \tag{2.30}$$

o que completa a prova de que os projetores propostos realizam a discriminação com erro mínimo.

A probabilidade de erro na detecção de Bob pode ser explicitamente calculada conforme a equação (2.10). Para isso, note que $\mathrm{Tr}(\hat{\Pi}_0\hat{\rho}_0) = \mathrm{Tr}(\hat{\Pi}_1\hat{\rho}_1) = 1/2 + \sin\theta\cos\theta$, e, portanto

$$\begin{aligned}P_{\text{erro}} &= 1 - \frac{1}{2}\left[\mathrm{Tr}(\hat{\Pi}_0\hat{\rho}_0) + \mathrm{Tr}(\hat{\Pi}_1\hat{\rho}_1)\right] \\ &= 1 - \frac{1}{2} - \sin\theta\cos\theta \\ &= \frac{1}{2}(1 - \sin 2\theta).\end{aligned} \tag{2.31}$$

A probabilidade de erro é explicitamente dependente do ângulo de separação entre os estados, conforme mostra o gráfico da figura 2.2. Quando o ângulo de separação dos estados é nulo a probabilidade de erro é equivalente a de adivinhar qual dos dois foi preparado sem realizar medição alguma, já que neste limite eles são idênticos e nenhum esquema de medição poderia fornecer informação sobre qual deles foi preparado. Quando $\theta = \pi/4$ os estados são ortogonais e, portanto, é possível distingui-los sem erros.

Encontrar POVMs que satisfaçam as equações (2.11) e (2.12) se mostra uma tarefa difícil. Poucos conjuntos de estados possuem soluções analíticas para a estratégia EM. Dentre eles, e de particular interesse, os conjuntos de estados simétricos equiprováveis, discutidos na referência [47]. Isto será abordada com maiores detalhes no próximo capítulo.

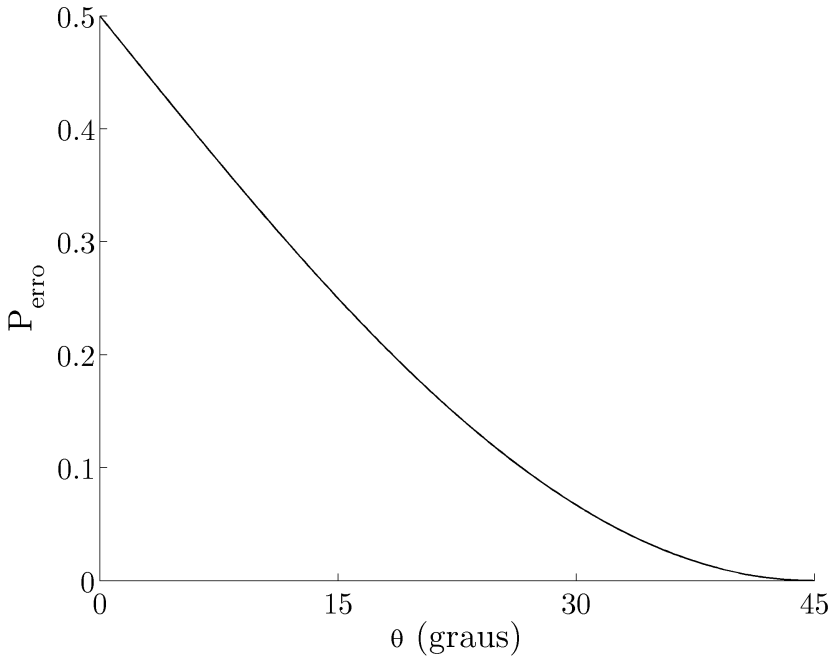

Figura 2.2: Gráfico que mostra a probabilidade de erro em função do ângulo de separação entre os estados $|\psi_0\rangle$ e $|\psi_1\rangle$.

2.2.2 Discriminação sem Ambiguidade

Discriminar entre estados não-ortogonais de forma inequívoca e determinística é impossível. Porém, admitindo-se a ocorrência de um resultado inconclusivo no processo de medição, se torna possível a identificação sem ambiguidade dos estados. A estratégia SA consiste em encontrar um POVM que permita identificar os estados inequivocamente e com probabilidade mínima de se obter um resultado inconclusivo.

Esse problema foi primeiramente investigado por Ivanovic [19], Dieks [20] e Peres [21], para o caso de dois estados puros e equiprováveis de um *qubit*, o qual é conhecido por problema IDP.[5] Posteriormente, a estratégia SA foi estendida a *qudits* [23, 49] e mostrou-se que ela se aplica somente a estados linearmente independentes.[6]

Para abordar o problema considere o conjunto de N estados puros linearmente independentes, $\{\hat{\rho}_j = |\psi_j\rangle\langle\psi_j| \mid j = 0, \ldots, N-1\}$, com respectivas probabilidades *a priori* η_j e onde espaço de Hilbert preenchido por eles é $\mathcal{H}$. O POVM que permite discriminar esses estados

[5] O problema IDP foi generalizado por Jaeger e Shimony [48] considerando estados com probabilidades *a priori* arbitrárias.

[6] Essa restrição é mostrada no apêndice B.

sem ambiguidade é descrito por

$$\hat{\Pi}_? + \sum_{j=0}^{N-1} \hat{\Pi}_j = \mathbb{1}, \tag{2.32}$$

onde cada elemento $\hat{\Pi}_j = \hat{A}_j^\dagger \hat{A}_j$ identifica o respectivo estado $|\psi_j\rangle$ sem erros. O elemento $\hat{\Pi}_? = \mathbb{1} - \sum_j \hat{\Pi}_j = \hat{A}_?^\dagger \hat{A}_?$ fornece um resultado inconclusivo e é necessário para relação de completeza ser satisfeita sempre que os estados $|\psi_j\rangle$ não forem ortogonais entre si. A condição de identificação livre de erros é expressada como

$$\mathrm{Tr}(\hat{\rho}_j \hat{\Pi}_k) = \langle\psi_j|\hat{A}_k^\dagger \hat{A}_k|\psi_j\rangle = p_j \delta_{jk}, \tag{2.33}$$

onde p_j é a probabilidade identificar o estado $|\psi_j\rangle$ sem ambiguidade. Dessa relação, pode-se inferir a forma dos operadores de detecção $\hat{A}_j$ como

$$\hat{A}_j = \frac{p_j^{1/2}}{\langle\psi_j^\perp|\psi_j\rangle} |\zeta_j\rangle\langle\psi_j^\perp|, \tag{2.34}$$

onde o conjunto de estados $\{|\psi_j^\perp\rangle\}$ satisfaz $\langle\psi_j^\perp|\psi_k\rangle = \delta_{jk}\langle\psi_j^\perp|\psi_j\rangle$ e o conjunto $\{|\zeta_j\rangle\}$ forma uma base ortonormal em $\mathcal{H}$. As probabilidades totais de sucesso em identificar corretamente o estado preparado ou de se obter um resultado inconclusivo são dadas, respectivamente, por

$$\begin{aligned} P_S &= \sum_{j=0}^{N-1} \eta_j \mathrm{Tr}(\hat{\rho}_j \hat{\Pi}_j) \\ &= \sum_{j=0}^{N-1} \eta_j p_j, \end{aligned} \tag{2.35}$$

$$\begin{aligned} P_? &= \sum_{j=0}^{N-1} \eta_j \mathrm{Tr}(\hat{\rho}_j \hat{\Pi}_?) \\ &= 1 - \sum_{j=0}^{N-1} \eta_j \mathrm{Tr}(\hat{\rho}_j \hat{\Pi}_j) \\ &= 1 - P_S. \end{aligned} \tag{2.36}$$

O POVM que cumpre as condições acima será ótimo para a estratégia SA se ele minimiza a probabilidade $P_?$ (ou, equivalentemente, maximiza P_S). Nessa situação é impossível de se realizar uma nova tentativa de execução da estratégia, já que isso implicaria em uma maior probabilidade de sucesso. Assim, após um resultado inconclusivo, o conjunto de estados inicial, $\{|\psi_k\rangle\}$, é mapeado em um conjunto de estados linearmente dependentes, os quais não podem ser discriminados sem ambiguidade [23] (veja também o apêndice B).

O teorema de Naimark pode ser utilizado para uma representação alternativa (e mais intuitiva) da estratégia. Estende-se o espaço de Hilbert inicial por produto tensorial com um

sistema auxiliar bidimensional no estado $|a\rangle_a$. Posteriormente, aplica-se a operação unitária que emaranha o estado dos dois sistemas, de modo que

$$\hat{\mathcal{U}}|\psi_j\rangle|a\rangle_a = \sqrt{p_j}|\zeta_j\rangle|0\rangle_a + \sqrt{1-p_j}|\xi_j\rangle|1\rangle_a. \tag{2.37}$$

Uma medição projetiva é feita para determinar o estado da *ancilla* após a evolução unitária. Se o estado $|0\rangle_a$ é encontrado, com probabilidade p_j, os estados $|\psi_j\rangle$ são mapeados no conjunto ortogonal $|\zeta_j\rangle$ e podem ser identificados sem ambiguidade. Nesse caso, o procedimento é considerado bem sucedido. Porém, se a *ancilla* é projetada em $|1\rangle_a$, com probabilidade $1-p_j$, o sistema inicial é mapeado nos estados $|\xi_j\rangle$, sendo esse caso identificado como falho. Se a estratégia for ótima, a probabilidade de falha é mínima e os estados $|\xi_j\rangle$ formam um conjunto de estados linearmente dependentes.

Exemplo: discriminação de dois estados puros equiprováveis de um *qubit*

Como no exemplo da seção anterior, o conjunto mais simples de estados que podem ser discriminados sem ambiguidade é formado por dois estados puros bidimensionais dados por

$$|\psi_0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \tag{2.38}$$

$$|\psi_1\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle, \tag{2.39}$$

com probabilidades *a priori* $\eta_0 = \eta_1 = \frac{1}{2}$. Alice envia o estado preparado a Bob, que deseja discriminá-los segundo a estratégia SA. No exemplo anterior, o trabalho de Bob era identificar o estado com a menor probabilidade de erro possível. Agora, Bob não admitirá erros em sua medição. Ele quer identificar o estado perfeitamente, mas, para isso ser possível, uma probabilidade de não identificar nenhum dos estados deve ser admitida. A melhor medição que Bob pode implementar é aquela que identifica o estado perfeitamente com a menor probabilidade possível de se obter um resultado inconclusivo.

Para realizar o processo de discriminação, Bob agrega uma *ancilla* no estado inicial $|0\rangle_a$ e aplica a operação unitária $\hat{\mathcal{U}}$ de tal modo que

$$\hat{\mathcal{U}}|\psi_0\rangle|0\rangle_a = \alpha|+\rangle|0\rangle_a + \beta|0\rangle|1\rangle_a, \tag{2.40}$$

$$\hat{\mathcal{U}}|\psi_1\rangle|0\rangle_a = \gamma|-\rangle|0\rangle_a + \delta|0\rangle|1\rangle_a, \tag{2.41}$$

onde $|+\rangle$ e $|-\rangle$ são os estados das equações (2.16) e (2.17), respectivamente. É importante salientar que operações que realizam essa transformação realmente existem. Um argumento geométrico para esse fato é discutido em [20]. Uma medição projetiva na *ancilla* indicando o estado $|0\rangle_a$ irá projetar o sistema em um dos estados ortogonais $|+\rangle$ ou $|-\rangle$, dependendo de qual estado foi preparado. Assim, Bob poderá inferir sem erro o estado preparado por Alice. Mas, se a medição da *ancilla* indicar o estado $|1\rangle_a$ o sistema será projetado no estado $|0\rangle$,

independentemente do estado preparado, sendo assim impossível discriminá-los com qualquer medição adicional. A otimização do protocolo é feita com a minimização probabilidade de falha, equação (2.36), o que equivale a encontrar os parâmetros α, β, γ e δ,[7] que definem a operação unitária $\hat{\mathcal{U}}$ do POVM ótimo. Explicitamente, a probabilidade de falha é dada por

$$\begin{aligned} P_? &= 1 - \frac{1}{2}\sum_{j=0}^{2} p_j \\ &= 1 - \frac{1}{2}\left(|\alpha|^2 + |\gamma|^2\right) \\ &= \frac{1}{2}\left(|\beta|^2 + |\delta|^2\right). \end{aligned} \tag{2.42}$$

Tomando o produto interno das equações (2.40) e (2.41), obtém-se a relação

$$|\beta|^2|\delta|^2 = |\langle\psi_0|\psi_1\rangle|. \tag{2.43}$$

Com esta, se torna fácil o cálculo do mínimo de $P_?$:

$$\begin{aligned} \frac{\mathrm{d}P_?}{\mathrm{d}\beta} &= \frac{\mathrm{d}}{\mathrm{d}\beta}\left(|\beta|^2 + \frac{|\langle\psi_0|\psi_1\rangle|^2}{|\beta|^2}\right) \\ &= |\beta| - \frac{|\langle\psi_0|\psi_1\rangle|^2}{|\beta|^3} \\ &= 0 \\ \therefore |\beta|^2 &= |\langle\psi_0|\psi_1\rangle|. \end{aligned} \tag{2.44}$$

É evidente que esse resultado se repete ao realizar o cálculo em relação a δ. Assim, a probabilidade mínima de falha é

$$\begin{aligned} [P_?]_{\min} &= |\langle\psi_0|\psi_1\rangle| \\ &= \cos 2\theta, \end{aligned} \tag{2.45}$$

conhecida como limite IDP. O gráfico da figura 2.3 mostra a relação da probabilidade mínima de falha de discriminação com o ângulo de separação entre os estados. Note que a probabilidade de sucesso para $\theta = 0$ é nula. Isso se deve ao fato de que neste limite os estados $|\psi_0\rangle$ e $|\psi_1\rangle$ são linearmente dependentes, o que impossibilita a discriminação SA. Quando $\theta = \pi/4$ a probabilidade de falha é zero, já que os estados são ortogonais. Nesse limite, o POVM que realiza a estratégia SA é simplesmente uma medição projetiva.

Além do problema de dois estados puros bidimensionais, conjuntos de estados simétricos equiprováveis d-dimensionais possuem solução analítica para os elementos de POVM que realizam a discriminação SA ótima [50]. No próximo capítulo esse resultado será discutido como um caso especial da estratégia CM apresentada a seguir.

[7] Submetidos aos vínculos $\alpha^2 = 1 - \beta^2$ e $\gamma^2 = 1 - \delta^2$.

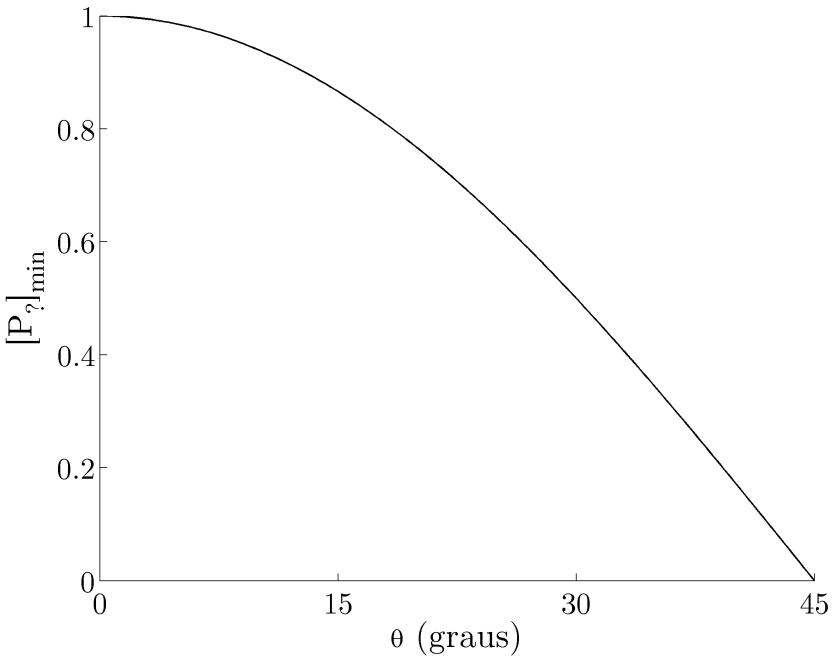

Figura 2.3: Variação do limite IDP, probabilidade de mínima de falha, em função do ângulo de separação dos estados $|\psi_0\rangle$ e $|\psi_1\rangle$.

2.2.3 Discriminação com Confiança Máxima

Nem sempre é possível distinguir um conjunto de estados sem ambiguidades associadas aos resultados das medições. Este é o caso, por exemplo, quando os estados são linearmente dependentes. Entretanto, é possível reelaborar o problema para se obter uma distinção de estados com a maior confiança possível. Assim, dado o conjunto $\{\hat{\rho}_j \mid j = 0, \ldots, N-1\}$, com probabilidades *a priori* η_j, se quer maximizar a confiança do resultado de uma medição realizada pelo POVM $\{\hat{\Pi}_j\}$. A probabilidade condicional $P(\hat{\rho}_j|\omega_j)$ faz o papel de quantificar a confiança da medição, onde ω_j indica o resultado associado ao operador $\hat{\Pi}_j$. Esta é interpretada como a probabilidade do estado $\hat{\rho}_j$ ter sido preparado, dado que o resultado da medição do sistema seja ω_j. A regra de Bayes [3, 24] fornece

$$P(\hat{\rho}_j|\omega_j) = \frac{P(\hat{\rho}_j)P(\omega_j|\hat{\rho}_j)}{P(\omega_j)}, \tag{2.46}$$

onde $P(\hat{\rho}_j)$ é a probabilidade de preparação do estado $\hat{\rho}_j$, $P(\omega_j|\hat{\rho}_j)$ é a probabilidade de se obter o resultado de medição ω_j, dado que o estado preparado é $\hat{\rho}_j$ e $P(\omega_j)$ é a probabilidade total de ocorrência do resultado ω_j. Portanto

$$P(\hat{\rho}_j|\omega_j) = \frac{\eta_j \mathrm{Tr}(\hat{\Pi}_j\hat{\rho}_j)}{\mathrm{Tr}(\hat{\Pi}_j\hat{\rho})}, \tag{2.47}$$

com $\hat{\rho} = \sum_j \eta_j \hat{\rho}_j$.

A maximização da confiança da medição, equação (2.47), em relação a cada operador $\hat{\Pi}_j$ é conhecida como discriminação com confiança máxima. A solução deste problema, dada por Croke *et al.* [24], possui forma explícita para conjuntos de estados puros dada por

$$\begin{aligned} \hat{\Pi}_j &= \frac{\mathrm{Tr}(\hat{\Pi}_j \hat{\rho})}{\mathrm{Tr}(\hat{\rho}^{-1}\hat{\rho}_j)} \hat{\rho}^{-1}\hat{\rho}_j\hat{\rho}^{-1} \\ &= a_j \hat{\rho}^{-1}\hat{\rho}_j\hat{\rho}^{-1}. \end{aligned} \tag{2.48}$$

Inserindo esse resultado na equação (2.47), tem-se

$$[P(\hat{\rho}_j|\omega_j)]_{\max} = \eta_j \mathrm{Tr}(\hat{\rho}_j\hat{\rho}^{-1}). \tag{2.49}$$

Mesmo com os operadores $\hat{\Pi}_j$ bem definidos, não é possível afirmar se o conjunto $\{\hat{\Pi}_j\}$ respeita a condição de completeza do postulado 2*b*, seção 2.1.2. As constantes $a_j \propto \mathrm{Tr}(\hat{\Pi}_j\hat{\rho}) = P(\omega_j)$ da equação (2.48) não afetam a confiança da medição e podem ser escolhidas livremente. Mas, ainda assim existem casos que nenhuma escolha dessas constantes garante que os operadores $\hat{\Pi}_j$ formem um POVM. Nesses casos, se torna necessário um elemento de POVM adicional, $\hat{\Pi}_?$, o qual é responsável por um resultado inconclusivo. Esse operador é dado por $\hat{\Pi}_? = \mathbb{1} - \sum_j \hat{\Pi}_j$ e, para otimizar o processo, este deve minimizar a probabilidade total de um resultado inconclusivo, $P_? = \mathrm{Tr}(\hat{\Pi}_?\hat{\rho})$, sujeito ao vínculo $\hat{\Pi}_? \geq 0$. Ou seja, a estratégia CM ótima é aquela que maximiza a confiança de identificação de cada estado do conjunto independentemente e minimiza a probabilidade total de um resultado inconclusivo. Se a confiança for 1 para todos os estados, essa estratégia se reduz à estratégia SA. Isso ocorrerá sempre que os estados a serem discriminados forem linearmente independentes.

Exemplo: discriminação de três estados puros equiprováveis de um *qubit*

Os exemplos das seções anteriores mostraram o caso mais simples de aplicação das estratégias EM e SA, que consistia em discriminar dois estados puros e equiprováveis de um *qubit*, os quais são linearmente independentes. Uma vez que a estratégia CM se reduz a SA para conjuntos de estados linearmente independentes, o exemplo mais simples de aplicação da discriminação via CM é feito com três estados puros e equiprováveis de um *qubit*. Considere, então, que Alice prepara, com probabilidade 1/3, um *qubit* em um dos três estados dados por

$$|\psi_j\rangle = \cos\theta|0\rangle + e^{\frac{2i\pi j}{3}} \sin\theta|1\rangle, \tag{2.50}$$

com $j = 0, 1, 2$ e $0 \leq \theta \leq \pi/4$. Como esses estados são linearmente dependentes, certamente não haverá como Bob realizar uma medição SA para distinguir entre eles. Porém, é possível

distinguí-los com a maior confiança possível. Para esses estados específicos, se tem

$$\begin{aligned}\hat{\rho} &= \frac{1}{3}\sum_{j=0}^{2}|\psi_j\rangle\langle\psi_j| \\ &= \cos^2\theta|0\rangle\langle 0| + \sin^2\theta|1\rangle\langle 1|\end{aligned} \tag{2.51}$$

e, portanto

$$\hat{\rho}^{-1} = \sec^2\theta|0\rangle\langle 0| + \csc^2\theta|1\rangle\langle 1|. \tag{2.52}$$

Os operadores que realizam a discriminação CM são calculados diretamente pela equação (2.48), e são dados por

$$\hat{\Pi}_j = a_j|\phi_j\rangle\langle\phi_j|, \tag{2.53}$$

onde

$$|\phi_j\rangle = \sec\theta|0\rangle + e^{\frac{2i\pi j}{3}}\csc\theta|1\rangle. \tag{2.54}$$

A confiança na identificação do estado $|\psi_j\rangle$ obtida com esses operadores, de acordo com a equação (2.49), é

$$[P(\hat{\rho}_j|\omega_j)]_{\max} = \frac{2}{3}. \tag{2.55}$$

Os estados $|\psi_j\rangle$ e $|\phi_j\rangle$ podem ser vistos na figura 2.4. Devido à simetria do problema, onde os estados estão igualmente espaçados na esfera de Bloch, espera-se que a probabilidade total de ocorrência do resultado ω_j, $P(\omega_j)$, seja a mesma para todos eles. Como a_j é proporcional a $P(\omega_j)$ [veja equação (2.48)], assume-se[8] $a_0 = a_1 = a_2 = a$.

Os elementos $\hat{\Pi}_j$ em (2.53) não formam um POVM independentemente da escolha de a (exceto quando $\theta = \pi/4$). Portanto, é necessário um elemento adicional, $\hat{\Pi}_?$, identificado aqui como o responsável pela falha na tentativa de discriminação, dado por

$$\begin{aligned}\hat{\Pi}_? &= \mathbb{1} - \sum_{j=0}^{2}\hat{\Pi}_j \\ &= \left(1 - \frac{3a}{\cos^2\theta}\right)|0\rangle\langle 0| + \left(1 - \frac{3a}{\sin^2\theta}\right)|1\rangle\langle 1|.\end{aligned} \tag{2.56}$$

Da forma explícita de $\hat{\Pi}_?$, é calculada a probabilidade de obter-se um resultado inconclusivo, sendo esta

$$\begin{aligned}P_? &= \mathrm{Tr}(\hat{\Pi}_?\hat{\rho}) \\ &= 1 - 6a.\end{aligned} \tag{2.57}$$

[8] Os estados $|\psi_j\rangle$ e $|\phi_j\rangle$ satisfazem, de fato, as condições de estados simétricos equiprováveis. Essa simetria será explorada em detalhes no próximo capítulo, deixando a suposição de $a_0 = a_1 = a_2 = a$ mais palpável. Ainda, é possível chegar nessa conclusão resolvendo um problema variacional sob o vínculo $\hat{\Pi}_? \geq 0$, conforme apontado em [24].

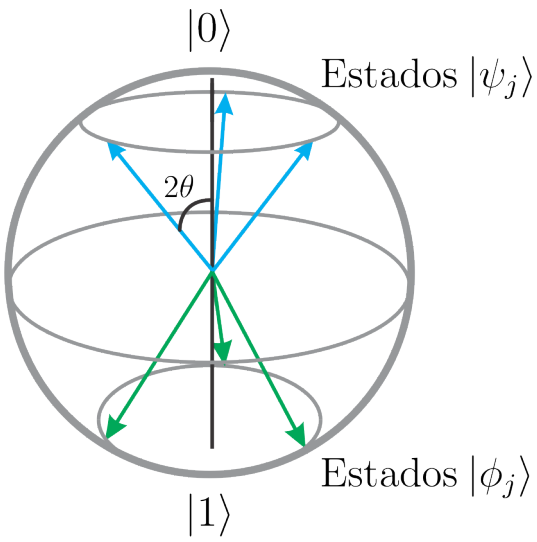

Figura 2.4: Representação dos estados $|\psi_j\rangle$ (azul), dados na equação (2.50), e $|\phi_j\rangle$ (verde), equação (2.54), na esfera de Bloch.

Portanto, quanto maior for o coeficiente a, menor será a probabilidade de falha. Como $\hat{\Pi}_?$ é um elemento de POVM, a positividade dele deve ser respeitada. De acordo com a equação (2.56), isso impõe que $a \leq (\sin^2\theta)/3$, já que $0 \leq \theta \leq \pi/4$. Assim, o processo de discriminação CM é otimizado com o coeficiente $a = (\sin^2\theta)/3$, e a probabilidade mínima de falha é dada por

$$[P_?]_{\min} = 1 - 2\sin^2\theta. \tag{2.58}$$

O gráfico da figura 2.5 mostra como a probabilidade de falha do procedimento diminui com o aumento do ângulo de separação entre os estados, atingindo seu mínimo em $\theta = \pi/4$. Nesse limite o elemento de POVM $\hat{\Pi}_?$ é nulo, o que indica que a medição sempre identifica o estado com a confiança máxima dada pela equação (2.55). O outro limite, onde $\theta = 0$ e $[P_?]_{\min} = 1$, indica que nenhuma medição pode fornecer informações sobre qual estado foi preparado.

Assim como nos casos anteriores, resultados analíticos para esse problema também são escassos. Estados simétricos equiprováveis bidimensionais são analisados na referência [24] e d-dimensionais na referência [42], os quais serão abordados no próximo capítulo.

2.2.4 Separação de Estados Quânticos

Qualquer estratégia de discriminação ótima de estados não-ortogonais poderá apresentar resultados errôneos ou inconclusivos. Foram apresentadas estratégias onde se tem como objetivo minimizar os erros sem admitir inconclusões (EM) ou maximizar a confiança tanto quanto possível às custas de resultados inconclusivos (CM e SA). Como alternativa, é possível

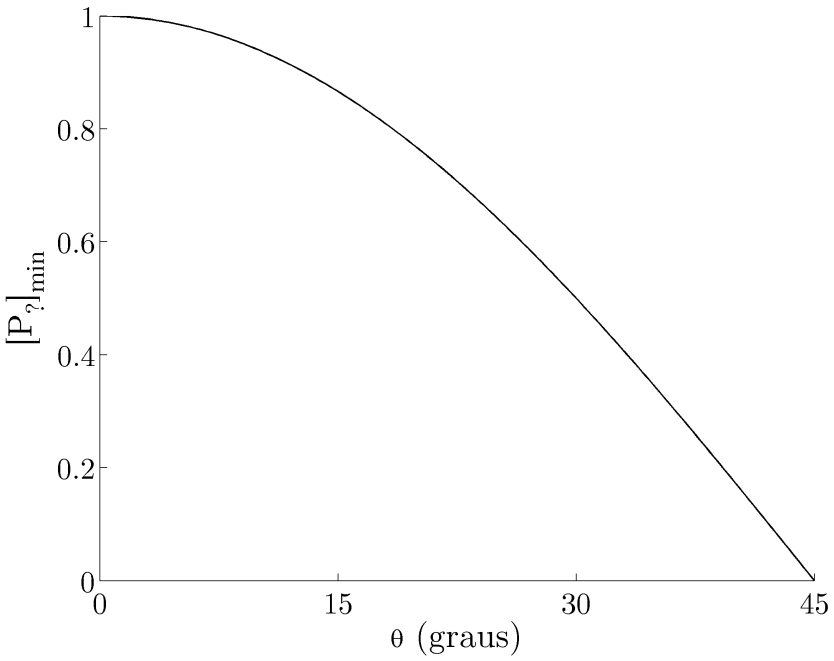

Figura 2.5: Probabilidade de se obter um resultado inconclusivo em função da separação entre os estados $|\psi_j\rangle$.

criar estratégias intermediárias às apresentadas nas seções anteriores. Uma possibilidade é fixar a probabilidade total de erro das medições abaixo daquela encontrada com a estratégia EM, ao custo de se introduzir resultados inconclusivos. Outra, é ter uma probabilidade de falha menor do que aquela encontrada na estratégia CM (SA), ao custo de diminuir a confiança da medição. A primeira abordagem para o problema, feita por Chefles e Barnnett [51], resolve a distinção entre dois estados puros bidimensionais com a probabilidade de falha fixada abaixo do limite IDP, equação (2.45). Mais tarde, os mesmos autores revisitaram o problema [52], abordando-o no contexto de separação de estados quânticos.

Para melhor compreensão desta abordagem, lembre-se da utilização do teorema de Naimark para a realização da discriminação SA, equação (2.37). Nesta, os estados de entrada, $|\psi_j\rangle$, são mapeados, com a medição da *ancilla*, em um conjunto de estados ortogonais, $|\zeta_j\rangle$, ou em estados linearmente dependentes, $|\xi_j\rangle$, os quais são menos distinguíveis[9] do que os estados de entrada. No caso de sucesso os estados iniciais se tornam perfeitamente distinguíveis. Então, quando se fala de separação de estados tem-se como intenção mapear um conjunto de estados iniciais num outro conjunto com estados mais distinguíveis, mas não necessariamente com os estados maximamente distinguíveis como no caso das estratégias SA e CM.

[9]Essa expressão indica que o *overlap* entre os estados iniciais aumentou. Ou seja, $|\langle\xi_j|\xi_k\rangle| > |\langle\psi_j|\psi_k\rangle|, \forall\, j \neq k$.

Quando esse for o caso, a probabilidade de falha será menor do que aquela onde os estados são maximamente distinguíveis.

O problema geral para separar N estados d-dimensionais, com $N \geq d$, pode ser descrito em termos dos operadores de detecção

$$\sum_{j=0}^{N-1} \hat{A}_j \hat{A}_j^\dagger + \hat{A}_? \hat{A}_?^\dagger = \mathbb{1}, \tag{2.59}$$

com

$$\hat{A}_j |\psi_j\rangle = \sqrt{p_j}|v_j\rangle, \tag{2.60}$$

$$\hat{A}_? |\psi_j\rangle = \sqrt{1-p_j}|\xi_j\rangle, \tag{2.61}$$

onde p_j é a probabilidade de sucesso da separação dos estados. Os estados $|v_j\rangle$ formam um conjunto de estados mais distinguíveis (ou separados) do que os $|\psi_j\rangle$. Já os $|\xi_j\rangle$ formam um conjunto de estados menos separados do que os $|\psi_j\rangle$. A forma explícita dos operadores e das probabilidades pode ser construída de duas formas equivalentes: i) fixa-se a probabilidade de falha, abaixo do limite ótimo (SA ou CM), e constroem-se os operadores $\hat{A}_j$ de tal modo que forneçam o erro mínimo possível após uma separação bem sucedida [51]. ii) Fixa-se uma margem de erro e calcula-se a mínima probabilidade de falha vinculada à condição de positividade do operador $\hat{\Pi}_?$ [53].

Exemplo: interpolação entre as estratégias EM e SA na discriminação de dois estados puros equiprováveis de um *qubit*

Considere novamente os dois estados puros bidimensionais equiprováveis dados pelas equações

$$|\psi_0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \tag{2.62}$$

$$|\psi_1\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle, \tag{2.63}$$

Estratégias intermediárias que interpolam entre a discriminação via EM e SA serão desenvolvidas no contexto de separação de estados quânticos. Considere a seguinte transformação, segundo o teorema de Naimark

$$\hat{\mathcal{U}}|\psi_j\rangle|0\rangle_a = \sqrt{P_{Sj}}|v_j\rangle|0\rangle_a + \sqrt{1-P_{Sj}}|0\rangle|1\rangle_a, \tag{2.64}$$

onde

$$|v_j\rangle = \cos\phi|0\rangle + e^{i\pi j}\sin\phi|1\rangle, \tag{2.65}$$

com $\theta \leq \phi \leq \pi/4$ e $j = 0, 1$. Essa transformação é responsável por aumentar o ângulo de separação entre os estados $|\psi_j\rangle$. A figura 2.6 esquematiza o procedimento. Pela simetria do problema, e de modo análogo ao exemplo da seção 2.2.2, as probabilidades de sucesso P_{Sj}

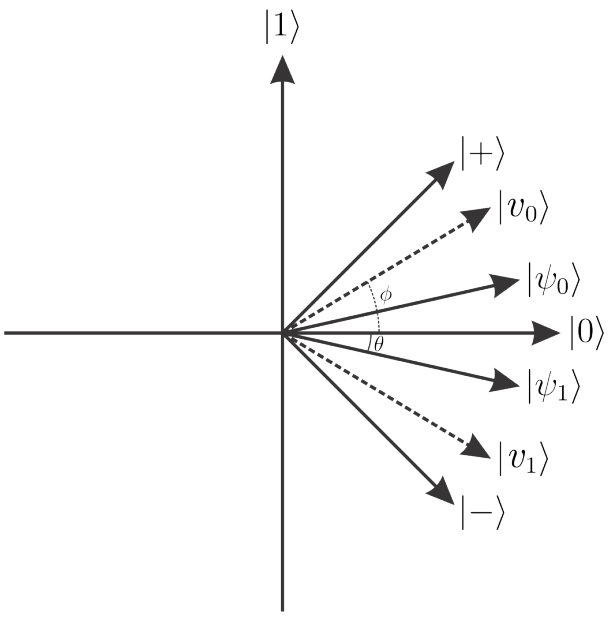

Figura 2.6: Representação dos estados iniciais, $|\psi_j\rangle$, e dos estados após uma separação bem sucedida $|v_0\rangle$ e $|v_1\rangle$.

serão independentes do estado preparado, portanto $P_{S0} = P_{S1} = P_S$. Tomando o produto interno entre os estados transformados, equação (2.64), tem-se

$$\langle\psi_0|\psi_1\rangle = P_S\langle v_0|v_1\rangle + 1 - P_S, \tag{2.66}$$

e, usando (2.62), (2.63) e (2.65), se obtém

$$\begin{aligned} P_S &= \frac{1 - \langle\psi_0|\psi_1\rangle}{1 - \langle v_0|v_1\rangle} \\ &= \frac{1 - \cos 2\theta}{1 - \cos 2\phi}. \end{aligned} \tag{2.67}$$

Esse resultado recupera o limite de máxima probabilidade de sucesso de separação encontrado de maneira mais rigorosa em [51]. Esse limite pode ser expressado em termos do limite IDP, $[P_S]_{\text{IDP}} = 1 - \langle\psi_0|\psi_1\rangle$, de modo que

$$P_S = \frac{[P_S]_{\text{IDP}}}{1 - \langle v_0|v_1\rangle} \geq [P_S]_{\text{IDP}}. \tag{2.68}$$

A igualdade se dá para $\langle v_0|v_1\rangle = 0$, que é a separação atingida na discriminação SA.

A figura 2.7 mostra o gráfico da probabilidade de sucesso da separação dos estados e o erro mínimo de discriminação após uma separação bem sucedida, equação (2.31), em função do ângulo de separação final, ϕ. Note que esse possui como limites o resultado da discriminação EM para $\phi = \theta$ e da discriminação SA para $\phi = \pi/4$. Para qualquer outro valor de ϕ,

$P_S > [P_S]_{\text{IDP}}$ e $P_{\text{erro}} < P_{\text{erro}}^{\text{EM}}$. Desse modo, é possível fixar a probabilidade de sucesso acima da probabilidade máxima de sucesso da estratégia SA às custas de admitir-se erros no resultado da medição. Outra possibilidade é definir o erro máximo abaixo do limite EM admitindo-se uma probabilidade de falha na estratégia.

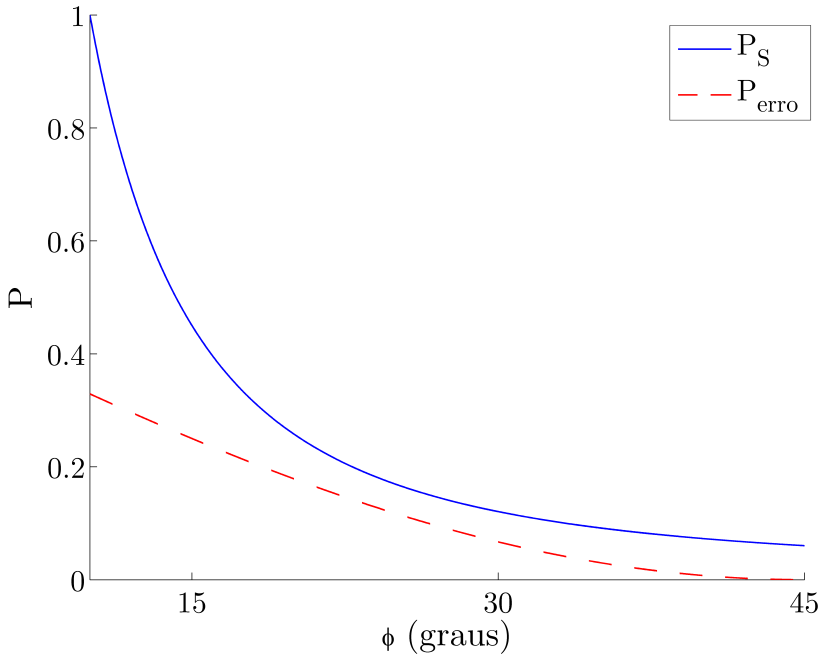

Figura 2.7: Variação, em função de ϕ, da probabilidade de sucesso de separação dos estados $|\psi_j\rangle$ e da probabilidade de se obter um resultado errôneo na medição após uma separação de estados bem sucedida. Para a construção do gráfico os estados iniciais foram considerados como separados por um ângulo de 20°, ou seja, $\theta = 10°$.

Como observado, a separação de estados quânticos pode ser utilizada na realização de estratégias que interpolam entre EM e SA (ou CM). Ainda, se a medição após a separação for ignorada, esse pode ser um método para separar estados antes de utilizá-los para outro fim, como, por exemplo, a concentração de emaranhamento [22, 23]. No próximo capítulo será explorada a separação paramétrica de estados simétricos equiprováveis, elaborada por Solís-Prosser *et al.* na referência [43].

3

Discriminação de Estados Simétricos Equiprováveis

Estados simétricos não-ortogonais e equiprováveis são uma classe de estados quânticos que desempenham um papel importante no estudo de protocolos de informação quântica. Eles aparecem, por exemplo, ao se tratar de problemas como teleportação quântica [37, 54, 55], troca de emaranhamento [38, 56] e codificação superdensa [12, 14] via canais parcialmente emaranhados. Então, a capacidade de discriminar estados simétricos está diretamente relacionada à capacidade de se executar esses protocolos de forma ótima. Soluções analíticas para a discriminação desses estados são conhecidas para as estratégias EM [47], SA [50] e CM [42], assim como para separação de estados [43], introduzidas no capítulo anterior. Essas soluções serão apresentadas neste capítulo e utilizadas nos capítulos posteriores como ferramentas para o estudo dos protocolos mencionados acima.

3.1 Estados Simétricos Equiprováveis

O conjunto de estados $\{|\psi_j\rangle \mid j = 0, \ldots, N-1\}$, que gera o espaço de Hilbert d-dimensional $\mathcal{H}_d$, onde $N \geq d$, é classificado como simétrico se existe uma transformação unitária $\hat{U}$ em $\mathcal{H}_d$ que satisfaz

$$|\psi_j\rangle = \hat{U}^j|\psi_0\rangle = \hat{U}|\psi_{j-1}\rangle, \tag{3.1}$$

$$|\psi_0\rangle = \hat{U}|\psi_{N-1}\rangle, \tag{3.2}$$

$$\hat{U}^N = \mathbb{1}_d, \tag{3.3}$$

onde o estado que gera os demais, $|\psi_0\rangle$, é denominado de estado fiducial. Sendo $\{|m\rangle \mid m = 0, \ldots, d-1\}$, a base que diagonaliza $\hat{U}$, escreve-se esse operador como

$$\hat{U} = \sum_{m=0}^{d-1} e^{\frac{2i\pi m}{N}} |m\rangle\langle m|. \tag{3.4}$$

Escrevendo os N estados simétricos do conjunto $\{|\psi_j\rangle\}$ nesta mesma base, tem-se

$$|\psi_0\rangle = \sum_{m=0}^{d-1} c_m |m\rangle, \tag{3.5}$$

$$|\psi_j\rangle = \hat{U}^j |\psi_0\rangle = \sum_{m=0}^{d-1} c_m e^{\frac{2i\pi jm}{N}} |m\rangle, \tag{3.6}$$

onde os coeficientes c_m são normalizados, isto é $\sum_m |c_m|^2 = 1$.

O operador densidade que descreve a preparação desses estados com probabilidades *a priori* η_j é dado por

$$\hat{\rho} = \sum_{j=0}^{N-1} \eta_j |\psi_j\rangle\langle\psi_j|. \tag{3.7}$$

Quando as probabilidades de preparação η_j são idênticas, ou seja $\eta_j = 1/N, \forall\, j$, o conjunto de estados simétricos é caracterizado como equiprovável. Usando as equações (3.6) e (3.7) escreve-se explicitamente o operador densidade que descreve essa situação como

$$\begin{aligned}
\hat{\rho} &= \frac{1}{N} \sum_{j=0}^{N-1} |\psi_j\rangle\langle\psi_j| \\
&= \frac{1}{N} \sum_{m,n=0}^{d-1} c_m c_n^* \left[\sum_{j=0}^{N-1} e^{\frac{2i\pi j(m-n)}{N}} \right] |m\rangle\langle n| \\
&= \frac{1}{N} \sum_{m,n=0}^{d-1} c_m c_n^* \left[N\delta_{mn} \right] |m\rangle\langle n| \\
&= \sum_{m=0}^{d-1} |c_m|^2 |m\rangle\langle m|,
\end{aligned} \tag{3.8}$$

onde foi utilizada a identidade da soma das raízes da unidade, equação (1.34), na parte entre colchetes. Dado esse conjunto de estados, o trabalho de Bob é discriminar entre eles da melhor maneira possível segundo alguma figura de mérito previamente estabelecida.

A seguir serão apresentadas duas estratégias distintas, EM e CM, para se discriminar entre estados simétricos equiprováveis. A discriminação SA se resume a um caso particular da discriminação CM. Ainda, serão apresentadas estratégias que interpolam entre EM e CM que utilizam a separação de estados.

3.2 Estratégia de Erro Mínimo

A estratégia EM, descrita na seção 2.2.1, tem como objetivo identificar estados quânticos deterministicamente com a menor probabilidade média de erros associada às medições. O

POVM que cumpre essas condições na discriminação de N estados simétricos equiprováveis, descrito por Ban *et al.* [47], é dado por

$$\hat{\Pi}_j = |\mu_j\rangle\langle\mu_j|, \tag{3.9}$$

onde

$$|\mu_j\rangle = \hat{\Upsilon}^{-1/2}|\psi_j\rangle, \tag{3.10}$$

com $|\psi_j\rangle$ dado pela equação (3.6) e

$$\hat{\Upsilon} = \sum_{j=0}^{N-1} |\psi_j\rangle\langle\psi_j|. \tag{3.11}$$

A prova de que esses operadores satisfazem as condições (2.11) e (2.12) é dada no apêndice C.

Tomando a definição da transformação unitária $\hat{U}$, equação (3.4), e os estados simétricos equiprováveis $|\psi_j\rangle$, dados pela equação (3.8), pode-se escrever explicitamente o POVM que realiza a discriminação EM. Por simplicidade, considere todos os coeficientes c_m como reais e não-negativos.[1] Inserindo essas definições na equação (3.11), tem-se

$$\begin{aligned}
\hat{\Upsilon} &= \sum_{j=0}^{N-1} |\psi_j\rangle\langle\psi_j| \\
&= \sum_{j=0}^{N-1} \sum_{m,n=0}^{d-1} c_m c_n e^{\frac{2i\pi l(m-n)}{N}} |m\rangle\langle n| \\
&= N \sum_{m,n=0}^{d-1} c_m c_n \delta_{mn} |m\rangle\langle n| \\
&= N \sum_{m=0}^{d-1} c_m^2 |m\rangle\langle m|,
\end{aligned} \tag{3.12}$$

onde a identidade oriunda da soma das raízes da unidade, equação (1.34), foi utilizada. Como o operador $\hat{\Upsilon}$ está em sua decomposição espectral na equação (3.12), o estado $|\mu_j\rangle$, de acordo

[1] É claro que estas considerações parecem retirar a generalidade do problema. Mas, como será visto na seção 3.3.1, as fases que esses coeficientes carregam poderiam ser removidas com uma operação unitária. Além disso, os estados aos quais as estratégias de discriminação serão aplicadas terão coeficientes oriundos de estados emaranhados descritos na decomposição de Schmidt, os quais sempre podem ser escolhidos como reais e não-negativos.

com a equação (3.10), é simplesmente

$$\begin{aligned} |\mu_j\rangle &= \hat{\Upsilon}^{-1/2}|\psi_j\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{m,n=0}^{d-1} e^{\frac{2i\pi jm}{N}} \frac{c_m}{c_n} |n\rangle\langle n|m\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{m=0}^{d-1} e^{\frac{2i\pi jm}{N}} |m\rangle. \end{aligned} \tag{3.13}$$

Com isso, calculam-se os elementos de POVM dados pela equação (3.9):

$$\begin{aligned} \hat{\Pi}_j &= |\mu_j\rangle\langle\mu_j| \\ &= \frac{1}{N} \sum_{m,n=0}^{d-1} e^{\frac{2i\pi j(m-n)}{N}} |m\rangle\langle n|. \end{aligned} \tag{3.14}$$

Portanto, a probabilidade média de erro, equação (2.10), será

$$\begin{aligned} P_{\text{erro}} &= 1 - \sum_{j=0}^{N-1} \eta_j \text{Tr}(\hat{\Pi}_j \hat{\rho}_j) \\ &= 1 - \frac{1}{N} \sum_{j=0}^{N-1} \left(\frac{1}{N} \sum_{m,n=0}^{d-1} c_m c_n \right) \\ &= 1 - \frac{1}{N} \left(\sum_{m=0}^{d-1} c_m \right)^2. \end{aligned} \tag{3.15}$$

De acordo com o teorema de Naimark, seção 2.1.3, a implementação física do POVM $\{\hat{\Pi}_j\}$ pode ser feita através de medições projetivas em um espaço de Hilbert estendido. Para a estratégia EM será utilizada a extensão por soma direta. Considere a seguinte medição projetiva no espaço de Hilbert N-dimensional ($\mathcal{H}_N$)

$$\hat{\Pi}'_j = |\mu'_j\rangle\langle\mu'_j|, \tag{3.16}$$

onde os estados da base ortonormal $\{|\mu'_j\rangle\}$ são dados por

$$\begin{aligned} |\mu'_j\rangle &= \hat{\mathcal{F}}_N |j\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} e^{\frac{2i\pi jm}{N}} |m\rangle \\ &= |\mu_j\rangle + \frac{1}{\sqrt{N}} \sum_{m=d}^{N-1} e^{\frac{2i\pi jm}{N}} |m\rangle, \end{aligned} \tag{3.17}$$

onde $j = 0, \ldots, N-1$, e $\hat{\mathcal{F}}_N$ é a transformada de Fourier discreta, equação(1.24), atuando em $\mathcal{H}_N$. Quando $N = d$, $|\mu_j\rangle = |\mu'_j\rangle$, e o POVM ótimo se reduz a uma medição projetiva.

Quando $N > d$, os estados $|\mu_j\rangle$ em (3.13) não são ortogonais nem normalizados, e, assim, os operadores $\hat{\Pi}_j$ em (3.14) formam um POVM. Os projetores (3.16) com os estados estendidos $|\mu'_j\rangle$ formam a medição projetiva em $\mathcal{H}_N$ que realiza este POVM em $\mathcal{H}_d$. Isso é facilmente verificado, calculando-se a probabilidade média de erro utilizando $\hat{\Pi}'_j$

$$\begin{aligned} P_{\text{erro}} &= 1 - \frac{1}{N}\sum_{j=0}^{N-1} \text{Tr}(\hat{\Pi}'_j \hat{\rho}_j) \\ &= 1 - \frac{1}{N}\left(\sum_{m=0}^{d-1} c_m\right)^2, \end{aligned} \tag{3.18}$$

que recupera o resultado da equação (3.15).

Exemplo: discriminação de três estados simétricos puros equiprováveis de um *qubit*

O exemplo da seção 2.2.3, onde é realizada a discriminação via CM de três estados puros bidimensionais equiprováveis, pode ser revisitado no contexto da estratégia EM. Os estados dados por

$$|\psi_j\rangle = \cos\theta|0\rangle + e^{\frac{2i\pi j}{3}} \sin\theta|1\rangle, \tag{3.19}$$

$j = 0, 1, 2$, satisfazem as condições de simetria das equações (3.1)–(3.3). Assim, medições com erro mínimo podem ser realizadas com o POVM dado pelas equações (3.9)–(3.11). Os estados não normalizados $|\mu_j\rangle$ assumem a forma explícita

$$|\mu_j\rangle = \frac{1}{\sqrt{3}}\left[|0\rangle + e^{\frac{2i\pi j}{3}}|1\rangle\right] \propto \frac{1}{\sqrt{2}}\left[|0\rangle + e^{\frac{2i\pi j}{3}}|1\rangle\right]. \tag{3.20}$$

A figura 3.1 mostra a posição dos vetores da equação (3.20) na esfera de Bloch, assim como os estados simétricos da equação (3.19) e a posição dos vetores que formam os elementos de POVM da estratégia CM, equação (2.54).

A probabilidade média de erro associada a uma medição utilizando a estratégia EM, de acordo com a equação (3.15), será

$$\begin{aligned} P_{\text{erro}} &= 1 - \frac{1}{3}\sum_{j=0}^{2} \text{Tr}(\hat{\Pi}_j \hat{\rho}_j) \\ &= \frac{2}{3}\left(1 - \frac{\sin 2\theta}{2}\right), \end{aligned} \tag{3.21}$$

e está mostrada na figura 3.2 em função do ângulo de separação dos estados a serem discriminados, θ.

Como esse exemplo foi resolvido na seção 2.2.3 no contexto da estratégia CM, é possível compará-lo com a solução da estratégia EM. Para isso, serão comparadas as confianças e as

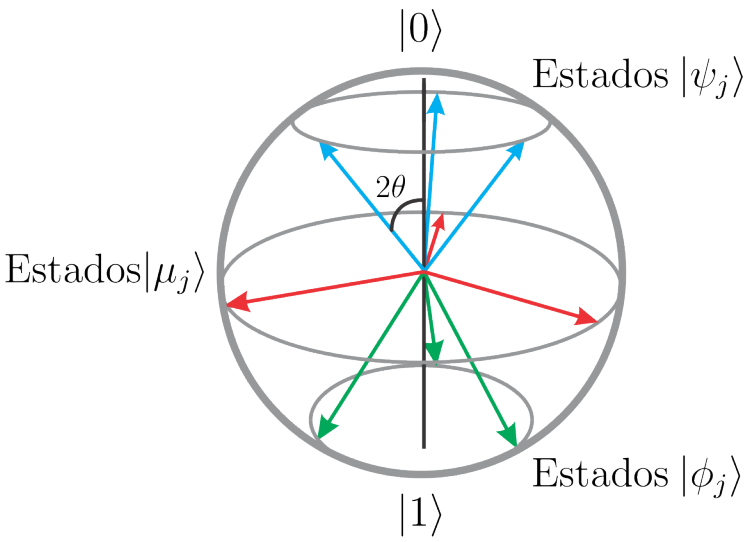

Figura 3.1: Estados simétricos equiprováveis $|\psi_j\rangle$ (azul), equação (3.19), e a posição dos vetores que formam os elementos de POVM da estratégia EM, $|\mu_j\rangle$ (vermelho), equação (3.20), e da estratégia CM, $|\phi_j\rangle$ (verde), equação (2.54).

probabilidades de inferir corretamente os estados. A confiança da estratégia EM, calculada a partir da equação (2.47), será dada por

$$\begin{aligned}[P(\hat{\rho}_j|\omega_j)]^{\mathrm{EM}} &= \frac{\eta_j \mathrm{Tr}(\hat{\Pi}_j \hat{\rho}_j)}{\mathrm{Tr}(\hat{\Pi}_j \hat{\rho})} \\ &= \frac{1}{3}\left(1 + \sin 2\theta\right).\end{aligned} \tag{3.22}$$

Esta é mostrada na figura 3.3 juntamente com a confiança máxima obtida pela estratégia CM, equação (2.55). Note que a confiança das duas estratégias coincide para $\theta = \pi/4$. Isso será melhor compreendido na seção 3.3, que mostra que as estratégias são coincidentes quando aplicadas a estados simétricos equiprováveis uniformes. O gráfico da figura 3.3 mostra que a estratégia CM fornece melhor confiança na identificação dos estados. Mas, se for levada em conta a probabilidade de falha, é possível observar que, em média, a estratégia EM fornece uma maior probabilidade de acerto, ou seja, um maior número de inferências corretas do estado medido. Da equação (3.21), a probabilidade de inferir corretamente o estado segundo a estratégia EM será dada por

$$\begin{aligned}P_{\mathrm{corr}}^{\mathrm{EM}} &= 1 - P_{\mathrm{erro}}^{\mathrm{EM}} \\ &= \frac{1}{3}\left(1 + \sin 2\theta\right).\end{aligned} \tag{3.23}$$

Levando em conta a probabilidade de falha, a probabilidade total de inferir corretamente o estado utilizando a estratégia CM é escrita como

$$P_{\mathrm{corr}}^{\mathrm{CM}} = (1 - P_?)\frac{2}{3} + (P_?)\frac{1}{3}, \tag{3.24}$$

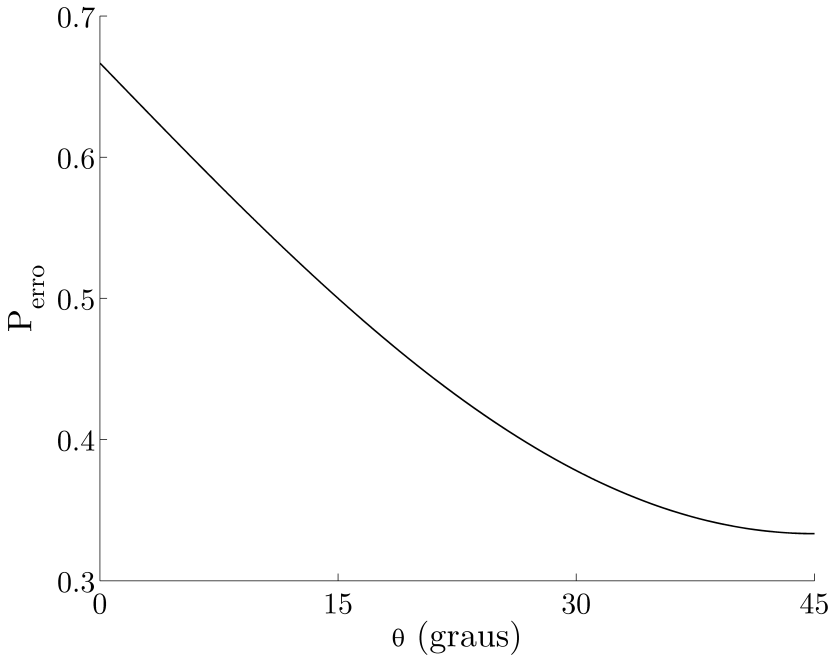

Figura 3.2: Probabilidade de erro mínimo obtido na discriminação dos estados $|\psi_j\rangle$, equação (3.19), em função do ângulo de separação entre eles.

onde $P_?$ é a probabilidade de falha dada pela equação (2.58), 2/3 é a confiança, equação (2.55), e 1/3 é a probabilidade de acerto após uma falha. Essa última é igual a uma adivinhação aleatória, já que, após uma falha, os estados $|\psi_j\rangle$ ficarão restritos a um espaço unidimensional. Assim, a probabilidade de acerto da estratégia CM será

$$P_{\text{corr}}^{\text{CM}} = \frac{1 + 2\sin^2\theta}{3}. \tag{3.25}$$

O gráfico da figura (3.4) mostra a variação das probabilidades de acerto das duas estratégias em função do ângulo de separação dos estados iniciais. A estratégia EM possui valores maiores em todo o gráfico, exceto em $\theta = 0$, onde nenhuma medição fornecerá informação sobre o estado, e em $\theta = \pi/4$, limite em que as estratégias EM e CM coincidem. Embora a confiança da medição via CM seja sempre maior, a admissão de uma probabilidade de falha faz com que, em média, menos acertos sejam alcançados. A estratégia mais conveniente a ser utilizada dependerá das condições do problema. Se a confiança na identificação dos estados for mais importante do que uma maior quantidade de acertos, a estratégia CM deve ser utilizada. Mas, se o problema exige um grande número de acertos, a estratégia EM se mostra mais eficiente.

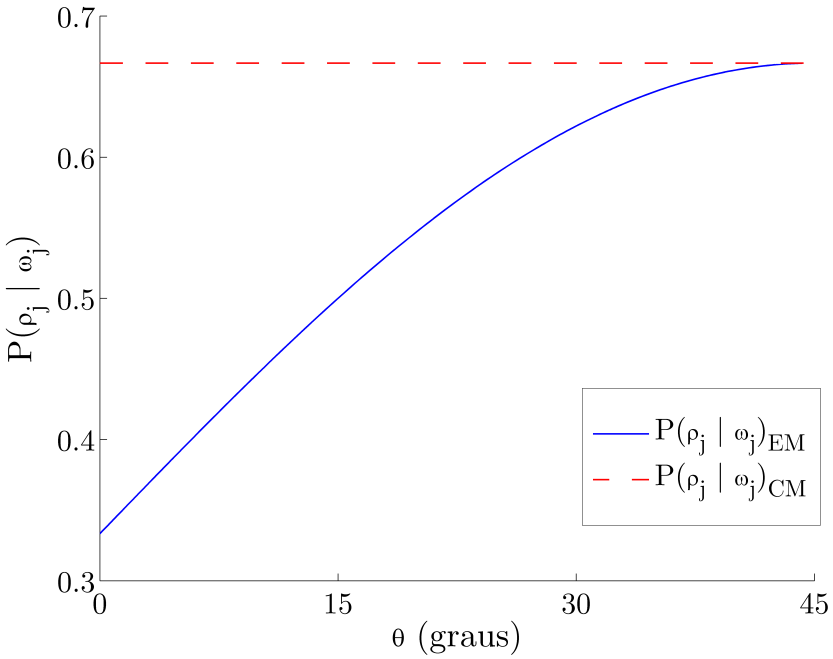

Figura 3.3: Variação da confiança na identificação dos estados $|\psi_j\rangle$, equação (3.19), em função do ângulo de separação entre eles. Linha contínua: confiança da estratégia EM. Linha tracejada: confiança da estratégia CM.

3.3 Estratégia de Confiança Máxima

A estratégia ótima de discriminação de estados quânticos com confiança máxima, apresentada na seção 2.2.3, tem como objetivo encontrar operadores que maximizam a confiança na identificação dos estados e minimizam a probabilidade de um resultado inconclusivo. A referência [42] mostra o POVM que realiza a discriminação CM de N estados simétricos equiprováveis de um *qudit*, o qual será estudado aqui.

O cálculo da confiança máxima, $[P(\hat{\rho}_j|\omega_j)]_{\max}$, definida pela equação (2.49), requer o inverso do operador densidade $\hat{\rho}$, equação (3.8), o qual será dado por

$$\hat{\rho}^{-1} = \sum_{m=0}^{d-1} |c_m|^{-2} |m\rangle\langle m|. \tag{3.26}$$

Por simplicidade, considere todos os coeficientes c_m não nulos[2]. A forma explícita do operador $\hat{\rho}^{-1}\hat{\rho}_j$ será

$$\hat{\rho}^{-1}\hat{\rho}_j = \sum_{m,n=0}^{d-1} c_n^* (c_m^*)^{-1} e^{\frac{2i\pi j(m-n)}{N}} |m\rangle\langle n|, \tag{3.27}$$

[2]Os coeficientes c_m são novamente considerados complexos. A remoção das fases associadas aos coeficientes será mostrada mais adiante.

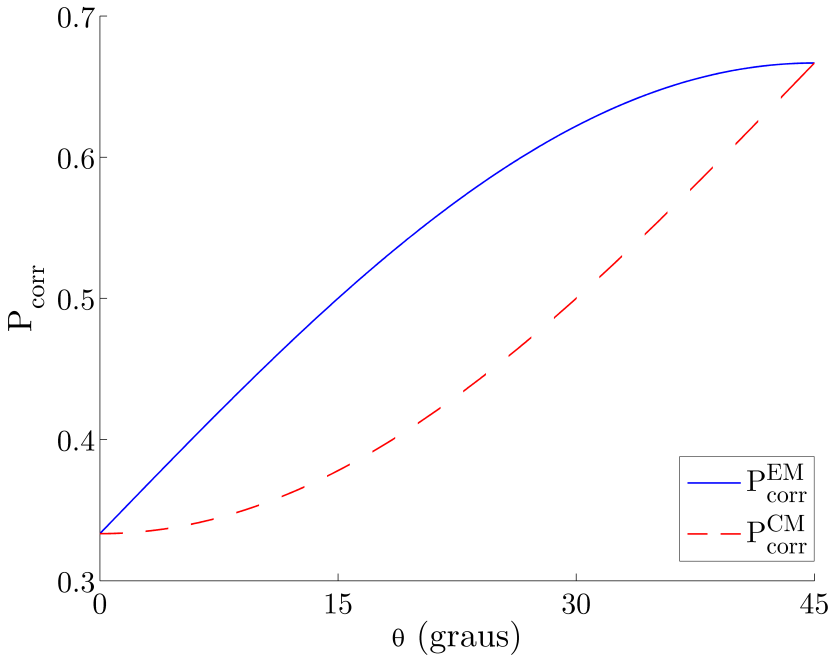

Figura 3.4: Probabilidade de inferir corretamente os estados $|\psi_j\rangle$, equação (3.19), de acordo com as estratégias EM (linha contínua) e CM (linha tracejada), em função do ângulo de separação entre eles.

e seu traço

$$\begin{aligned} \mathrm{Tr}(\hat{\rho}^{-1}\hat{\rho}_j) &= \sum_{m,n=0}^{d-1} c_n^*(c_m^*)^{-1} e^{\frac{2i\pi j(m-n)}{N}} \langle n|m\rangle \\ &= \sum_{m=0}^{d-1} \frac{c_m^*}{c_m^*} \\ &= d. \end{aligned} \tag{3.28}$$

Inserindo essa equação na definição de $[P(\hat{\rho}_j|\omega_j)]_{\max}$, em conjunto com a condição de equiprobabilidade, $\eta_j = 1/N$, se obtém

$$\begin{aligned} [P(\hat{\rho}_j|\omega_j)]_{\max} &= \eta_j \mathrm{Tr}(\hat{\rho}_j\hat{\rho}^{-1}) \\ &= \frac{d}{N}, \ \forall\ j. \end{aligned} \tag{3.29}$$

Para três estados simétricos de um *qubit* ($N = 3$ e $d = 2$), recupera-se o resultado do exemplo da seção 2.2.3, equação (2.55).

Os elementos de POVM que maximizam a confiança são calculados pela equação (2.48) e possuem a forma

$$\hat{\Pi}_j = a_j|\phi_j\rangle\langle\phi_j|, \tag{3.30}$$

onde

$$|\phi_j\rangle = \sum_{m=0}^{d-1} (c_m^*)^{-1} \hat{U}^j |m\rangle. \tag{3.31}$$

Assim como os estados de entrada, os estados de medição $|\phi_j\rangle$ também são simétricos sob a ação de $\hat{U}$, dado pela equação (3.4). Sendo assim, a probabilidade total de ocorrência de cada resultado de medição, ω_j, é a mesma. Os coeficientes a_j, definidos pela equação (2.48), são proporcionais a essa probabilidade e, portanto, podem ser simplificados por $a_j = a$. Embora o coeficiente a seja arbitrário, é possível que nenhuma escolha dele faça com que os elementos de POVM da equação (3.30) satisfaçam a relação de completeza. Se torna necessário, então, um novo elemento de POVM responsável por um resultado inconclusivo. Esse operador é dado por

$$\begin{aligned}
\hat{\Pi}_? &= \mathbb{1}_d - \sum_{j=0}^{N-1} \hat{\Pi}_j \\
&= \sum_{m=0}^{d-1} |m\rangle\langle m| - \sum_{j=0}^{N-1} a|\phi_j\rangle\langle\phi_j| \\
&= \sum_{m=0}^{d-1} |m\rangle\langle m| - a \sum_{m,n=0}^{d-1} \frac{1}{c_m^* c_n} \left[\sum_{j=0}^{N-1} e^{\frac{2i\pi j(m-n)}{N}} \right] |m\rangle\langle n| \\
&= \sum_{m=0}^{d-1} |m\rangle\langle m| - a \sum_{m,n=0}^{d-1} \frac{\delta_{mn}}{c_m^* c_n} |m\rangle\langle n| \\
&= \sum_{m=0}^{d-1} \left(1 - \frac{aN}{|c_m|^2} \right) |m\rangle\langle m|,
\end{aligned} \tag{3.32}$$

onde foram usadas a decomposição da identidade, $\mathbb{1}_d = \sum_{j=0}^{d-1} |j\rangle\langle j|$, as definições dos elementos de POVM $\hat{\Pi}_j$, equações (3.30) e (3.31), e a identidade da equação (1.34). A condição de positividade $\hat{\Pi}_? \geq 0$ impõe que $a \leq |c_m|^2/N, \forall\ m$. A probabilidade total de um resultado inconclusivo é $P_? = \mathrm{Tr}(\hat{\Pi}_? \hat{\rho}) = 1 - aNd$. Com o intuito de minimizar essa probabilidade, adota-se o máximo valor possível de a imposto pela positividade, sendo este $a = c_{\min}^2/N$, onde $c_{\min} = \min(|c_j|)_{j=0}^{d-1}$. Substituindo esse valor de a nas definições (3.30) e (3.32), tem-se

$$\begin{aligned}
\hat{\Pi}_j &= \frac{c_{\min}^2}{N} |\phi_j\rangle\langle\phi_j| \\
&= \frac{1}{N} \sum_{m,n}^{d-1} \frac{c_{\min}^2}{c_m^* c_n} e^{\frac{2i\pi j(m-n)}{N}} |m\rangle\langle n|,
\end{aligned} \tag{3.33}$$

e

$$\hat{\Pi}_? = \sum_{m=0}^{d-1} \left(1 - \frac{c_{\min}^2}{|c_m|^2} \right) |m\rangle\langle m|. \tag{3.34}$$

Esses são os operadores que discriminam estados simétricos equiprováveis de forma ótima, ou seja, com maior confiança possível, equação (3.29), e probabilidade de falha mínima, sendo esta dada por

$$[P_?]_{\min} = 1 - dc^2_{\min}. \tag{3.35}$$

No caso particular onde os estados simétricos são uniformes, ou seja, com $|c_m| = 1/\sqrt{d}, \forall\, m$, o operador $\hat{\Pi}_?$ é nulo e o conjunto $\{\hat{\Pi}_j\}$, dado pela equação (3.33), forma um POVM. Nesse caso, as estratégias de discriminação CM e EM coincidem, já que

$$\begin{aligned} \hat{\Pi}_j &= \frac{1}{N}\sum_{m,n=0}^{d-1} e^{\frac{2i\pi j(m-n)}{N}} |m\rangle\langle n| \\ &= \hat{\Pi}_j^{\mathrm{EM}}, \end{aligned} \tag{3.36}$$

onde $\hat{\Pi}_j^{\mathrm{EM}}$ é dado pela equação (3.14). Na referência [42] é mostrado que a confiança máxima possível para a estratégia EM respeita a desigualdade $[P(\hat{\rho}_j|\omega_j)]^{\mathrm{EM}}_{\max} \leq d/N$, onde a igualdade só é alcançada no caso onde as estratégias CM e EM são coincidentes. Isso mostra que a confiança no processo de discriminação de estados pode ser aumentada às custas da admissão de resultados inconclusivos, como pôde ser visto no gráfico 3.3 do exemplo da seção 3.2.

Um outro caso particular interessante é quando $N = d$. Neste, a confiança máxima, $[P(\hat{\rho}_j|\omega_j)]_{\max}$, equação (3.29), será igual a $1, \forall\, j$. Isso ocorre devido à independência linear dos estados $|\psi_j\rangle$, situação onde as estratégias CM e SA coincidem. A probabilidade mínima de falha encontrada na referência [50], coincide com a equação (3.35), o que corrobora a equivalência das estratégias. Se nesta situação os estados ainda forem uniformes, estes formarão um conjunto ortonormal, reduzindo o POVM a uma medição projetiva.

3.3.1 Implementação da Estratégia CM via Teorema de Naimark

Como discutido na seção 2.1.3, considere a implementação de um POVM via extensão do espaço de Hilbert por produto tensorial. Essa forma de representar uma medição generalizada será útil para uma melhor compreensão da estratégia CM, a qual será dividida em duas partes: i) descobrir se a medição será bem sucedida ou não, ou, equivalentemente, saber em qual conjunto os estados iniciais são mapeados e ii) decidir sobre o que fazer em cada uma das duas situações possíveis, sendo essas sucesso ou falha.

Considere o sistema inicialmente em um dos estados simétricos $|\psi_j\rangle$ e uma *ancilla* bidimensional no estado $|0\rangle$. A operação unitária que acopla o estado desses sistemas para a realização do POVM ótimo é dada por [42, 57]

$$\hat{\mathcal{U}} = \hat{A}_S \otimes \mathbb{1}_a - \hat{A}_? \otimes \hat{X}_a \hat{Z}_a, \tag{3.37}$$

onde $\hat{X}_a$ e $\hat{Z}_a$ são as matrizes de Pauli mostradas na tabela 1.2 e $\hat{A}_S$ e $\hat{A}_?$ são os operadores de detecção associados aos casos de sucesso e falha, respectivamente. Eles transformam o

estado inicial do sistema de acordo com o resultado da medição da *ancilla* e são dados por

$$\hat{A}_S = \hat{W} \sum_{m=0}^{d-1} \frac{c_{\min}}{|c_m|} |m\rangle\langle m|, \tag{3.38}$$

$$\hat{A}_? = \hat{W} \sum_{m=0}^{d-1} \sqrt{1 - \frac{c_{\min}^2}{|c_m|}} |m\rangle\langle m|. \tag{3.39}$$

O operador unitário $\hat{W}$ não influenciará nas probabilidades das medições, como visto na equação (2.1), sendo assim arbitrário. Afim de eliminar as fases dos coeficientes c_m, este será dado por

$$\hat{W} = \sum_n e^{-i\arg(c_m)} |k\rangle\langle k|, \tag{3.40}$$

onde $e^{-i\arg(c_m)} = |c_m|/c_m$. A atuação do operador de detecção $\hat{A}_S$ nos estados iniciais, equação (3.6), fornece

$$\begin{aligned} \hat{A}_S|\psi_j\rangle &= \sqrt{1 - P_?} \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{\frac{2i\pi jm}{N}} |m\rangle \\ &= \sqrt{1 - P_?} |u_j\rangle, \end{aligned} \tag{3.41}$$

mapeando estes em

$$|u_j\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{\frac{2i\pi jm}{N}} |m\rangle, \tag{3.42}$$

os quais são simétricos e uniformes. $P_?$ é a probabilidade mínima de resultado inconclusivo, dada por (3.35). A atuação de $\hat{A}_?$ fornece

$$\begin{aligned} \hat{A}_?|\psi_j\rangle &= \sqrt{P_?} \sum_{m=0}^{d-1} \sqrt{\frac{|c_m|^2 - c_{\min}^2}{P_?}} e^{\frac{2i\pi jm}{N}} |m\rangle \\ &= \sqrt{P_?} \sum_{m=0}^{d-1} C_m e^{\frac{2i\pi jm}{N}} |m\rangle \\ &= \sqrt{P_?} |\xi_j\rangle, \end{aligned} \tag{3.43}$$

mapeando os estados iniciais em

$$|\xi_j\rangle = \sum_{m=0}^{d-1} C_m e^{\frac{2i\pi jm}{N}} |m\rangle. \tag{3.44}$$

Os estados $|\xi_j\rangle$ formam um conjunto de estados simétricos normalizados, isto é, $\sum_m C_m^2 = 1$, onde

$$C_m = \sqrt{\frac{|c_m|^2 - c_{\min}^2}{P_?}}. \tag{3.45}$$

Pelo menos um dos termos C_m é nulo, o que diminui a dimensão acessível aos estados do novo conjunto. Ou seja, após uma falha, os estados iniciais são projetados em estados simétricos de menor dimensão, sendo necessariamente linearmente dependentes. Portanto, é impossível a realização da estratégia SA após uma falha. O número de coeficientes nulos depende da degenerescência ($\mathfrak{d}$) do coeficiente $c_{\min}$. Assim, a dimensão acessível ao conjunto $\{|\xi_j\rangle\}$ é $d - \mathfrak{d}$.

Utilizando as definições acima, a atuação da transformação unitária $\hat{\mathcal{U}}$, equação (3.37), no estado conjunto $|\psi_j\rangle|0\rangle_a$ será dada por

$$\begin{aligned}\hat{\mathcal{U}}|\psi_j\rangle|0\rangle_a &= \hat{A}_S|\psi_j\rangle|0\rangle_a + \hat{A}_?|\psi_j\rangle|1\rangle_a \\ &= \sqrt{1-P_?}|u_j\rangle|0\rangle_a + \sqrt{P_?}|\xi_j\rangle|1\rangle_a.\end{aligned} \tag{3.46}$$

Após a medição da *ancilla*, se conhece o conjunto de estados no qual os estados iniciais foram mapeados, o que leva ao segundo passo do processo de discriminação, dividido nas situações de sucesso e falha.

A. Sucesso

Após uma medição na *ancilla* que indica que o processo é bem sucedido, ou seja, uma projeção dela em $|0\rangle_a$, os estados iniciais, equação (3.6), são mapeados em um conjunto de estados simétricos equiprováveis uniformes, $\{|u_j\rangle \mid j = 0, \ldots, N-1\}$, dados pela equação (3.42). Isso ocorre com probabilidade de sucesso máxima, $P_j = 1 - P_?, \forall\, j$, o que é garantido pelo lema da uniformização demonstrado em [58].

Observação 2. O lema da uniformização diz que se existe uma transformação probabilística que leva os estados simétricos do conjunto $\{|\psi_j\rangle\}$ nos estados simétricos do conjunto $\{|u_j\rangle\}$ com probabilidades $\{p_j\}$, também existirá uma transformação probabilística $\{|\psi_j\rangle\} \to \{|u_j\rangle\}$, a qual é realizada com probabilidade $p = \frac{1}{N}\sum_j p_j$.

Nesse caso específico, como apontado na seção 3.3, as estratégias CM e EM coincidem. Desta maneira, o POVM ótimo para a realização da discriminação é dado pela equação (3.14), e pode ser escrito como

$$\begin{aligned}\hat{\Pi}_j &= \frac{1}{N}\sum_{m,n=0}^{d-1} e^{\frac{2i\pi j(m-n)}{N}}|m\rangle\langle n| \\ &= \frac{d}{N}|u_j\rangle\langle u_j|.\end{aligned} \tag{3.47}$$

A confiança na identificação dos estados $|u_j\rangle$ (e, consequentemente, $|\psi_j\rangle$) alcançada com esse

POVM, conforme a definição (2.47), é dada por

$$\begin{aligned} P(\hat{\rho}_j|\omega_j) &= \frac{P(\hat{\rho}_j)P(\omega_j|\hat{\rho}_j)}{P(\omega_j)} \\ &= \frac{\eta_j \mathrm{Tr}(\hat{\Pi}_j\hat{\rho}_j)}{\mathrm{Tr}(\hat{\Pi}_j\hat{\rho})}, \end{aligned} \tag{3.48}$$

onde $\eta_j = 1/N$. A probabilidade se obter o resultado de medição ω_j, dado que o estado preparado é $\hat{\rho}_j$ é dada por

$$\begin{aligned} \mathrm{Tr}(\hat{\Pi}_j\hat{\rho}_j) &= \frac{d}{N}\mathrm{Tr}(|u_j\rangle\langle u_j|u_j\rangle\langle u_j|) \\ &= \frac{d}{N}|\langle u_j|u_j\rangle|^2 \\ &= \frac{d}{N}, \end{aligned} \tag{3.49}$$

e a probabilidade total de se obter ω_j é

$$\begin{aligned} \mathrm{Tr}(\hat{\Pi}_j\hat{\rho}) &= \frac{d}{N^2}\sum_{k=0}^{N-1}\mathrm{Tr}(|u_j\rangle\langle u_j|u_k\rangle\langle u_k|) \\ &= \frac{d}{N^2}\sum_{k=0}^{N-1}\left|\frac{1}{d}\sum_{m,n=0}^{d-1} e^{\frac{2i\pi jm}{N}} e^{\frac{-2i\pi kn}{N}}\langle n|m\rangle\right|^2 \\ &= \frac{1}{dN^2}\sum_{k=0}^{N-1}\sum_{m,n=0}^{d-1} e^{\frac{2i\pi j(m-n)}{N}} e^{\frac{2i\pi k(n-m)}{N}} \\ &= \frac{1}{dN^2}\sum_{m,n=0}^{d-1} e^{\frac{2i\pi j(m-n)}{N}} N\delta_{mn} \\ &= \frac{1}{N}, \end{aligned} \tag{3.50}$$

onde o operador $\hat{\rho}$ é dado pela equação (3.7) e se fez uso da identidade da equação (1.34). Substituindo esses resultados na equação (3.48), obtém-se

$$P(\hat{\rho}_j|\omega_j) = \frac{d}{N}, \tag{3.51}$$

que, como esperado, coincide com a confiança máxima na discriminação de estados simétricos equiprováveis, equação (3.29). Portanto, o procedimento apresentado via teorema de Naimark é equivalente ao POVM ótimo de discriminação CM da seção 3.3.

B. Falha

Como pode ser visto da equação (3.46), se a *ancilla* é projetada no estado $|1\rangle_a$, o conjunto de estados iniciais é mapeado no conjunto de estados simétricos equiprováveis $\{|\xi_j\rangle \mid j =$

$0, \ldots, N-1\}$, dados pela equação (3.44). Nesse caso, o processo é considerado falho e a probabilidade mínima de falha, $P_?$, é dada pela equação (3.35). O espaço de Hilbert acessível a esses estados possui dimensão $d' = d - \mathfrak{d}$, onde $\mathfrak{d}$ é a multiplicidade do coeficiente $c_{\min}$. Existem três possibilidades distintas para o conjunto de estados $\{|\xi_j\rangle\}$ dependentes do valor de $\mathfrak{d}$:

(i) Se $\mathfrak{d} = d$, todos os coeficientes são iguais a $1/\sqrt{d}$, sendo assim o conjunto inicial uniforme. Nesta situação as estratégias CM e EM coincidem e não existe probabilidade de falha, isto é, $P_? = 0$.

(ii) Se $\mathfrak{d} = d-1$, todos os estados $|\xi_j\rangle$ serão idênticos, a menos de fases globais. Neste caso o espaço de Hilbert é unidimensional e nenhuma medição irá fornecer informação sobre o estado do sistema.

(iii) Se $\mathfrak{d} < d-1$, o espaço de Hilbert acessível aos N estados simétricos equiprováveis terá dimensão maior do que 1. Neste caso é possível realizar medições que forneçam informação dos estados de entrada do sistema.

Considerando que a situação (iii) é respeitada, existem diversas possibilidade para se extrair informação do sistema, como medições projetivas e implementação das estratégias EM ou CM. Tome, por exemplo, uma nova discriminação via CM. Como os estados $|\xi_j\rangle$ respeitam as condições de simetria e equiprobabilidade, existe um novo POVM $\{\hat{\Pi}'_j\}$ que realiza a distinção dos estados de forma ótima, dado pelas equações (3.33) e (3.34). A nova confiança máxima nesse espaço $(d-\mathfrak{d})$-dimensional, de acordo com a equação (3.29), será

$$[P'(\hat{\rho}_j|\omega'_j)]_{\max} = \frac{d-\mathfrak{d}}{N}, \tag{3.52}$$

e a probabilidade mínima de falha, equação (3.35), será dada por

$$[P'_?]_{\min} = 1 - (d-\mathfrak{d})C^2_{\min}, \tag{3.53}$$

com $C^2_{\min} = \min_{C_m \neq 0} (C_m)^{d-1}_{m=0}$, onde C_m é definido pela equação (3.45).

Esses resultados são referentes à aplicação da estratégia CM no conjunto de estados $|\xi_j\rangle$, de forma análoga à feita no passo anterior. A esse procedimento é dado o nome de confiança máxima sequencial (CMS) [42]. A implementação desta também é feita pelo teorema de Naimark, tendo novas projeções em estados simétricos equiprováveis uniformes (sucesso) ou em um conjunto de estados simétricos equiprováveis em um espaço de Hilbert menor (falha). Caso a medição seja novamente mal sucedida, pode ser possível uma nova repetição do processo. Esta é dependente da satisfação da condição (iii) da lista anterior. Na próxima seção será avaliado o caso onde tantas medições via CM quanto possíveis são implementadas.

3.3.2 Confiança Máxima Sequencial

Como visto na seção anterior, é possível implementar a estratégia CM de forma sequencial na discriminação de estados. Essa sequência é dependente dos coeficientes dos estados iniciais e da dimensão do espaço de Hilbert acessível. Sempre que a nova dimensão acessível do sistema após uma falha for maior do que 1, é possível uma nova iteração do procedimento de discriminação via CM.

A cada estágio da estratégia CMS, a confiança na identificação dos estados iniciais $|\psi_j\rangle$ decresce, mas a probabilidade total de identificá-los corretamente aumenta. Considerando um total de $\mathbb{n}$ estágios, essa probabilidade será

$$P_{\text{corr}}^{\text{CMS}} = [1 - P_?^{\mathbb{1}}]\frac{d}{N} + P_?^{\mathbb{1}}[1 - P_?^{2}]\frac{d - \mathfrak{d}^{\mathbb{1}}}{N} + \ldots + P_?^{\mathbb{1}}P_?^{2}\ldots[1 - P_?^{\mathbb{n}}]\frac{d - \mathfrak{d}^{\mathbb{1}} - \mathfrak{d}^{2} - \ldots - \mathfrak{d}^{\mathbb{n}-\mathbb{1}}}{N}, \tag{3.54}$$

onde os índices $\mathbb{1}, \ldots, \mathbb{n}$ indicam o estágio da CMS. Ou seja, $P_?^{\mathbb{i}}$ indica a probabilidade de falha no $\mathbb{i}$-ésimo estágio e $\mathfrak{d}^{\mathbb{i}}$ indica a degenerescência do coeficiente mínimo no $\mathbb{i}$-ésimo estágio. Se a estratégia se restringir apenas à aplicação da estratégia CM ótima a cada passo, a probabilidade $P_{\text{corr}}^{\text{CMS}}$ também será ótima, assim como a confiança de uma medição bem sucedida ao longo das iterações.

A probabilidade total de falha da estratégia é expressada, simplesmente, por

$$P_?^{\text{CMS}} = P_?^{\mathbb{1}}P_?^{2}\ldots P_?^{\mathbb{n}}. \tag{3.55}$$

Se a última transformação dos estados, no caso de falha, for em um conjunto de estados uniformes, essa probabilidade se reduz a zero. Caso contrário, no último estágio da estratégia, o espaço de Hilbert será unidimensional e nenhuma informação poderá ser obtida através de medições, ou seja, $P_?^{\mathbb{n}} = 1$.

O limite superior da probabilidade de sucesso $P_{\text{corr}}^{\text{CMS}}$ é d/N e é atingida apenas quando as estratégias CM e EM coincidem, $P_?^{\mathbb{1}} = 0$. De fato, enquanto a estratégia CM garante maior confiança na identificação dos estados de entrada, a estratégia EM garante um maior número médio de identificações corretas, como discutido no exemplo da seção 3.2 e observado no gráfico da figura 3.4. A estratégia mais conveniente a ser aplicada dependerá da situação em que a discriminação de estados está inserida.

Exemplo: comparação de estratégias na discriminação de quatro estados equiprováveis de um *qutrit*

Para a aplicação da estratégia CMS, a dimensão mínima do espaço de Hilbert acessível aos estados deve ser igual a 3. Caso contrário, a condição (iii) da seção 3.3.2 não pode ser satisfeita. O caso mais simples consiste de $N = 4$ estados simétricos equiprováveis de um

qutrit, dados por

$$|\psi_j\rangle = \sum_{m=0}^{2} c_m e^{\frac{2i\pi jm}{4}} |m\rangle, \tag{3.56}$$

com $j = 0, \ldots, 3$. Da definição da equação (2.47) e usando as equações (3.14) e (3.56), a confiança máxima na identificação desses estados via estratégia EM será dada por

$$\begin{aligned}[P(\hat{\rho}_j|\omega_j)]^{\mathrm{EM}} &= \frac{\eta_j \mathrm{Tr}(\hat{\Pi}_j \hat{\rho}_j)}{\mathrm{Tr}(\hat{\Pi}_j \hat{\rho})} \\ &= \frac{1}{4}\left(\sum_{m=0}^{2} |c_m|\right)^2, \ \forall\, j.\end{aligned} \tag{3.57}$$

A confiança máxima na discriminação CM, equação (3.29), é

$$[P(\hat{\rho}_j|\omega_j)]^{\mathrm{CM}}_{\mathbb{1}} = \frac{3}{4}. \tag{3.58}$$

Se o coeficiente $c_{\min}$ não for degenerado, é possível realizar medições via CMS, tendo como confiança máxima na segunda iteração

$$[P(\hat{\rho}_j|\omega_j)]^{\mathrm{CM}}_{2} = \frac{1}{2}. \tag{3.59}$$

Caso contrário, a confiança será

$$[P(\hat{\rho}_j|\omega_j)]^{\mathrm{CM}}_{2} = \frac{1}{4}, \tag{3.60}$$

a qual corresponde a uma adivinhação aleatória. Após a segunda tentativa, nenhuma nova é possível, pois os estados serão projetados num espaço unidimensional no caso de uma segunda falha.

O gráfico da figura 3.5 mostra como a confiança varia com os módulos dos coeficientes c_0 e c_1 dos estados iniciais. O módulo do terceiro coeficiente é dado por $|c_2| = \sqrt{1 - |c_0|^2 - |c_1|^2}$. Note que existem regiões do gráfico onde um sucesso na segunda iteração da estratégia CMS ainda fornece uma confiança maior do que aquela obtida com a discriminação via EM. Entretanto, se a segunda iteração falhar, a confiança corresponderá a uma adivinhação aleatória, como explicado acima.

A conveniência da utilização dessa estratégia varia conforme os coeficientes dos estados que formam o conjunto simétrico. Como o conhecimento dos estados que compõem o conjunto foi tomado como uma premissa na formulação dos problemas de discriminação apresentados, essa estratégia pode se mostrar útil sempre que for dado um limite inferior para a confiança desejada.

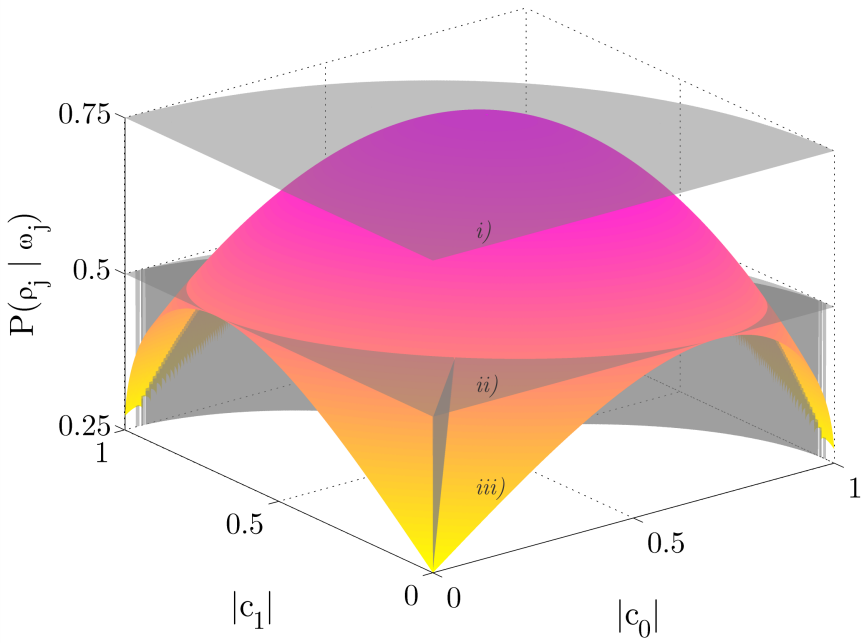

Figura 3.5: A figura mostra três superfícies que indicam a confiança na identificação dos estados simétricos equiprováveis da equação (3.56). i) Confiança máxima no caso de sucesso na primeira iteração da estratégia CMS. ii) Confiança máxima no caso de sucesso na segunda iteração da estratégia CMS. iii) Confiança máxima segundo a estratégia EM.

3.4 Separação de Estados Simétricos

A separação de estados foi mostrada na seção 2.2.4 como um dos passos de estratégias que interpolam entre o erro mínimo e a confiança máxima[3]. Essa mesma abordagem pode ser aplicada a grupos de estados simétricos equiprováveis [43, 58].

Considere o conjunto de estados simétricos $\{|\psi_j\rangle \mid j = 0, \ldots, N-1\}$, dados pela equação (3.6), com todos os seus coeficientes não-nulos. Se tem como objetivo o mapeamento destes estados num novo conjunto de estados simétricos equiprováveis $\{|v_j(\varsigma)\rangle\}$ que sejam mais distinguíveis entre si, onde ς é o parâmetro que definirá o "grau de distinguibilidade" desejado. Os novos estados, após o mapeamento, serão dados por

$$|v_j(\varsigma)\rangle = \sum_{m=0}^{d-1} b_m(\varsigma) e^{\frac{2i\pi jm}{N}} |m\rangle. \tag{3.61}$$

Para esse mapa ser aceitável, a parametrização deve respeitar $|v_j(0)\rangle = |\psi_j\rangle$ e $|v_j(1)\rangle = |u_j\rangle$, onde $|u_j\rangle$ são estados pertencentes a um conjunto de estados simétricos equiprováveis

[3]De fato, foi mostrada a interpolação entre ME e SA. Entretanto, lembre-se que a estratégia SA é um caso particular da estratégia CM, onde os estados a serem discriminados são linearmente independentes.

uniformes, equação (3.42). Uma possível parametrização é dada por

$$|b_m(\varsigma)|^2 = (1-\varsigma)|c_m|^2 + \frac{\varsigma}{d}, \tag{3.62}$$

com fases descritas por

$$e^{i\arg(b_m(\varsigma))} = e^{i(1-\varsigma)\arg(c_m)}, \tag{3.63}$$

como mostrado na referência [43]. Essa definição de $b_m(\varsigma)$, baseada na equação paramétrica do segmento de reta entre os pontos $|c_m|^2$ e $1/d$, preserva a norma e o ordenamento dos coeficientes, $c_m \geq c_{m+1} \rightarrow b_m(\varsigma) \geq b_{m+1}(\varsigma)$.

A efetuação do mapeamento pode ser descrita via teorema de Naimark, como

$$\begin{aligned} \hat{\mathcal{U}}|\psi_j\rangle|0\rangle_a &= \hat{A}_S(\varsigma)|\psi_j\rangle|0\rangle_a + \hat{A}_?(\varsigma)|\psi_j\rangle|1\rangle_a \\ &= \sqrt{P_S(\varsigma)}|v_j(\varsigma)\rangle|0\rangle_a + \sqrt{P_?(\varsigma)}|\chi_j(\varsigma)\rangle|1\rangle_a. \end{aligned} \tag{3.64}$$

Uma medição na *ancilla* indicará se a separação de estados é bem sucedida ou não. Os estados nos quais os $|\psi_j\rangle$ são projetados no caso de falha, $|\chi_j(\varsigma)\rangle$, serão apresentados após a construção explícita dos operadores de detecção. As probabilidades $P_S(\varsigma)$ e $P_?(\varsigma)$ são independentes do índice j. Ou seja, as probabilidades são iguais para qualquer estado $|\psi_j\rangle$, conforme o lema da uniformização [58], comentado na observação 2.

Os operadores de detecção, $\hat{A}_S(\varsigma)$ e $\hat{A}_?(\varsigma)$, devem formar um POVM. Para isso, deve ser respeitada a condição $\hat{A}_S^\dagger(\varsigma)\hat{A}_S(\varsigma) + \hat{A}_?^\dagger(\varsigma)\hat{A}_?(\varsigma) = \mathbb{1}$. Das equações (3.6) e (3.61), o operador $\hat{A}_S(\varsigma)$ pode ser escrito explicitamente na forma

$$\hat{A}_S(\varsigma) = \sqrt{P_S}\sum_{m=0}^{d-1}\frac{b_m(\varsigma)}{c_m}|m\rangle\langle m|. \tag{3.65}$$

A otimização do procedimento é feita com a maximização da probabilidade de sucesso. Esta deve ser feita respeitando o vínculo $P_? = 1 - P_S \geq 0$. Ou, equivalentemente, $\hat{A}_?^\dagger(\varsigma)\hat{A}_?(\varsigma) = \mathbb{1} - \hat{A}_S^\dagger(\varsigma)\hat{A}_S(\varsigma) \geq 0$. A referência [43] fornece como solução do problema

$$P_S(\varsigma) = \min\left(\frac{|c_m|^2}{|b_m(\varsigma)|^2}\right)_{m=0}^{d-1} = \frac{1}{(1-\varsigma) + \frac{\varsigma}{d|c_{\min}|^2}}, \tag{3.66}$$

onde $|c_{\min}|^2 = \min(|c_m|^2)_{m=0}^{d-1}$. Os operadores de detecção assumem, então, a forma explícita

$$\hat{A}_S(\varsigma) = \sum_m^{d-1}\sqrt{\frac{1-\varsigma+\varsigma/d|c_m|^2}{1-\varsigma+\varsigma/d|c_{\min}|^2}}e^{-i\varsigma\arg(c_m)}|m\rangle\langle m|, \tag{3.67}$$

e

$$\hat{A}_?(\varsigma) = \sum_m^{d-1}\sqrt{\frac{\varsigma}{d}\frac{1/|c_{\min}|^2 - 1/|c_m|^2}{1-\varsigma+\varsigma/d|c_m|^2}}e^{-i\varsigma\arg(c_m)}|m\rangle\langle m|. \tag{3.68}$$

Como $\hat{A}_?(\varsigma)|\psi_j\rangle = \sqrt{1-P_S}|\chi_j(\varsigma)\rangle$, obtém-se

$$|\chi_j(\varsigma)\rangle = \sum_{m=0}^{d-1} \sqrt{\frac{|c_m|^2 - |c_{\min}|^2}{1-d|c_{\min}|^2}} e^{i(1-\varsigma)\arg(c_m)} e^{\frac{2i\pi jm}{N}} |m\rangle. \tag{3.69}$$

Esses estados fazem parte de um conjunto de estados simétricos equiprováveis, porém com um *overlap* maior entre eles, ou seja, $|\langle\chi_j(\varsigma)|\chi_k(\varsigma)\rangle| \geq |\langle\psi_j|\psi_k\rangle|, \forall\ j \neq k$, o que os torna, portanto, menos distinguíveis. Isso fica claro se observado que ao menos um dos coeficientes desses estados é nulo, deixando-os assim distribuídos num espaço de Hilbert menor que o anterior à transformação.

O parâmetro ς também caracteriza uma interpolação entre as estratégia EM e CM quando uma medição com erro mínimo, discutida na seção 2.2.1, é feita logo após uma separação de estados bem sucedida. A probabilidade ótima de sucesso, equação (3.66), varia de modo que $P_S(0) = P_S^{\text{EM}} = 1$ e $P_S(1) = P_S^{\text{CM}} = d|c_{\min}|^2$. Para $\varsigma = 0$, os estados de entrada permanecem os mesmos. Já para $\varsigma = 1$, os estados $|v_j(\varsigma)\rangle$ serão maximamente separados, se tornando ortogonais caso os estados de entrada sejam linearmente independentes. Para os casos intermediários, a separação dos estados, e, consequentemente sua distinguibilidade, aumenta com o parâmetro ς.

Estratégias desse tipo são interessantes pois permitem impor limites na probabilidade de falha ou na confiança de medição. Com um desses limites fixado é possível encontrar o parâmetro ς que gera a melhor estratégia possível de discriminação entre EM e CM. Além disso, com a medição da *ancilla*, é possível ter certeza da nova separação entre os estados. Portanto, essa estratégia pode ser utilizada fora do contexto de discriminação, onde o único objetivo seria a própria separação entre os estados do conjunto. Por exemplo, um estado bipartido puro parcialmente emaranhado pode ter seu emaranhamento aumentado com a separação de estados [23, 59]. O procedimento mostrado nessa seção mostra como realizar essa separação de forma ótima. Para $\varsigma = 0$, não haveria alteração no emaranhamento do estado. Já para $\varsigma = 1$ a separação de estados corresponderia à concentração para um estado maximamente emaranhado.

4

Teleportação Quântica e Troca de Emaranhamento via Canais Parcialmente Emaranhados

Estados emaranhados bipartidos são uma parte fundamental de diversos protocolos de informação quântica, tais como teleportação quântica, mostrada na seção 1.6.2, troca de emaranhamento, seção 1.6.3 e codificação superdensa, seção 1.6.4. Quando, nos exemplos citados, o estado compartilhado por Alice e Bob é maximamente emaranhado, os objetivos dos protocolos são plenamente cumpridos, isto é, são sempre bem sucedidos e não possuem erros associados. Entretanto, se esses protocolos utilizam estados parcialmente emaranhados, imperfeições associadas às suas respectivas tarefas serão inevitáveis. Como será mostrado aqui, a minimização dessas imperfeições está relacionada com o problema de discriminação de estados simétricos não-ortogonais. Assim, as estratégias de discriminação discutidas nos capítulos 2 e 3 serão utilizadas com o objetivo de otimizar os protocolos de informação quântica de acordo com alguma figura de mérito pré-estabelecida. Neste capítulo, serão estudados alguns resultados conhecidos para teleportação quântica e troca de emaranhamento via canais parcialmente emaranhados. Devido a semelhança do tratamento, o primeiro será analisado com mais detalhes que o segundo.

4.1 Teleportação Quântica

O protocolo de teleportação quântica padrão [28] foi discutido na seção 1.6.2. Se mostrou que, utilizando um estado puro maximamente emaranhado, é possível teleportar um estado quântico de forma determinística e com fidelidade 1 (veja seção 1.3). Porém, se o estado for parcialmente emaranhado, essa tarefa se torna impossível, como mostrado a seguir. Suponha

que Alice deseja teleportar para Bob um estado puro de um *qudit* dado por

$$|\phi\rangle_3 = \sum_{m=0}^{d-1} c_m |m\rangle_3, \tag{4.1}$$

onde $\{|m\rangle_3\}$ é a base computacional do espaço de Hilbert d-dimensional $\mathcal{H}_3$. O estado compartilhado por Alice e Bob, $|\Psi\rangle_{12}$, na decomposição de Schmidt (veja seção 1.2), possui a forma

$$|\Psi\rangle_{12} = \sum_{l=0}^{N_S-1} \lambda_l |l\rangle_1 |l\rangle_2, \tag{4.2}$$

onde o sistema 1 pertence a Bob e o sistema 2 a Alice. Assume-se, sem perda de generalidade, que os sistemas pertencem aos respectivos espaços de Hilbert d-dimensionais $\mathcal{H}_1$ e $\mathcal{H}_2$, e, portanto, $N_S \leq d$. Considere ainda que as bases de Schmidt $\{|l\rangle_i\}$ de $\mathcal{H}_i, i = 1, 2$, coincidem com as bases computacionais dos seus respectivos espaços (veja a observação 1). Utilizando as operações unitárias $\hat{X}$, $\hat{Z}$ e $\hat{G}^{\text{XOR}}$, definidas na tabela 1.3, o processo de teleportação é facilmente compreendido com o uso da identidade demonstrada no apêndice A.1

$$|\Psi\rangle_{12}|\phi\rangle_3 = \frac{1}{d} \sum_{l,k=0}^{d-1} \hat{Z}_1^{-l} \hat{X}_1^k |\phi\rangle_1 \hat{G}_{23}^{\text{XOR}} |\nu_l\rangle_2 |k\rangle_3, \tag{4.3}$$

onde

$$|\nu_l\rangle_2 = \hat{Z}_2^l \sum_{j=0}^{N_S-1} \lambda_j |j\rangle_2, \tag{4.4}$$

com $l = 0, \ldots, d-1$. Seguindo o protocolo de teleportação quântica padrão, Alice deve realizar uma medição conjunta nos sistemas em sua posse. Medições conjuntas, em uma base maximamente emaranhada, podem ser feitas de acordo com o procedimento descrito na seção 1.6.1. Este consiste da aplicação da porta $\hat{G}^{\text{XOR}}$ seguida de uma transformada inversa de Fourier, $\hat{\mathcal{F}}^{-1}$, dada pela equação (1.25). A atuação de $\hat{G}^{\text{XOR}}$ nos sistemas 2 e 3 fornece, de acordo com a equação (4.3),

$$\hat{G}_{23}^{\text{XOR}} |\Psi\rangle_{12}|\phi\rangle_3 = \frac{1}{d} \sum_{l,k=0}^{d-1} \hat{Z}_1^{-l} \hat{X}_1^k |\phi\rangle_1 |\nu_l\rangle_2 |k\rangle_3, \tag{4.5}$$

onde foram utilizadas as propriedades do operador $\hat{G}_{23}^{\text{XOR}}$, o qual é unitário e hermitiano. O estado do sistema 3 é perfeitamente determinado com uma medição projetiva na base computacional. Já o estado do sistema 2 faz parte de um conjunto de estados simétricos equiprováveis[1], os quais serão não-ortogonais se $|\Psi\rangle_{12}$ for parcialmente emaranhado. Por-

[1] O termo $1/d$ da equação (4.3) é equivalente à probabilidade *a priori* dos estados $|\nu_l\rangle_2$. O conjunto $\{|\nu_l\rangle_2\}$ é composto por d estados simétricos em um espaço de Hilbert N_S-dimensional, onde N_S é o número de Schmidt do estado $|\Psi\rangle_{12}$, dado pela equação (4.2). Os estados $|\nu_l\rangle_2$ serão linearmente independentes se $N_S = d$ e linearmente dependentes se $N_S < d$.

tanto, após uma medição arbitrária $|\alpha_{l'}\rangle\langle\alpha_{l'}|$ em 2, o estado do sistema 1 será dado por

$$|\tilde{\phi}\rangle_1 \propto \hat{U}_{l',k'} \sum_{l=0}^{d-1} c_{ll'} \hat{Z}_1^{-l} \hat{X}_1^{k'} |\phi\rangle_1, \tag{4.6}$$

onde $\hat{U}_{l',k'}$ é a transformação unitária aplicada por Bob condicionada ao resultado (l', k') da medição de Alice e $c_{ll'} = \langle\alpha_{l'}|\nu_l\rangle$. A menos que $c_{ll'} \propto \delta_{ll'}$, o estado $|\tilde{\phi}\rangle_1$ não poderá ser transformado em $|\phi\rangle_1$, e, portanto, a teleportação não poderá ser concluída com fidelidade unitária. Isso somente será possível de forma determinística se os estados $|\nu_l\rangle_2$ forem ortogonais. Caso contrário, Alice deve optar por uma estratégia de discriminação que identifique o estado $|\nu_l\rangle_2$ de modo a maximizar a fidelidade do estado teleportado, $|\tilde{\phi}\rangle_1$. A figura 4.1 mostra o circuito que descreve o protocolo de teleportação, onde a caixa preta com a operação $\hat{\Xi}$ assumirá diferentes formas, de acordo com a estratégia adotada por Alice.

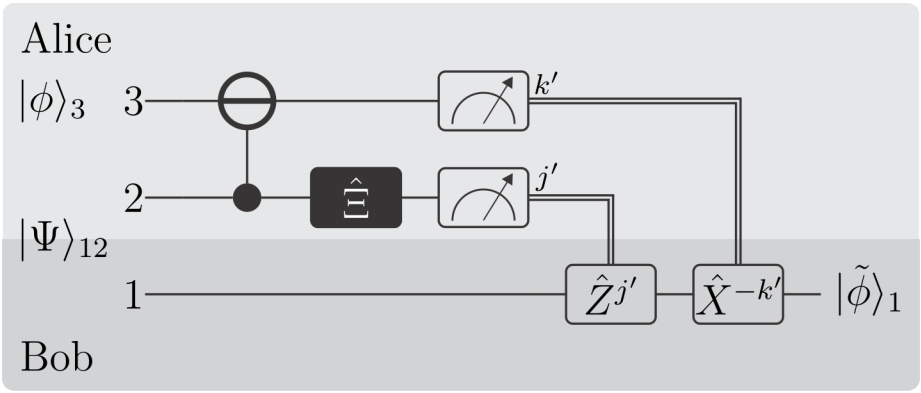

Figura 4.1: Circuito quântico do protocolo de teleportação com um estado compartilhado $|\Psi\rangle_{12}$ parcialmente emaranhado. A caixa preta com a operação $\hat{\Xi}$ contém um circuito que varia conforme a estratégia de discriminação adotada por Alice. O estado de saída $|\tilde{\phi}\rangle_1$ indica que este pode ser diferente do estado que se deseja teleportar.

As diferentes estratégias apresentadas no capítulo 3 serão exploradas para a realização da discriminação dos estados $|\nu_l\rangle_2$, dados por (4.4). Ao final do protocolo, será analisada a fidelidade entre o estado a ser teleportado, $|\phi\rangle_3$, e o estado final obtido por Bob, $|\tilde{\phi}\rangle_1$, e esta quantidade será tomada como figura de mérito do processo. Os protocolos apresentados neste capítulo serão divididos em duas categorias, determinísticos [60–63] e probabilísticos [37, 54, 55, 64–66]. O termo determinístico indica que a teleportação será sempre realizada independentemente da fidelidade alcançada. Já o termo probabilístico indica que existe uma probabilidade de falha para o protocolo, a qual é admitida com o intuito de aumentar a fidelidade da teleportação.

4.1.1 Fidelidade e Fração de Singleto na Teleportação Quântica

Dado um estado emaranhado qualquer, $\hat{\rho}_{12}$, inicialmente compartilhado por Alice e Bob, Horodecki *et al.* demonstraram na referência [60] que a fidelidade máxima atingida em qualquer protocolo de teleportação realizado com operações locais e comunicação clássica é dada por

$$F^S = \frac{df^S + 1}{d+1}, \tag{4.7}$$

onde d é a dimensão de $\mathcal{H}_1$ e $\mathcal{H}_2$ e o índice S indica a classe à qual o protocolo pertence, sendo essa classificada aqui de acordo com a estratégia de medição adotada por Alice. O parâmetro f é chamado fração de singleto e mede a máxima fidelidade atingida entre $\hat{\rho}_{12}$ e um estado maximamente emaranhado $|\tilde{\Psi}\rangle_{12}$, sendo definida por

$$f^S = \max_{\tilde{\Psi}} [\langle \tilde{\Psi} | \hat{\rho} | \tilde{\Psi} \rangle]_{12}. \tag{4.8}$$

Posteriormente, foi observado em [37] que a fração de singleto é idêntica à confiança, equação (2.47), obtida na discriminação de estados simétricos equiprováveis, de acordo com a estratégia adotada. Ou seja,

$$f^{\mathrm{EM}} = [P(\hat{\rho}_l|\omega_l)]^{\mathrm{EM}}, \tag{4.9}$$

$$f^{\mathrm{CM}} = [P(\hat{\rho}_l|\omega_l)]^{\mathrm{CM}}, \tag{4.10}$$

$$f^{\mathrm{SA}} = [P(\hat{\rho}_l|\omega_l)]^{\mathrm{SA}} = 1, \tag{4.11}$$

onde $\hat{\rho}_l = |\nu_l\rangle\langle\nu_l|$ é dado pelo equação (4.4). Portanto, as fidelidades dos protocolos de teleportação descritos neste capítulo podem ser expressadas na forma

$$F^S = \frac{d[P(\hat{\rho}_l|\omega_l)]^S + 1}{d+1}. \tag{4.12}$$

Desse modo, quanto maior a confiança na identificação do estado do sistema 2, maior será a fidelidade do protocolo de teleportação descrito na seção 4.1. Se o estado compartilhado por Alice e Bob for maximamente emaranhado, os estados $|\nu_l\rangle_2$ serão ortogonais. Assim, $P(\hat{\rho}_l|\omega_l) = 1$, e, portanto, $F = 1$, conforme esperado.

4.1.2 Teleportação Determinística Ótima

Neste protocolo, a teleportação será realizada sem se admitir falha no procedimento. Para isso, a medição de Alice sobre o sistema 2 deve sempre inferir um dos d estados simétricos $|\nu_l\rangle_2$, dados por (4.4). Quando esses estados são não-ortogonais, o erro na inferência de Alice será inevitável. A fim de maximizar a fidelidade da teleportação, ela deve minimizar a probabilidade de erro do processo de discriminação, ou seja, aplicar a estratégia EM apresenta na seção 3.2. A equação (3.14) fornece os operadores $\hat{\Pi}_l$ que compõem o POVM ótimo para

a realização da discriminação EM entre d estados simétricos equiprováveis em um espaço N_S-dimensional. Na notação utilizada nessa seção, eles serão escritos como

$$\hat{\Pi}_l = \frac{1}{d} \sum_{m,n=0}^{N_S-1} e^{\frac{2i\pi l(m-n)}{d}} |m\rangle\langle n|. \tag{4.13}$$

Conforme descrito na seção 3.2, a implementação desse POVM, via teorema de Naimark, é feita por uma medição projetiva no espaço estendido por soma direta, dada por

$$\hat{\Pi}'_l = |\mu'_l\rangle\langle\mu'_l|, \tag{4.14}$$

$$|\mu'_l\rangle = \hat{\mathcal{F}}_2|l\rangle, \tag{4.15}$$

onde $l = 0, \ldots, d-1$ e $\hat{\mathcal{F}}_2$ é a transformada de Fourier atuando no espaço d-dimensional do sistema 2, dada pela equação (1.24). Como $\langle\mu'_l|\nu_l\rangle = \langle l|\hat{\mathcal{F}}^{-1}|\nu_l\rangle$, essa medição pode ser descrita no circuito quântico por uma transformada inversa de Fourier, equação (1.25), seguida de uma medição na base computacional em 2. Assim, a operação $\hat{\Xi}$ apresentada na figura 4.1 é substituída por $\hat{\mathcal{F}}^{-1}$, gerando o circuito da figura 4.2. Esse circuito é idêntico ao

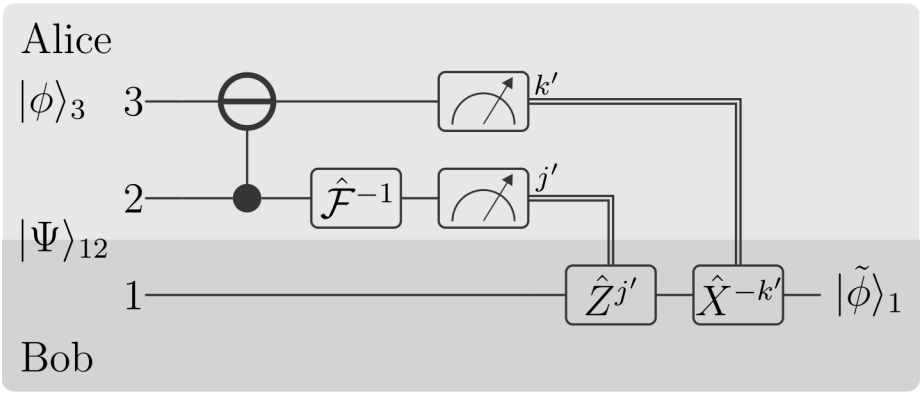

Figura 4.2: Circuito quântico que realiza o protocolo de teleportação determinística ótima. Este é idêntico ao circuito do protocolo padrão mostrado na figura 1.6.

apresentado na figura 1.6, o que indica que ao aplicar a estratégia EM para discriminar os estados do sistema 2, Alice está realizando o protocolo padrão de teleportação. A seguir será mostrado que esse protocolo é ótimo uma vez que alcança, com probabilidade de falha nula, a fidelidade máxima permitida para um dado canal parcialmente emaranhado.

Conforme apontado na figura 4.2, Alice obtém os resultados j' e k', respectivos à medição dos sistemas 2 e 3, onde j' infere estado $|\nu_{j'}\rangle_2$ e k' o estado $|k'\rangle_3$. Ela então comunica seus resultados para Bob através de um canal clássico com $2\log_2 d$ bits de capacidade. Bob, por fim, realiza as transformações unitárias $\hat{Z}_1^{j'}$ e $\hat{X}_1^{-k'}$, definidas na tabela 1.3, ficando com o estado $|\tilde{\phi}\rangle_1$ em mãos. A fidelidade do estado teleportado pode ser expressada em função

da confiança na identificação dos estados $|\nu_l\rangle_2$, como visto na equação (4.12). Neste caso, usando as equações (2.47), (4.4) e (4.14), é fácil mostrar que a confiança na estratégia EM será dada por

$$[P(\hat{\rho}_l|\omega_l)]^{\mathrm{EM}} = \frac{1}{d}\left(\sum_{j=0}^{N_S-1}\lambda_j\right)^2 . \tag{4.16}$$

Inserindo esse resultado em (4.12), obtém-se

$$\begin{aligned} F^{\mathrm{EM}} &= \frac{d[P(\hat{\rho}_l|\omega_l)]^{\mathrm{EM}}+1}{d+1} \\ &= \frac{1}{1+d}\left[1+\left(\sum_{j=0}^{N_S-1}\lambda_j\right)^2\right], \end{aligned} \tag{4.17}$$

onde λ_j são os coeficientes de Schmidt do estado emaranhado apresentado na equação (4.2). A fidelidade de teleportação respeita a condição $F^{\mathrm{EM}} \leq 1$, onde a igualdade é obtida apenas para um estado maximamente emaranhado, ou seja, $N_S = d$ e $\lambda_j = 1/\sqrt{d}, \forall\ j$. Esse resultado é idêntico ao obtido nas referências [61, 62], que garantem que a fidelidade entre os estados $|\phi\rangle_3$ e $|\tilde{\phi}\rangle_1$, através da solução da medida de Haar, é a máxima possível. Assim, o protocolo padrão, que corresponde à implementação da estratégia EM em uma etapa da medição de Alice, é aquele que realiza a teleportação determinística ótima.

4.1.3 Teleportação Probabilística Ótima

Se uma probabilidade de falha for admissível, Alice e Bob podem realizar o protocolo de teleportação quântica com emaranhamento parcial de modo a aumentar, em comparação com o protocolo determinístico, a fidelidade do estado teleportado. Neste caso, o protocolo ótimo será aquele que maximiza essa fidelidade e minimiza a probabilidade de falha. Uma forma realizá-lo é adotando-se a estratégia CM, discutida nas seções 2.2.3 e 3.3, para a discriminação dos estados $|\nu_l\rangle_2$, dados pela equação (4.4). Lembrando do procedimento descrito na seção 3.3.1, a realização de uma medição via CM pode ser feita, inicialmente, com uma operação unitária $\hat{\mathcal{U}}_{2a}$ no sistema 2 em conjunto com um *qubit* auxiliar. Uma projeção na *ancilla* indicará se o procedimento é bem sucedido ou não. Alice informa seu resultado para Bob com um bit de comunicação clássica e prossegue com a realização do protocolo conforme condições previamente estabelecidas. A figura 4.3 ilustra esse procedimento, onde $|\Phi^x\rangle_{123}$ indica o estado global dos sistemas 1, 2 e 3 após a medição da *ancilla* resultante em x $(= 0, 1)$ e $\hat{\Theta}_{x,\text{ṅ}}$ é uma caixa variável que será substituída de acordo com x e com o número de tentativas de se executar uma discriminação bem sucedida, ṅ.

Antes proceder com a conclusão do protocolo, serão analisados os estados $|\Phi^x\rangle_{123}$. Para tanto, será primeiramente descrito matematicamente o procedimento indicado na figura 4.3.

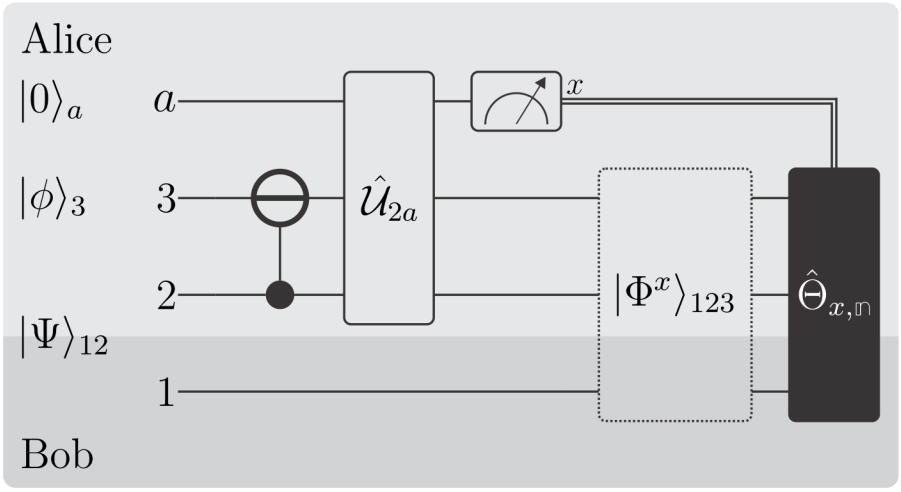

Figura 4.3: Circuito quântico que realiza o protocolo probabilístico de teleportação. A caixa preta com a operação $\hat{\Theta}_{x,\Pi}$ é variável e depende do resultado da medição da *ancilla*, x. Se este for 0, a discriminação é bem sucedida, gerando o estado $|\Phi^0\rangle_{123}$, equação (4.24), e o protocolo de teleportação é realizado conforme a figura 4.4. Se o resultado for 1, o sistema é projetado em $|\Phi^1\rangle_{123}$, equação (4.25). Nesse caso, o protocolo pode ser descartado ou uma nova tentativa de discriminar os estados pode ser realizada. O índice Π indica a quantidade de tentativas de discriminação via CMS (seção 3.3.2) que serão realizadas.

Da identidade da equação (4.3), tem-se o estado total do sistema conjunto dado por

$$|\Psi\rangle_{12}|\phi\rangle_3|0\rangle_a = \frac{1}{d}\sum_{l,k=0}^{d-1} \hat{Z}_1^{-l}\hat{X}_1^k|\phi\rangle_1 \hat{G}_{23}^{\text{XOR}}|\nu_l\rangle_2|k\rangle_3|0\rangle_a. \tag{4.18}$$

A atuação da operação unitária $\hat{\mathcal{U}}_{2a}$, equação (3.37), nos estados $|\nu_l\rangle_2|0\rangle_a$ fornece, segundo a equação (3.46)

$$\hat{\mathcal{U}}_{2a}|\nu_l\rangle_2|0\rangle_a = \sqrt{1-P_?^{\mathbb{1}}}|u_l\rangle_2|0\rangle_a + \sqrt{P_?^{\mathbb{1}}}|\xi_l\rangle_2|1\rangle_a, \tag{4.19}$$

onde

$$\hat{P}_?^{\mathbb{1}} = 1 - N_S\lambda_{\text{min}}^2, \tag{4.20}$$

é a probabilidade mínima de se obter um resultado inconclusivo, conforme a equação (3.35) e λ_{min} é o menor coeficiente de Schmidt da equação (4.2). O índice $\mathbb{1}$ indica o estágio de uma possível implementação da estratégia CMS, descrita na seção 3.3.2, sendo $\mathbb{1}$ indicativo da primeira tentativa. Os estados $|u_l\rangle_2$ e $|\xi_l\rangle_2$, são dados, respectivamente, por

$$|u_l\rangle_2 = \frac{1}{\sqrt{N_S}}\sum_{j=0}^{N_S-1} e^{\frac{2i\pi lj}{d}}|j\rangle_2, \tag{4.21}$$

$$|\xi_l\rangle_2 = \sum_{j=0}^{N_S-1}\sqrt{\frac{\lambda_j^2-\lambda_{\text{min}}^2}{P_?^{\mathbb{1}}}}e^{\frac{2i\pi lj}{d}}|j\rangle_2, \tag{4.22}$$

os quais são simétricos e normalizados. Assim, a atuação dos operadores $\hat{G}_{23}^{\text{XOR}}$ e $\hat{\mathcal{U}}_{2a}$ na equação (4.18) fornece

$$\hat{\mathcal{U}}_{2a}\hat{G}_{23}^{\text{XOR}}|\Psi\rangle_{12}|\phi\rangle_3|0\rangle_a = \sqrt{1-P_?^{\mathbb{1}}}|\Phi^0\rangle_{123}|0\rangle_a + \sqrt{P_?^{\mathbb{1}}}|\Phi^1\rangle_{123}|1\rangle_a, \tag{4.23}$$

onde os estados $|\Phi^0\rangle_{123}$ e $|\Phi^1\rangle_{123}$ representam o sistema tripartido após a medição da *ancilla* e são dados, respectivamente, por

$$|\Phi^0\rangle_{123} = \frac{1}{d}\sum_{l,k=0}^{d-1}\hat{Z}_1^{-l}\hat{X}_l^k|\phi\rangle_1|u_l\rangle_2|k\rangle_3, \tag{4.24}$$

$$|\Phi^1\rangle_{123} = \frac{1}{d}\sum_{l,k=0}^{d-1}\hat{Z}_1^{-l}\hat{X}_l^k|\phi\rangle_1|\xi_l\rangle_2|k\rangle_3. \tag{4.25}$$

Após a atuação da operação $\hat{\mathcal{U}}_{2a}$ Alice realiza uma medição da *ancilla* na base computacional e informa seu resultado para Bob enviando-lhe um bit através de um canal clássico. Cada um dos dois resultados possíveis leva o sistema tripartido a um dos estados das equações (4.24) ou (4.25), os quais serão utilizados para completar o processo de teleportação. Como o restante do protocolo depende do resultado dessa medição, o procedimento será dividido em duas partes, sucesso e falha, apresentadas abaixo.

A. Sucesso

No caso de uma medição na *ancilla* resultante em 0, indicando que a tentativa de medição via CM é bem sucedida, os estados simétricos $|\nu_l\rangle_2$, dados pela equação (4.4), são mapeados no conjunto de estados simétricos uniformes, $|u_l\rangle_2$, equação (4.21). Conforme discutido na seção 3.3.1, o procedimento adotado para finalizar o processo de discriminação via CM é a implementação da estratégia EM. Esta se dá por uma transformada inversa de Fourier seguida de uma medição na base computacional, conforme discutido na seção 4.1.2, e ilustrado na figura 4.4. Após a medição dos sistemas 2 e 3, Alice informa seus resultados a Bob através de um canal clássico com capacidade $2\log_2 d$ bits. Ele, por fim, realiza transformações unitárias em seu sistema, condicionais aos resultados de Alice, ficando com o estado $|\tilde{\phi}\rangle_1$, cuja fidelidade em relação a $|\phi\rangle_3$ será calculada a seguir.

Utilizando a equação (3.29), a confiança máxima na identificação dos estados $|\nu_l\rangle_2$ será

$$[P(\nu_l|l)]_{0,\mathbb{1}}^{\text{CM}} = \frac{N_S}{d},\ \forall\, l, \tag{4.26}$$

onde o índice 0 indica o resultado da medição da *ancilla* e o índice $\mathbb{1}$ o número de tentativas de discriminação via CM dos estados do sistema 2. A fidelidade da teleportação se relaciona

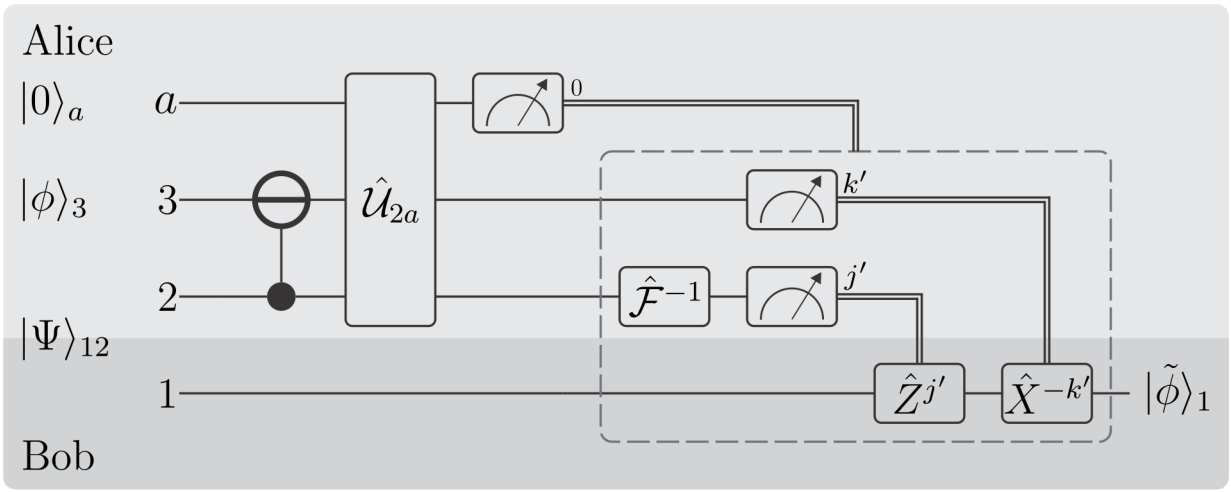

Figura 4.4: Circuito quântico que mostra a realização do protocolo de teleportação para o caso de sucesso da estratégia de discriminação CM. Note que, após a medição da *ancilla* este é realizado de modo idêntico ao protocolo de teleportação padrão.

com a confiança pela equação (4.12), sendo esta, portanto

$$\begin{aligned} F_{0,\mathbb{1}}^{\mathrm{CM}} &= \frac{d[P(\hat{\rho}_l|\omega_l)]^{\mathrm{CM}} + 1}{d+1} \\ &= \frac{N_S + 1}{d+1}. \end{aligned} \tag{4.27}$$

Essa fidelidade depende apenas da dimensão acessível aos estados $|\nu_l\rangle_2$, dada, nesse caso, pelo número de Schmidt do estado emaranhado compartilhado por Alice e Bob, diferentemente do protocolo determinístico, equação (4.17), no qual a fidelidade depende da forma do estado emaranhado, através dos coeficientes de Schmidt. Como evidenciado em [42] e nos exemplos das seções 3.2 e 3.3.2, $[P(\nu_l|l)]_{0,\mathbb{1}}^{\mathrm{CM}} \geq [P(\nu_l|l)]^{\mathrm{EM}}$, o que é equivalente a dizer, em termos da fração de singleto, que $f_{0,\mathbb{1}}^{\mathrm{CM}} \geq f^{\mathrm{EM}}$. Então,

$$F_{0,\mathbb{1}}^{\mathrm{CM}} \geq F^{\mathrm{EM}}. \tag{4.28}$$

Isso mostra que a utilização da estratégia CM permite a realização do protocolo de teleportação com uma fidelidade maior que no caso determinístico. No entanto, o protocolo é probabilístico e estará sujeito a uma falha com probabilidade mínima, $P_?^{\mathbb{1}}$, equação (4.20), a qual, ao contrário da fidelidade, dependerá da forma do estado emaranhado utilizado. A igualdade em (4.28) é atingida apenas no caso em que $|\nu_l\rangle_2 = |u_l\rangle_2$, onde $P_?^{\mathbb{1}} = 0$.

Um caso particular interessante é quando $N_S = d$. Se isso for verdade, os estados $|\nu_l\rangle_2$ são linearmente independentes, e, consequentemente, os estados $|u_l\rangle_2$ em (4.21) serão ortogonais, tendo a forma $\hat{\mathcal{F}}|l\rangle_2$. A realização do protocolo agora fornece uma discriminação sem erros

dos estados, gerando uma teleportação perfeita, $F^{\mathrm{CM}}_{0,\mathbb{1}} = 1$, com probabilidade de sucesso $1 - P^{\mathbb{1}}_{?}$. Nessa situação as estratégias CM e SA coincidem, conforme discutido na seção 3.3.

B. Falha

Uma projeção da *ancilla* em $|1\rangle_a$ indica uma falha no processo de discriminação. Se observa da equação (4.19) que os estados $|\nu_l\rangle_2$ serão mapeados nos estados $|\xi_l\rangle_2$, dados por (4.22). Esses novos estados estarão restritos a um espaço de Hilbert de dimensão menor que N_S, já que ao menos um dos seus coeficientes será nulo. Nesse caso, existem diversas maneiras de prosseguir. Alice e Bob podem desistir do protocolo e recomeçá-lo com um novo estado emaranhado, ou prosseguir com a teleportação considerando o estado tripartido $|\Phi^1\rangle_{123}$, dado por (4.25). Caso desejem continuar, eles devem escolher uma estratégia de discriminação para os estados $|\xi_l\rangle_2$. Dependendo da multiplicidade, $\mathfrak{d}^{\mathbb{1}}$, do menor coeficiente de Schmidt em (4.2), uma nova tentativa de discriminação CM pode ser feita, como apontado na seção 3.3.2. Em caso de sucesso nessa nova tentativa, os estados $|\xi_l\rangle_2$ serão mapeados em estados simétrico uniformes limitados a um subespaço de dimensão $N_S - \mathfrak{d}^{\mathbb{1}}$. Uma discriminação via EM fornecerá a melhor confiança possível. De acordo com a equação (3.52), esta será

$$[P(\nu_l|l)]^{\mathrm{CM}}_{0,2} = \frac{N_S - \mathfrak{d}^{\mathbb{1}}}{d}. \tag{4.29}$$

Portanto, a fidelidade de teleportação, equação (4.12), será

$$\begin{aligned} F^{\mathrm{CM}}_{0,2} &= \frac{N_S - \mathfrak{d}^{\mathbb{1}} + 1}{d+1} \\ &= F^{\mathrm{CM}}_{0,\mathbb{1}} - \frac{\mathfrak{d}^{\mathbb{1}}}{d+1}, \end{aligned} \tag{4.30}$$

a qual é certamente menor que $F^{\mathrm{CM}}_{0,\mathbb{1}}$, porém não necessariamente menor que F^{EM}, equação (4.17). Assim, a teleportação via CMS pode continuar apresentando vantagens na fidelidade, se comparada com o caso determinístico.

A situação de sucesso na segunda iteração da estratégia CMS para a realização da teleportação está ilustrada na figura 4.5. Após enviar o bit 0 comunicando o resultado da medição da *ancilla*, o protocolo segue conforme o caso padrão. A realização desse tipo de teleportação exige um sistema auxiliar bidimensional adicional, assim como um bit extra de comunicação clássica. No caso de uma nova falha, novas tentativas podem ser feitas reiterando o procedimento. A cada nova falha, menor será a fidelidade alcançada, devido à redução do espaço de Hilbert acessível aos estados, e maior será o custo de recursos quânticos e clássicos. Outras estratégias também podem ser utilizadas, cada qual com suas particularidades [37, 43, 55].

Em suma, estratégias probabilísticas são interessantes por poderem fornecer uma maior fidelidade no protocolo de teleportação. Porém, estas exigem um maior número de recursos e possuem probabilidade não nula de falhar. Alice e Bob devem levar essas particularidades em

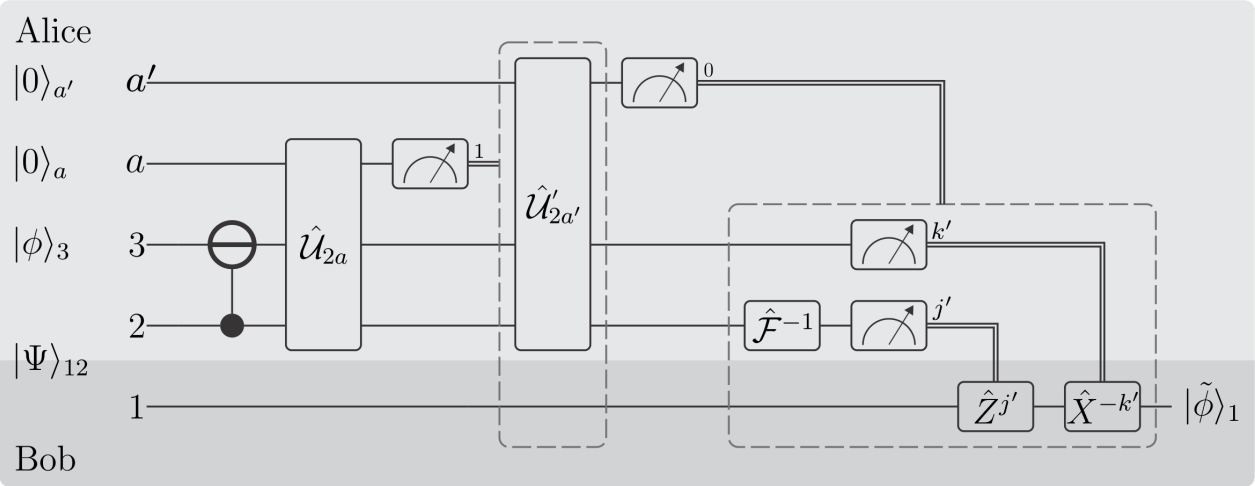

Figura 4.5: Circuito quântico que mostra a realização do protocolo de teleportação para o caso de sucesso da segunda iteração da estratégia CMS.

conta para escolher a estratégia mais conveniente a ser utilizada no processo de teleportação quântica.

4.2 Troca de Emaranhamento

O protocolo de troca de emaranhamento [29] foi apresentado na seção 1.6.3. Dois pares de estados maximamente emaranhados, um compartilhado entre Charlie e Alice e o outro entre Charlie e Bob, são utilizados para criar, de forma determinística, um estado maximamente emaranhado entre os sistemas de Alice e Bob, os quais nunca interagiram entre si. Assim como no caso de teleportação, será mostrado a seguir que, se as partes compartilham estados parcialmente emaranhados, essa tarefa se torna impossível. Suponha, então, que Alice e Bob compartilhem com Charlie os respectivos estados parcialmente emaranhados escritos na decomposição de Schmidt como:

$$|\phi\rangle_A = \sum_{m=0}^{d_A-1} \alpha_m |m\rangle_1 |m\rangle_2, \tag{4.31}$$

$$|\varphi\rangle_B = \sum_{n=0}^{d_B-1} \beta_n |n\rangle_3 |n\rangle_4. \tag{4.32}$$

Por simplicidade assume-se $d_A = d_B = d$.[2] As bases de Schmidt $\{|l\rangle_i\}$ em $\mathcal{H}_i, i = 1, \ldots, 4$, coincidem com a base computacional dos seus respectivos espaços de Hilbert (veja a observação 1). Para melhor entendimento do protocolo, considere a identidade, deduzida no

[2]Para um tratamento mais geral, com $d_A \neq d_B$, veja a referência [38].

apêndice A.2, dada por

$$|\phi\rangle_A|\varphi\rangle_B = \frac{1}{\sqrt{d}}\sum_{k,l=0}^{d-1}\sqrt{p_k}|\Psi_{lk}\rangle_{14}\hat{G}_{23}^{\text{XOR}}|\nu_{lk}\rangle_2|k\rangle_3, \tag{4.33}$$

onde p_k é a probabilidade de encontrar o sistema 3 no estado $|k\rangle_3$, $|\Psi_{lk}\rangle_{14}$ são estados maximamente emaranhados da forma da equação (1.30) e os estados $|\nu_{lk}\rangle_2$ são dados por

$$|\nu_{lk}\rangle_2 = \sum_{s=0}^{d-1}\lambda_{sk}e^{\frac{2i\pi ls}{d}}|s\rangle_2, \tag{4.34}$$

com $\lambda_{sk} = \alpha_s\beta_{s\ominus k}/\sqrt{p_k}$. Os estados $|\nu_{lk}\rangle_2$ formam conjuntos de estados simétricos. A dependência deles com o índice k indica que o sistema 2 é mapeado em d ($k = 0,\ldots,d-1$) diferentes conjuntos, $\Omega_k = \{|\nu_{lk}\rangle_2 \mid l = 0,\ldots,d-1\}$, dependentes da projeção do sistema 3.

Na seção 1.6.1 mostrou-se que uma medição conjunta em uma base maximamente emaranhada pode ser feita com a atuação da porta $\hat{G}^{\text{XOR}}$, seguida de uma transformada inversa de Fourier e de medições na base computacional. Com o uso da equação (4.33), após a atuação da porta $\hat{G}_{23}^{\text{XOR}}$ no estado inicial, tem-se

$$\hat{G}_{23}^{\text{XOR}}|\phi\rangle_A|\varphi\rangle_B = \frac{1}{\sqrt{d}}\sum_{k,l=0}^{d-1}\sqrt{p_k}|\Psi_{lk}\rangle_{14}|\nu_{lk}\rangle_2|k\rangle_3. \tag{4.35}$$

Veja que o sistema 3 pode ser perfeitamente discriminado com uma medição projetiva. Supondo que Charlie realize, nesse sistema, uma medição resultante em k', o estado tripartido dos sistemas 1, 2 e 4 será, com probabilidade $p_{k'}$, dado por

$$|\Phi_{k'}\rangle_{124} = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}|\Psi_{lk'}\rangle_{14}|\nu_{lk'}\rangle_2, \tag{4.36}$$

onde os estados $|\nu_{lk'}\rangle_2$, dados pela equação (4.34), pertencem ao conjunto $\Omega_{k'} = \{|\nu_{lk'}\rangle_2\}$. Embora existam d conjuntos possíveis, todos são compostos por estados simétricos equiprováveis.[3] Estes serão não-ortogonais se qualquer um dos estados $|\phi\rangle_A$ ou $|\varphi\rangle_B$, dados, respectivamente, por (4.31) e (4.32), for parcialmente emaranhado. Portanto, após uma medição arbitrária $|\alpha_{j'}\rangle\langle\alpha_{j'}|$ em 2, o estado emaranhado dos sistemas 1 e 4, compartilhados entre Alice e Bob, será

$$|\tilde{\Psi}_{l'k'}\rangle_{14} \propto \sum_{l=0}^{d-1}c_{ll'}^{(k')}|\Psi_{lk'}\rangle_{14}, \tag{4.37}$$

onde $c_{ll'}^{(k')} = \langle\alpha_{l'}|\nu_{lk'}\rangle$. A menos que $c_{ll'}^{(k')} \propto \delta_{ll'}$, $|\tilde{\Psi}_{l'k'}\rangle_{14}$ não será maximamente emaranhado. Isso somente será possível de forma determinística se os estados $|\nu_{lk'}\rangle_2$ forem ortogonais. Caso

[3] Da equação (4.36), o operador densidade reduzido do sistema 2 será $\hat{\rho} = \frac{1}{d}\sum_l|\nu_{lk'}\rangle\langle\nu_{lk'}|$, mostrando que cada estado $|\nu_{lk'}\rangle$ possui a mesma probabilidade *a priori* $1/d$.

contrário, Charlie deve optar por uma estratégia de discriminação que identifique os estados $|\nu_{lk'}\rangle_2$ de modo a maximizar o grau de emaranhamento de $|\tilde{\Psi}_{l'k'}\rangle_{14}$. A figura 4.6 mostra o circuito do procedimento descrito até então. A caixa preta com a operação $\hat{\Xi}$ é variável

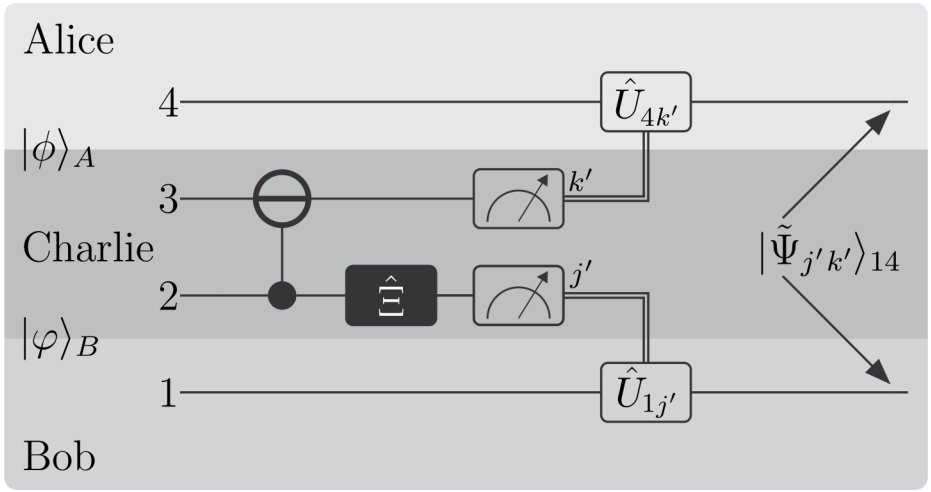

Figura 4.6: Circuito que realiza o protocolo de troca de emaranhamento, onde a caixa preta com a operação $\hat{\Xi}$ é variável conforme a estratégia adotada por Charlie para discriminar os estados simétricos $|\nu_l\rangle_2$, dados por (4.34).

conforme a estratégia adotada por Charlie. O circuito não especifica as transformações unitárias, condicionais aos resultados de Charlie, que Alice e Bob aplicam para gerar um estado emaranhado pré-estabelecido, sendo essas representadas pelas operações $\hat{U}_{1j'}$ e $\hat{U}_{4k'}$. Estas serão arbitrárias, uma vez que o emaranhamento não é alterado por operações unitárias locais.

Assim como no caso da teleportação, dois tipos de protocolos podem ser estudados: determinísticos [38], onde a estratégia EM é adotada para a discriminação dos estados do sistema 2, e probabilísticos [38, 43, 56], onde é realizada a discriminação CM ou estratégias intermediárias entre EM e CM. Como figura de mérito a se otimizar, pode-se utilizar a entropia linear, discutida na seção 1.2, a qual quantifica o emaranhamento de um sistema bipartido. As descrições desses possíveis protocolos são semelhantes àquelas mostradas no caso de teleportação e não serão tratadas aqui. O leitor interessado pode consultar as referências mencionadas acima.

5

Codificação Superdensa via Canais Parcialmente Emaranhados

O protocolo de codificação superdensa [1] foi discutido na seção 1.6.4 para o caso em que Alice e Bob compartilhavam um sistema quântico bipartido em um estado maximamente emaranhado. Mostrou-se que um total de Dd_2 mensagens perfeitamente distinguíveis poderiam ser transmitidas pelo canal quântico de forma determinística, onde $D \equiv \min(d_1, d_2)$ e d_1 e d_2 são as dimensões dos respectivos sistemas de Bob e Alice. Se não houvesse emaranhamento, apenas d_2 mensagens perfeitamente distinguíveis poderiam ser enviadas, mostrando, assim, a vantagem do protocolo quântico.

Quando o estado compartilhado por Alice e Bob não é maximamente emaranhado, a codificação superdensa não será tão eficiente quanto no caso de emaranhamento máximo, mas, ainda assim, apresentará vantagens sobre um protocolo realizado sem emaranhamento. Isso é mostrado neste capítulo, onde serão apresentados os resultados originais da dissertação. O problema de codificação superdensa via canais parcialmente emaranhados é abordado de forma similar àquela apresentada no capítulo anterior para teleportação quântica e troca de emaranhamento. Dessa maneira, as estratégias de discriminação de estados simétricos equiprováveis, apresentadas no capítulo 3, são utilizadas para otimizar o protocolo. A otimização corresponderá à maximização da informação mútua entre Alice e Bob, quantidade que será definida mais adiante e que foi adotada como figura de mérito. Mostra-se que os protocolos determinísticos são otimizados através da estratégia EM, enquanto os probabilísticos, através das estratégias CM, CMS ou estratégias intermediárias entre EM e CM.

Este capítulo está dividido da seguinte maneira: na seção 5.1, se formula o problema geral da codificação superdensa via canais parcialmente emaranhados. A informação mútua é definida na seção 5.2 e se obtém uma expressão geral dessa quantidade para o problema estudado. Protocolos e exemplos para os casos determinístico e probabilístico são apresentados respectivamente, nas seções 5.3 e 5.4.

5.1 Formulação Geral do Problema

Suponha que Alice e Bob compartilhem um sistema bipartido em um estado emaranhado, escrito na decomposição de Schmidt (veja seção 1.2) como

$$|\Psi\rangle_{12} = \sum_{r=0}^{N_S-1} \lambda_r |r\rangle_1 |r\rangle_2, \tag{5.1}$$

onde será assumido que as bases de Schmidt $\{|r\rangle_1\}$ e $\{|r\rangle_2\}$ coincidem com as bases computacionais dos espaços $\mathcal{H}_1$ e $\mathcal{H}_2$ (veja a observação 1), cujas dimensões são d_1 e d_2, respectivamente. Assim, o número de Schmidt deve respeitar o vínculo $N_S \leq \min(d_1, d_2) \equiv D$. Em seu sistema (2), Alice realiza operações unitárias para codificar uma de $\mathcal{N}$ mensagens.[1] Ela, então, envia seu sistema para Bob, que decodifica a mensagem através de uma medição no sistema conjunto. A figura 5.1 ilustra esse procedimento na forma de circuito quântico, onde a caixa preta com a operação $\hat{\Xi}$ é variável de acordo com as operações unitárias que Alice utiliza na codificação e a caixa preta com a operação $\hat{\Theta}$ varia com o esquema de medição de Bob.

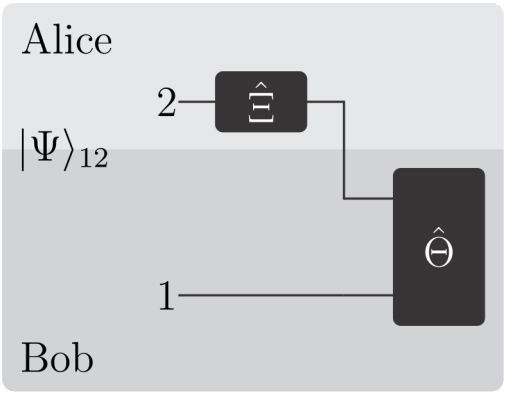

Figura 5.1: Circuito que representa o protocolo de codificação superdensa, onde tanto a codificação, caixa preta com a operação $\hat{\Xi}$, quanto a decodificação, caixa preta com a operação $\hat{\Theta}$, são variáveis.

Há duas maneiras de se abordar o problema descrito acima. A primeira delas consiste em buscar o número máximo de mensagens perfeitamente distinguíveis que podem ser transmitidas através do canal quântico. Para isso, Alice deve encontrar um conjunto arbitrário de operadores $\{\hat{W}_j \mid j = 0, \ldots, \mathcal{N}-1\}$ que permitam a codificação de tais mensagens. Esse problema foi introduzido por Mozes *et al.* [8], onde foram encontradas soluções analíticas para estados iniciais específicos e soluções numéricas para a codificação de até $\mathcal{N} = 7$ mensagens

[1] Por hora, não será imposta nenhuma condição sobre $\mathcal{N}$.

em estados parcialmente emaranhados de *qutrits*. Na referência [9], Ji *et al.* determinaram que o número máximo de mensagens codificáveis em estados parcialmente emaranhados deve respeitar o vínculo $\mathcal{N}_{\max} < d_2 D - 1$. Posteriormente, Wu *et al.* [10] expressaram o limite superior de $\mathcal{N}$ em função do maior coeficiente de Schmidt do estado compartilhado, analisaram protocolos realizados com sistemas de dimensões diferentes (o que já está sendo considerado aqui) e utilizaram a estratégia de discriminação SA (veja seção 2.2.2) para a discriminação probabilística de mensagens codificadas em subespaços de dimensão $d_2 N_S$. Bourdon *et al.* [11] analisaram a relação desse problema com a entropia de emaranhamento do estado inicial. Embora seja evidente o interesse nesse tipo de abordagem, esta não será tratada no presente trabalho.

A segunda maneira de abordar o problema é a mais usual e será investigada aqui. Ela consiste em se tentar transmitir tanta informação quanto seria possível por um canal maximamente emaranhado. Nesse contexto, um importante resultado foi apresentado em [67]. Foi demonstrado que, para estados puros, a capacidade de transmissão de informação é ótima quando, no processo de codificação, Alice atua com os mesmos operadores do protocolo padrão descrito na seção 1.6.4, com mesma probabilidade *a priori*. Portanto, o problema estudado aqui pode ser formulado da seguinte maneira: dado o estado da equação (5.1), Alice realiza as operações $\hat{X}_2^{-k}\hat{\mathcal{Z}}_2^j$ ($k = 0, \ldots, d_2 - 1$ e $j = 0, \ldots, D-1$) para codificar uma de $\mathcal{N} = D d_2$ mensagens com as mesmas probabilidades *a priori* $1/\mathcal{N}$. O estado total, após a codificação, será dado por

$$\begin{aligned}
|\tilde{\Psi}_{jk}\rangle_{12} &= \hat{X}_2^{-k}\hat{\mathcal{Z}}_2^j|\Psi\rangle_{12} \\
&= \sum_{r=0}^{N_S-1} \lambda_r |r\rangle_1 \hat{X}_2^{-k}\hat{\mathcal{Z}}_2^j |r\rangle_2 \\
&= \sum_{r=0}^{N_S-1} \lambda_r e^{\frac{2i\pi jr}{D}} |r\rangle_1 |r \ominus k\rangle_2 \\
&= \sum_{r=0}^{N_S-1} \lambda_r e^{\frac{2i\pi jr}{D}} \hat{G}_{12}^{\text{XOR}} |r\rangle_1 |k\rangle_2 \\
&= \hat{G}_{12}^{\text{XOR}} |\nu_j\rangle_1 |k\rangle_2,
\end{aligned} \tag{5.2}$$

onde

$$|\nu_j\rangle_1 = \sum_{r=0}^{N_S-1} \lambda_r e^{\frac{2i\pi jr}{D}} |r\rangle_1, \tag{5.3}$$

e o operador $\hat{G}_{12}^{\text{XOR}}$ é definido na tabela 1.3. Alice envia seu sistema para Bob que deve identificar o estado $|\tilde{\Psi}_{jk}\rangle_{12}$. Primeiramente, ele atua com a porta $\hat{G}_{12}^{\text{XOR}}$, deixando o sistema composto no estado

$$\hat{G}_{12}^{\text{XOR}} |\tilde{\Psi}_{jk}\rangle_{12} = |\nu_j\rangle_1 |k\rangle_2. \tag{5.4}$$

O estado sistema 2 pode ser perfeitamente discriminado com uma medição projetiva na base computacional. Resta a Bob identificar $|\nu_j\rangle_1$ para concluir o processo de decodificação da mensagem enviada por Alice. Os estados $|\nu_j\rangle_1$ em (5.3) formam um conjunto de D ($j = 0, \ldots, D-1$) estados simétricos sob a operação $\hat{\mathcal{Z}}_2$, os quais são equiprováveis uma vez que Alice codifica suas mensagens com a mesma probabilidade *a priori*. Estes estados serão não-ortogonais para um canal parcialmente emaranhado e a dependência linear deles dependerá do número de Schmidt de $|\Psi\rangle_{12}$ em (5.1): se este número não for máximo, isto é, se $N_S < D$, eles serão linearmente dependentes. Caso contrário, se $N_S = D$, eles serão linearmente independentes. Portanto, a realização do protocolo de codificação superdensa pode ser concluída de forma ótima com a utilização das estratégias de discriminação apresentadas no capítulo 3. A figura 5.2 mostra o protocolo descrito, onde a caixa preta com a operação $\hat{\Theta}$ é variável de acordo com a estratégia de discriminação adotada por Bob.

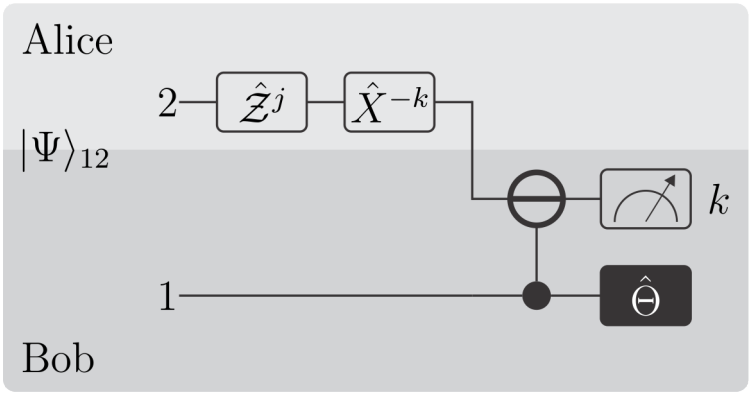

Figura 5.2: Representação em forma de circuito quântico do protocolo de codificação superdensa investigado neste trabalho, onde a caixa preta com a operação $\hat{\Theta}$ varia conforme a estratégia adotada para discriminação do conjunto de estados do sistema 1.

5.2 Informação Mútua na Codificação Superdensa

O objetivo de diversos protocolos de informação quântica é a transmissão de informação clássica através de canais quânticos. Esse procedimento pode ser descrito da seguinte maneira: i) Alice codifica uma de N mensagens preparando um sistema quântico em determinado estado com certa probabilidade *a priori*. Às mensagens de Alice será atribuída a variável M. ii) O sistema é enviado para Bob, que "lê" a mensagem determinando seu estado através de uma medição. Em um caso ideal, onde os estados preparados por Alice são ortogonais e o canal quântico não apresentar ruído[2], Bob irá identificar a mensagem perfeitamente. Porém,

[2]O ruído do canal é uma interação indesejada entre o sistema e o ambiente em que ele está imerso, resultando em alterações no estado preparado por Alice. Portanto, o sistema não pode mais ser exatamente

se eles forem não-ortogonais, será impossível para Bob discriminar o estado sem erros e de forma determinística. Seja L a variável associada à leitura de Bob. Considerando que ele obtenha um resultado de medição ω_l que o leva a inferir a mensagem $L = l$, surge a questão: quanto da mensagem M é aprendido com a leitura L? Essa questão é respondida pela teoria *clássica* de informação. Pode parecer contraintuitivo, uma vez que canais quânticos estão sendo utilizados. Entretanto, a mensagem enviada é clássica e é acerca de quanto se aprende sobre ela que o problema é construído. O canal quântico é utilizado no processamento da informação, o que permite, por exemplo, a codificação superdensa.

Para a análise do protocolo de codificação superdensa definido na seção anterior, será tomada como figura de mérito a informação mútua. Neste contexto, essa grandeza dita a quantidade média de informação sobre a mensagem M enviada por Alice adquirida com a leitura L de Bob, e é definida como

$$I(M;L) = H(M) - H(M|L), \tag{5.5}$$

onde $H(M)$ é a entropia de Shannon e $H(M|L)$ é a entropia condicional (veja seção 1.4). De acordo com a equação (5.4), a mensagem é codificada no estado $\hat{\rho}_{jk} = |\nu_j\rangle_1\langle\nu_j| \otimes |k\rangle_2\langle k|$ ($j = 0, \ldots, D-1$ e $k = 0, \ldots, d_2 - 1$) do sistema composto, com probabilidade *a priori* $p(\hat{\rho}_{jk}) = 1/(Dd_2)$. A leitura corresponde ao resultado da medição de Bob, ω_{lm}, associada ao operador $\hat{\Pi}_{lm}$. Dessa forma, a entropia de Shannon será

$$\begin{aligned} H(M) &= -\sum_{j=0}^{D-1}\sum_{k=0}^{d_2-1} p(\hat{\rho}_{jk}) \log_2 p(\hat{\rho}_{jk}) \\ &= -\sum_{j=0}^{D-1}\sum_{k=0}^{d_2-1} \frac{1}{Dd_2} \log_2 \frac{1}{Dd_2} \\ &= \log_2 Dd_2, \end{aligned} \tag{5.6}$$

e a entropia condicional,

$$H(M|L) = -\sum_{j,l=0}^{D-1}\sum_{k,m=0}^{d_2-1} p(\omega_{lm}) p(\hat{\rho}_{jk}|\omega_{lm}) \log_2 p(\hat{\rho}_{jk}|\omega_{lm}). \tag{5.7}$$

Utilizando a regra de Bayes,

$$p(\hat{\rho}_{jk}|\omega_{lm}) = p(\omega_{lm}|\hat{\rho}_{jk}) \frac{p(\hat{\rho}_{jk})}{p(\omega_{lm})}, \tag{5.8}$$

a entropia condicional pode ser escrita como

$$H(M|L) = -\sum_{j,l=0}^{D-1}\sum_{k,m=0}^{d_2-1} p(\hat{\rho}_{jk}) p(\omega_{lm}|\hat{\rho}_{jk}) \log_2 \left[p(\omega_{lm}|\hat{\rho}_{jk}) \frac{p(\hat{\rho}_{jk})}{p(\omega_{lm})} \right], \tag{5.9}$$

especificado. Frequentemente, sistemas sujeitos a (pequenos) ruídos podem ser descritos por estados mistos, equação (1.4) [3, 44]. Neste trabalho, esses casos não serão analisados.

onde $p(\omega_{lm}|\hat{\rho}_{jk})$ é a probabilidade de se obter o resultado de medição ω_{lm} dado que o estado preparado foi $\hat{\rho}_{jk}$ e $p(\omega_{lm})$ é a probabilidade total de se obter o resultado ω_{lm}. Os estados do sistema 2 são ortogonais, podendo ser discriminados com uma medição na base computacional. Os estados do sistema 1, são não-ortogonais sempre que o canal quântico descrito pela equação (5.1) não for maximamente emaranhado. Neste caso, esses estados devem ser determinados de acordo com alguma estratégia de discriminação. Considerando que somente as estratégias discutidas no capítulo 3 serão utilizadas, tem-se

$$\begin{aligned} p(\omega_{lm}|\hat{\rho}_{jk}) &= \mathrm{Tr}(\hat{\rho}_{jk}\hat{\Pi}_{lm}) \\ &= \mathrm{Tr}\left[\Big(|\nu_j\rangle\langle\nu_j| \otimes |k\rangle\langle k|\Big)\left(\hat{\Pi}_l^S \otimes |m\rangle\langle m|\right)\right] \\ &= \mathrm{Tr}(\hat{\rho}_j\hat{\Pi}_l^S)\delta_{km}, \end{aligned} \tag{5.10}$$

onde $\hat{\Pi}_l^S$ é o elemento de POVM da estratégia S (S = EM, CM, etc.) adotada para determinar o estado simétrico $|\nu_j\rangle_1$, dado pela equação (5.3). Da simetria do problema,

$$p(\omega_{lm}) = \frac{1}{Dd_2}. \tag{5.11}$$

Substituindo esses resultados na equação (5.9), obtém-se

$$\begin{aligned} [H(M|L)]^S &= -\frac{1}{Dd_2}\sum_{j,l=0}^{D-1}\sum_{k,m=0}^{d_2-1}\mathrm{Tr}(\hat{\rho}_j\hat{\Pi}_l^S)\delta_{km}\log_2\left[\mathrm{Tr}(\hat{\rho}_j\hat{\Pi}_l^S)\right] \\ &= -\frac{1}{D}\sum_{j,l=0}^{D-1}\mathrm{Tr}(\hat{\rho}_j\hat{\Pi}_l^S)\log_2\left[\mathrm{Tr}(\hat{\rho}_j\hat{\Pi}_l^S)\right] \\ &= [H(L_1|M_1)]^S, \end{aligned} \tag{5.12}$$

onde L_1 é a variável correspondente à leitura da parte da mensagem codificada no sistema 1, indicada pela variável M_1. Dada a estratégia S, a entropia condicional $[H(L_1|M_1)]^S$ quantifica a incerteza de L_1 dado M_1. Portanto, essa grandeza está associada a erros no processo de discriminação dos estados do sistema 1. Utilizando as equações (5.5), (5.6) e (5.12), a informação mútua entre Alice e Bob no protocolo de codificação superdensa descrito na seção 5.1 será

$$[I(M;L)]^S = \log_2 Dd_2 - [H(L_1|M_1)]^S. \tag{5.13}$$

A entropia condicional em (5.12) obedece a relação $0 \leq [H(M_1|L_1)]^S \leq \log_2 D$, onde 0 indica nenhuma incerteza e $\log_2 D$ a incerteza máxima. Assim, a informação mútua assume valores no intervalo $\log_2 d_2 \leq [I(M;L)]^S \leq \log_2 Dd_2$. Seu valor máximo somente é alcançado de forma determinística se o canal quântico do protocolo for maximamente emaranhado. Neste caso, os estados $|\nu_j\rangle_1$ serão ortogonais, de modo que $[H(L_1|M_1)]^S = 0$. Portanto, a

informação mútua será $I(M;L) = \log_2 Dd_2$, o que equivale a um canal quântico com capacidade de transmitir $\mathcal{N} = Dd_2$ mensagens clássicas e recupera o resultado da seção 1.6.4, conforme esperado. A informação mútua mínima, $[I(M;L)]^S = \log_2 d_2$, ocorre para um canal sem emaranhamento, onde os $|\nu_j\rangle_1$ serão idênticos e, portanto, nenhuma informação poderá ser extraída deles, de maneira que $[H(M|L)]^S = \log_2 D$. Para canais parcialmente emaranhados, serão adotadas estratégias de discriminação de estados com o intuito de minimizar $[H(L_1|M_1)]^S$, e, assim, maximizar a informação mútua de forma determinística ou probabilística.

5.3 Codificação Superdensa Determinística

Como descrito na seção 5.1, a conclusão do protocolo de codificação superdensa é feita com a discriminação dos estados $|\nu_j\rangle_1$, dados pela equação (5.3). Supondo que Bob não admita resultados inconclusivos, erros associados à sua medição serão invetáveis sempre que o conjunto $\{|\nu_j\rangle_1 \mid j = 0, \ldots, D-1\}$ for não-ortogonal. Afim de maximizar a informação mútua, Bob deve discriminar entre os estados desse conjunto de modo a obter o menor erro possível, tarefa realizada pela estratégia EM (veja seção 2.2.1). Como os $|\nu_j\rangle_1$ formam um conjunto de estados simétricos equiprováveis, o POVM que os discrimina com erro mínimo é dado pelas equações (3.9)–(3.11).[3] Conforme mostrado na seção 3.2, a implementação desse POVM é feita, via teorema de Naimark, através de uma medição projetiva no espaço de Hilbert estendido por soma direta, dada por

$$\hat{\Pi}'_l = |\mu'_l\rangle\langle\mu'_l|, \tag{5.14}$$

com

$$\begin{aligned} |\mu'_l\rangle &= \hat{\mathcal{F}}_D|l\rangle \\ &= \frac{1}{\sqrt{D}} \sum_{s=0}^{D-1} e^{\frac{2i\pi ls}{D}} |s\rangle, \end{aligned} \tag{5.15}$$

onde $\hat{\mathcal{F}}_D$ é a transformada de Fourier, dada pela equação (1.24), atuando no subespaço $\mathcal{H}_D$ de $\mathcal{H}_1$, o qual será d_1-dimensional ($\mathcal{H}_D = \mathcal{H}_1$) se $d_1 < d_2$ e d_2-dimensional se $d_2 < d_1$. Como $\langle\mu'_l|\nu_j\rangle = \langle l|\hat{\mathcal{F}}_D^{-1}|\nu_j\rangle$, essa medição pode ser representada em forma de circuito quântico por uma transformada inversa de Fourier seguida de uma medição na base computacional em 1, conforme ilustrado na figura 5.3. Esse procedimento é idêntico ao mostrado na seção 1.6.4, figura 1.9. Portanto, assim como mostrado para a teleportação (seção 4.1), ao aplicar a estratégia EM na etapa de decodificação, está se realizando, de fato, o protocolo padrão de codificação superdensa [1]. Para canais parcialmente emaranhados, o protocolo padrão

[3] Além de minimizar o erro, mostrou-se em [47] que esse POVM satisfaz a condição necessária para a maximização da informação mútua no processo de discriminação de estados simétricos equiprováveis.

realiza a codificação superdensa ótima com probabilidade de falha nula, conforme mostrado nas referências [12, 67, 68].

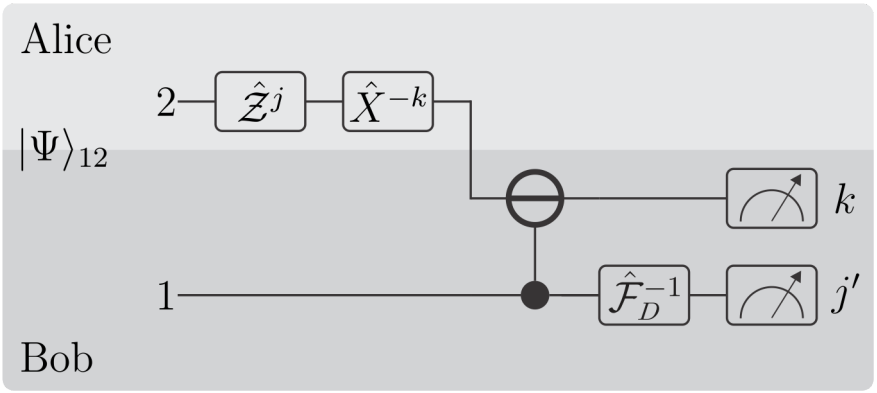

Figura 5.3: Representação em forma de circuito do protocolo de codificação superdensa determinístico ótimo. O resultado da medição do sistema 1 está indicado por j' para enfatizar que podem ocorrer erros na discriminação da mensagem.

De acordo com as equações (5.3), (5.14) e (5.15), a probabilidade de se obter o resultado de medição ω_l, dado que o estado preparado por Alice é $|\nu_j\rangle_1$, será

$$\begin{aligned}
[\mathrm{Tr}(\hat{\rho}_j \hat{\Pi}'_l)]^{\mathrm{EM}} &= |\langle \mu'_l | \nu_j \rangle|^2 \\
&= \frac{1}{D} \sum_{r,s=0}^{N_S-1} \lambda_r \lambda_s e^{\frac{2i\pi(r-s)(j-l)}{D}} \\
&= \frac{1}{D} \sum_{r=0}^{N_S-1} \lambda_r^2 + \frac{1}{D} \sum_{\substack{r,s=0 \\ s>r}}^{N_S-1} \lambda_r \lambda_s \left(e^{\frac{2i\pi(r-s)(j-l)}{D}} + e^{\frac{-2i\pi(r-s)(j-l)}{D}} \right) \\
&= \frac{1}{D} + \frac{2}{D} \sum_{\substack{r,s=0 \\ s>r}}^{N_S-1} \lambda_r \lambda_s \cos\left(\frac{2\pi(j-l)(r-s)}{D} \right) \\
&\equiv P_{jl}^{\mathrm{EM}}(\{\lambda_r\}, N_S) \equiv P_{jl}^{\mathrm{EM}},
\end{aligned} \tag{5.16}$$

onde a última definição foi adotada com o intuito de simplificar a notação. Substituindo esse resultado nas equações (5.12) e (5.13), a informação mútua entre Alice e Bob pode ser escrita como

$$[I(M;L)]^{\mathrm{EM}} = \log_2 Dd_2 + \frac{1}{D} \sum_{j,l=0}^{D-1} P_{jl}^{\mathrm{EM}} \log_2 \left(P_{jl}^{\mathrm{EM}} \right), \tag{5.17}$$

a qual depende, através de P_{jl}^{EM}, dos coeficientes e do número de Schmidt do estado emaranhado inicial, dado por (5.1). Veja que, se houver emaranhamento máximo, $P_{jl}^{\mathrm{EM}} = \delta_{jl}$ e, portanto, $[I(M;L)]^{\mathrm{EM}} = \log_2 Dd_2$. Por outro lado, se não existir emaranhamento, $P_{jl}^{\mathrm{EM}} = 1/D$ e $[I(M;L)]^{\mathrm{EM}} = \log_2 d_2$. Esses resultados recuperam os limites apresentados na seção 5.2.

Exemplo 1: codificação superdensa determinística com estado parcialmente emaranhado de *qubits*

O exemplo mais simples de aplicação desse tipo de protocolo é com um par de *qubits* emaranhados [12]. Considere, então, que Alice e Bob compartilham o estado dado por

$$|\Psi\rangle_{12} = \cos\theta|0\rangle_1|0\rangle_2 + \sin\theta|1\rangle_1|1\rangle_2. \tag{5.18}$$

Alice codifica uma de quatro mensagens atuando com os operadores $\hat{X}_2^{-k}$ $(k = 0, 1)$ e $\hat{Z}^j$ $(j = 0, 1)$, dados na tabela 1.2. O estado após a codificação de Alice será dado por

$$\begin{aligned} |\tilde{\Psi}_{jk}\rangle_{12} &= \hat{X}_2^{-k}\hat{Z}_2^j|\Psi\rangle_{12} \\ &= \hat{C}_{12}^{\text{NOT}}|\nu_j\rangle_1|k\rangle_2, \end{aligned} \tag{5.19}$$

onde $\hat{C}_{12}^{\text{NOT}}$ é definida também na tabela 1.2, e

$$|\nu_j\rangle_1 = \cos\theta|0\rangle_1 + e^{\frac{2i\pi j}{2}}\sin\theta|1\rangle_1. \tag{5.20}$$

Segundo o circuito da figura 5.3, Bob primeiramente atua com a porta $\hat{C}_{12}^{\text{NOT}}$, resultando em

$$\hat{C}_{12}^{\text{NOT}}|\tilde{\Psi}_{jk}\rangle = |\nu_j\rangle_1|k\rangle_2. \tag{5.21}$$

Uma medição na base computacional em 2 determina seu estado perfeitamente, contribuindo com 1 bit para a informação mútua.

A discriminação dos estados $|\nu_j\rangle_1$ será feita segundo a estratégia de discriminação EM e coincide com o exemplo da seção 2.2.1. Utilizando os projetores (2.18) e (2.19) daquele exemplo para calcular P_{jl}^{EM} definido em (5.16) e inserindo o resultado na equação (5.17), obtém-se a informação mútua

$$[I(M;L)]^{\text{EM}} = 2 + \sum_{j=0}^{1}\left(\frac{1+(-1)^j\sin 2\theta}{2}\right)\log_2\left[\frac{1+(-1)^j\sin 2\theta}{2}\right]. \tag{5.22}$$

A demonstração dessa equação encontra-se no apêndice D.1. O gráfico da figura 5.4 mostra a variação da informação mútua com o ângulo de separação dos estados $|\nu_j\rangle_1$. O valor máximo de dois bits ocorre em $\theta = \pi/4$, limite onde o estado inicial é maximamente emaranhado e os estados $|\nu_j\rangle_1$ são ortogonais. O mínimo do gráfico se dá onde $(\langle\nu_0|\nu_1\rangle)_1 = 1$. Nesse caso, o sistema compartilhado por Alice e Bob está em um estado produto e não existe mais correlação entre eles.

Exemplo 2: codificação superdensa determinística com sistemas de dimensões $\mathbf{d_1 = 3}$ e $\mathbf{d_2 = 8}$

Suponha que o estado compartilhado inicial seja dado por

$$|\Psi\rangle_{12} = \sum_{m=0}^{2}\lambda_m|m\rangle_1|m\rangle_2, \tag{5.23}$$

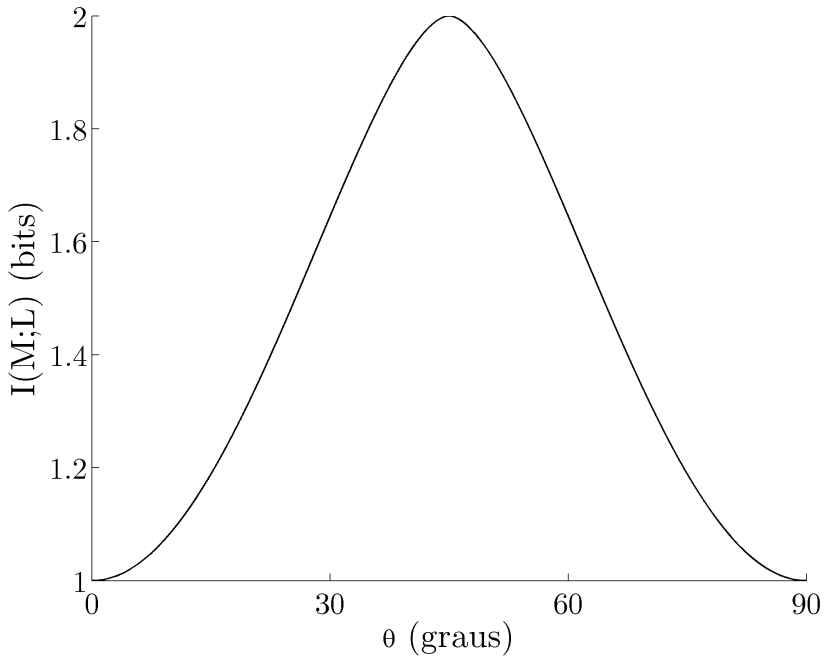

Figura 5.4: Informação mútua em função do ângulo de separação dos estados $|\nu_j\rangle_1$. Este gráfico corresponde ao protocolo determinístico de codificação superdensa descrito no exemplo 1.

onde o espaço $\mathcal{H}_1$ possui dimensão 3 e $\mathcal{H}_2$ dimensão 8. De acordo com o procedimento mostrado na seção (5.1), Alice codifica uma de $\mathcal{N} = d_1 d_2 = 24$ mensagens, com o objetivo de transmitir $\log_2 24 \approx 4{,}585$ bits de informação clássica pelo canal quântico. Bob deve determinar o estado preparado por Alice, dado pela equação (5.4). Uma medição na base computacional em $\mathcal{H}_2$ determina o estado do sistema 2 perfeitamente, contribuindo com $\log_2 8 = 3$ bits para a informação mútua. Para completar o protocolo, Bob discrimina entre os três estados simétricos $|\nu_j\rangle_1$, equação (5.3), de acordo com a estratégia EM. O cálculo da informação mútua deste exemplo é mostrado no apêndice D.2. O gráfico da figura 5.5, obtido da equação (D.21), mostra a variação de $[I(M;L)]^{\mathrm{EM}}$ em função dos coeficientes de Schmidt λ_0 e $\lambda_1(\lambda_2 = \sqrt{1-\lambda_0^2-\lambda_1^2})$. O valor máximo da informação mútua, $[I(M;L)]^{\mathrm{EM}} = \log_2 24$ bits, é alcançado quando o estado (5.23) é maximamente emaranhado, ou seja, $\lambda_0 = \lambda_1 = \lambda_2 = 1/\sqrt{3}$. Os valores mínimos de 3 bits correspondem a um canal sem emaranhamento ($\lambda_0 = \lambda_1 = 0$, $\lambda_0 = \lambda_2 = 0$ e $\lambda_1 = \lambda_2 = 0$). As curvas em $\lambda_0 = 0$, $\lambda_1 = 0$ e $\lambda_2 = 0$, correspondem a um canal com número de Schmidt não máximo, neste caso com $N_S = 2$. O próximo exemplo ilustrará, com mais detalhes, este tipo de situação.

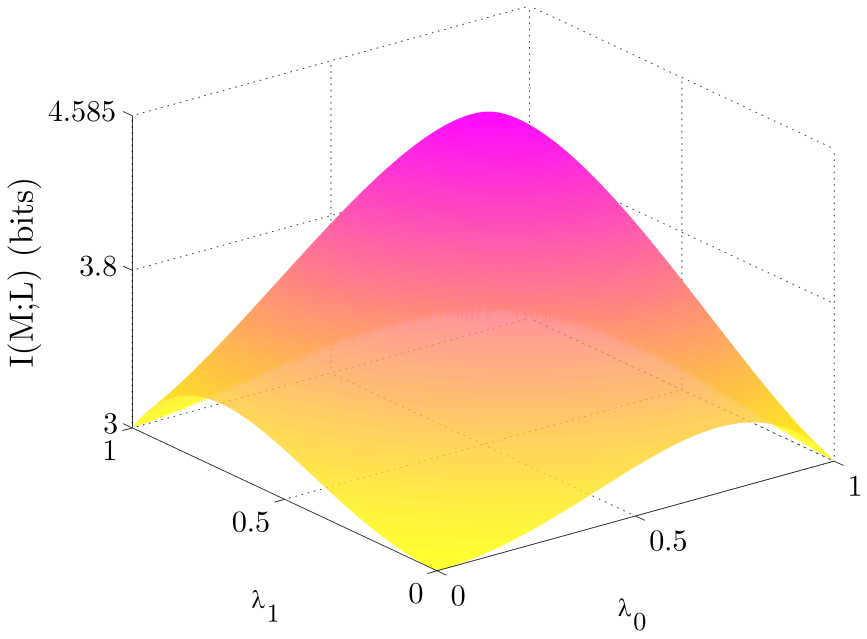

Figura 5.5: Variação da informação mútua, em função dos coeficientes de Schmidt λ_0 e λ_1. Este gráfico corresponde ao protocolo determinístico de codificação superdensa com emaranhamento parcial descrito no exemplo 2.

Exemplo 3: codificação superdensa determinística com $\mathbf{N_S < D}$

Considere que Alice e Bob compartilhem um estado emaranhado onde $d_1 = 8$ e $d_2 = 4$, o qual possui número de Schmidt não máximo, isto é, $N_S < D = 4$. Usando (5.1), esse será dado por

$$|\Psi\rangle_{12} = \sum_{l=0}^{2} \lambda_l |l\rangle_1 |l\rangle_2. \tag{5.24}$$

Agora, suponha que Alice deseja codificar uma de $\mathcal{N} = 32$ mensagens no sistema conjunto, equivalente ao número máximo de mensagens perfeitamente distinguíveis de um estado maximamente emaranhado deste canal. Neste caso, a informação mútua do protocolo, em função dos coeficientes λ_0 e λ_1 ($\lambda_2 = \sqrt{1-\lambda_0^2-\lambda_1^2}$), é mostrada no gráfico da figura 5.6, e está demonstrada no apêndice D.3, equação (D.31). A base do gráfico é de 3 bits, resultado referente à uma medição projetiva no sistema 2. Os estados $|\nu_j\rangle_1$ ($j = 0, \ldots, 3$), dados por

$$|\nu_j\rangle_1 = \sum_{l=0}^{2} \lambda_l e^{\frac{2i\pi jl}{4}} |l\rangle_1, \tag{5.25}$$

estão restritos a um subespaço tridimensional, e, portanto, são linearmente dependentes. Desse modo, independentemente da distribuição dos coeficientes λ_l, as mensagens de Alice

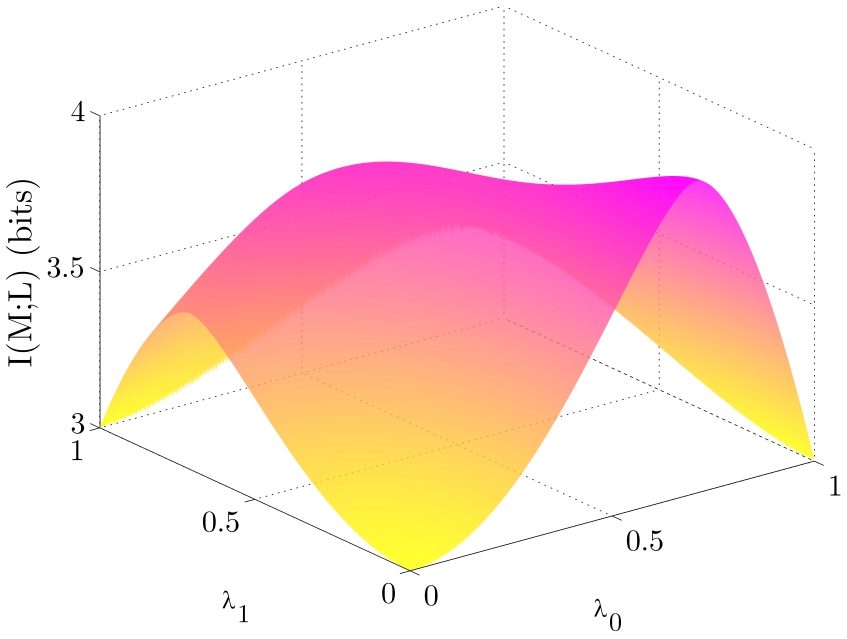

Figura 5.6: Variação da informação mútua, em função dos coeficientes λ_0 e λ_1, do protocolo de codificação superdensa com estado inicial parcialmente emaranhado com o número de Schmidt não máximo, apresentado no exemplo 3.

nunca serão perfeitamente distinguíveis. Ou seja, $[I(M;L)]^{\mathrm{EM}} < \log_2 Dd_2 = 5$.

O resultado da figura 5.6 não tem uma interpretação simples. Se os estados $|\nu_j\rangle_1$ são simétricos e equiprováveis, por que existem pontos no gráfico com valor maior do que outros gerados pela simples permutação dos coeficientes de Schmidt? Para tentar responder essa questão, serão analisados dois pontos do gráfico: i) $\lambda_1 = 0$ e $\lambda_0 = \lambda_2 = 1/\sqrt{2}$, e ii) $\lambda_0 = 0$ e $\lambda_1 = \lambda_2 = 1/\sqrt{2}$ (o qual é equivalente ao ponto $\lambda_2 = 0$ e $\lambda_0 = \lambda_1 = 1/\sqrt{2}$). Em i) $[I(M;L)]^{\mathrm{EM}} = 4$ bits e em ii) a informação mútua é 3,5 bits. Essa diferença pode ser entendida se observando os estados a serem discriminados em cada caso (a normalização será desconsiderada), dados por

$$\text{i)} \begin{cases} |\nu_0\rangle_1 = |0\rangle + |2\rangle, \\ |\nu_1\rangle_1 = |0\rangle - |2\rangle, \\ |\nu_2\rangle_1 = |0\rangle + |2\rangle, \\ |\nu_3\rangle_1 = |0\rangle - |2\rangle, \end{cases} \qquad \text{ii)} \begin{cases} |\nu_0\rangle_1 = |1\rangle + |2\rangle, \\ |\nu_1\rangle_1 = |1\rangle + i|2\rangle, \\ |\nu_2\rangle_1 = |1\rangle - |2\rangle, \\ |\nu_3\rangle_1 = |1\rangle - i|2\rangle. \end{cases} \tag{5.26}$$

Na situação i), existem dois pares de estados perfeitamente distinguíveis, os quais são idênticos entre assim. Portanto, são codificadas quatro mensagens, onde duas delas são redundantes, o que é equivalente à codificação de apenas duas mensagens.[4] Assim, a medição de Bob con-

[4] A codificação de apenas duas mensagens pode ser vista, também, através da simetria dos estados em i),

tribui, neste caso, com 1 bit para a informação mútua. Na situação ii) também existem dois pares de estados ortogonais, porém, estes não são idênticos entre si. As quatro mensagens codificadas não podem ser perfeitamente discriminadas, e, de acordo com a equação (D.31), a medição de Bob fornecerá apenas 0,5 bit para a informação mútua.

É interessante perceber que esse exemplo é equivalente à uma tentativa de realizar o protocolo de codificação superdensa com um número de mensagens maior que a capacidade do canal quântico, ou seja, $\mathcal{N} > d_2 D$. Suponha que Alice e Bob compartilhem o estado da equação (5.24), mas que agora o sistema 1 seja um *qutrit*. De acordo com o protocolo padrão, Alice deveria preparar uma de 24 mensagens com a utilização dos operadores $\hat{\mathcal{Z}}_2^j$ $(j = 0, 1, 2)$, dado pela equação (1.51), e $\hat{X}_2^{-k}$ $(k = 0, \ldots, 7)$, definido na tabela 1.3. Porém, ao invés de realizar o protocolo com esses operadores, Alice utiliza uma outra transformação, dada por

$$\hat{Z}'^j \equiv \sum_{m=0}^{2} e^{\frac{2i\pi jm}{4}} |m\rangle\langle m|, \tag{5.27}$$

com $j = 0, \ldots, 3$, afim de codificar 32 mensagens. Após a codificação, o estado conjunto é dado por

$$\begin{aligned} \hat{X}_2^{-k} \hat{Z}_2'^j |\Psi\rangle_{12} &= \sum_{l=0}^{2} \lambda_l e^{\frac{2i\pi m}{4}} |l\rangle_1 |l \ominus k\rangle_2 \\ &= \hat{G}_{12}^{\text{XOR}} |\nu_j\rangle_1 |k\rangle_2, \end{aligned} \tag{5.28}$$

onde os estados $|\nu_j\rangle_1$ são idênticos aos da equação (5.25), o que mostra a equivalência entre esses procedimentos. Portanto, embora exista uma diferença conceitual entre o protocolo padrão com número de Schmidt não máximo e um protocolo onde se codifica um número maior de mensagens com a substituição do operador $\hat{\mathcal{Z}}$, eles são matematicamente equivalentes.

Ao se tentar enviar um número de mensagens maior que a capacidade do canal, estas se tornam menos distinguíveis, causando, assim, uma redução na informação mútua. Como Alice e Bob conhecem o estado emaranhado (5.24), pode ser mais conveniente a transmissão de um número de mensagens restrito à capacidade de um canal maximamente emaranhado no subespaço $(N_S d_2)$-dimensional. Ou seja, Alice codificará uma de $\mathcal{N} = N_S d_2$ mensagens utilizando a operação unitária $\hat{X}_2^{-k} \hat{Z}_2''^j$ $(k = 0, \ldots, 7$ e $j = 0, 1, 2)$, onde

$$\hat{Z}_2'' = \sum_{m=0}^{2} e^{\frac{2i\pi m}{3}} |m\rangle\langle m|. \tag{5.29}$$

Essa situação é equivalente à do exemplo anterior, uma vez que os estados simétricos gerados com essa codificação serão iguais aos da equação (D.14). A figura 5.7 mostra a comparação

os quais são simétricos em relação ao operador $\hat{\mathcal{Z}}' = \sum_{r=0}^{4} e^{\frac{2i\pi r}{2}} |r\rangle\langle r|$.

da informação mútua entre a codificação superdensa realizada com $\mathcal{N} = Dd_2$ (superfície preenchida) e com $\mathcal{N} = N_S d_2$ (superfície em forma de rede), onde $N_S < D$. Como pode ser observado, a informação mútua entre Alice e Bob, para a maior parte dos canais descritos por (5.24), é maior quando o número de mensagens é $\mathcal{N} = N_S d_2$.

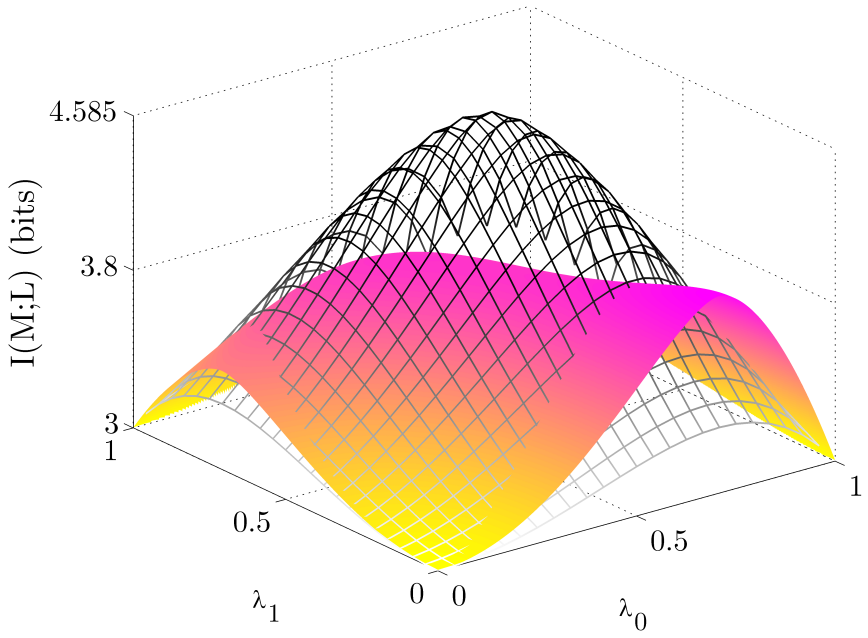

Figura 5.7: Informação mútua, em função dos coeficientes de Schmidt λ_0 e λ_1, para protocolos realizados com estados emaranhados onde $N_S < D$. Superfície preenchida: $\mathcal{N} = Dd_2$. Superfície em forma de rede: $\mathcal{N} = N_S d_2$. A figura é referente aos casos discutidos no exemplo 3.

5.4 Codificação Superdensa Probabilística

A identificação do estado simétrico $|\nu_j\rangle_1$ é o passo final para Bob decodificar, da melhor maneira possível, a mensagem enviada por Alice. Como visto na seção 3.3, ao se admitir um resultado inconclusivo no processo de discriminação, é possível obter uma confiança maior do que seria possível com estratégias determinísticas. Isso implica em uma redução da entropia condicional, equação (5.12), uma vez que ela quantifica a incerteza na leitura da parte da mensagem codificada no sistema 1. Consequentemente, é possível aumentar a informação mútua entre Alice e Bob, se comparada à do protocolo da seção anterior. Nesta situação, se analisará a codificação superdensa assistida pelas estratégias probabilísticas CM, CMS e intermediárias entre EM e CM, apresentadas nas respectivas seções 3.3, 3.3.2, 3.4.

5.4.1 Codificação Superdensa Assistida Pela Estratégia CM

Suponha que Bob decida discriminar os estados $|\nu_j\rangle_1$, equação (5.3), com a estratégia CM. Para realizar esse procedimento, conforme descrito na seção 3.3.1, ele aplica uma transformação unitária sobre o sistema 1 em conjunto com um sistema auxiliar bidimensional, de modo que

$$\hat{\mathcal{U}}_{1a}|\nu_j\rangle_1|0\rangle_a = \sqrt{1-P_?^{\mathbb{1}}}|u_j\rangle_1|0\rangle_a + \sqrt{P_?^{\mathbb{1}}}|\xi_j\rangle_1|1\rangle_a, \tag{5.30}$$

onde

$$|u_j\rangle_1 = \frac{1}{\sqrt{N_S}}\sum_{r=0}^{N_S-1} e^{\frac{2i\pi jr}{D}}|r\rangle_1, \tag{5.31}$$

$$|\xi_j\rangle_1 = \sum_{r=0}^{N_S-1}\sqrt{\frac{\lambda_r^2-\lambda_{\min}^2}{P_?^{\mathbb{1}}}}e^{\frac{2i\pi jr}{D}}|r\rangle_1, \tag{5.32}$$

com $\lambda_{\min} = \min(\lambda_r)_{r=0}^{N_S-1}$. Uma medição na *ancilla* resultando em 0 indicará que o procedimento foi bem sucedido. Nesse caso, os estados $|\nu_j\rangle_1$ são projetados em $|u_j\rangle_1$, os quais são maximamente distinguíveis. Entretanto, se a medição da *ancilla* resultar em 1, acusando uma falha no processo de discriminação, os estados iniciais serão projetados em $|\xi_j\rangle_1$, os quais formam um conjunto de estados simétricos restritos a um espaço de Hilbert menor que o espaço inicial, e, portanto, serão menos separados. A otimização desse procedimento é feita com a minimização da probabilidade de falha, a qual, de acordo com a equação (3.35), será dada por

$$P_?^{\mathbb{1}} = 1 - N_S\lambda_{\min}^2, \tag{5.33}$$

onde o índice $\mathbb{1}$ indica o número de tentativas de execução da discriminação via CMS (veja seção 3.3.2). O circuito que implementa esse protocolo é mostrado na figura 5.8, onde a caixa preta com a operação $\hat{\Theta}_{x\mathbb{n}}$ será substituída com a medição de Bob que conclui o procedimento, a qual dependerá do resultado da medição da *ancilla*, x. Os casos de sucesso e falha serão discutidos em detalhes a seguir.

A. Sucesso

Se o resultado da medição da *ancilla* for 0, com probabilidade $1 - P_?^{\mathbb{1}} = N_S\lambda_{\min}^2$, a discriminação via CM é bem sucedida e os estados $|\nu_j\rangle_1$, dados pela equação (5.3), são mapeados nos $|u_j\rangle_1$, equação (5.31), os quais formam um conjunto de estados simétricos equiprováveis uniformes. A conclusão do processo de discriminação é feita com uma transformada inversa de Fourier, atuando em um subespaço $\mathcal{H}_D$ de $\mathcal{H}_1$,[5] seguida de uma medição na base computacional, conforme apontado na seção 3.3.1. Esse passo da medição é equivalente à discriminação EM, que é realizada pelo POVM $\{\hat{\Pi}'_l \mid l = 0, \ldots, D\}$, dado pelas equações (5.14)

[5] Veja discussão abaixo da equação (5.15).

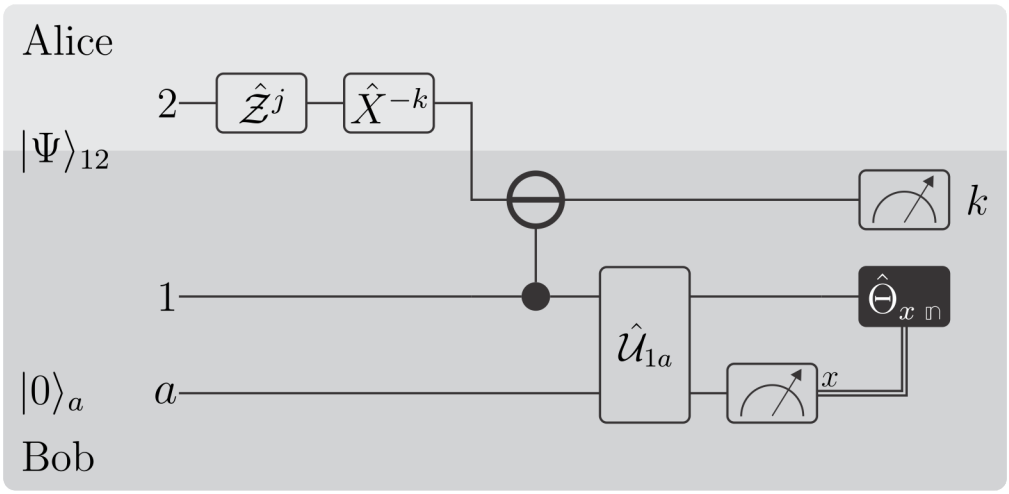

Figura 5.8: Representação em forma de circuito do protocolo de codificação superdensa com decodificação via discriminação CM. A caixa preta com a operação $\hat{\Theta}_{x\mathbb{n}}$ varia conforme o resultado da medição da *ancilla*. O índice $\mathbb{n}$ indica o número de tentativas de discriminação via CMS realizadas.

e (5.15). A figura 5.9 mostra o circuito que realiza o protocolo de codificação superdensa com esse procedimento.

Para determinar a informação mútua neste caso, calcula-se, primeiramente, a probabilidade de se obter o resultado de medição ω_l, dado que o estado preparado é $|\nu_j\rangle_1$. Utilizando as equações (5.14), (5.15) e (5.31), esta será dada por

$$\begin{aligned}
[\mathrm{Tr}(\hat{\rho}_j\hat{\Pi}'_l)]^{\mathrm{CM}} &= \frac{1}{DN_S}\sum_{r,s=0}^{N_S-1} e^{\frac{2i\pi(r-s)(j-l)}{D}} \\
&= \frac{1}{DN_S}\sum_{r=0}^{N_S-1} 1 + \frac{1}{DN_S}\sum_{\substack{r,s=0\\ s>r}}^{N_S-1}\left(e^{\frac{2i\pi(r-s)(j-l)}{D}} + e^{\frac{-2i\pi(r-s)(j-l)}{D}}\right) \\
&= \frac{1}{D} + \frac{2}{DN_S}\sum_{\substack{r,s=0\\ s>r}}^{N_S-1}\cos\left(\frac{2\pi(r-s)(j-l)}{D}\right) \\
&\equiv P_{jl}^{\mathrm{CM}}(N_S) \equiv P_{jl}^{\mathrm{CM}},
\end{aligned} \tag{5.34}$$

onde P_{jl}^{CM} foi definido para simplificar a notação. Substituindo esse resultado nas equações (5.12) e (5.13), obtém-se

$$[I(M;L)]^{\mathrm{CM},\mathbb{1}} = \log_2 Dd_2 + \frac{1}{D}\sum_{j,l=0}^{D-1} P_{jl}^{\mathrm{CM}}\log_2\left(P_{jl}^{\mathrm{CM}}\right), \tag{5.35}$$

sendo esse um dos resultados originais da presente dissertação. Observe que, ao contrário de (5.17), a informação mútua em (5.35) não depende dos coeficientes de Schmidt do estado

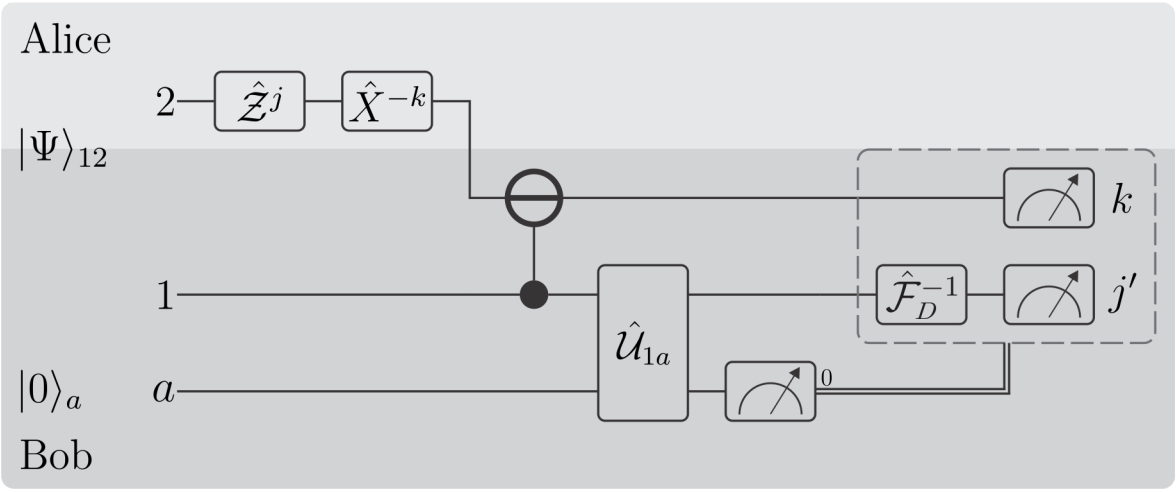

Figura 5.9: Representação em forma de circuito do protocolo de codificação superdensa com decodificação via discriminação CM bem sucedida na primeira tentativa. Após a medição da *ancilla* o circuito é idêntico ao do protocolo padrão, já que este realiza a identificação ótima (discriminação EM) dos estados $|u_j\rangle_1$.

emaranhado (5.1), mas somente do número de Schmidt através de P_{jl}^{CM}. Com isso, definidas as dimensões d_1 e d_2 dos sistemas de Bob e Alice, respectivamente, a informação mútua será constante para um dado N_S, qualquer que seja o grau de emaranhamento do canal quântico. Entretanto, o processo será probabilístico e a probabilidade de sucesso, $N_S\lambda_{\mathrm{min}}^2$, dependerá do canal quântico utilizado.

Quando o número de Schmidt do estado (5.1) for máximo, ou seja, $N_S = D$, os estados $|u_j\rangle_1$ serão ortogonais entre si. Portanto, $P_{jl}^{\mathrm{CM}} = \delta_{jl}$ e $[I(M;L)]^{\mathrm{CM},\mathbb{1}} = \log_2 Dd_2$. Essa situação é equivalente ao uso da estratégia SA para a realização de protocolos de codificação superdensa [13,14], o que se torna possível por conta da independência linear dos estados $|\nu_j\rangle_1$. A equação (5.35) generaliza esses casos e fornece a informação mútua ótima para protocolos probabilísticos de codificação superdensa independentemente da dependência linear dos $|\nu_j\rangle_1$. Na situação onde não há emaranhamento, $P_{jl}^{\mathrm{CM}} = 1/D$ e, portanto, $[I(M;L)]^{\mathrm{CM},\mathbb{1}} = \log_2 d_2$, o que está de acordo com o que foi apontado na seção 5.2.

Exemplo 4: codificação superdensa probabilística com estado emaranhado de *ququarts*

Considere que Alice e Bob compartilham o estado

$$|\Psi\rangle_{12} = \sum_{m=0}^{N_S-1} \lambda_m |m\rangle_1 |m\rangle_2, \tag{5.36}$$

com ambos os sistemas pertencentes a espaços de Hilbert quadridimensionais (*ququarts*). Alice codifica uma de 16 mensagens com a atuação das portas $\hat{X}^{-k}$ ($k = 0, \ldots, 3$) e $\hat{\mathcal{Z}}^{j}$ ($j = 0, \ldots, 3$), com o objetivo de transmitir $\log_2 16 = 4$ bits de informação. De acordo com a equação (5.4), uma medição na base computacional no sistema 2 contribui com 2 bits para a informação mútua. A discriminação dos estados do sistema 1 será feita de acordo com a estratégia CM. Se ele é bem sucedido, os estados $|\nu_j\rangle_1$ são mapeados em $|u_j\rangle_1$, dados por (5.31), os quais são discriminados via EM. A informação mútua entre Alice e Bob dependerá do número de Schmidt do estado compartilhado, e será analisada a seguir para todos os casos possíveis. Os resultados abaixo são demonstrados em detalhes no apêndice D.4.

Se o número de Schmidt for máximo, $N_S = 4$, as estratégias CM e SA coincidem. Os estados $|u_j\rangle_1 = \hat{\mathcal{F}}_D|j\rangle_1$ serão ortogonais e $P_{jl}^{\mathrm{CM}} = \delta_{jl}$. Assim, de (5.35), a informação mútua será

$$[I(M;L)]_{N_S=4}^{\mathrm{CM},\mathbb{1}} = 4 \text{ bits}, \tag{5.37}$$

a qual é equivalente à informação mútua em um protocolo com emaranhamento máximo.

Se o número de Schmidt não for máximo, a informação mútua entre Alice e Bob será consideravelmente reduzida, uma vez que os estados $|u_j\rangle_1$ serão, necessariamente, não-ortogonais. Para $N_S = 3$, tem-se

$$[I(M;L)]_{N_S=3}^{\mathrm{CM},\mathbb{1}} \approx 2{,}792 \text{ bits}, \tag{5.38}$$

e para $N_S = 2$

$$[I(M;L)]_{N_S=2}^{\mathrm{CM},\mathbb{1}} = 2{,}5 \text{ bits}. \tag{5.39}$$

Em todos os casos se nota a vantagem trazida pelo emaranhamento, visto que a informação mútua seria, no máximo, de 2 bits se este não estivesse presente.

B. Falha

Caso a tentativa de discriminação via CM falhe, ou seja, se a *ancilla* é projetada em $|1\rangle_a$, os estados iniciais $|\nu_j\rangle_1$, dados pela equação (5.3), são mapeados nos $|\xi_j\rangle_1$, equação (5.32). Esses estados estão restritos a um subespaço N^2-dimensional, com

$$N^2 = N_S - \mathfrak{d}^{\mathbb{1}}, \tag{5.40}$$

onde $\mathfrak{d}^{\mathbb{1}}$ é a degenerescência do coeficiente de Schmidt $\lambda_{\min}$. Se $\mathfrak{d}^{\mathbb{1}} < N_S - 1$ [condição (iii) da seção 3.3.1], Bob poderá realizar uma nova medição que forneça informação sobre o estado do sistema 1, caso que será considerado aqui.

Suponha que Bob utiliza a estratégia CMS, discutida na seção 3.3.2, para tentar discriminar os estados do sistemas 1 tantas vezes quanto possível. A dimensão acessível a esses estados após a $\mathfrak{n}$-ésima tentativa de discriminação será

$$N_1^{\mathfrak{n}} = N_S - \mathfrak{d}^{\mathbb{1}} - \ldots - \mathfrak{d}^{\mathfrak{n}-\mathbb{1}}. \tag{5.41}$$

O procedimento será bem sucedido com probabilidade

$$P_S^{\mathbb{n}} = 1 - P_?^{\mathbb{1}} P_?^{2} \dots P_?^{\mathbb{n}}, \tag{5.42}$$

onde

$$P_?^{\mathbb{n}} = 1 - N^{\mathbb{n}} \left(\lambda_{\min}^{\mathbb{n}}\right)^2, \tag{5.43}$$

com $\lambda_{\min}^{\mathbb{n}}$ sendo o coeficiente mínimo do estado a ser discriminado na $\mathbb{n}$-ésima iteração. Como visto previamente, após um sucesso, Bob segue com o protocolo como no caso padrão. Neste caso, a probabilidade de se obter o resultado ω_l na $\mathbb{n}$-ésima tentativa de discriminação, dado que o estado do sistema 1 era inicialmente $|\nu_j\rangle_1$, é dada por

$$\begin{aligned}
[\mathrm{Tr}(\hat{\rho}_j \hat{\Pi}'_l)]^{\mathrm{CMS},\mathbb{n}} &= \frac{1}{DN^{\mathbb{n}}} \sum_{r,s=0}^{N^{\mathbb{n}}-1} e^{\frac{2i\pi(r-s)(j-l)}{D}} \\
&= \frac{1}{DN^{\mathbb{n}}} \sum_{r=0}^{N^{\mathbb{n}}-1} 1 + \frac{1}{DN^{\mathbb{n}}} \sum_{\substack{r,s=0 \\ s>r}}^{N^{\mathbb{n}}-1} \left(e^{\frac{2i\pi(r-s)(j-l)}{D}} + e^{\frac{-2i\pi(r-s)(j-l)}{D}} \right) \\
&= \frac{1}{D} + \frac{2}{DN^{\mathbb{n}}} \sum_{\substack{r,s=0 \\ s>r}}^{N^{\mathbb{n}}-1} \cos\left(\frac{2\pi(r-s)(j-l)}{D} \right) \\
&\equiv P_{jl}^{\mathrm{CMS}}(N^{\mathbb{n}}) \equiv P_{jl}^{\mathrm{CMS},\mathbb{n}}.
\end{aligned} \tag{5.44}$$

Portanto, de (5.12) e (5.13),

$$[I(M;L)]^{\mathrm{CMS},\mathbb{n}} = \log_2 Dd_2 + \frac{1}{D} \sum_{j,l=0}^{D-1} P_{jl}^{\mathrm{CMS},\mathbb{n}} \log_2 \left(P_{jl}^{\mathrm{CMS},\mathbb{n}} \right). \tag{5.45}$$

A cada iteração da estratégia, a informação mútua respeitará a relação $[I(M;L)]^{\mathrm{CMS},\mathbb{n}} < [I(M;L)]^{\mathrm{CMS},\mathbb{n}-1}$. Isso ocorre porque os estados (5.32) resultantes de uma falha serão menos distinguíveis, o que aumenta a entropia condicional (seção 5.2) e, consequentemente, reduz a informação mútua, como pode ser visto na equação (5.13). Apesar disso, existirão canais quânticos para os quais esta quantidade ainda será maior na $\mathbb{n}$-ésima tentativa do que seria para o protocolo determinístico, seção 5.3. Neste caso, ao aplicar a estratégia CMS, aumenta-se a chance de se realizar a codificação superdensa com informação mútua maior que aquela alcançada de forma determinística aplicando a estratégia EM.

Exemplo 5: codificação superdensa via estratégia CMS para estado emaranhado de *ququarts*

Considere, como no exemplo anterior, que Alice e Bob compartilhem um par de ququarts no estado emaranhado (5.36), com número de Schmidt máximo, $N_S = 4$. Suponha que Bob obtenha um resultado inconclusivo na sua tentativa de discriminar o estado $|\nu_j\rangle_1$ com a estratégia

CM. Ele então prossegue com a estratégia CMS e é bem sucedido na segunda tentativa, conforme ilustrado na figura 5.10. Como mostrado no apêndice D.5, se a degenerescência de $\lambda_{\min}$ for igual a 1, a informação mútua será

$$[I(M;L)]^{\mathrm{CMS},2} \approx 2{,}792 \text{ bits}, \tag{5.46}$$

a qual possui o mesmo valor do exemplo anterior, para $N_S = 3$. Se a degenerescência é $\mathfrak{d}^{\mathbb{1}} = 2$, obtém-se

$$[I(M;L)]^{\mathrm{CMS},2} = 2{,}5 \text{ bits}, \tag{5.47}$$

resultado igual ao do exemplo anterior para $N_S = 2$. Esses resultados mostram a equivalência entre os casos onde o número de Schmidt não é máximo e casos onde o espaço de Hilbert acessível aos estados é diminuído após tentativas mal sucedidas de discriminação CM. Isso se torna evidente ao observar que as equações (5.35) e (5.45) dependem apenas da dimensão acessível aos estados que serão discriminados.

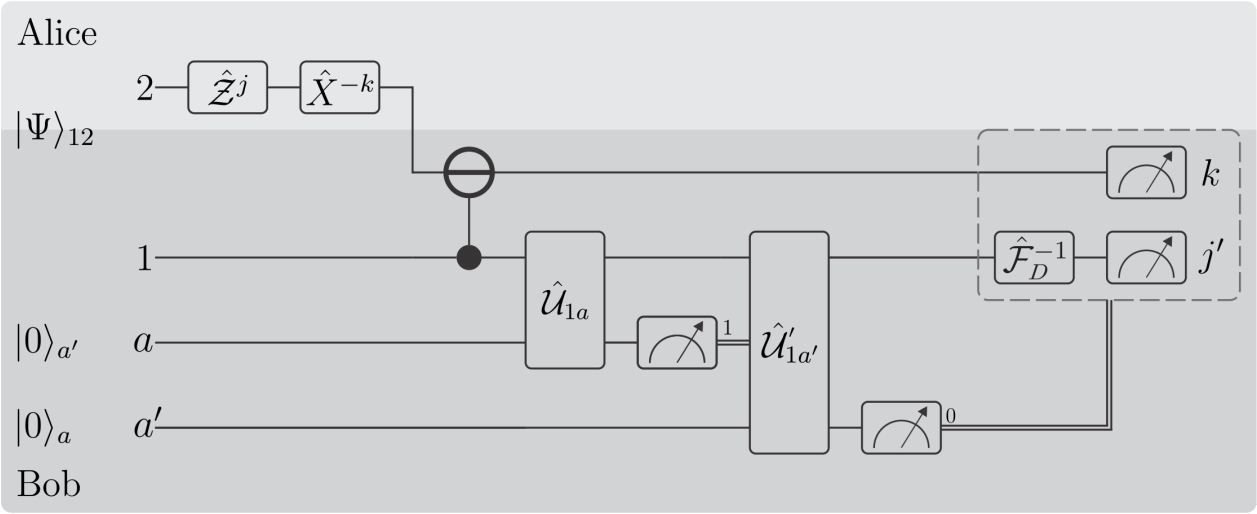

Figura 5.10: Circuito quântico que realiza o protocolo de codificação superdensa com a estratégia CMS bem sucedida na segunda tentativa de discriminação, conforme descrito no exemplo 5.

Exemplo 6: comparação das estratégias EM e CMS na realização da codificação superdensa com número de Schmidt máximo

Para comparar a informação mútua dos protocolos de codificação superdensa determinístico e probabilístico, considere o estado emaranhado do exemplo 2, dado pela equação (5.23). Como o número de Schmidt é máximo, as estratégias CM e SA coincidem, e, em caso de discriminação bem sucedida, a informação mútua será

$$[I(M;L)]^{\mathrm{CM},\mathbb{1}} = \log_2 24 \approx 4{,}585 \text{ bits}. \tag{5.48}$$

Se sua primeira tentativa de discriminação falhar, Bob tentará, se possível, realizar uma nova iteração da estratégia CM. Caso ele seja bem sucedido em sua segunda tentativa, a informação mútua, de acordo com a equação (5.45), será

$$[I(M;L)]^{\mathrm{CMS},2} \approx 3{,}333 \text{ bits}. \tag{5.49}$$

Em caso de falha na etapa anterior, uma terceira tentativa de discriminação via CMS se torna impossível, uma vez que a dimensão acessível aos estados do sistema 1 será unitária. O resultado (5.49) está demonstrado no apêndice D.6. O gráfico da figura 5.11 mostra a comparação das estratégias EM e CMS, onde as superfícies i), ii) e iii) são dadas pelas respectivas equações (5.48), (5.49) e (5.17). Na superfície ii), as curvas que atingem o limite inferior de 3 bits de informação mútua correspondem aos estados (5.23) cuja multiplicidade de $\lambda_{\min}$ é dois, de forma que a segunda tentativa de discriminação é inútil. As regiões da superfície iii) abaixo da superfície ii), indicam os estados emaranhados para os quais o sucesso na segunda tentativa da estratégia CMS ainda produz uma informação mútua maior que aquela obtida via estratégia EM.

A figura 5.12(a) mostra a probabilidade de sucesso, P_S, de se realizar a codificação superdensa na primeira tentativa da estratégia CMS, dada por $3\lambda_{\min}^2$. Com esta probabilidade, a informação mútua entre Alice e Bob será sempre maior que no caso determinístico para qualquer estado emaranhado (5.23). A figura 5.12(b) mostra a probabilidade total de se realizar a codificação superdensa com a condição que a informação mútua seja maior que no protocolo determinístico. Note que a região deste gráfico onde as probabilidades são maiores que aquela do gráfico 5.12(a) representam os estados emaranhados para os quais é mais vantajoso aplicar a estratégia CMS.

Segundo o gráfico da figura 5.11, a informação mútua da realização bem sucedida do protocolo via CM é sempre superior (ou igual, no caso maximamente emaranhado) à de protocolos determinísticos. Entretanto, se a probabilidade de falha for levada em conta, estratégias determinísticas, em média, realizam a codificação superdensa com maior informação mútua. Em (5.48) esta quantidade possui contribuições da medição do sistema 2, $[I(M_2;L_2)] = 3$ bits, o qual é perfeitamente distinguível, e do sistema 1, $[I(M_1;L_1)]^{\mathrm{CM},\mathbb{1}} = \log_2 3$ bits, do qual a informação será extraída com probabilidade $1 - P_?^{\mathbb{1}} = 3\lambda_{\min}^2$ (veja a equação (5.33)). Levando essa probabilidade em conta, a informação mútua entre Alice e Bob, em média, será dada por

$$\begin{aligned}[\overline{I}(M;L)]^{\mathrm{CM},\mathbb{1}} &= \left(1 - P_?^{\mathbb{1}}\right)[I(M_1;L_1)]^{\mathrm{CM},\mathbb{1}} + [I(M_2;L_2)] \\ &= 3\lambda_{\min}^2 \log_2 3 + 3 \text{ bits}.\end{aligned} \tag{5.50}$$

O gráfico da figura 5.13 mostra esse resultado em comparação com a curva iii) da figura 5.11.

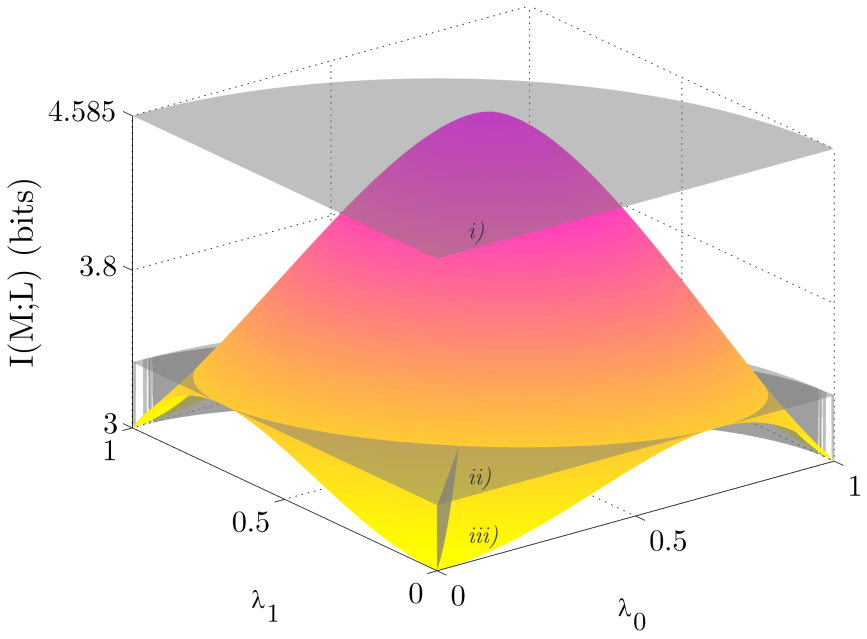

Figura 5.11: As superfícies do gráfico mostram a informação mútua em função dos coeficientes de Schmidt λ_0 e λ_1 ($\lambda_2 = \sqrt{1-\lambda_0^2-\lambda_1^2}$) da equação (5.23), e correspondem a: i) Informação mútua de uma medição bem sucedida na primeira tentativa de discriminação via CM, equação (5.35). ii) Informação mútua de uma medição bem sucedida na segunda tentativa de discriminação via CMS, equação (5.45). iii) Informação mútua segundo a estratégia EM, equação (5.17). O gráfico fornece uma comparação entre os protocolos de codificação superdensa descritos nos exemplos 2 e 6 deste capítulo.

Exemplo 7: comparação das estratégias EM e CMS na realização da codificação superdensa com número de Schmidt não máximo

Considere novamente a situação apresentada no exemplo 3, onde Alice e Bob compartilhavam o estado dado por (5.24). Agora, porém, Bob tentará discriminar o estado do sistema 1 de acordo com a estratégia CMS. Os resultados a seguir estão demonstrados no apêndice D.7. Se Bob obtiver um sucesso na primeira tentativa de discriminação, a informação mútua será

$$[I(M;L)]^{\mathrm{CM},\mathbb{1}} \approx 3{,}792 \text{ bits}. \tag{5.51}$$

No caso de falha, uma nova tentativa de discriminação pode ser feita, desde que o coeficiente $\lambda_{\min}$ não seja degenerado. Se bem sucedida, a informação mútua terá o valor de

$$[I(M;L)]^{\mathrm{CMS},2} = 3{,}5 \text{ bits}. \tag{5.52}$$

O gráfico da figura 5.14 compara a informação mútua entre os protocolos determinístico (via EM) e probabilístico (via CMS). Nesta situação, podem ser observadas regiões onde o

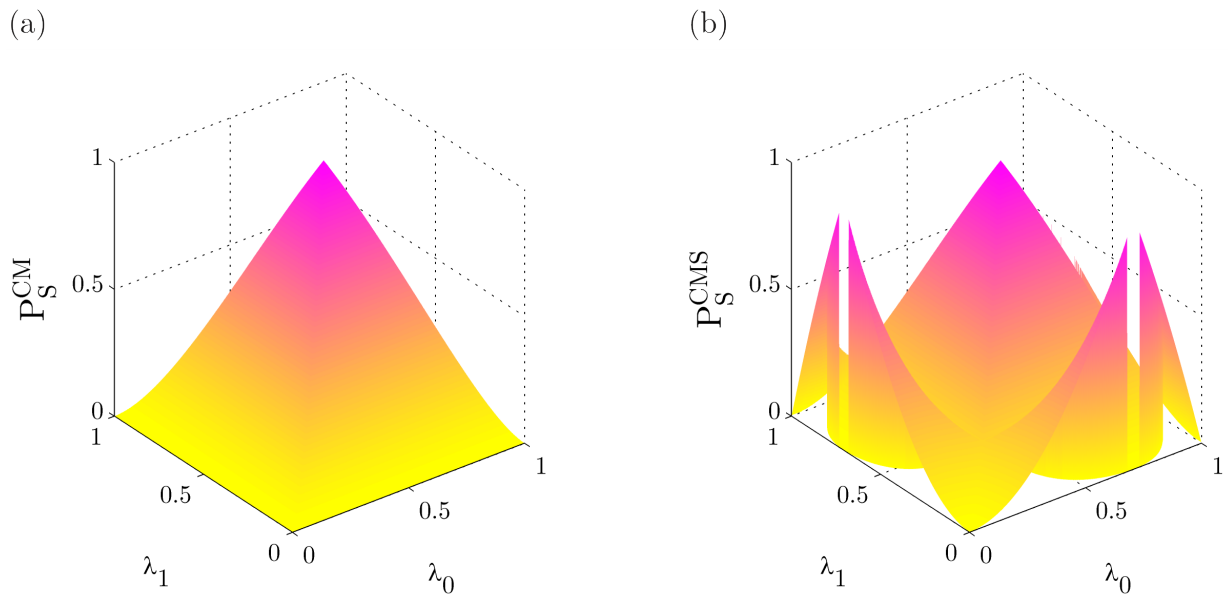

Figura 5.12: Os gráficos mostram a probabilidade de sucesso, P_S, de realizar a codificação superdensa em função dos coeficientes λ_0 e λ_1 ($\lambda_2 = \sqrt{1-\lambda_0^2-\lambda_1^2}$), e correspondem ao exemplo 6. (a) Realização do protocolo via CM. (b) Realização do protocolo via CMS com informação mútua superior à do protocolo determinístico.

protocolo determinístico apresenta maior informação mútua que o caso probabilístico, mesmo se bem sucedido na primeira tentativa. Em contra partida, existem situações que mesmo um sucesso na segunda tentativa de discriminação via CMS se mostra vantajoso.

Como visto no exemplo 3, se Alice e Bob decidirem enviar um número menor de mensagens, limitando-se à capacidade do canal descrito pelo estado (5.24), dada por $\mathcal{N} = N_S d_2$, é possível aumentar a informação mútua se comparada à situação onde $\mathcal{N} = D d_2$. Ao se realizar este tipo de procedimento, os estados $|\nu_j\rangle_1$ serão equivalentes aos da equação (D.54) e, portanto, as informações mútuas para um sucesso na primeira e na segunda tentativa de discriminação CMS serão dadas, respectivamente, pelas equações (5.48) e (5.49). Para um sucesso na primeira tentativa, a informação mútua será sempre superior às mostradas na figura 5.14. Para um sucesso na segunda tentativa, ainda é possível se realizar, para determinados canais, a codificação superdensa com informação mútua maior se comparada à do caso determinístico. Porém, essa situação será pior se comparada à mesma etapa do protocolo com $\mathcal{N} = D d_2$.

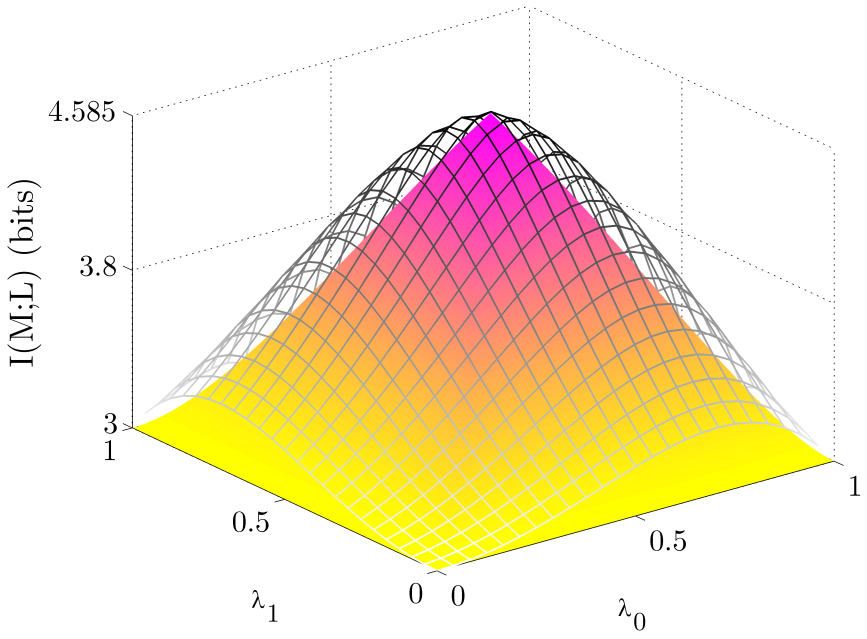

Figura 5.13: Comparação entre a informação mútua média do protocolo de codificação superdensa via EM e CM. A superfície em formato de rede é a mesma que a superfície iii) da figura 5.11. A superfície colorida (preenchida) é a informação mútua média de protocolos realizados com a estratégia CM, equação (5.50), a qual é sempre menor que o caso determinístico (exceto quando o estado compartilhado é maximamente emaranhado). O gráfico corresponde aos protocolos abordados nos exemplos 2 e 6.

5.4.2 Codificação Superdensa Assistida por Separação de Estados Quânticos

Utilizando o método de separação de estados quânticos, discutido nas seções 2.2.4 e 3.4, é possível realizar o protocolo de codificação superdensa com uma probabilidade de falha menor que aplicando-se a estratégia CM e com informação mútua superior àquela do protocolo determinístico em que se aplica a estratégia EM. Para isso, Bob deve, primeiramente, mapear os estados $\{|\nu_j\rangle_1\}$, dados pela equação (5.3), em um conjunto de estados mais distinguíveis entre si. De acordo com o procedimento descrito na seção 3.4, ele aplica uma transformação unitária no sistema 1 em conjunto com um *qubit* auxiliar, de modo que

$$\hat{\mathcal{U}}|\nu_j\rangle_1|0\rangle_a = \sqrt{P_S(\varsigma)}|v_j(\varsigma)\rangle_1|0\rangle_a + \sqrt{P_?(\varsigma)}|\chi_j(\varsigma)\rangle_1|1\rangle_a, \tag{5.53}$$

onde ς é o parâmetro que define o grau de distinguibilidade desejado. Usando as equações (3.61), (3.62), (3.66) e (3.69), as probabilidades de sucesso e falha e os estados correspondentes

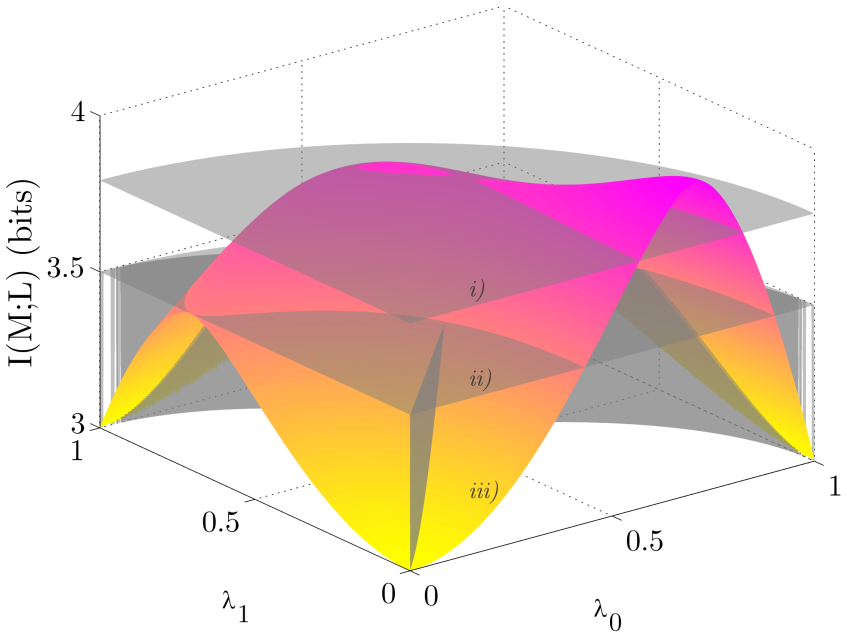

Figura 5.14: Informação mútua em função dos coeficientes de Schmidt λ_0 e λ_1 ($\lambda_2 = \sqrt{1-\lambda_0-\lambda_1}$), do estado (5.24). i) Estratégia CM bem sucedida. ii) Estratégia CMS bem sucedida na segunda tentativa. As quedas dessa superfície para a base do gráfio ocorrem nos pontos onde $\lambda_{\min}$ é degenerado. iii) Estratégia EM. Este gráfico corresponde aos protocolos de codificação superdensa descritos nos exemplos 3 e 7.

serão dados, respectivamente, por

$$P_S(\varsigma) = \frac{1}{(1-\varsigma) + \frac{\varsigma}{N_S\lambda_{\min}^2}}, \tag{5.54}$$

$$P_?(\varsigma) = 1 - \frac{1}{(1-\varsigma) + \frac{\varsigma}{N_S\lambda_{\min}^2}}, \tag{5.55}$$

e

$$|v_j(\varsigma)\rangle_1 = \sum_{r=0}^{N_S-1} \sqrt{(1-\varsigma)\lambda_r^2 + \frac{\varsigma}{N_S}} e^{\frac{2i\pi jr}{D}} |r\rangle_1, \tag{5.56}$$

$$|\chi_j(\varsigma)\rangle_1 = \sum_{r=0}^{N_S-1} \sqrt{\frac{\lambda_r^2 - \lambda_{\min}^2}{1 - N_S\lambda_{\min}^2}} e^{\frac{2i\pi jr}{D}} |r\rangle_1. \tag{5.57}$$

Bob realiza uma medição da *ancilla* na base computacional, a qual indica se o processo é bem sucedido ou não. Se o processo for bem sucedido, os estados $|\nu_j\rangle_1$ são mapeados em $|v_j(\varsigma)\rangle_1$, os quais serão discriminados por Bob com a estratégia EM. No caso de falha, os estados iniciais são mapeados em $|\chi_j(\varsigma)\rangle_1$, os quais são menos distinguíveis por estarem restritos a um subespaço de Hilbert menor.

Considerando apenas o caso de sucesso e utilizando os operadores $\hat{\Pi}'_l$, dados em (5.14), associados aos vetores $|\mu'_l\rangle$ em (5.15), a probabilidade $[\mathrm{Tr}(\hat{\rho}_j\hat{\Pi}'_l)]^{\mathrm{SE}}$ será dada por

$$\begin{aligned}[\mathrm{Tr}(\hat{\rho}_j\hat{\Pi}'_l)]^{\mathrm{SE}} &= \frac{1}{D} + \frac{2}{D}\sum_{\substack{r,s=0\\ s>r}}^{N_S-1}\Lambda_r\Lambda_s\cos\left(\frac{2\pi(j-l)(r-s)}{D}\right)\\ &\equiv P_{jl}^{\mathrm{SE}}(\{\lambda_r\},N_S,\varsigma)\equiv P_{jl}^{\mathrm{SE}}(\varsigma),\end{aligned} \tag{5.58}$$

onde o sobrescrito SE indica a separação de estados, e

$$\Lambda_r \equiv \sqrt{(1-\varsigma)\lambda_r^2+\frac{\varsigma}{N_S}}. \tag{5.59}$$

A definição $P_{jl}^{\mathrm{SE}}(\varsigma)$ foi adotada para simplificar a notação. Substituindo esse resultado nas equações (5.12) e (5.13), a informação mútua entre Alice e Bob pode ser escrita como

$$[I(M;L)]^{\mathrm{SE}} = \log_2 Dd_2 + \frac{1}{D}\sum_{j,l=0}^{D-1}P_{jl}^{\mathrm{SE}}(\varsigma)\log_2\left[P_{jl}^{\mathrm{SE}}(\varsigma)\right]. \tag{5.60}$$

É evidente que, para $\varsigma = 0$, os coeficientes dos estados $|v_j(\varsigma)\rangle_1$, equação (5.56), permanecem inalterados, sendo a informação mútua idêntica ao caso determinístico, equação (5.17). Já para $\varsigma = 1$, todos os coeficientes serão iguais, isto é, $\lambda_r = 1/\sqrt{N_S}$, tornando a informação mútua idêntica à do protocolo realizado via CM em caso de sucesso, dada por (5.35). O mesmo vale para as probabilidades de sucesso em cada caso, como pode ser visto na equação (5.54). Embora a informação mútua em (5.60) dependa dos coeficientes de Schmidt λ_r, ela respeita a relação $[I(M;L)]^{\mathrm{SE}} \geq [I(M;L)]^{\mathrm{EM}}$, uma vez que os estados $|v_j(\varsigma)\rangle_1$ são mais distinguíveis que os $|\nu_j\rangle_1$.

Estratégias intermediárias servem para aumentar a informação mútua com uma probabilidade de falha controlada. Ou, equivalentemente, para definir um mínimo aceitável para a informação mútua, onde a probabilidade de sucesso será maior que em protocolos assistidos pela estratégia CM. Caso a estratégia falhe, Bob poderá seguir com medições nos estados $|\chi_j(\varsigma)\rangle_1$, se estas puderem fornecer alguma informação sobre o estado inicial. Até o presente momento não foram encontradas referências na literatura que estudam a aplicação de estratégias intermediárias de discriminação aplicadas à protocolos de codificação superdensa.

Exemplo 8: protocolos intermediários de codificação superdensa para estados emaranhados de *qubits*

Para ilustrar a estratégia descrita acima, considere como exemplo o estado inicial dado por

$$|\Psi\rangle_{12} = \cos(10^\circ)|0\rangle_1|0\rangle_2 + \sin(10^\circ)|1\rangle_1|1\rangle_2, \tag{5.61}$$

onde ambos os sistemas são bidimensionais. De acordo com o protocolo padrão, seção 1.6.4, Alice realiza a codificação com as portas $\hat{X}_2^{-k}$ $(k = 0, 1)$, dada na equação (1.19), e $\hat{\mathcal{Z}}_2^j$ $(j = 0, 1)$, equação (1.51), e envia seu sistema para Bob. Ele, então, atua com a porta $\hat{G}_{12}^{\text{XOR}}$, definida na tabela 1.3, ficando com o estado

$$\hat{G}_{12}^{\text{XOR}}\hat{X}^{-k}\hat{\mathcal{Z}}^j|\Psi\rangle_{12} = \left(\cos(10^\circ)|0\rangle_1 + e^{\frac{2i\pi j}{2}}\sin(10^\circ)|1\rangle_1\right)|k\rangle_2. \tag{5.62}$$

O estado do sistema 2 é perfeitamente distinguível por uma medição projetiva. Já o estado do sistema 1 será discriminado, após a separação de estados, com uma medição via EM. Este problema foi analisado no exemplo da seção 2.2.4, onde mostrou-se que, caso o procedimento seja bem sucedido, o estado do sistema 1 é projetado em

$$|v_j(\phi)\rangle_1 = \cos\phi|0\rangle_1 + e^{\frac{2i\pi j}{2}}\sin\phi|1\rangle_1, \tag{5.63}$$

com $10^\circ \leq \phi \leq 45^\circ$. Agora, este problema é idêntico ao descrito no exemplo 1 e apêndice D.1, substituindo θ por ϕ. Portanto, como mostrado em D.1, a informação mútua entre Alice e Bob será

$$[I(M;L)]^{\text{SE}} = 2 + \sum_{j=0}^{1}\left(\frac{1+(-1)^j\sin 2\phi}{2}\right)\log_2\left[\frac{1+(-1)^j\sin 2\phi}{2}\right]. \tag{5.64}$$

Usando a equação (2.67), a probabilidade de sucesso será

$$P_S = \frac{1-\cos 20^\circ}{1-\cos 2\phi}. \tag{5.65}$$

O gráfico da figura 5.15 mostra essas duas grandezas em função do ângulo de separação ϕ. Os extremos do gráfico fornecem os limites EM ($\phi = 10^\circ$) e CM ($\phi = 45^\circ$) da estratégia. Em todos os casos intermediários entre $\phi = 10^\circ$ e $\phi = 45^\circ$, se cumpre o objetivo de realizar a codificação superdensa com informação mútua maior que no caso determinístico e probabilidade de sucesso maior que a obtida via CM. Caso o processo falhe, os estados iniciais do sistema 1 serão mapeados em um espaço de Hilbert unidimensional. Portanto, nenhuma medição fornecerá informação sobre eles, e a informação mútua será de apenas 1 bit.

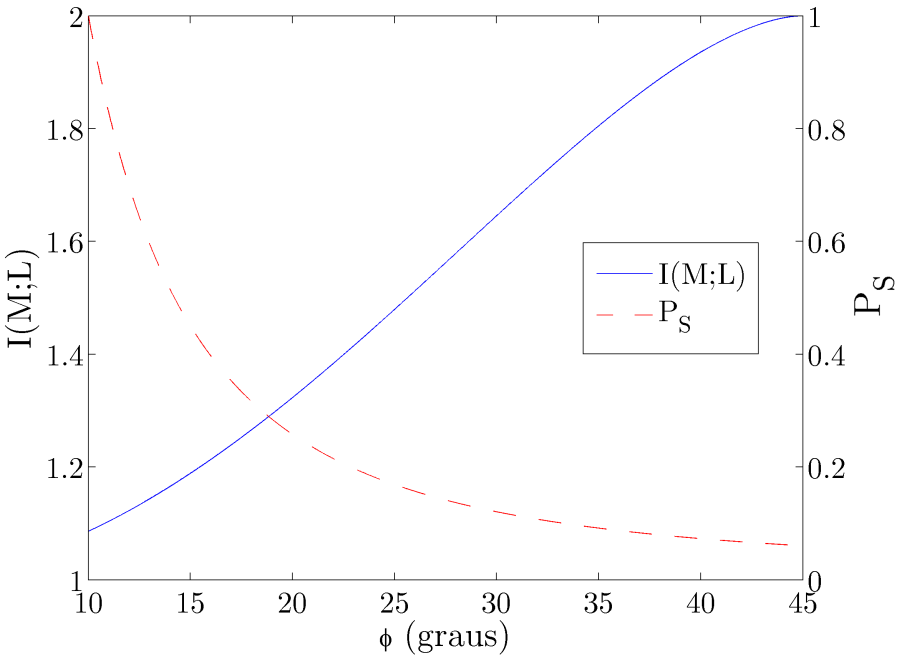

Figura 5.15: Linha contínua azul: Informação mútua em função do ângulo ϕ de separação final dos estados $|v_j(\phi)\rangle_1$. Linha tracejada vermelha: Probabilidade de sucesso de separar os estados $|\nu_j\rangle_1$ em um ângulo $10^\circ \leq \phi \leq 45^\circ$.

6

Conclusão

Nesta dissertação investigou-se o protocolo de codificação superdensa realizado através de canais quânticos puros e parcialmente emaranhados. Para isso, diversos tópicos de informação quântica e fundamentos de mecânica quântica foram estudados. A seguir será feito um breve resumo desses estudos e dos resultados que foram obtidos.

No capítulo 1, foram introduzidos os fundamentos matemáticos e conceituais básicos de informação e computação quântica, necessários para o entendimento do trabalho. Apresentou-se o *qubit* e o *qudit*, o emaranhamento de estados puros bipartidos e as portas lógicas quânticas, definidas por operadores quânticos. Com a utilização desses fundamentos, foram apresentados, em forma de circuitos, o canal de emaranhamento e os protocolos de teleportação, troca de emaranhamento e codificação superdensa. No caso do último, foi mostrado como sua tarefa é executada em situações onde os sistemas emaranhados possuem dimensões diferentes.

Os conceitos de medições projetivas e generalizadas foram apresentados em seguida, no capítulo 2, pois são fundamentais para a extração de informação em protocolos quânticos de comunicação. Neste mesmo capítulo, foi estudada a discriminação de estados não-ortogonais no contexto das estratégias de erro mínimo (EM), confiança máxima (CM), confiança máxima sequencial (CMS) e estratégias intermediárias entre EM e CM, onde foram apresentados exemplos simples de aplicação de cada uma. No capítulo 3, estas estratégias foram aplicadas a conjuntos de estados simétricos equiprováveis, os quais desempenham um papel importante na realização de diversos protocolos de informação quântica. Foram apresentados os POVMs que realizam a discriminação ótima desses estados e diversos exemplos foram analisados.

A teleportação quântica e a troca de emaranhamento via canais puros e parcialmente emaranhados foram discutidas no capítulo 4. Mostrou-se que a capacidade de realizar esses protocolos está relacionada com a capacidade de discriminação ótima entre estados simétricos equiprováveis. Então, foram discutidos alguns resultados alcançados ao se realizar os protocolos com o uso das estratégias apresentadas no capítulo 3.

No capítulo 5 foram apresentados os resultados originais deste trabalho. Primeiramente, formulou-se o problema geral de codificação superdensa via canais quânticos puros e parcialmente emaranhados. Se mostrou que, de modo semelhante aos protocolos apresentados no capítulo 4, este problema se relacionada com a capacidade de discriminar entre estados simétricos equiprováveis. Assim, as estratégias ótimas de discriminação (EM, CM, etc.) foram utilizadas para a realização do protocolo. A informação mútua, adotada como figura de mérito, foi analisada de acordo com o procedimento de discriminação adotado. Mostrou-se que a estratégia EM realiza o protocolo ótimo de forma determinística. Admitindo-se uma probabilidade não nula de se obter um resultado inconclusivo, foi evidenciado que é possível, em caso de sucesso, alcançar uma informação mútua maior que no caso determinístico. Isso foi feito com a estratégia CM. Ainda, utilizando a estratégia CM de modo sequencial, foi mostrado que existem situações onde aumenta-se a probabilidade de se concluir o protocolo com informação mútua maior que o caso determinístico. O uso de estratégias intermediárias permitiu a realização da codificação superdensa com informação mútua maior, se compara à de protocolos determinísticos, com uma probabilidade de falha controlada. Equivalentemente, observou-se que é possível definir um mínimo aceitável para a informação mútua, onde a probabilidade de falha é menor que em protocolos via CM.

A codificação superdensa utiliza estados emaranhados para aumentar a quantidade de informação clássica transmitida por um canal quântico com o envio de um *qudit*. Quando o emaranhamento não é máximo, o protocolo não realizará sua tarefa perfeitamente, e, portanto, a informação mútua entre as partes comunicantes é reduzida. Ainda assim, esta quantidade é superior aos casos onde não há emaranhamento presente. Os resultados obtidos nesta dissertação mostraram como realizar a codificação superdensa via canais puros e parcialmente emaranhados de forma ótima, maximizando, assim, a informação mútua.

A

Prova das Identidades dos Protocolos de Teleportação Quântica e Troca de Emaranhamento

Neste apêndice serão demonstradas as identidades utilizadas para a descrição dos protocolos de teleportação quântica e troca de emaranhamento.

A.1 Teleportação Quântica

Os protocolos de teleportação quântica das seções 1.6.2 e 4.1 foram descritos utilizando as identidades (1.38) e (4.3), respectivamente. Para demonstrar essas equações, considere primeiramente o estado parcialmente emaranhado dado, em sua decomposição de Schmidt, por

$$|\Psi\rangle_{12} = \sum_{l=0}^{N_S-1} \lambda_l |l\rangle_1 |l\rangle_2, \tag{A.1}$$

onde $d_1 = d_2 = d$ e $N_S \leq d$. Considere ainda que as bases de Schmidt coincidam com as bases computacionais de seus respectivos espaços. O estado desconhecido a ser teleportado, escrito na base computacional, é dado por

$$|\phi\rangle_3 = \sum_{m=0}^{d-1} c_m |m\rangle_3, \tag{A.2}$$

o qual é normalizado. O estado conjunto, descrito por essas duas equações, será

$$|\Psi\rangle_{12}|\phi\rangle_3 = \sum_{l,m=0}^{d-1} c_m \lambda_l |l\rangle_1 |l\rangle_2 |m\rangle_3, \tag{A.3}$$

onde o limite da soma foi fixado em $d-1$. Para isso, são inseridos, se necessário, coeficientes λ_l nulos na equação, os quais serão removidos posteriormente. Definindo o número inteiro,

$n \equiv l \ominus m$, pode-se incluir uma soma juntamente com um delta de Kroneker na equação (A.3) sem alterar a igualdade, de modo que

$$|\Psi\rangle_{12}|\phi\rangle_3 = \sum_{l,m,n=0}^{d-1} c_m \lambda_l \delta_{l,n\oplus m} |n \oplus m\rangle_1 |l\rangle_2 |l \ominus n\rangle_3. \tag{A.4}$$

Utilizando a identidade da soma das raízes da unidade, equação (1.34), dada por

$$\delta_{l,n\oplus m} = \frac{1}{d} \sum_{p=0}^{d-1} e^{\frac{2i\pi p[l-(n\oplus m)]}{d}}, \tag{A.5}$$

na equação (A.4), tem-se

$$|\Psi\rangle_{12}|\phi\rangle_3 = \frac{1}{d} \sum_{l,m,n,p=0}^{d-1} c_m \lambda_l e^{\frac{2i\pi pl}{d}} e^{\frac{-2i\pi p(n\oplus m)}{d}} |n \oplus m\rangle_1 |l\rangle_2 |l \ominus n\rangle_3. \tag{A.6}$$

Das definições das portas $\hat{X}$, $\hat{Z}$ e $\hat{G}^{\text{XOR}}$, dadas na tabela 1.3, pode-se escrever

$$\begin{aligned} |\Psi\rangle_{12}|\phi\rangle_3 &= \frac{1}{d} \sum_{l,m,n,p=0}^{d-1} c_m \lambda_l e^{\frac{2i\pi pl}{d}} \hat{Z}_1^{-p} \hat{X}_1^n |m\rangle_1 \hat{G}_{23}^{\text{XOR}} |l\rangle_2 |n\rangle_3 \\ &= \frac{1}{d} \sum_{n,p=0}^{d-1} \hat{Z}_1^{-p} \hat{X}_1^n \left[\sum_{m=0}^{d-1} c_m |m\rangle_1 \right] \hat{G}_{23}^{\text{XOR}} \left[\sum_{l}^{d-1} \lambda_l e^{\frac{2i\pi pl}{d}} |l\rangle_2 \right] |n\rangle_3 \\ &= \frac{1}{d} \sum_{n,p=0}^{d-1} \hat{Z}_1^{-p} \hat{X}_1^n |\phi\rangle_1 \hat{G}_{23}^{\text{XOR}} |\nu_p\rangle_2 |n\rangle_3, \end{aligned} \tag{A.7}$$

o que é equivalente à identidade da equação (4.3). Os estados $|\nu_p\rangle_2$ formam um conjunto de estados simétricos e são dados por

$$|\nu_p\rangle_2 = \sum_{l}^{N_S-1} \lambda_l e^{\frac{2i\pi pl}{d}} |l\rangle_2, \tag{A.8}$$

onde o limite N_S da soma é o número de Schmidt, recuperado ao se excluir os coeficientes nulos.

Se $N_S = d$ e todos os coeficientes de Schmidt forem iguais, $\lambda_l = 1/\sqrt{d}, \forall\ l$, o estado da equação (A.3) é maximamente emaranhado. Os estados $|\nu_p\rangle_2$ assumem, então, a forma

$$|\nu_p\rangle_2 = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} e^{\frac{2i\pi pl}{d}} |l\rangle_2 = \hat{\mathcal{F}}_2 |p\rangle_2, \tag{A.9}$$

onde $\hat{\mathcal{F}}_2$ é a transformada discreta de Fourier dada na equação (1.24). Substituindo esse resultado em (A.7) recupera-se a identidade (1.38),

$$|\Psi\rangle_{12}|\phi\rangle_3 = \frac{1}{d} \sum_{n,p=0}^{d-1} \hat{Z}_1^{-p} \hat{X}_1^n |\phi\rangle_1 \hat{G}_{23}^{\text{XOR}} \hat{\mathcal{F}}_2 |p\rangle_2 |n\rangle_3. \tag{A.10}$$

■

A.2 Troca de Emaranhamento

As equações (1.42) e (4.33), utilizadas nas descrições dos protocolos de troca de emaranhamento das respectivas seções 1.6.3 e 4.2, serão demonstradas a seguir. Para isso, considere dois estados emaranhados dados por

$$|\phi\rangle_A = \sum_{m=0}^{d_A-1} \alpha_m |m\rangle_1 |m\rangle_2, \tag{A.11}$$

$$|\varphi\rangle_B = \sum_{n=0}^{d_B-1} \beta_n |n\rangle_3 |n\rangle_4, \tag{A.12}$$

onde podem existir coeficientes nulos. Assume-se que as bases de Schmidt $\{|l\rangle_i\}$ em $\mathcal{H}_i, i = 1,\ldots,4,$, coincidem com a base computacional dos seus respectivos espaços de Hilbert. Considerando ainda que $d_A = d_B = d$, o estado conjunto dos sistemas 1, 2, 3 e 4 é escrito como

$$|\phi\rangle_A |\varphi\rangle_B = \sum_{m,n=0}^{d-1} \alpha_m \beta_n |m\rangle_1 |m\rangle_2 |n\rangle_3 |n\rangle_4. \tag{A.13}$$

Definindo $r = m \ominus n$ e utilizando a identidade da equação (A.5), obtém-se

$$\begin{aligned}
|\phi\rangle_A |\varphi\rangle_B &= \frac{1}{d} \sum_{m,n,r,s=0}^{d-1} \alpha_m \beta_{m\ominus r} e^{\frac{2i\pi s[n-(m\ominus r)]}{d}} |m\rangle_1 |m\rangle_2 |n\rangle_3 |m \ominus r\rangle_4 \\
&= \frac{1}{\sqrt{d}} \sum_{n,r,s=0}^{d-1} \alpha_{r\oplus n} \beta_n e^{\frac{2i\pi s(n\oplus r)}{d}} \left[\frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{\frac{-2i\pi sm}{d}} |m\rangle_1 |m \ominus r\rangle_4 \right] \hat{G}_{23}^{\text{XOR}} |r \oplus n\rangle_2 |r\rangle_3 \\
&= \frac{1}{\sqrt{d}} \sum_{r,s=0}^{d-1} |\Psi_{sr}\rangle_{14} \hat{G}_{23}^{\text{XOR}} \left[\sum_{n=0}^{d-1} \frac{\alpha_{r\oplus n}\beta_n}{\sqrt{p_r}} e^{\frac{2i\pi s(n\oplus r)}{d}} |r \oplus n\rangle_2 \right] \sqrt{p_r} |r\rangle_3 \\
&= \frac{1}{\sqrt{d}} \sum_{r,s=0}^{d-1} |\Psi_{sr}\rangle_{14} \hat{G}_{23}^{\text{XOR}} |\nu_{sr}\rangle_2 \sqrt{p_r} |r\rangle_3,
\end{aligned} \tag{A.14}$$

onde p_r é a probabilidade de se obter o resultado r com uma medição projetiva no sistema 3 e

$$|\Psi_{sr}\rangle_{14} = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{\frac{-2i\pi sm}{d}} |m\rangle_1 |m \ominus r\rangle_4, \tag{A.15}$$

é um estado maximamente emaranhado que, a menos de uma fase global, é equivalente aos estados dados pela equação (1.30). A operação unitária $\hat{G}_{23}^{\text{XOR}}$ é definida na tabela 1.3. Os estados $|\nu_{sr}\rangle_2$ são dados por

$$|\nu_{sr}\rangle_2 = \sum_{n=0}^{N_S-1} \frac{\alpha_{r\oplus n}\beta_n}{\sqrt{p_r}} e^{\frac{2i\pi s(n\oplus r)}{d}} |r \oplus n\rangle_2, \tag{A.16}$$

onde N_S é o número de coeficientes de Schmidt não nulos, o que recupera a equação (4.34). Assim, a identidade da equação (A.14) é idêntica a identidade (4.33).

Se os estados $|\phi\rangle_A$ e $|\varphi\rangle_B$ forem maximamente emaranhados, ou seja, $\alpha_m = \beta_n = 1/\sqrt{d}, \forall\, m, n$, os estados $|\nu_{sr}\rangle_2$ se reduzem a

$$|\nu_{sr}\rangle_2 = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} e^{\frac{2i\pi s(n\oplus r)}{d}} |r \oplus n\rangle_2 = \hat{\mathcal{F}}_2 |s\rangle_2, \tag{A.17}$$

onde $\hat{\mathcal{F}}_2$ é a transformada de Fourier, definida na tabela 1.3. Substituindo esse resultado na equação (A.14), tem-se

$$|\phi\rangle_A |\varphi\rangle_B = \frac{1}{d} \sum_{r,s=0}^{d-1} |\Psi_{sr}\rangle_{14} \hat{G}_{23}^{\text{XOR}} \hat{\mathcal{F}}_2 |s\rangle_2 |r\rangle_3, \tag{A.18}$$

o que é equivalente à equação (1.42). ■

B

Discriminação Sem Ambiguidade de Estados Linearmente Dependentes

A estratégia SA, descrita na seção 2.2.2, não pode ser aplicada a qualquer conjunto de estados quânticos. Se os estados forem linearmente dependentes, é impossível discriminá-los sem ambiguidade [23]. Para mostrar isso, considere o conjunto de N estados puros, $\{\hat{\rho}_j = |\psi_j\rangle\langle\psi_j| \mid j = 0, \ldots, N-1\}$, com probabilidades *a priori* η_j. De acordo com a equação (2.32), o POVM que realiza a estratégia SA deve satisfazer a seguinte condição:

$$\hat{\Pi}_? + \sum_{j=0}^{N-1} \hat{\Pi}_j = \mathbb{1}, \tag{B.1}$$

onde cada elemento de POVM $\hat{\Pi}_j$ identifica o respectivo estado $\hat{\rho}_j$ sem erros. Ou seja,

$$\begin{aligned} \mathrm{Tr}(\hat{\rho}_j \hat{\Pi}_j) &= \langle\psi_j|\hat{A}_l^\dagger \hat{A}_l|\psi_j\rangle \\ &= p_j \delta_{jl}. \end{aligned} \tag{B.2}$$

Se os estados $|\psi_j\rangle$ forem linearmente dependentes, pode-se escrever cada um deles como uma superposição dos demais, ou seja

$$|\psi_j\rangle = \sum_{k=0}^{N-1} f_{jk}|\psi_k\rangle. \tag{B.3}$$

Substituindo esse estado na equação (B.2), obtém-se

$$\sum_{k,k'=0}^{N-1} f_{jk'}^* f_{jk} \langle\psi_{k'}|\hat{A}_l^\dagger \hat{A}_l|\psi_k\rangle = p_j \delta_{jl}. \tag{B.4}$$

Utilizando a desigualdade de Cauchy-Schwarz [3], dada por[1]

$$|\langle\psi_{k'}|\hat{A}_l^\dagger \hat{A}_l|\psi_k\rangle|^2 \leq \langle\psi_k|\hat{A}_l^\dagger \hat{A}_l|\psi_k\rangle\langle\psi_{k'}|\hat{A}_l^\dagger \hat{A}_l|\psi_{k'}\rangle, \tag{B.5}$$

[1] A desigualdade de Cauchy-Schwarz pode ser expressada como $\langle A|A\rangle\langle B|B\rangle \geq |\langle A|B\rangle|^2$.

e a equação (B.2), tem-se

$$\langle\psi_{k'}|\hat{A}_l^\dagger\hat{A}_l|\psi_k\rangle \leq \sqrt{p_k p_{k'}}\delta_{lk}\delta_{lk'} = p_k\delta_{lk}\delta_{kk'}. \tag{B.6}$$

Inserindo esse resultado na equação (B.4) se chega na contradição

$$\sum_{k,k'=0}^{N-1} f_{jk'}^* f_{jk} p_k \delta_{kk'}\delta_{lk} = p_j\delta_{jk} \Rightarrow |f_{jk}|^2 = \delta_{jk}, \tag{B.7}$$

a qual implica que nenhum dos estados do conjunto pode ser linearmente dependente. ■

C

POVM que Realiza a Discriminação com Erro Mínimo de Estados Simétricos Equiprováveis

Na seção 3.2 apresentou-se o POVM que realiza a discriminação EM de estados simétricos equiprováveis, descrito pelas equações (3.9)–(3.11), as quais são reproduzidas aqui

$$\hat{\Pi}_j = |\mu_j\rangle\langle\mu_j|, \tag{C.1}$$

$$|\mu_j\rangle = \hat{\Upsilon}^{-1/2}|\psi_j\rangle, \tag{C.2}$$

$$\hat{\Upsilon} = \sum_{j=0}^{N-1}|\psi_j\rangle\langle\psi_j|, \tag{C.3}$$

onde os estados $|\psi_j\rangle$ são dados pela equação (3.6). Para garantir que a probabilidade média de erro, P_{erro}, dada pela equação (2.10), seja mínima, esse POVM deve satisfazer as condições das equações (2.11) e (2.12). Ban *et al.* mostraram em [47] que essas condições são de fato satisfeitas, prova que será reproduzida a seguir.

Primeiramente, determina-se a relação de comutação entre $\hat{\Upsilon}$ e $\hat{U}$, onde $\hat{U}$ é definido na equação (3.4). O produto de operadores $\hat{U}\hat{\Upsilon}\hat{U}^\dagger$ resulta em

$$\begin{aligned}\hat{U}\hat{\Upsilon}\hat{U}^\dagger &= \sum_{j=0}^{N-1}\hat{U}|\psi_j\rangle\langle\psi_j|\hat{U}^\dagger \\ &= \sum_{j=1}^{N-1}|\psi_j\rangle\langle\psi_j| + |\psi_N\rangle\langle\psi_N|,\end{aligned} \tag{C.4}$$

mas $|\psi_N\rangle = \hat{U}^N|\psi_0\rangle = |\psi_0\rangle$, e, portanto

$$\hat{U}\hat{\Upsilon}\hat{U}^\dagger = \hat{\Upsilon}. \tag{C.5}$$

Com esse resultado calcula-se explicitamente o comutador

$$\begin{aligned}[\hat{\Upsilon},\hat{U}] &= \hat{\Upsilon}\hat{U} - \hat{U}\hat{\Upsilon} \\ &= \hat{U}\hat{\Upsilon}\hat{U}^{\dagger}\hat{U} - \hat{U}\hat{\Upsilon} \\ &= \hat{U}\hat{\Upsilon} - \hat{U}\hat{\Upsilon} \\ &= 0.\end{aligned} \tag{C.6}$$

Escrevendo o lado esquerdo da equação (2.11) explicitamente, se obtém

$$\begin{aligned}\hat{\Pi}_j(\eta_j\hat{\rho}_j - \eta_k\hat{\rho}_k)\hat{\Pi}_k &= \frac{1}{N}|\mu_j\rangle\langle\mu_j|\left(|\psi_j\rangle\langle\psi_j| - |\psi_k\rangle\langle\psi_k|\right)|\mu_k\rangle\langle\mu_k| \\ &= \frac{1}{N}|\mu_j\rangle\left(\langle\mu_j|\psi_j\rangle\langle\psi_j|\mu_k\rangle - \langle\mu_j|\psi_k\rangle\langle\psi_k|\mu_k\rangle\right)\langle\mu_k| \\ &\equiv \frac{\mathfrak{F}}{N}|\mu_j\rangle\langle\mu_k|.\end{aligned} \tag{C.7}$$

Esta equação satisfará a condição (2.11) se $\mathfrak{F}$ for igual a zero, o que, de fato, ocorre

$$\begin{aligned}\mathfrak{F} &= \langle\mu_j|\psi_j\rangle\langle\psi_j|\mu_k\rangle - \langle\mu_j|\psi_k\rangle\langle\psi_k|\mu_k\rangle \\ &= \langle\psi_0|\hat{U}^{\dagger j}\hat{\Upsilon}^{-1/2}\hat{U}^{j}|\psi_0\rangle\langle\psi_0|\hat{U}^{\dagger j}\hat{\Upsilon}^{-1/2}\hat{U}^{k}|\psi_0\rangle - \langle\psi_0|\hat{U}^{\dagger j}\hat{\Upsilon}^{-1/2}\hat{U}^{k}|\psi_0\rangle\langle\psi_0|\hat{U}^{\dagger k}\hat{\Upsilon}^{-1/2}\hat{U}^{k}|\psi_0\rangle \\ &= \langle\psi_0|\hat{\Upsilon}^{-1/2}|\psi_0\rangle\langle\psi_0|\hat{\Upsilon}^{-1/2}\hat{U}^{\dagger j}\hat{U}^{k}|\psi_0\rangle - \langle\psi_0|\hat{\Upsilon}^{-1/2}\hat{U}^{\dagger j}\hat{U}^{k}|\psi_0\rangle\langle\psi_0|\hat{\Upsilon}^{-1/2}|\psi_0\rangle \\ &= 0,\end{aligned} \tag{C.8}$$

onde a definição dos estados simétricos, equação (3.1), foi utilizada, assim como a relação de comutação dos operadores $\hat{U}$ e $\hat{\Upsilon}$, equação (C.6). O operador de Lagrange, equação (2.13), é dado por

$$\begin{aligned}\hat{\Gamma} &= \sum_{j=0}^{N-1}\eta_j\hat{\rho}_j\hat{\Pi}_j \\ &= \frac{1}{N}\sum_{j=0}^{N-1}|\psi_j\rangle\langle\psi_j|\mu_j\rangle\langle\mu_j| \\ &= \frac{1}{N}\sum_{j=0}^{N-1}|\psi_j\rangle\langle\psi_0|\hat{U}^{\dagger j}\hat{\Upsilon}^{-1/2}\hat{U}^{j}|\psi_0\rangle\langle\mu_j| \\ &= \frac{1}{N}\langle\psi_0|\hat{\Upsilon}^{-1/2}|\psi_0\rangle\sum_{j=0}^{N-1}|\psi_j\rangle\langle\psi_j|\hat{\Upsilon}^{-1/2} \\ &= \frac{1}{N}\langle\psi_0|\hat{\Upsilon}^{-1/2}|\psi_0\rangle\hat{\Upsilon}^{1/2},\end{aligned} \tag{C.9}$$

onde as definições de $|\mu_j\rangle$ e de $\hat{\Upsilon}$, equações (C.2) e (C.3), foram utilizadas junto com o fato de $\hat{\Upsilon}$ ser hermitiano. Inserindo essa forma do operador no lado esquerdo da equação (2.12),

obtém-se

$$\begin{aligned}\frac{1}{N}\left(\langle\psi_0|\hat{\Upsilon}^{-1/2}|\psi_0\rangle\hat{\Upsilon}^{1/2}-|\psi_j\rangle\langle\psi_j|\right) &= \frac{1}{N}\hat{U}^j\left(\langle\psi_0|\hat{\Upsilon}^{-1/2}|\psi_0\rangle\hat{\Upsilon}^{1/2}-|\psi_j\rangle\langle\psi_j|\right)\hat{U}^{\dagger j}\\ &\equiv \frac{1}{N}\hat{U}^j\hat{\mathfrak{G}}\hat{U}^{\dagger j},\end{aligned} \tag{C.10}$$

onde se fez uso da equação (C.5). O operador $\hat{\mathfrak{G}}$ deve ser não-negativo, o que é equivalente a mostrar que todos os seus elementos diagonais também o são. Escrevendo o elemento diagonal $\langle j|\hat{\mathfrak{G}}|j\rangle$ na forma

$$\begin{aligned}\langle j|\hat{\mathfrak{G}}|j\rangle &= \langle\psi_0|\hat{\Upsilon}^{-1/2}|\psi_0\rangle\langle j|\hat{\Upsilon}^{1/2}|j\rangle-\langle j|\psi_0\rangle\langle\psi_0|j\rangle\\ &= \langle\psi_0|\hat{\Upsilon}^{\dagger-1/4}\hat{\Upsilon}^{-1/4}|\psi_0\rangle\langle j|\hat{\Upsilon}^{\dagger 1/4}\hat{\Upsilon}^{1/4}|j\rangle-|\langle\psi_0|j\rangle|^2,\end{aligned} \tag{C.11}$$

e utilizando a desigualdade de Cauchy-Schwarz, equação (B.5), obtém-se

$$\begin{aligned}\langle j|\hat{\mathfrak{G}}|j\rangle &\geq |\langle\psi_0|\hat{\Upsilon}^{-1/4}\hat{\Upsilon}^{1/4}|\psi_0\rangle|^2-|\langle\psi_0|j\rangle|^2\\ &= |\langle\psi_0|j\rangle|^2-|\langle\psi_0|j\rangle|^2\\ &= 0.\end{aligned} \tag{C.12}$$

Portando, o POVM dado pelas equações (C.1)–(C.3) satisfaz as condições (2.11) e (2.12), sendo assim ótimo na discriminação com erro mínimo entre estados simétricos equiprováveis. ■

D

Cálculo da Informação Mútua dos Exemplos do Capítulo 5

Neste apêndice serão demonstrados os resultados para a informação mútua, equação (5.13), dos exemplos mostrados no capítulo 5.

D.1 Exemplo 1: codificação superdensa determinística com estado parcialmente emaranhado de *qubits*

Alice e Bob compartilham o estado $|\Psi\rangle_{12}$ da equação (5.18). Alice prepara uma das quatro mensagens dadas por

$$|\tilde{\Psi}_{00}\rangle_{12} = \mathbb{1}_1|\Psi\rangle_{12} = \cos\theta|0\rangle_2|0\rangle_1 + \sin\theta|1\rangle_2|1\rangle_2, \tag{D.1}$$
$$|\tilde{\Psi}_{10}\rangle_{12} = \hat{\mathcal{Z}}_2|\Psi\rangle_{12} = \cos\theta|0\rangle_1|0\rangle_2 - \sin\theta|1\rangle_1|1\rangle_2, \tag{D.2}$$
$$|\tilde{\Psi}_{01}\rangle_{12} = \hat{X}_2^{-1}|\Psi\rangle_{12} = \cos\theta|0\rangle_1|1\rangle_2 + \sin\theta|1\rangle_1|0\rangle_2, \tag{D.3}$$
$$|\tilde{\Psi}_{11}\rangle_{12} = \hat{X}_2^{-1}\hat{\mathcal{Z}}_2|\Psi\rangle_{12} = \cos\theta|0\rangle_1|1\rangle_2 - \sin\theta|1\rangle_1|0\rangle_2. \tag{D.4}$$

Os estados $|\tilde{\Psi}_{00}\rangle_{12}$ e $|\tilde{\Psi}_{10}\rangle_{12}$ são ortogonais aos estados $|\tilde{\Psi}_{01}\rangle_{12}$ e $|\tilde{\Psi}_{11}\rangle_{12}$. Essa é uma consequência direta da ortogonalidade dos estados do sistema 2. Uma medição na base computacional no sistema 2 deixa o sistema 1 em um dos estados

$$|\nu_0\rangle_1 = \cos\theta|0\rangle_1 + \sin\theta|1\rangle_1, \tag{D.5}$$
$$|\nu_1\rangle_1 = \cos\theta|0\rangle_1 - \sin\theta|1\rangle_1. \tag{D.6}$$

Bob opta por discriminá-los deterministicamente, conforme a seção 5.3. Os vetores que definem os projetores que realizam a medição via EM, de acordo com as equações (5.14) e

(5.15), são dados por

$$|\mu_0'\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{D.7}$$

$$|\mu_1'\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{D.8}$$

os quais foram demonstrados no exemplo da seção 2.2.1. As probabilidades de uma medição resultar em ω_l $(l = 0, 1)$, dado que o estado do sistema 1 é $\hat{\rho}_j = |\nu_j\rangle\langle\nu_j|$ $(j = 0, 1)$, são definidas em (5.16) e serão dadas por

$$|\langle\mu_0'|\nu_0\rangle|^2 = \frac{1 + 2\cos\theta\sin\theta}{2}, \tag{D.9}$$

$$|\langle\mu_1'|\nu_1\rangle|^2 = \frac{1 + 2\cos\theta\sin\theta}{2}, \tag{D.10}$$

$$|\langle\mu_0'|\nu_1\rangle|^2 = \frac{1 - 2\cos\theta\sin\theta}{2}, \tag{D.11}$$

$$|\langle\mu_1'|\nu_0\rangle|^2 = \frac{1 - 2\cos\theta\sin\theta}{2}. \tag{D.12}$$

Portanto, a informação mútua total do protocolo, de acordo com a equação (5.17), é dada por

$$[I(M;L)]^{\mathrm{EM}} = 2 + \sum_{j=0}^{1} \left(\frac{1 + (-1)^j \sin 2\theta}{2}\right) \log_2 \left[\frac{1 + (-1)^j \sin 2\theta}{2}\right], \tag{D.13}$$

demonstrando, assim, o resultado apresentado na equação (5.22). ■

D.2 Exemplo 2: codificação superdensa determinística com sistemas de dimensões 3 e 8

Alice e Bob compartilham o estado da equação (5.23). De acordo com a descrição do protocolo de codificação superdensa, Bob deverá discriminar entre os três estados simétricos da equação (5.3), dados por

$$|\nu_0\rangle_1 = \lambda_0|0\rangle_1 + \lambda_1|1\rangle_1 + \lambda_2|2\rangle_1, \tag{D.14}$$

$$|\nu_1\rangle_1 = \lambda_0|0\rangle_1 + \lambda_1 e^{\frac{2i\pi}{3}}|1\rangle_1 + \lambda_2 e^{\frac{4i\pi}{3}}|2\rangle_1, \tag{D.15}$$

$$|\nu_2\rangle_1 = \lambda_0|0\rangle_1 + \lambda_1 e^{\frac{-2i\pi}{3}}|1\rangle_1 + \lambda_2 e^{\frac{-4i\pi}{3}}|2\rangle_1. \tag{D.16}$$

Os vetores $|\mu'_k\rangle$ que geram os elementos de POVM ótimos para a realização da estratégia EM, de acordo com as equações (5.14) e (5.15), são dados por

$$|\mu'_0\rangle = \frac{1}{\sqrt{3}}\left[|0\rangle + |1\rangle + |2\rangle\right], \tag{D.17}$$

$$|\mu'_1\rangle = \frac{1}{\sqrt{3}}\left[|0\rangle + e^{\frac{2i\pi}{3}}|1\rangle + e^{\frac{4i\pi}{3}}|2\rangle\right], \tag{D.18}$$

$$|\mu'_2\rangle = \frac{1}{\sqrt{3}}\left[|0\rangle + e^{\frac{-2i\pi}{3}}|1\rangle + e^{\frac{-4i\pi}{3}}|2\rangle\right]. \tag{D.19}$$

As probabilidades P_{jl}^{EM}, definidas na equação (5.16), serão dadas por

$$P_{jl}^{\mathrm{EM}} = \begin{cases} |\langle\mu'_l|\nu_j\rangle|^2 = \frac{1}{3}\left[\lambda_0 + \lambda_1 + \lambda_2\right]^2, & \text{se } j = l, \\ |\langle\mu'_l|\nu_j\rangle|^2 = \frac{1}{3}\left(1 - \lambda_0\lambda_1 - \lambda_0\lambda_2 - \lambda_1\lambda_2\right), & \text{se } j \neq l. \end{cases} \tag{D.20}$$

Portanto, substituindo esses resultados em (5.17), a informação mútua entre Alice e Bob será

$$\begin{aligned}[I(M;L)]^{\mathrm{EM}} = \log_2 24 &+ \frac{1}{3}\left(\lambda_0 + \lambda_1 + \lambda_2\right)^2 \log_2\left[\frac{1}{3}\left(\lambda_0 + \lambda_1 + \lambda_2\right)^2\right] \\ &+ \frac{2}{3}\left(1 - \lambda_0\lambda_1 - \lambda_0\lambda_2 - \lambda_1\lambda_2\right)\log_2\left[\frac{1}{3}\left(1 - \lambda_0\lambda_1 - \lambda_0\lambda_2 - \lambda_1\lambda_2\right)\right],\end{aligned} \tag{D.21}$$

a qual gera a curva do gráfico 5.5. ■

D.3 Exemplo 3: codificação superdensa determinística com número de Schmidt não máximo

Neste exemplo, Alice e Bob compartilham o estado da equação (5.24). Ao final do protocolo de codificação superdensa, a tarefa de Bob será discriminar entre os estados simétricos equiprováveis $|\nu_j\rangle$, equação (5.25), dados por

$$|\nu_0\rangle = \lambda_0|0\rangle + \lambda_1|1\rangle + \lambda_2|2\rangle, \tag{D.22}$$

$$|\nu_1\rangle = \lambda_0|0\rangle + \lambda_1 e^{\frac{2i\pi}{4}}|1\rangle + \lambda_2 e^{\frac{4i\pi}{4}}|2\rangle, \tag{D.23}$$

$$|\nu_2\rangle = \lambda_0|0\rangle + \lambda_1 e^{\frac{4i\pi}{4}}|1\rangle + \lambda_2 e^{\frac{8i\pi}{4}}|2\rangle, \tag{D.24}$$

$$|\nu_3\rangle = \lambda_0|0\rangle + \lambda_1 e^{\frac{6i\pi}{4}}|1\rangle + \lambda_2 e^{\frac{12i\pi}{4}}|2\rangle. \tag{D.25}$$

Os elementos de POVM $\hat{\Pi}'_l$, dados na equação (5.14), que realizam a discriminação com erro mínimo dos estados $|\nu_j\rangle$ são definidos a partir dos vetores $|\mu'_l\rangle$, equação (5.15), dados por

$$|\mu'_0\rangle = \frac{1}{2}\left[|0\rangle + |1\rangle + |2\rangle + |3\rangle\right], \tag{D.26}$$

$$|\mu'_1\rangle = \frac{1}{2}\left[|0\rangle + e^{\frac{2i\pi}{4}}|1\rangle + e^{\frac{4i\pi}{4}}|2\rangle + e^{\frac{6i\pi}{4}}|3\rangle\right], \tag{D.27}$$

$$|\mu'_2\rangle = \frac{1}{2}\left[|0\rangle + e^{\frac{4i\pi}{4}}|1\rangle + e^{\frac{8i\pi}{4}}|2\rangle e^{\frac{12i\pi}{4}}|3\rangle\right], \tag{D.28}$$

$$|\mu'_3\rangle = \frac{1}{2}\left[|0\rangle + e^{\frac{6i\pi}{4}}|1\rangle + e^{\frac{12i\pi}{4}}|2\rangle e^{\frac{18i\pi}{4}}|3\rangle\right]. \tag{D.29}$$

As probabilidades P_{jl}^{EM}, de acordo com a equação (5.16), agrupadas por termos semelhantes, são

$$P_{jl}^{\mathrm{EM}} = \begin{cases} |\langle\mu'_l|\nu_j\rangle|^2 = \frac{1}{4}\left[\lambda_0 + \lambda_1 + \lambda_2\right]^2, & \text{se } |j-l| = 0, \\ |\langle\mu'_l|\nu_j\rangle|^2 = \frac{1}{4}\left[1 - 2\lambda_0\lambda_2\right], & \text{se } |j-l| = 1, \\ |\langle\mu'_l|\nu_j\rangle|^2 = \frac{1}{4}\left[1 - 2\lambda_0\lambda_1 - 2\lambda_1\lambda_2 + 2\lambda_0\lambda_2\right], & \text{se } |j-l| = 2, \\ |\langle\mu'_l|\nu_j\rangle|^2 = \frac{1}{4}\left[1 - 2\lambda_0\lambda_2\right], & \text{se } |j-l| = 3. \end{cases} \tag{D.30}$$

Inserindo esses resultados na equação (5.17) se obtém a informação mútua do protocolo, dada por

$$\begin{aligned}[I(M;L)]^{\mathrm{EM}} = \log_2 32 &+ \frac{1}{4}\left[\lambda_0 + \lambda_1 + \lambda_2\right]^2 \log_2\left[\frac{1}{4}\left(\lambda_0 + \lambda_1 + \lambda_2\right)^2\right] \\ &+ \frac{1}{2}\left[1 - 2\lambda_0\lambda_2\right]\log_2\left[\frac{1}{4}\left(1 - 2\lambda_0\lambda_2\right)\right] \\ &+ \frac{1}{4}\left[1 - 2\lambda_0\lambda_1 - 2\lambda_1\lambda_2 + 2\lambda_0\lambda_2\right]\log_2\left[\frac{1}{4}\left(1 - 2\lambda_0\lambda_1 - 2\lambda_1\lambda_2 + 2\lambda_0\lambda_2\right)\right].\end{aligned} \tag{D.31}$$

A superfície da figura 5.6 é obtida através desse resultado. ■

D.4 Exemplo 4: codificação superdensa probabilística com estado emaranhado de *ququarts*

Alice e Bob compartilham o estado da equação (5.36). Para concluir o protocolo de codificação superdensa, Bob deve discriminar os estados do sistema 1, dados por

$$|\nu_j\rangle_1 = \sum_{r=0}^{N_S-1} \lambda_r e^{\frac{2i\pi jr}{4}}|r\rangle_1. \tag{D.32}$$

Para isso, ele utilizará a estratégia CM. Se ele é bem sucedido, esses estados são mapeados nos estados

$$|u_j\rangle_1 = \frac{1}{\sqrt{N_S}} \sum_{r=0}^{N_S-1} e^{\frac{2i\pi jr}{4}} |r\rangle_1. \tag{D.33}$$

Como o número de Schmidt não foi definido, esse exemplo se divide em três possibilidades, discutidas a seguir.

i) $N_S = 4$

Se $N_S = 4$, os estados $|u_j\rangle_1 = \hat{\mathcal{F}}_D|j\rangle$ são ortogonais entre si e a estratégia CM coincide com a estratégia SA. Neste caso, $P_{jl}^{\text{CM}} = \delta_{jl}$ [veja equação (5.34)] e a informação mútua será

$$[I(M;L)]^{\text{CM},\mathbb{1}}_{N_S=4} = 2\log_2 4 = 4 \text{ bits}. \tag{D.34}$$

■

ii) $N_S = 3$

Para $N_S = 3$, tem-se os estados $|u_j\rangle_1$ dados por

$$|u_0\rangle_1 = \frac{1}{\sqrt{3}} \left[|0\rangle + |1\rangle + |2\rangle\right], \tag{D.35}$$

$$|u_1\rangle_1 = \frac{1}{\sqrt{3}} \left[|0\rangle + e^{\frac{2i\pi}{4}}|1\rangle + e^{\frac{4i\pi}{4}}|2\rangle\right], \tag{D.36}$$

$$|u_2\rangle_1 = \frac{1}{\sqrt{3}} \left[|0\rangle + e^{\frac{4i\pi}{4}}|1\rangle + e^{\frac{8i\pi}{4}}|2\rangle\right], \tag{D.37}$$

$$|u_3\rangle_1 = \frac{1}{\sqrt{3}} \left[|0\rangle + e^{\frac{6i\pi}{4}}|1\rangle + e^{\frac{12i\pi}{4}}|2\rangle\right]. \tag{D.38}$$

De acordo com a seção 3.3.1, o próximo passo da estratégia é a discriminação EM dos estados $|u_j\rangle_1$. Os vetores que definem os elementos de POVM que realizam essa tarefa, equações (5.14) e (5.15), são dados por

$$|\mu_0'\rangle = \frac{1}{\sqrt{4}} \left[|0\rangle + |1\rangle + |2\rangle + |3\rangle\right], \tag{D.39}$$

$$|\mu_1'\rangle = \frac{1}{\sqrt{4}} \left[|0\rangle + e^{\frac{2i\pi}{4}}|1\rangle + e^{\frac{4i\pi}{4}}|2\rangle + e^{\frac{8i\pi}{4}}|3\rangle\right], \tag{D.40}$$

$$|\mu_2'\rangle = \frac{1}{\sqrt{4}} \left[|0\rangle + e^{\frac{4i\pi}{4}}|1\rangle + e^{\frac{8i\pi}{4}}|2\rangle + e^{\frac{12i\pi}{4}}|3\rangle\right], \tag{D.41}$$

$$|\mu_3'\rangle = \frac{1}{\sqrt{4}} \left[|0\rangle + e^{\frac{6i\pi}{4}}|1\rangle + e^{\frac{12i\pi}{4}}|2\rangle + e^{\frac{18i\pi}{4}}|3\rangle\right]. \tag{D.42}$$

As probabilidades P_{jl}^{CM}, equação (5.34), serão

$$P_{jl}^{\mathrm{CM}} = \begin{cases} |\langle \mu_l' | \nu_j \rangle|^2 = \frac{9}{12}, & \text{se } j = l, \\ |\langle \mu_l' | \nu_j \rangle|^2 = \frac{1}{12}, & \text{se } j \neq l. \end{cases} \tag{D.43}$$

A informação mútua do protocolo, de acordo com a equação (5.35), será, portanto

$$[I(M;L)]_{N_S=3}^{\mathrm{CM},\mathbb{1}} \approx 2{,}792 \text{ bits}, \tag{D.44}$$

resultado que recupera a equação (5.38). ■

iii) $N_S = 2$

Quando $N_S = 2$, os estados $|u_j\rangle_1$, após um sucesso na discriminação CM, são dados por

$$|u_0\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + |1\rangle \right], \tag{D.45}$$

$$|u_1\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + i|1\rangle \right], \tag{D.46}$$

$$|u_2\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle - |1\rangle \right], \tag{D.47}$$

$$|u_3\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle - i|1\rangle \right]. \tag{D.48}$$

Os vetores que realizam a discriminação EM desses estados são dados pelas equações (D.39)–(D.42). De acordo com a equação (5.34) as probabilidades P_{jl}^{CM} serão

$$P_{jl}^{\mathrm{CM}} = \begin{cases} |\langle \mu_l' | \nu_j \rangle|^2 = \frac{1}{2}, & \text{se } |j-l| = 0, \\ |\langle \mu_l' | \nu_j \rangle|^2 = \frac{1}{4}, & \text{se } |j-l| = 1, \\ |\langle \mu_l' | \nu_j \rangle|^2 = 0, & \text{se } |j-l| = 2, \\ |\langle \mu_l' | \nu_j \rangle|^2 = \frac{1}{4}, & \text{se } |j-l| = 3. \end{cases} \tag{D.49}$$

Portanto, a informação mútua em (5.35) será

$$[I(M;L)]_{N_S=2}^{\mathrm{CM},\mathbb{1}} = 2{,}5 \text{ bits}, \tag{D.50}$$

que é o resultado da equação (5.39). ■

D.5 Exemplo 5: codificação superdensa via estratégia CMS para estado emaranhado de *ququarts*

Os seguintes exemplos consideram o estado inicial da equação (5.36). Para a realização do protocolo de codificação superdensa, Bob deve discriminar os estados $|\nu_j\rangle_1$, equação (5.3), e

para isso ele utiliza estratégia CM. Considerando que Bob obtém uma falha, os estados $|\nu_j\rangle_1$ são mapeados em

$$|\xi_j\rangle_1 = \sum_{l=0}^{3} \sqrt{\frac{\lambda_l^2 - \lambda_{\min}^2}{1 - 4\lambda_{\min}^2}} e^{\frac{2i\pi lj}{4}} |l\rangle_1, \tag{D.51}$$

onde $\lambda_{\min}$ é o menor coeficiente de Schmidt de (5.36). Considere que Bob discrimina com sucesso os estados $|\xi_j\rangle_1$ com o uso da estratégia CMS. Dependendo da degenerescência de $\lambda_{\min}$, dada por $\mathfrak{d}^{\mathbb{1}}$, diferentes resultados para a informação mútua são obtidos, os quais serão demonstrados a seguir. Os casos onde $\mathfrak{d}^{\mathbb{1}} > 2$ não são tratados, pois não satisfazem as condições necessárias para a realização da estratégia CMS, conforme discutido na seção 3.3.1.

i) $\mathfrak{d}^{\mathbb{1}} = 1$

Se a degenerescência de $\lambda_{\min}$ é unitária, após um sucesso, os estados $|\xi_j\rangle_1$ são mapeados em

$$|u_j\rangle = \frac{1}{\sqrt{3}} \left[|0\rangle + e^{\frac{2i\pi j}{4}} |1\rangle + e^{\frac{4i\pi j}{4}} |2\rangle \right], \tag{D.52}$$

$j = 0, \ldots, 3$. Esse conjunto de estados é idêntico ao conjunto das equações (D.35)–(D.38), e, portanto, terá a mesma solução para a informação mútua, dada na equação (D.44). Essa solução é equivalente à mostrada na equação (5.46). ■

ii) $\mathfrak{d}^{\mathbb{1}} = 2$

Quando $\mathfrak{d}^{\mathbb{1}} = 2$, após uma segunda tentativa bem sucedida da estratégia CMS, os estados $|\xi_j\rangle_1$ são mapeados em

$$|u_j\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{2i\pi j}{4}} |1\rangle \right], \tag{D.53}$$

com $j = 0, \ldots, 3$. Esse conjunto é idêntico ao mostrado nas equações (D.45)–(D.48), e, portanto, a informação mútua é idêntica à da equação (5.47). ■

D.6 Exemplo 6: comparação entre EM e CMS para estados com número de Schmidt máximo

Esse exemplo dá continuidade ao apresentado na seção 5.3 e mostrado no apêndice D.2. Alice e Bob compartilham o estado da equação (5.23). Portanto, ao fim do protocolo de codificação superdensa, Bob deve discriminar entre os estados $|\nu_j\rangle_1$, dados por

$$|\nu_j\rangle_1 = \sum_{l=0}^{2} \lambda_l e^{\frac{2i\pi jl}{3}} |l\rangle_1. \tag{D.54}$$

O gráfico da figura 5.11 apresenta três superfícies distintas, portanto essa seção será dividida em três partes, cada qual correspondente à uma delas.

Superfície i)

De acordo com a estratégia CM, se Bob obtém um resultado indicativo de sucesso após a medição da *ancilla*, os estados $|\nu_j\rangle_1$ são mapeados em um conjunto ortogonal, pois são linearmente independentes. Assim, $P_{jl}^{\mathrm{CM}} = \delta_{jl}$ [veja equação (5.34)] e a informação mútua (5.35) será dada por

$$[I(M;L)]^{\mathrm{CM},\mathbb{1}} = \log_2 Dd_2 = \log_2 24 \text{ bits}. \tag{D.55}$$

■

Superfície ii)

Se a tentativa de discriminação dos estados $|\nu_j\rangle_1$ via CM fracassar, é possível realizar uma nova tentativa (desde que $\lambda_{\min}$ não seja degenerado). Após a falha, os estados $|\nu_j\rangle_1$ são mapeados, segundo a equação (5.32), em

$$|\xi_j\rangle_1 = \sum_{l=0}^{1} \sqrt{\frac{\lambda_l^2 - \lambda_{\min}^2}{1 - 3\lambda_{\min}^2}} e^{\frac{2i\pi lj}{3}} |l\rangle_1. \tag{D.56}$$

Se uma nova tentativa de discriminação via CM é bem sucedida, esses estados são mapeados, por sua vez, em

$$|u_0^2\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + |1\rangle\right], \tag{D.57}$$

$$|u_1^2\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{2i\pi}{3}} |1\rangle\right], \tag{D.58}$$

$$|u_1^2\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{4i\pi}{3}} |1\rangle\right], \tag{D.59}$$

onde o índice 2 indica o número de iterações da estratégia CMS. A discriminação entre esse novo conjunto de estados é feita segundo a estratégia EM. Os estados $|\mu_l'\rangle$ que geram os elementos de POVM ótimos, $\hat{\Pi}_l'$, de acordo com as equações (5.14) e (5.15), são dados por

$$|\mu_0'^2\rangle = \frac{1}{\sqrt{3}} \left[|0\rangle + |1\rangle + |2\rangle\right], \tag{D.60}$$

$$|\mu_1'^2\rangle = \frac{1}{\sqrt{3}} \left[|0\rangle + e^{\frac{2i\pi}{3}} |1\rangle + e^{\frac{4i\pi}{3}} |2\rangle\right], \tag{D.61}$$

$$|\mu_1'^2\rangle = \frac{1}{\sqrt{3}} \left[|0\rangle + e^{\frac{4i\pi}{3}} |1\rangle + e^{\frac{8i\pi}{3}} |2\rangle\right]. \tag{D.62}$$

Agrupando os termos equivalentes das probabilidades $P_{jl}^{\mathrm{CMS},2}$, equação (5.44), tem-se

$$P_{jl}^{\mathrm{CMS},2} = \begin{cases} |\langle \mu_j'^2 | \nu_k^2 \rangle|^2 = \frac{4}{6}, & \text{se } j = k, \\ |\langle \mu_j'^2 | \nu_k^2 \rangle|^2 = \frac{1}{6}, & \text{se } j \neq k. \end{cases} \tag{D.63}$$

Inserindo esses resultados na equação (5.45), obtém-se

$$[I(M;L)]^{\mathrm{CM},2} = \frac{10}{3} \text{ bits.} \tag{D.64}$$

■

Superfície iii)

Essa superfície é gerada pela discriminação EM dos estados $|\nu_j\rangle_1$. Esse resultado está mostrado no apêndice D.2. ■

D.7 Exemplo 7: comparação entre EM e CMS para estados com número de Schmidt não máximo

Neste exemplo, Alice e Bob compartilham o estado da equação (5.24). A tarefa de Bob é discriminar entre os estados simétricos equiprováveis do sistema 1, equação (5.3), dados por

$$|\nu_0\rangle = \lambda_0|0\rangle + \lambda_1|1\rangle + \lambda_2|2\rangle, \tag{D.65}$$

$$|\nu_1\rangle = \lambda_0|0\rangle + \lambda_1 e^{\frac{2i\pi}{4}}|1\rangle + \lambda_2 e^{\frac{4i\pi}{4}}|2\rangle, \tag{D.66}$$

$$|\nu_2\rangle = \lambda_0|0\rangle + \lambda_1 e^{\frac{4i\pi}{4}}|1\rangle + \lambda_2 e^{\frac{8i\pi}{4}}|2\rangle, \tag{D.67}$$

$$|\nu_1\rangle = \lambda_0|0\rangle + \lambda_1 e^{\frac{6i\pi}{4}}|1\rangle + \lambda_2 e^{\frac{12i\pi}{4}}|2\rangle. \tag{D.68}$$

O gráfico da figura 5.14 apresenta três superfícies distintas. Essa seção será dividida conforme o cálculo de cada uma delas.

Superfície i)

Esta superfície é gerada a partir da discriminação CM bem sucedida na primeira tentativa. Nesse caso, os estados $|\nu_j\rangle_1$ são mapeados em

$$|u_j\rangle = \frac{1}{\sqrt{3}}\left[|0\rangle + e^{\frac{2i\pi j}{4}}|1\rangle + e^{\frac{4i\pi j}{4}}|2\rangle\right], \tag{D.69}$$

com $j = 0, \ldots, 3$. Esse conjunto de estados é idêntico ao conjunto das equações (D.35)–(D.38). Portanto, os vetores que definem o POVM que os discrimina de forma ótima são dados por

(D.39)–(D.42), e as probabilidades $P_{jl}^{\mathrm{CMS},\mathbb{1}}$ por (D.43) [veja equação (5.34)]. Utilizando esses resultados, a informação mútua entre Alice e Bob, de acordo com a equação (5.35), será

$$[I(M;L)]^{\mathrm{CM},\mathbb{1}} \approx 3{,}792 \text{ bits}, \tag{D.70}$$

que é o resultado apresentado em (5.51). ■

Superfície ii)

Caso o processo de discriminação da estratégia CM falhe, os estados $|\nu_j\rangle_1$ são mapeados em

$$|\xi_j\rangle_1 = \sum_{l=0}^{2} \sqrt{\frac{\lambda_l^2 - \lambda_{\mathrm{min}}^2}{1 - 3\lambda_{\mathrm{min}}^2}} e^{\frac{2i\pi lj}{4}} |l\rangle_1, \tag{D.71}$$

onde $j = 0, \ldots, 3$. Esses estados podem ser discriminados de acordo com a estratégia CMS desde que λ_{min} não seja degenerado. Nesse caso, um sucesso na segunda tentativa gera os estados

$$|u_j\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\frac{2i\pi j}{4}} |1\rangle \right]. \tag{D.72}$$

Esse conjunto é idêntico ao conjunto de estados das equações (D.45)–(D.48), e, então, as probabilidades $P_{jl}^{\mathrm{CMS},2}$ [equação (5.44)] serão iguais às dadas em (D.49). Utilizando a equação (5.45), a informação mútua será

$$[I(M;L)]^{\mathrm{CMS},2} \approx 3{,}5 \text{ bits}, \tag{D.73}$$

resultado mostrado na equação (5.52). ■

Superfície iii)

Essa superfície é a mesma do exemplo 3 da seção 5.3 e está demonstrada no apêndice D.3. ■

Referências Bibliográficas

[1] C. H. Bennett e S. J. Wiesner. **Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states**. *Physical Review Letters* **69**, 2881 (1992).

[2] A. Einstein , B. Podolsky e N. Rosen. **Can quantum-mechanical description of physical reality be considered complete?** *Physycal Review* **47**, 777 (1935).

[3] M. A. Nielsen e I. L. Chuang. **Quantum Computation and Quantum Information**. Cambridge University Press (2010).

[4] J. A. Bergou e M. Hillery. **Introduction to the Theory of Quantum Information Processing**. Springer Science & Business Media (2013).

[5] M. Nakahara e T. Ohmi. **Quantum Computing: From Linear Algebra to Physical Realizations**. CRC Press (2008).

[6] S. Barnett. **Quantum Information**. Oxford University Press (2009).

[7] A. Peres. **Quantum Theory: Concepts and Methods**. Springer Science & Business Media (1995).

[8] S. Mozes, J. Oppenheim e B. Reznik. **Deterministic dense coding with partially entangled states**. *Physical Review A* **71**, 012311 (2005).

[9] Z. Ji, Y. Feng, R. Duan e M. Ying. **Boundary effect of deterministic dense coding**. *Physycal Review A* **73**, 034307 (2006).

[10] S. Wu, S. M. Cohen, Y. Sun e R. B. Griffiths. **Deterministic and unambiguous dense coding**. *Physical Review A* **73**, 042311 (2006).

[11] P. S. Bourdon, E. Gerjuoy, J. P. McDonald e H. T. Williams. **Deterministic dense coding and entanglement entropy**. *Physical Review A* **77**, 022305 (2008).

[12] A. Barenco e A. K. Ekert. **Dense coding based on quantum entanglement**. *Journal of Modern Optics* **42**, 1253 (1995).

[13] J.-C. Hao, C.-F. Li, e G.-C. Guo. **Probabilistic dense coding and teleportation**. *Physics Letters A* **278**, 113 (2000).

[14] A. K. Pati, P. Parashar e P. Agrawal. **Probabilistic superdense coding**. *Physical Review A* **72**, 012329 (2005).

[15] C. W. Helstrom. **Quantum detection and estimation theory**. *Journal of Statistical Physics* **1**, 231 (1969).

[16] A. S. Holevo. **Statistical decision theory for quantum systems**. *Journal of Multivariate Analysis* **3**, 337 (1973).

[17] H. P. Yuen, R. S. Kennedy e M. Lax. **Optimum testing of multiple hypotheses in quantum detection theory**. *IEEE Transactions on Information Theory* **21**, 125 (1975).

[18] S. M. Barnett e S. Croke. **On the conditions for discrimination between quantum states with minimum error**. *Journal of Physics A: Mathematical and Theoretical* **42**, 062001 (2009).

[19] I. D. Ivanovic. **How to differentiate between non-orthogonal states**. *Physics Letters A* **123**, 257 (1987).

[20] D. Dieks. **Overlap and distinguishability of quantum states**. *Physics Letters A* **126**, 303 (1988).

[21] A. Peres. **How to differentiate between non-orthogonal states**. *Physics Letters A* **128**, 19 (1988).

[22] A. Chefles e S. M. Barnett. **Entanglement and unambiguous discrimination between non-orthogonal states**. *Physics Letters A* **236**, 177 (1997).

[23] A. Chefles. **Unambiguous discrimination between linearly independent quantum states**. *Physics Letters A* **239**, 339 (1998).

[24] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson e J. Jeffers. **Maximum confidence quantum measurements**. *Physical Review Letters* **96**, 070401 (2006).

[25] R. P. Feynman. **Simulating physics with computers**. *International Journal of Theoretical Physics* **21**, 467 (1982).

[26] D. Deutsch. **Quantum theory, the Church-Turing principle and the universal quantum computer**. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **400**, 97 (1985).

[27] D. Deutsch e R. Jozsa. **Rapid solution of problems by quantum computation**. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **439**, 553 (1992).

[28] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres e W. K. Wootters. **Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels**. *Physical Review Letters* **70**, 1895 (1993).

[29] M. Zukowski, A. Zeilinger, M. A. Horne e A. K. Ekert. **"Event-ready-detectors" Bell experiment via entanglement swapping**. *Physical Review Letters* **71**, 4287 (1993).

[30] M. B. Plenio e S. Virmani. **An introduction to entanglement measures**. *arXiv preprint quant-ph/0504163* (2005).

[31] P. Rungta, V. Bužek, C. M. Caves, M. Hillery e G. J. Milburn. **Universal state inversion and concurrence in arbitrary dimensions**. *Physical Review A* **64**, 042315 (2001).

[32] C. E. Shannon. **A mathematical theory of communication**. *Bell System Technical Journal* **27**, 379, 623 (1948).

[33] T. M. Cover e J. A. Thomas. **Elements of Information Theory**. Oxford University Press (2006).

[34] J. Daboul, X. Wang e B. C. Sanders. **Quantum gates on hybrid qudits**. *Journal of Physics A: Mathematical and General* **36**, 2525 (2003).

[35] G. Alber, A. Delgado, N. Gisin e I. Jex. **Efficient bipartite quantum state purification in arbitrary dimensional Hilbert spaces**. *Journal of Physics A: Mathematical and General* **34**, 8821 (2001).

[36] G. Brassard, S. L. Braunstein e R. Cleve. **Teleportation as a quantum computation**. *Physica D: Nonlinear Phenomena* **120**, 43 (1998).

[37] L. Neves, M. A. Solís-Prosser, A. Delgado e O. Jiménez. **Quantum teleportation via maximum-confidence quantum measurements**. *Physical Review A* **85**, 062322 (2012).

[38] M. A. Solís-Prosser, A. Delgado, O. Jiménez e L. Neves. **Deterministic and probabilistic entanglement swapping of nonmaximally entangled states assisted by optimal quantum state discrimination**. *Physical Review A* **89**, 012337 (2014).

[39] P.-X. Chen, J. A. Bergou, S.-Y. Zhu e G.-C. Guo. **Ancilla dimensions needed to carry out positive-operator-valued measurement**. *Physical Review A* **76**, 060303 (2007).

[40] B. Coecke e É. O. Paquette. **POVMs and Naimark's theorem without sums**. *Electronic Notes in Theoretical Computer Science* **210**, 15 (2008).

[41] R. B. M. Clarke, A. Chefles, S. M. Barnett e E. Riis. **Experimental demonstration of optimal unambiguous state discrimination**. *Physycal Review A* **63**, 040305 (2001).

[42] O. Jiménez, M. A. Solís-Prosser, A. Delgado e L. Neves. **Maximum-confidence discrimination among symmetric qudit states**. *Physical Review A* **84**, 062315 (2011).

[43] M. A. Solís-Prosser, A. Delgado, O. Jiménez e L. Neves. **Parametric separation of symmetric pure quantum states**. *Physical Review A* **93**, 012337 (2016).

[44] A. Chefles. **Quantum state discrimination**. *Contemporary Physics* **41**, 401 (2000).

[45] S. M. Barnett e S. Croke. **Quantum state discrimination**. *Advances in Optics and Photonics* **1**, 238 (2009).

[46] J. A. Bergou. **Discrimination of quantum states**. *Journal of Modern Optics* **57**, 160 (2010).

[47] M. Ban, K. Kurokawa, R. Momose e O. Hirota. **Optimum measurements for discrimination among symmetric quantum states and parameter estimation**. *International Journal of Theoretical Physics* **36**, 1269 (1997).

[48] G. Jaeger e A. Shimony. **Optimal distinction between two non-orthogonal quantum states**. *Physics Letters A* **197**, 83 (1995).

[49] A. Peres e D. R. Terno. **Optimal distinction between non-orthogonal quantum states**. *Journal of Physics A: Mathematical and General* **34**, 7105 (1998).

[50] A. Chefles e S. M. Barnett. **Optimum unambiguous discrimination between linearly independent symmetric states**. *Physics Letters A* **250**, 223 (1998).

[51] A. Chefles e S. M. Barnett. **Strategies for discriminating between non-orthogonal quantum states**. *Journal of Modern Optics* **45**, 1295 (1998).

[52] A. Chefles e S. M. Barnett. **Quantum state separation, unambiguous discrimination and exact cloning**. *Journal of Physics A: Mathematical and General* **31**, 10097 (1998).

[53] A. Hayashi, T. Hashimoto e M. Horibe. **State discrimination with error margin and its locality**. *Physycal Review A* **78**, 012333 (2008).

[54] L. Roa, A. Delgado e I. Fuentes-Guridi. **Optimal conclusive teleportation of quantum states**. *Physical Review A* **68**, 022310 (2003).

[55] M. A. Solís-Prosser, O. Jiménez, L. Neves e A. Delgado. **Quantum teleportation via quantum channels with non-maximal Schmidt rank**. *Physica Scripta Volume T* **153**, 4058 (2013).

[56] A. Delgado, L. Roa, J. C. Retamal e C. Saavedra. **Entanglement swapping via quantum state discrimination**. *Physical Review A* **71**, 012303 (2005).

[57] B. He e J. A. Bergou. **A general approach to physical realization of unambiguous quantum-state discrimination**. *Physics Letters A* **356**, 306 (2006).

[58] V. Dunjko e E. Andersson. **Transformations between symmetric sets of quantum states**. *Journal of Physics A: Mathematical and Theoretical* **45**, 365304 (2012).

[59] S. Croke, E. Andersson e S. M. Barnett. **No-signaling bound on quantum state discrimination**. *Physical Review A* **77**, 012113 (2008).

[60] M. Horodecki, P. Horodecki e R. Horodecki. **General teleportation channel, singlet fraction, and quasidistillation**. *Physical Review A* **60**, 1888 (1999).

[61] G. Vidal, D. Jonathan e M. A. Nielsen. **Approximate transformations and robust manipulation of bipartite pure-state entanglement**. *Physical Review A* **62**, 012304 (2000).

[62] K. Banaszek. **Optimal quantum teleportation with an arbitrary pure state**. *Physical Review A* **62**, 024301 (2000).

[63] K. Banaszek. **Fidelity balance in quantum operations**. *Physical Review Letters* **86**, 1366 (2008).

[64] T. Mor. **TelePOVM–New faces of teleportation**. *arXiv preprint quant-ph/9608005* (1996).

[65] T. Mor e P. Horodecki. **Teleportation via generalized measurements, and conclusive teleportation**. *arXiv preprint quant-ph/9906039*, *arXiv preprint quant-ph/9906039* (1999).

[66] G. Brassard, P. Horodecki e T. Mor. **TelePOVM–A generalized quantum teleportation scheme**. *IBM Journal of Research and Development* **48**, 87 (2004).

[67] S. Bose, M. B. Plenio e V. Vedral. **Mixed state dense coding and its relation to entanglement measures**. *Journal of Modern Optics* **47**, 291 (2000).

[68] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland e W. K. Wootters. **Classical information capacity of a quantum channel**. *Physical Review A* **54**, 1869 (1996).