Fundamentos de Discriminação de Estados Quânticos

Conference Paper · August 2016

DOI: 10.21528/CBRN2005-221

Francisco M. de Assis
Universidade Federal de Campina Grande (UFCG)

Fundamentos de Discriminação de Estados Quânticos

Edmar J. Nascimento*, Francisco M. Assis*, Alessandra R. Souza†
*Departamento de Engenharia Elétrica
Universidade Federal de Campina Grande, Campina Grande, PB
Email: {jnedmar,fmarcos}@dee.ufcg.edu.br
†Departamento de Ciências da Computação
Universidade Federal de Campina Grande, Campina Grande, PB
Email: alesouza@dsc.ufcg.edu.br

***Resumo*— Neste artigo, é apresentado uma revisão dos principais resultados referentes ao problema de discriminação de estados quânticos. É abordado o problema da indistinguibilidade de estados quânticos não ortogonais, além das estratégias de medição usadas para obter o máximo de informação sobre os estados transmitidos. Particularmente, são analisadas estratégias de medições generalizadas conhecidas como POVM (*positive operator-valued measure*). Na obtenção dos POVMs é necessário resolver problemas de otimização que envolvem critérios como a probabilidade de erro, o erro médio quadrático ou a informação mútua. Além disso, aborda-se neste artigo, o problema da realização física desses operadores.**

I. Introdução

Nas últimas décadas, houve um interesse considerável pela utilização de sistemas quânticos nas áreas de computação, de transmissão da informação e de criptografia [1]. A razão desse interesse crescente é motivada pelas vantagens obtidas através da utilização de recursos quânticos tais como o emaranhamento e a indistinguibilidade de estados quânticos não ortogonais. Essas e outras propriedades foram utilizadas com sucesso no desenvolvimento de protocolos de criptografia, na transmissão de informação clássica através de estados quânticos [1] e em redes neurais quânticas [13], [14]. Em inúmeros problemas nas áreas de computação e informação quântica, pressupõe-se que possível distinguir estados quânticos não ortogonais, o que em geral não é possível. Esse problema, conhecido como *discriminação de estados quânticos*, foi tema de inúmeros artigos de pesquisa ao longo dos últimos anos.

O problema de discriminação de estados quânticos consiste em dado uma fonte quântica, um conjunto de M estados quânticos caracterizados pelos operadores densidade $\rho_j, j = 1 \cdots M$ cada um com uma probabilidade ξ_j associada, determinar através de um processo de medição qual estado ρ_j foi transmitido com o menor número de erros possível. No processo de medição, são utilizadas estratégias de detecção descritas por POVMs (*positive operator-valued measure*). Um POVM é qualquer conjunto de operadores hermitianos positivos Π_j que formam uma resolução da identidade, ou seja:

$$\Pi_j^\dagger = \Pi_j, \quad \Pi_j \geq 0 \ \ \forall j, \quad \sum_j \Pi_j = I. \tag{1}$$

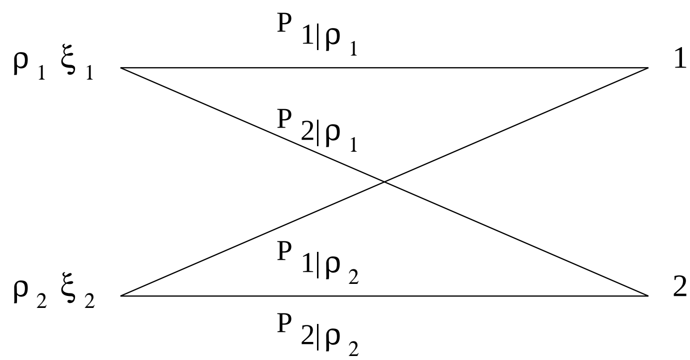

Fig. 1. Equivalência do problema de detecção quântico com um modelo de canal clássico. A matriz do canal é função do POVM escolhido.

Cada operador Π_j corresponde a uma saída possível do processo de medição, assim como mostrado na Figura 1, na qual:

$$P(j|i) = tr(\Pi_j \rho_i). \tag{2}$$

Pode-se observar, nessa figura, a correspondência entre o problema de detecção quântico e o modelo de um canal de comunicacão clássico no qual a matriz de transição do canal depende da escolha do POVM. Nesse artigo, é apresentada uma revisão acerca dos principais trabalhos realizados tendo como tema a obtenção de POVMs visando satisfazer critérios ótimos pré-estabelecidos. Na seção II, é apresentada uma revisão sobre alguns conceitos de sistemas quânticos e propriedades de POVMs. Na seção III são apresentados os principais resultados disponíveis na literatura referentes aos métodos de obtenção de POVMs. Na seção IV é destacada a estratégia de medição da raiz quadrada (*Square-Root Measurement*) para estados geometricamente uniformes. Ainda nessa seção, são apresentados exemplos de cálculo de POVMs. Na seção V é feito um breve comentário sobre os procedimentos necessários para realizar um POVM experimentalmente. Na seção VI são apresentadas algumas perspectivas de trabalhos futuros.

II. Medições e Sistemas Quânticos

Os sistemas quânticos são descritos pelas leis da mecânica quântica e esta, por sua vez, se baseia num conjunto de postulados que servem de base para toda a teoria quântica. A qualquer sistema quântico isolado há um espaço de Hilbert associado, conhecido como o espaço de estados do sistema, de modo que o sistema é complemente descrito por um vetor de estados unitário $|\psi\rangle$ ou pelo operador densidade equivalente ρ. O sistema quântico mais simples é o *qubit* (bit quântico). O qubit é um sistema associado a um espaço de Hilbert bidimensional, de modo que um vetor de estados arbitrário pode ser escrito como:

$$|\psi\rangle = a|0\rangle + b|1\rangle. \tag{3}$$

Sendo que $|0\rangle = [1\ 0]^T$ e $|1\rangle = [0\ 1]^T$ formam uma base ortonormal para o espaço de estados do sistema e a e b são números complexos arbitrários que satisfazem a relação $|a|^2 + |b|^2 = 1$.

Uma outra característica de sistemas quânticos isolados, é que a sua evolução é descrita por meio de transformações unitárias, de forma que o vetor de estados $|\psi\rangle$ no instante de tempo t_1 está relacionado com o vetor de estados $|\psi'\rangle$ no instante de tempo t_2 pela relação

$$|\psi'\rangle = U|\psi\rangle. \tag{4}$$

Sendo que U é um operador unitário que depende apenas dos instantes t_1 e t_2.

A fim de observar um sistema quântico é necessário interagir com ele através de um aparato de medição. Com essa interação, o sistema não é mais isolado e conseqüentemente não é mais descrito por transformações unitárias. As medições quânticas são descritas genericamente por uma coleção de operadores de medição $\{M_m\}$. O índice m se refere às saídas possíveis do processo de medição. Estes operadores atuam no espaço de estados do sistema que está sendo medido. Para um estado puro $|\psi_i\rangle$ com operador densidade $\rho_i = |\psi_i\rangle\langle\psi_i|$, a probabilidade de obter um resultado m dado o estado $|\psi_i\rangle$ dada por:

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi\rangle = tr(M_m^\dagger M_m \rho_i). \tag{5}$$

O POVM é então definido como

$$\Pi_m \equiv M_m^\dagger M_m. \tag{6}$$

Pela definição, verifica-se facilmente as propriedades indicadas pela equação 1. O fato da soma dos operadores ser igual à identidade é conseqüência do somatório das probabilidades ser igual a um.

III. Estratégias de Medição Ótimas

A partir da analogia feita entre o problema de detecção quântico e os canais de comunicação clássicos, torna-se natural usar medidas como a probabilidade de erro, o erro médio quadrático e a informação mútua de Shannon como critérios para a escolha de POVMs.

A. *Informação Mútua*

A informação mútua de Shannon [9] definida como

$$I(X:Y) = \sum_{i,j} \xi_i P(j|i) \log \frac{P(j|i)}{\sum_k \xi_k P(j|k)}, \tag{7}$$

mede a quantidade de informação obtida sobre uma variável aleatória X ao se realizar uma medição sobre uma variável Y. Objetiva-se então maximizar a informação mútua de modo a extrair o máximo de informação possível sobre a variável X.

Levando a definição de informação mútua para o contexto quântico tem-se um problema de otimização que tem como parâmetros um conjunto de estados $\rho_i, i = 1, \cdots, M$ com as suas respectivas probabilidades a priori associadas $\xi_i, i = 1, \cdots, M$. A otimização é realizada com relação à escolha do POVM $\{\Pi_j\}, j = 1, \cdots, N$. Os valores de M e N não são necessariamente os mesmos, assim como mostrado em [5]. Nesse problema, o valor máximo da informação mútua é chamado de informação acessível que é formalmente definida como:

$$I_{Ac} = \max_{\{\Pi_k\}} I(X:Y) \tag{8}$$

O problema de otimização definido pela equação 8 é um problema que ainda não foi resolvido para o caso geral [5], são conhecidas apenas as condições necessárias para a solução ótima. Essas condições são dadas pelo teorema citado a seguir [4].

Teorema 1 (Holevo): Seja $\mathbf{P} = \{P(j|i)\}$ o conjunto de todas as probabilidades de transição, $Q(\mathbf{P}) = I(\mathbf{P})$ uma medida de qualidade que nesse caso é igual a informação mútua (equação 7), $\mathbf{\Pi}' = \{\Pi'_j\}$ um conjunto de operadores de medição que otimiza Q e seja Q diferenciável no ponto $\mathbf{P}= \mathbf{P}_{\mathbf{\Pi}'}$. Além disso, define-se

$$F_j = \sum_i \rho_i \frac{\partial Q}{\partial P(j|i)}\Big|_{\mathbf{P}=\mathbf{P}_{\mathbf{\Pi}'}}. \tag{9}$$

Então, as duas condições equivalentes são asseguradas:

$$\Pi'_j(F_j - F_i)\Pi'_i = 0; \quad i, j \in \{1, \cdots N\} \tag{10}$$

e o operador

$$\Lambda = \sum_j F_j \Pi_j, \tag{11}$$

é hermitiano, satisfazendo a relação

$$(F_j - \Lambda)\Pi_j = 0, \quad j \in \{1, \cdots N\}. \tag{12}$$

Além disso, para $Q(\mathbf{P}) = I(\mathbf{P})$, F_j é dada por

$$F_j = \sum_i \xi_i \log \frac{P(j|i)}{\sum_k \xi_k P(j|k)} \rho_i. \tag{13}$$

Um outro resultado teórico bastante importante é o limitante de Holevo [1], o qual estabelece um limite superior para a informação acessível. O limitante de Holevo é dado pela seguinte expressão:

$$I_{Ac} \leq S(\rho) - \sum_i \xi_i S(\rho_i), \tag{14}$$

sendo que $\rho = \sum_i \xi_i \rho_i$ e $S(.)$ representa a entropia de Von Neumann definida como

$$S(\rho) = -tr(\rho \log \rho). \tag{15}$$

Apesar de não existir uma solução geral para o problema de maximização da informação mútua, é possível obter uma solução analítica para esse problema em casos em que os estados quânticos apresentam uma certa simetria. Resultados nessa linha foram apresentados em [3] e [5]. Particularmente em [5], foi obtida uma solução analítica para a informação acessível para uma família de M estados quânticos puros pertencentes a um espaço de Hilbert bidimensional quando estes possuem simetria no grupo do inteiros módulo M.

B. *Probabilidade de Erro*

Um outro critério bastante utilizado na obtenção de POVMs é a probabilidade de erro ou de modo equivalente, a probabilidade de acerto. Observando a Figura 1, verifica-se que a detecção dos estados quânticos é realizada com sucesso quando ao se transmitir o estado ρ_1 obtém-se a saída 1 (a detecção se deu através de Π_1) e ao se transmitir o estado ρ_2 obtém-se a saída 2 (a detecção se deu através de Π_2). Nos demais casos houve um erro de detecção. Dessa forma, para uma estratégia de medição com N saídas possíveis, a probabilidade de erro é calculada como [11]:

$$P_e = 1 - \sum_{j=1}^{N} \xi_j tr(\rho_j \Pi_j) \tag{16}$$

Assim como foi verificado para o problema de informação acessível, não existe uma solução analítica geral para o problema da minimização da probabilidade de erro [11]. Entretanto, as condições necessárias para a existência de uma solução ótima ainda são dadas pelo Teorema 1, com $Q(\mathbf{P}) = -P_e(\mathbf{P})$.

Em [7] é proposto um algoritmo para se obter numericamente um POVM que minimiza a probabilidade de erro definida pela equação (16), sem impor nenhuma restrição ao número de estados quânticos nem considerações de simetria. O algoritmo é iniciado com um POVM inicial não polarizado $\{\Pi_j^0\}$. Esse POVM é usado para calcular o operador de Lagrange λ dado por:

$$\lambda = \left(\sum_{j=1}^{N} \xi_j^2 \rho_j \Pi_j \rho_j \right)^{\frac{1}{2}}. \tag{17}$$

O operador de Lagrange calculado pela equação (17) é então usado para atualizar o POVM de acordo como a expressão seguinte:

$$\Pi_j^{n+1} = \xi_j^2 \lambda^{-1} \rho_j \Pi_j^n \rho_j \lambda^{-1}. \tag{18}$$

O processo é então repetido até que o POVM convirja para um valor estacionário.

C. *Erro Médio Quadrático*

Um terceiro critério usado para a obtenção de POVMs é o erro quadrático. Em [6], esse critério foi utilizado para o cálculo do POVM para uma fonte quântica com um número de estados menor ou igual à dimensão do espaço de Hilbert $\mathcal{H}$ do sistema. No problema abordado, os POVMs são operadores de posto 1 da forma $\Pi_j = |\mu_j\rangle\langle\mu_j|,\ j = 1, \cdots, m$, no qual os vetores $|\mu_j\rangle$ são vetores de medição pertencentes a um subespaço $\mathcal{U} \subseteq \mathcal{H}$. Para um conjunto de estados quânticos puros $|\phi_j\rangle$ e vetores de medição $|\mu_j\rangle$, o erro quadrático a ser minimizado é dado por:

$$E = \sum_{j=1}^{m} \langle e_j | e_j \rangle, \tag{19}$$

com $|e_j\rangle = |\phi_j\rangle - |\mu_j\rangle$.

Observando-se a equação (19), verifica-se que quanto mais próximos estiverem os vetores $|\phi_j\rangle$ e $|\mu_j\rangle$, menor é o erro. Tendo como base essa observação, constrói-se uma matriz Φ tendo como colunas os vetores de estado $|\phi_j\rangle$. Em seguida, realiza-se uma decomposição de valor singular (SVD) dessa matriz a fim de obter o POVM que minimiza o erro médio quadrático. Esse procedimento de obtenção de POVMs é detalhado na seção IV.

IV. Medição da Raiz Quadrada (SRM) para estados geometricamente uniformes

A medição da raiz quadrada corresponde a um POVM consistindo de operadores de posto um com bom poder de separação entre estados puros, sendo o número de estados menor que a dimensão do espaço de Hilbert gerado por eles. Para um conjunto de estados geometricamente uniforme (GU), o SRM minimiza a probabilidade de erro de detecção indicada pela equação (16).

Um conjunto de estados $S = \{|\phi_i\rangle = U_i|\phi\rangle\, U_i \in G\}$, sendo $|\phi\rangle$ um estado arbitrário, é chamado geometricamente uniforme se for gerado por um grupo abeliano finito G de m matrizes unitárias. Sendo $U_i^\dagger = U_i^{-1}$, o produto interno de dois vetores em S é $\langle\phi_i|\phi_j\rangle = \langle\phi|U_i^{-1}U_j|\phi\rangle = s(U_i^{-1}U_j)$, em que s é uma função em G definida por $s(U_i) = \langle\phi|U_i|\phi\rangle$. Toda linha e coluna da matriz de Gram $S_{m\times m} = \{\langle\phi_i|\phi_j\rangle\}$ é uma permutação dos números $\{s(U_i), 1 \leq i \leq m\}$.

Para facilitar os cálculos é importante substituir o grupo multiplicativo G por um grupo aditivo G' para o qual G é isomorfo. Todo grupo abeliano finito G é isomorfo a um produto direto G' de um número finito de grupos cíclicos: $G \cong G' = \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_p}$, em que $\mathbb{Z}_{m_k}$ é o grupo aditivo cíclico de inteiros módulo m_k, e $m = \prod_k m_k$. Logo, todo elemento $U_i \in G$ pode ser associado com um elemento $g \in G'$ da forma $g = (g_1, g_2, ..., g_p)$, sendo $g_k \in \mathbb{Z}_{m_k}$. Essa correspondência é denotada por $U_i \leftrightarrow g$. Cada vetor $|\phi_i\rangle = U_i|\phi\rangle$ será denotado como $|\phi(g)\rangle$, em que $g \in G'$ e corresponde a $U_i \in G$. O elemento $0 = (0, 0, ..., 0) \in G'$ corresponde à matriz identidade $I \in G$, e o inverso aditivo $-g \in G'$ corresponde ao inverso multiplicativo $U_i^{-1} = U_i^\dagger$.

Logo, a matriz de Gram S é dada por:

$$\begin{aligned} S &= \{\langle\phi(g')|\phi(g)\rangle, g', g \in G'\} \\ &= \{s(g-g'), g', g \in G'\} \end{aligned} \quad (20)$$

sendo que $s(g) = \langle\phi(0)|\phi(g)\rangle$.

Para obter o SRM para um conjunto de estados GU primeiramente determina-se a SVD de Φ, sendo Φ uma matriz $n \times m$ cujas colunas são os vetores $|\phi_i\rangle$. A transformada de Fourier (FT) de uma função de valor complexo $\varphi : G' \to \mathbb{C}$ definida em $G' = \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_p}$ é uma função de valor complexo $\hat{\varphi} : G' \to \mathbb{C}$ definida por:

$$\hat{\varphi(h)} = \frac{1}{m} \sum_{g \in G'} \langle h, g\rangle \varphi(g) \quad (21)$$

sendo $\langle h, g\rangle$ o núcleo de Fourier definido da seguinte forma:

$$\langle h, g\rangle = \prod_{k=1}^{p} e^{-2\pi i h_k g_k / m_k} \quad (22)$$

sendo h_k e g_k os k-ésimos componentes de h e g, respectivamente e o produto $h_k g_k$ um inteiro modulo m_k.

A matriz FT $m \times m$ sobre G' é definida da seguinte forma:

$$F = \{\frac{1}{\sqrt{m}}\langle h, g\rangle, h, g \in G'\} \quad (23)$$

Os autovetores da matriz de Gram S são os vetores coluna de F:

$$|F(h)\rangle = \{\frac{1}{\sqrt{m}}\langle h, g\rangle, g \in G'\} \quad (24)$$

Deste modo, S tem uma autodecomposição da forma $S = F\Sigma^2 F^\dagger$, sendo Σ uma matriz diagonal com elementos diagonais $\{\sigma(h) = m^{1/4}\sqrt{\hat{s}(h)}, h \in G'\}$, em que $\sigma^2(h)$ são os autovalores reais e não negativos de S.

A SVD de Φ é da forma

$$\Phi = \Upsilon\Sigma F^\dagger = \sum_{h \in G'} \sigma(h)|u(h)\rangle\langle F^\dagger(h)|, \quad (25)$$

sendo Υ uma matriz $n \times m$ cujas colunas $|u(h)\rangle$ são as colunas da base U da SVD de Φ, de modo que:

$$|u(h)\rangle = \begin{cases} \Phi|F(h)\rangle/\sigma(h) = |\hat{\phi}(h)\rangle/\sigma(h), & \text{se } \sigma(h) \neq 0; \\ \mathbf{0}, & \text{caso contrário.} \end{cases} \quad (26)$$

sendo,

$$|\hat{\phi}(h)\rangle = \frac{1}{m} \sum_{g \in G'} \langle h, g\rangle |\phi(g)\rangle \quad (27)$$

o h-ésimo elemento da FT de Φ visto como um vetor linha dos vetores colunas $\Phi = \{|\phi(g)\rangle, g \in G'\}$.

O SRM é dado pela matriz de medição M:

$$M = \Upsilon F^\dagger = \sum_{h \in G'} |u(h)\rangle\langle F^\dagger(h)| \quad (28)$$

em que as colunas de M são os vetores do POVM procurado.

A. Exemplo 1

Considera-se o grupo G das seguintes matrizes unitárias:

$$U_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad U_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$U_3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad U_4 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Seja $|\phi\rangle = \frac{1}{2}\begin{bmatrix} \sqrt{3} & -1 \end{bmatrix}^T$ um estado arbitrário e $S = \{|\phi_i\rangle = U_i|\phi\rangle, 1 \leq i \leq 4\}$ o conjunto de estados gerado pelo grupo G. Logo, a matriz Φ é:

$$\Phi = \frac{1}{2}\begin{bmatrix} \sqrt{3} & \sqrt{3} & -\sqrt{3} & -\sqrt{3} \\ -1 & 1 & 1 & -1 \end{bmatrix} \quad (29)$$

e a matriz de Gram S é dada por:

$$S = \begin{bmatrix} 1 & 0.5 & -1 & -0.5 \\ 0.5 & 1 & -0.5 & -1 \\ -1 & -0.5 & 1 & 0.5 \\ -0.5 & -1 & 0.5 & 1 \end{bmatrix} \quad (30)$$

Nesse caso, o grupo G' isomorfo ao grupo G é:

$$G' = \{(0,0), (0,1), (1,0), (1,1)\}$$

A tabela de multiplicação do do grupo G é:

	U_1	U_2	U_3	U_4
U_1	U_1	U_2	U_3	U_4
U_2	U_2	U_1	U_4	U_3
U_3	U_3	U_4	U_1	U_2
U_4	U_4	U_3	U_2	U_1

Definindo as correspondências:

$$U_1 \leftrightarrow (0,0) \quad U_2 \leftrightarrow (0,1) \quad U_3 \leftrightarrow (1,0) \quad U_4 \leftrightarrow (1,1)$$

tem-se a seguinte tabela de adição do grupo G':

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

A matriz de Fourier F é a seguinte matriz de Hadamard:

$$F = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (31)$$

A matriz Υ é:

$$\Upsilon = \frac{1}{2}\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (32)$$

Assim, a matriz de medição do SRM é:

$$M = \Upsilon F^\dagger = \begin{bmatrix} 0.5 & 0.5 & -0.5 & -0.5 \\ -0.5 & 0.5 & 0.5 & -0.5 \end{bmatrix} \quad (33)$$

O POVM é dado pelas matrizes $\Pi_i = |\mu_i\rangle\langle\mu_i|, i = 1, \cdots, 4$, em que os vetores $|\mu_i\rangle$ são as colunas da matriz M, e é dado por:

$$\Pi_1 = \frac{1}{4}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, \Pi_2 = \frac{1}{4}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$
$$\Pi_3 = \frac{1}{4}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, \Pi_4 = \frac{1}{4}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

B. *Exemplo 2*

Considera-se o grupo G das seguintes matrizes unitárias:

$$U_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, U_2 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$
$$U_3 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, U_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Seja $|\phi\rangle = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}^T$ um estado arbitrário e $S = \{|\phi_i\rangle = U_i|\phi\rangle, 1 \leq i \leq 4\}$ o conjunto de estados gerado pelo grupo G. Logo, a matriz Φ é:

$$\Phi = \frac{1}{2}\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{34}$$

e a matriz de Gram S é dada por:

$$S = \frac{1}{2}\begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ 0 & -1 & -1 & 2 \end{bmatrix} \tag{35}$$

Nesse caso, o grupo G' isomorfo ao grupo G é:

$$G' = \{(0,0), (0,1), (1,0), (1,1)\}$$

As correspondências e as tabelas de multiplicação e adição são as mesmas do exemplo anterior. A matriz de Fourier F é a seguinte matriz de Hadamard:

$$F = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{36}$$

A matriz Υ é:

$$\Upsilon = \begin{bmatrix} 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{37}$$

Assim, a matriz de medição do SRM é:

$$M = \Upsilon F^\dagger = \frac{1}{2\sqrt{2}}\begin{bmatrix} 1 & -1 & -1 & 1 \\ \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\ \sqrt{2} & -\sqrt{2} & \sqrt{2} & -\sqrt{2} \\ 1 & -1 & -1 & 1 \end{bmatrix} \tag{38}$$

Assim como foi feito no exemplo 1, o POVM é dado pelas matrizes $\Pi_i = |\mu_i\rangle\langle\mu_i|, i = 1, \cdots, 4$, em que os vetores $|\mu_i\rangle$ são as colunas da matriz M.

V. Realização Física do POVM

A implementação física dos POVMs é bem mais complicada do que a implementação de medições projetivas, medições de Von Neumann [2]. Para implementar um POVM é necessário primeiramente interagir o estado quântico que está sendo medido com um sistema quântico auxiliar chamado de *ancilla* resultando num estado conjunto descrito pelo operador $\rho_i \otimes \rho_{auxiliar}$. Em seguida, é efetuada uma medição projetiva no espaço de Hilbert combinado, ou seja, para cada possível saída do sistema composto, há um projetor correspondente P_i. Num teste deste tipo, a probabilidade de obter uma saída μ dado que o sistema original se encontrava no estado i é dada por

$$P_{\mu|i} = tr[P_\mu(\rho_i \otimes \rho_{aux})] \tag{39}$$
$$\equiv \sum_{mr,ns} (P_\mu)_{mr,ns}(\rho_i)_{nm}(\rho_{aux})_{sr} \tag{40}$$
$$= tr[A_\mu \rho_i]. \tag{41}$$

Sendo que, mr, ns, nm representam a dimensão dos operadores e

$$(A_\mu)_{mn} = \sum_{rs} (P_\mu)_{mr,ns}(\rho_{aux})_{sr} \tag{42}$$

é um operador atuando no espaço de Hilbert do sistema que se deseja efetuar a medição. Este operador é o POVM.

VI. Conclusões

Nesse tutorial, foi realizada uma revisão dos principais resultados disponíveis na literatura a respeito das estratégias utilizadas na discriminação de estados quânticos não ortogonais. Os objetivos dessa revisão foram: mostrar a relevância desse tópico para áreas como a computação e a criptografia quânticas; destacar os problemas que permanecem em aberto e fornecer subsídios para estudos futuros nessa área.

Um tema de bastante relevância para a área da computação e da teoria da informação quântica é o desenvolvimento de algoritmos para a obtenção de POVMs que maximizem a informação mútua. Nessa linha de trabalho, está sendo investigada a possibilidade de utilizar algoritmos para o cálculo da capacidade de canais [10] na obtenção de POVMs. Como a obtenção de POVMs para estados quânticos genéricos é um problema de difícil solução, a busca de POVMs pode ser facilitada para estados com uma dada simetria, assim como foi feito para os estados geometricamente uniformes. A análise das propriedades dessas estruturas simétricas é um tópico a ser explorado.

Agradecimentos

Os autores gostariam de agradecer ao Conselho Nacional de Desenvolvimento e Pesquisa (CNPq) pelo apoio financeiro.

REFERÊNCIAS

[1] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[2] Asher Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, 1993.

[3] E. B. Davies, Information and Quantum Measurement, IEEE Transactions on Information Theory 24, 5, September 1978

[4] A. S. Holevo, Statistical Decision Theory for Quantum Systems, Journal of Multivariate Analysis 3,337-394, 1973

[5] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki and O. Hirota, Accessible Information and Optimal Strategies for Real Symmetrical Quantum Sources, Physical Review A, 59, (5), 3325-3335, 1999

[6] Yonina C. Eldar and G. David Forney, On Quantum Detection and the Square-Root Measurement, IEEE Transactions on Information Theory, vol. 47, no 3, march 2001

[7] M. Ježek, J. Řeháček and J. Fiurášek, Finding Optimal Strategies for Minimum-error Quantum-state Discrimination, Physical Review A, 65, 060301, 2002

[8] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden and N. Gisin, Unambiguos Quantum Measurement of Nonorthogonal States, Physical Review A, 54, (5), 3783-3789

[9] Thomas M. Cover and Joy A. Thomas, Elements of Information Theory, John Wiley and Sons, INC. New York, 1991

[10] Richard E. Blahut, Computation of Channel Capacity and Rate-Distortion Functions IEEE Transactions on Information Theory, vol 18, no 4, july 1972

[11] Anthony Chefles, Quantum States: Discrimination and Classical Information Transmission. A Review of Experimental Progress, Quantum State Estimation, Springer, 2004

[12] Jànos A. Bergou, Ulrike Herzog and Mark Hillery, Discrimination of Quantum States, Quantum State Estimation, Springer, 2004

[13] D. Ventura, On the utility of entanglement in quantum neural computing, Neural Networks, 2001. Proceedings. IJCNN '01. International Joint Conference on, Vol.2, Iss., 2001 Pages:1565-1570 vol.2

[14] E.C. Behrman, J.E. Steck, and S.R. Skinner, A spatial quantum neural computer, Neural Networks, 1999. IJCNN '99. International Joint Conference on, Vol.2, Iss., Jul 1999 Pages:874-877 vol.2

[15] Yonina C. Eldar and Helmut Bölcskei, Geometrically Uniform Frames, IEEE Transactions on Information Theory, vol. 49, no 4, April 2003