

Informação Acessível Erro-Zero de Fontes Quânticas

Elloá B. Guedes e Francisco M. de Assis

Resumo— Neste artigo é apresentado um conceito denominado *informação acessível erro-zero de uma fonte quântica* o qual mede a quantidade de informação compartilhada por duas partes, uma que possui uma fonte quântica e outra que possui um esquema de medição dos estados desta fonte, com a restrição de que não deve haver erros de decodificação. Nenhum método geral é conhecido para o cálculo da informação acessível em um cenário quântico geral e, em virtude disto, o limitante superior de Holevo é utilizado. Porém, no cenário erro-zero descrito, é possível obter uma fórmula fechada para tal medida, a qual coincide com a capacidade erro-zero clássica de um canal discreto e sem memória equivalente. Os resultados propostos ampliam o entendimento da Teoria da Informação Quântica Erro-Zero e de suas particularidades.

Palavras-Chave— Teoria da Informação Quântica Erro-Zero; Informação Acessível; Fontes Quânticas; Limitante de Holevo.

Abstract— We introduce a new concept called *zero-error accessible information of a quantum source* which measures the amount of information shared by two parties, one which has a quantum source, and the other which uses a measurement scheme to decode the quantum states received, upon the restriction that no decoding errors must occur. No general method to obtain the accessible information in a general quantum scenario is known and due to that the Holevo upper bound is widely used. However, in the zero-error scenario described, it is possible to determine a closed formula for such measure which coincides with the classical zero-error capacity of an equivalent discrete memoryless channel. The results described increase the understanding of Quantum Zero-Error Information Theory and its particularities.

Keywords— Quantum Zero-Error Information Theory; Accessible Information; Quantum Source; Holevo Bound.

I. INTRODUÇÃO

A Teoria da Informação Quântica é um novo paradigma para o processamento e transmissão da informação por considerar as Leis da Física Quântica. Em consequência, a informação não encontra-se representada apenas sob a forma de bits, mas também de *qubits* (abreviação de *quantum bits*). Algumas características como *superposição*, *emaranhamento*, *não-clonagem* de estados arbitrários, dentre outras, são inerentes à este paradigma [1].

Uma maneira natural de explorar novos conceitos da Teoria da Informação Quântica é por meio da analogia com os conceitos clássicos equivalentes. A partir desta estratégia é que foi proposta a Teoria da Informação Erro-Zero Quântica, a qual trata do envio de informação clássica por canais quânticos sem erros de decodificação [2]. Esta teoria foi inspirada na Teoria

da Informação Erro-Zero Clássica, proposta por Shannon, que considera comunicações clássicas sem erros de decodificação, ainda que o canal seja ruidoso [3].

Ao considerar comunicações livres de erro, mesmo no cenário clássico, novos conceitos e interpretações foram formulados, tais como a capacidade erro-zero de um canal e o estabelecimento de uma relação com a Teoria dos Grafos [3], [4]. No cenário quântico, a proposição de tal teoria também teve impactos de mesma natureza, a exemplo da definição da capacidade quântica erro-zero clássica, da capacidade quântica erro-zero quântica, de uma relação análoga ao caso clássico em termos de Teoria dos Grafos, a identificação de outras capacidades e outros avanços, como a identificação de uma relação entre a capacidade erro-zero e a capacidade de sigilo de um canal quântico [2], [5]–[7].

Visando a continuação da expansão do corpo de conhecimento sobre a Teoria da Informação Quântica Erro-Zero, este artigo apresenta a definição de *Informação Acessível Erro-Zero de uma Fonte Quântica*, a qual não possui contrapartida clássica e está intrinsecamente ligada à capacidade erro-zero de canais clássicos. Enquanto a informação acessível no cenário clássico não é considerada uma medida não relevante, visto que dois estados clássicos são trivialmente distinguíveis, no cenário quântico isto não acontece devido à natureza mais complexa do tipo de informação. No cenário erro-zero quântico, em particular, ao invés obter uma aproximação da informação acessível por um limitante superior, a quantidade de Holevo, será mostrado como obter tal valor diretamente.

Para apresentar os resultados propostos, este artigo está organizado como segue. Os conceitos de informação acessível para os casos clássico e quântico serão apresentados na Seção II. Uma breve fundamentação teórica sobre a Teoria da Informação Clássica Erro-Zero será apresentada na Seção III. A definição da Informação Acessível Erro-Zero de uma Fonte Quântica será caracterizada na Seção IV. Por fim, as considerações finais e sugestões de trabalhos futuros serão apresentados na Seção V.

Notação e Convenções: – A notação de Dirac será utilizada para denotar estados quânticos e operações sobre eles [8]. O símbolo $\mathbb{1}$ denota a *matriz identidade*. Os logaritmos são tomados na base 2.

II. INFORMAÇÃO ACESSÍVEL CLÁSSICA E QUÂNTICA

Esta seção tem como objetivo a caracterização da informação acessível de fontes nos cenários clássico e quântico. A caracterização da parte clássica, em particular, é baseada na obra de Cover e Thomas [9].

Elloá B. Guedes, e Francisco M. de Assis, Instituto de Estudos em Computação e Informação Quânticas (IQuanta), Universidade Federal de Campina Grande, Av. Aprígio Veloso, 882 – Campina Grande-PB – Brazil, E-mails: {elloaguedes, fmarassis}@gmail.com. Os autores agradecem ao CNPQ, a CAPES e ao projeto QUANTA/RENASIC/FINEP.

A. Cenário Clássico

No estudo da Teoria da Informação Clássica, toma-se como ponto de partida um modelo de um sistema de comunicações digitais ponto-a-ponto, como ilustrado na Figura 1. Neste modelo, há uma fonte transmissora e um receptor.

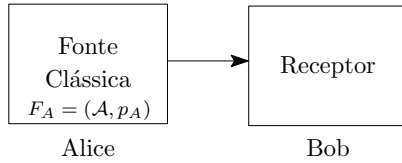


Fig. 1. Modelo simplificado de um sistema de comunicações clássico em que há apenas uma fonte e um receptor.

A *fonte*, em particular, pode ser classificada como sendo de dois tipos:

- 1) **Analgógica.** Este tipo de fonte gera mensagens em forma de onda, a exemplo de um sinal de voz;
- 2) **Discreta.** Este tipo de mensagens gera símbolos de um conjunto discreto e finito, a exemplo dos bits gerados por um computador digital.

Considerando o uso de fontes discretas, uma definição formal para as mesmas é apresentada a seguir.

Definição 1 (Fonte Clássica Discreta): Uma fonte clássica discreta F_A é dada por um par $F_A = (A, p_A)$ em que A é um alfabeto discreto e finito e p_A é a probabilidade de F_A gerar uma certa mensagem a_i , em que $\sum_{i=1}^{|A|} p_A(a_i) = 1$.

Uma medida que pode ser obtida sobre a fonte é a sua *entropia*, calculada de acordo com a entropia de Shannon, definida como segue.

Definição 2 (Entropia de uma Fonte Clássica Discreta): A entropia de uma fonte clássica $F_A = (A, p_A)$ é dada por

$$H(F_A) = - \sum_{i=1}^{|A|} p_A(a_i) \log(p_A(a_i)), \quad (1)$$

em que H denota a entropia de Shannon. Esta medida revela o grau de incerteza sobre os símbolos gerados pela fonte.

Suponha que a fonte transmissora e o receptor realizem o seguinte “jogo”: a entidade Alice possui uma fonte clássica discreta A , a qual emite n símbolos para a entidade Bob, cujo objetivo é medir corretamente o máximo de símbolos enviados pela fonte A , ou seja, descobrir $H(A)$. Uma boa medida da Teoria da Informação para este fim é a *informação mútua*, $H(A : B)$, supondo B os resultados da medição obtidos por Bob. A partir da definição de informação mútua, define-se o conceito de *informação acessível de uma fonte clássica discreta*, conforme formalizado a seguir.

Definição 3 (Informação Acessível de uma Fonte Clássica Discreta): Sejam duas variáveis aleatórias A e B . A informação acessível entre estas duas variáveis, denotada por I_{acc} é dada por

$$I_{acc} = \max H(A : B), \quad (2)$$

em que $H(A : B)$ denota a informação mútua entre as duas variáveis aleatórias em questão; e o máximo é tomado sobre todos os esquemas de medição possíveis.

Graças à desigualdade no processamento de dados, sabe-se que Bob pode inferir A a partir de B se, e somente se, $H(A : B) = H(A)$ mas, em geral, $H(A : B) \leq H(A)$. Pode-se afirmar, portanto, que a proximidade entre $H(A : B)$ e $H(A)$ é uma medida quantitativa sobre a capacidade de Bob em determinar A .

No caso clássico, a informação acessível entre duas variáveis aleatórias não é objeto de tantas pesquisas, pois, em princípio, é sempre possível distinguir dois símbolos clássicos quaisquer, o que faz com que $I_{acc} = H(A : B) = H(A)$. No caso quântico, porém, como será mostrado a seguir, isto não acontece, fato que motiva a realização de estudos e pesquisas em relação a esta medida.

B. Cenário Quântico

No estudo da informação acessível no contexto da Teoria da Informação Quântica, toma-se como ponto de partida o sistema de comunicações como ilustrado na Figura 2. A fonte quântica efetua a codificação de mensagens clássicas em estados quânticos, como apresentado na Definição 4.

Definição 4 (Fonte Quântica): Seja um conjunto de índices de mensagens clássicas dado por $\{1, \dots, \ell\}$. Uma fonte quântica é um ensemble de estados quânticos $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$ mapeados univocamente com o conjunto de índices de mensagens clássicas. A cada um destes estados quânticos está associada uma probabilidade p_i , $i = 1, \dots, \ell$, tal que $\sum_{i=1}^{\ell} p_i = 1$.

Inicialmente, tem-se um conjunto $\{1, \dots, \ell\}$ de mensagem clássicas e uma fonte quântica que mapeia tais mensagens em um conjunto $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$. O receptor Bob realiza uma medição POVM (*Positive Operator-Valued Measurement*) no estado recebido. As saídas da medição são argumentos para a função de decodificação. O decodificador deve decidir qual mensagem clássica foi enviada por Alice.

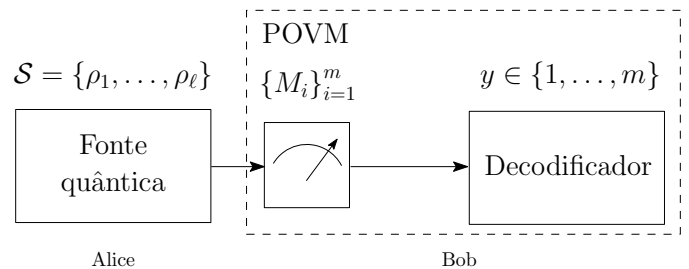


Fig. 2. Modelo simplificado de um sistema de comunicações quântico em que há apenas uma fonte e um receptor.

Levando a caracterização da fonte quântica em consideração, a mesma é um *ensemble* de estados puros ou mistos, dados por $\mathcal{S} = \{\rho_1, \dots, \rho_\ell\}$ com probabilidades p_1, \dots, p_ℓ . Assim como uma fonte clássica ao emitir uma sequência de n bits pode transmitir 2^n mensagens diferentes, uma fonte quântica ao enviar n qubits pode transmitir um estado quântico em um espaço de Hilbert de dimensão até 2^n [10].

Se os estados de \mathcal{S} forem todos ortogonais entre si, a fonte pode ser considerada *puramente clássica*, pois os estados são completamente distinguíveis no receptor. Se os estados de \mathcal{S} são puros, porém não-ortogonais, então não há medição clássica capaz de extrair a informação completa sobre o estado da fonte. Uma terceira situação considera que os estados da fonte são não-ortogonais, mas cujas matrizes de densidade comutam. Para esta última situação, a fonte é considerada de *broadcast*, ou seja, dados dois sistemas quânticos que não são cópias da fonte, o traço parcial de ambos os sistemas resulta no estado da fonte [11].

A entropia de uma fonte quântica é dada pelo análogo quântico da entropia de Shannon, denominada *entropia de von Neumann*. A definição da entropia de tais fontes é apresentada na Definição 5.

Definição 5 (Entropia de uma Fonte Quântica): *Seja uma fonte quântica F tal como apresentada na Definição 4. Seja $\rho = \sum_{i=1}^{\ell} p_i \rho_i$ uma média dos estados quânticos emitidos por esta fonte. A entropia de tal fonte quântica é dada por*

$$S(F) = -\text{Tr } \rho \log \rho, \quad (3)$$

em que S denota a entropia de von Neumann.

Na Teoria da Informação Quântica, nenhum método geral é conhecido para o cálculo da informação acessível de uma fonte quântica. Porém, alguns limitantes para tal medidas foram desenvolvidos, a exemplo do limitante de Holevo [10, Cap. 12].

Teorema 1 (Limitante de Holevo): *Suponha que Alice prepare um estado quântico ρ_A , com $A = \{\rho_0, \dots, \rho_n\}$ e probabilidades p_0, \dots, p_n , e o envie para Bob, que realiza medições com um POVM $\{M_i\}_{i=0}^m$ no estado recebido, obtendo B . O limitante de Holevo enuncia que, para qualquer esquema de medições que Bob utilize, tem-se*

$$H(A : B) \leq S(\rho) - \sum_{a \in A} p_a S(\rho_a), \quad (4)$$

em que $\rho = \sum_{a \in A} p_a \rho_a$.

O limitante de Holevo, frequentemente denotado por χ , é um limitante superior para a informação acessível entre as variáveis A e B num cenário quântico. Levando em consideração a convicavidade das entropias, tem-se que $H(A : B) \leq \chi \leq H(A)$. De acordo com tais condições, não existe possibilidade de Bob recuperar completamente a informação enviada por Alice, independente do esquema de medições que venha a usar. Esta situação constitui um cenário contraintuitivo quando comparado ao caso clássico equivalente.

Para exemplificar tal cenário, suponha que Alice possa enviar para Bob, de maneira equiprovável, dois estados quânticos $\rho_0 = |0\rangle$ e $\rho_1 = \cos\theta|0\rangle + \sin\theta|1\rangle$, em que θ é um parâmetro real. O limitante de Holevo em função do valor de θ é mostrado na Figura 3, em que o máximo é atingido quando $\theta = \pi/2$ e os estados ρ_0 e ρ_1 são ortogonais. Esta é a única situação em que Bob pode determinar exatamente qual estado foi preparado por Alice.

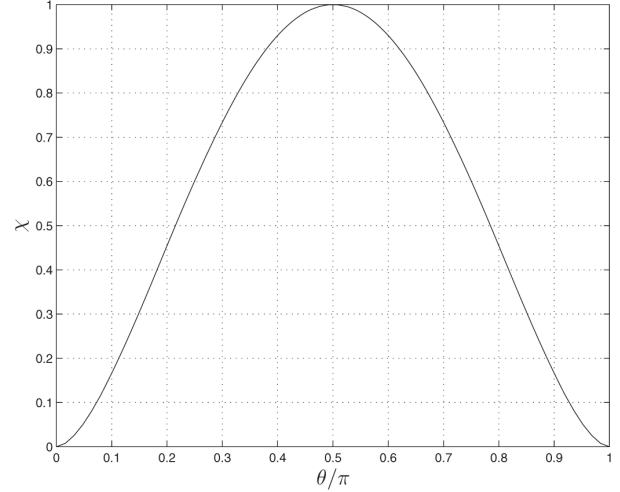


Fig. 3. Valor da quantidade de Holevo para o exemplo em questão, exibido em função da relação θ/π [10, pp. 569].

III. TEORIA DA INFORMAÇÃO ERRO-ZERO

A *capacidade erro-zero* de um canal clássico discreto e sem-memória (DSM) W foi definida por Shannon como a maior das taxas segundo a qual é possível transmitir informação com probabilidade nula de ocorrência de erros [3]. Para tanto, deve-se utilizar um código (M, n) livre de erros, cuja definição é dada a seguir.

Definição 6 (Código (M, n) Livre de Erros): *Um código (M, n) livre de erros para um DSM $W : \mathcal{A} \rightarrow \mathcal{B}$ é composto dos seguintes elementos:*

- 1) Um conjunto de índices $\{1, 2, \dots, M\}$, em que cada índice está associado a uma mensagem clássica;
- 2) Uma função de codificação $f_n : \{1, \dots, M\} \rightarrow \mathcal{A}^n$, gerando palavras-código $\mathbf{a}^1 = f_n(1), \dots, \mathbf{a}^M = f_n(M)$;
- 3) Uma função de decodificação $g^n : \mathcal{B}^n \rightarrow \{1, \dots, M\}$ que associa deterministicamente um palpite para cada palavra recebida, com a seguinte propriedade

$$\Pr[g_n(B^n) \neq i | \mathbf{A} = f_n(i)] = 0, \forall i \in \{1, \dots, M\}. \quad (5)$$

- 4) A taxa deste código é igual a $R = \frac{1}{n} \log M$ bits por símbolo por uso do canal.

Na Definição 6, a Eq. (5) impõe a restrição de que erros de decodificação não são tolerados.

Definição 7 (Capacidade Clássica Erro-Zero): *Seja $N(n)$ a cardinalidade máxima de um conjunto de vetores ortogonais entre os vetores de $W^n(\cdot | \mathbf{a}^n)$. A capacidade erro-zero clássica do canal DSM W é dada por*

$$C_0 = \limsup_{n \rightarrow \infty} \frac{1}{n} \log N(n). \quad (6)$$

A. Relação com a Teoria dos Grafos

A capacidade clássica erro-zero permite uma interpretação em termos da Teoria dos Grafos [3]. Dado um canal DSM W e

um conjunto de índices de mensagens $\{1, \dots, M\}$, é possível construir um grafo característico $\mathcal{G} = \langle V, E \rangle$ como segue:

- $V = \{1, \dots, M\}$ é o conjunto de vértices contendo os índices do conjunto de mensagens clássicas;
- $E = \{(i, j) | f_n(i) \perp_W f_n(j), i \neq j\}$, em que \perp_W denota dois vetores ortogonais na saída do canal W .

Esta noção de grafo característico também pode ser estendida para o n -produto de \mathcal{G}^n , em que $V = V^n$ e E é composto pelos pares cujos índices correspondentes na seqüência são não-adjacentes em W .

Definição 8 (Capacidade Erro-Zero em Termos de Grafos): A capacidade erro-zero de um canal DSM W é dada por

$$C_0(W) = \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n), \quad (7)$$

em que $\omega(\mathcal{G}^n)$ é o número de clique do n -produto do grafo característico \mathcal{G} .

Para ilustrar a capacidade erro-zero, suponha um canal clássico W_1 tal como ilustrado na Figura 4a. O grafo característico deste canal é mostrado na Figura 4b. Embora possa-se a priori cogitar que a capacidade erro-zero deste canal é 1 bit por símbolo por uso do canal, este é um caso não-trivial em que esta capacidade só é atingida após 2 ou mais usos do canal, sendo igual a $C_0(W_1) = \frac{1}{2} \log 5$ bits por símbolo por uso do canal por meio do código $\{00, 12, 24, 31, 43\}$. O cálculo da capacidade erro-zero do canal em questão foi um problema proposto por Shannon [3] e resolvido mais de 20 anos depois por Lovász [12].

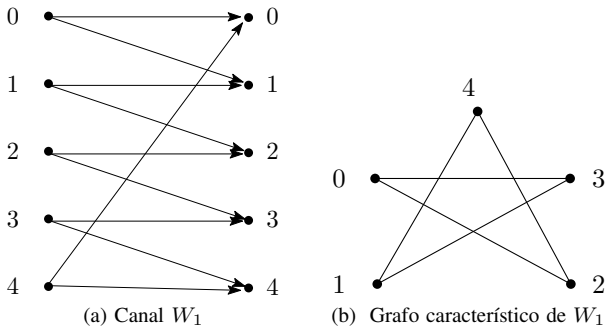


Fig. 4. Exemplo de positividade e não-trivialidade de capacidade erro-zero do canal DSM W_1 .

IV. INFORMAÇÃO ACESSÍVEL ERRO-ZERO DE UMA FONTE QUÂNTICA

Seja uma fonte quântica discreta e sem-memória produzindo uma seqüência i.i.d. de *letras quânticas* obtidas a partir de um conjunto $\mathcal{S} = \{|\psi_0\rangle, |\psi_1\rangle, \dots, |\psi_\ell\rangle\}$ com probabilidades p_0, p_1, \dots, p_ℓ associadas a um conjunto de índices de mensagens clássicas $\{0, 1, \dots, \ell\}$. O conjunto \mathcal{S} é o *alfabeto* da fonte quântica e, para fins de conveniência, será adotada a notação $\rho_i = |\psi_i\rangle\langle\psi_i|$ em favor de $|\psi_i\rangle$. As letras de \mathcal{S} são estados puros, mas não necessariamente ortogonais entre si. À fonte quântica em questão está associada a seguinte matriz densidade

$$\rho = \sum_{i=0}^{\ell} p_i \rho_i. \quad (8)$$

Assume-se que *Alice* possui uma fonte quântica com a descrição dada. Ela envia diretamente os símbolos produzidos pela fonte para *Bob*, o qual utiliza *medições de letra isolada* via um POVM $\mathcal{M} = \{M_i\}_{i=0}^m$ com o intuito de identificar qual mensagem correspondente foi enviada por Alice.

No processo de identificação das mensagens recebidas por Bob, admite-se que *erros de decodificação não são tolerados*, ou seja, considera-se apenas o caso que, com 100% de certeza, Bob é capaz de identificar precisamente, por meio da medição realizada, qual estado foi enviado por Alice. A partir destas considerações é possível definir o conceito de *Informação Acessível Erro-Zero* (IAEZ) de uma fonte quântica.

Definição 9 (Informação Acessível Erro-Zero de uma Fonte Quântica): Seja A uma variável aleatória discreta correspondendo ao índice de uma mensagem associado a uma letra quântica enviada por uma fonte quântica discreta e sem memória. Seja B , por sua vez, uma variável aleatória discreta correspondendo ao resultado da medição da letra quântica enviada pela fonte por meio da utilização de uma medição de letra isolada com um POVM \mathcal{M} . A informação acessível erro-zero da fonte quântica em questão, denotada por $I_{acc}^{(0)}$, corresponde ao maior número de mensagens enviadas pela fonte tais que $H(A|B) = 0$.

Teorema 2 (Expressão Numérica para a IAEZ): Seja $N(n)$ o número de letras quânticas de comprimento n que podem ser enviados por uma fonte quântica discreta e sem memória e recuperados livres de erro por um POVM via medições de letra isolada. A informação acessível erro-zero de uma fonte quântica discreta e sem-memória é dada por

$$I_{acc}^{(0)} \triangleq \sup_{n \rightarrow \infty} \frac{1}{n} \log N(n). \quad (9)$$

Demonstração: A demonstração deste teorema utiliza como estratégia a equivalência entre a emissão de uma letra pela fonte e a sua respectiva medição de letra isolada com um canal clássico discreto e sem-memória.

Levando em consideração o tipo de medição adotada, é possível descrever o estado produzido pela fonte e a saída do POVM como um canal clássico discreto sem memória $W : A \rightarrow B$ com a seguinte matriz estocástica

$$W(a, b) \triangleq \Pr[B = b | A = a] = \text{Tr}(\rho_a M_b), (a, b) \in \mathcal{A} \times \mathcal{B}, \quad (10)$$

em que ρ_a é a letra quântica emitida pela fonte; M_b é o elemento de operação do POVM utilizado para medição; e \mathcal{A} e \mathcal{B} são os alfabetos das variáveis aleatórias A e B . No caso da fonte emitir k letras quânticas, tem-se

$$W^k(a^k, b^k) = \prod_{i=1}^k W(a_i, b_i). \quad (11)$$

Considerando esta interpretação, a maior quantidade de símbolos que podem ser enviados pelo canal W sem erros de decodificação é igual à sua capacidade erro-zero, ou seja, $I_{acc}^{(0)} = C_0(W) = \sup_{n \rightarrow \infty} \frac{1}{n} \log N(n)$. Conclui-se, então, a prova em questão. ■

A Definição 9 e o Teorema 2 revelam um aspecto interessante a respeito das fontes quânticas. Se medições de letra isolada forem adotadas, a IAEZ das fontes quânticas reduz-se ao caso de calcular a capacidade erro-zero de um canal clássico, isto é, os aspectos quânticos de obter tal medida de informação não emergem neste cenário em particular. Vale salientar ainda que não há a qualquer imposição sobre a ortogonalidade das letras quânticas emitidas pela fonte, o que poderia forçá-la, por exemplo, a equivaler a uma fonte clássica.

É importante enfatizar que a definição de informação acessível erro-zero de uma fonte quântica impõe uma restrição, que é a ausência de erros. Com isto, tem-se que as desigualdades $I_{\text{acc}}^{(0)} \leq I_{\text{acc}} \leq \chi$ podem ser verificadas.

Para ilustrar os conceitos apresentados nesta seção, um exemplo detalhado será apresentado a seguir, no qual a IAEZ de uma fonte quântica será obtida e comparada com a quantidade de Holevo.

A. Exemplo

Suponha que Alice possui uma fonte quântica discreta e sem-memória cujo conjunto de mensagens clássicas $\{0, 1, 2, 3\}$ é mapeado univocamente para o conjunto de letras quânticas $\mathcal{S} = \{\rho_0, \rho_1, \rho_2, \rho_3\}$, em que $\rho_0 = |0\rangle\langle 0|$, $\rho_1 = |1\rangle\langle 1|$, $\rho_2 = |+\rangle\langle +|$ e $\rho_3 = |-\rangle\langle -|$ com $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Tais letras são emitidas pela fonte de maneira equiprovável, ou seja, $p_i = \frac{1}{4}$, $i = 0, \dots, 3$. É interessante notar que os estados emitidos pela fonte são puros, embora não necessariamente ortogonais entre si. Por exemplo, embora $\langle 0|1\rangle = 0$, tem-se que $\langle 0|+\rangle = \frac{1}{\sqrt{2}}$. Para efetuar as medições de letra isolada, Bob utiliza o POVM $\mathcal{M} = \{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$.

Levando em consideração a fonte quântica e o POVM utilizado para medição, como consequência do Teorema 2, é possível construir um canal clássico W_2 como mostrado na Figura 5a. A partir desta representação é possível obter o grafo característico deste canal, o qual encontra-se ilustrado na Figura 5b.

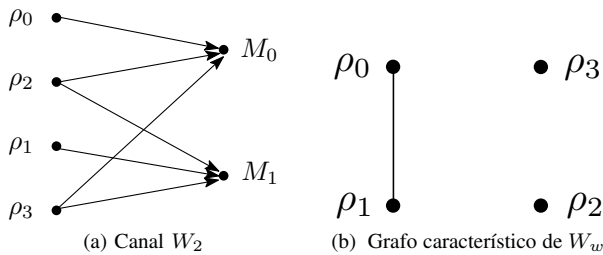


Fig. 5. Exemplo de canal clássico W_2 construído a partir de uma fonte quântica conforme Teorema 2.

A partir do grafo característico de W_2 é possível constatar que o número de clique do mesmo é igual a 2, ou seja, tem-se $C_0(W_2) = \log 2 = 1$ bit por símbolo por uso do canal. Em virtude do Teorema 2, tem-se que a informação acessível erro-zero desta fonte quântica é igual a $I_{\text{acc}}^{(0)} = 1$ bit por símbolo. A partir do exemplo em questão, embora a fonte quântica não seja redutível a uma fonte clássica, é possível que 1 bit por símbolo seja obtido a partir desta fonte por uma medição de letra isolada e livre de erros.

Utilizando os dados do conjunto \mathcal{S} , tem-se que a quantidade de Holevo para esta situação é igual a $\chi = 1$. Nota-se que, como previsto, $\chi \geq I_{\text{acc}}^{(0)}$.

V. CONSIDERAÇÕES FINAIS

Neste artigo foi apresentado o conceito de informação acessível erro-zero de uma fonte quântica, definido como sendo o maior conjunto de mensagens que podem ser emitidas por esta fonte e recuperadas por medições de letra isolada e sem erros de decodificação. Foi visto que esta medida de informação pode ser compreendida como a capacidade erro-zero de um canal clássico elaborado a partir de uma interpretação do cenário proposto.

A informação acessível de uma fonte clássica é trivialmente obtida. Para as fontes quânticas com estados não-ortogonais, não há uma forma direta de obtenção da informação acessível e, portanto, utiliza-se o limitante de Holevo. Em relação à informação acessível erro-zero de uma fonte quântica, por sua vez, existe uma fórmula conhecida para a sua obtenção. Embora a fonte seja verdadeiramente quântica, esta fórmula envolve a representação de um canal clássico, revelando uma característica peculiar e não-trivial do cenário erro-zero das comunicações quânticas.

Em trabalhos futuros almeja-se explorar esta medida das fontes quânticas, porém considerando o uso de medições coletivas e também pares ótimos de letras quânticas e POVMs para o cenário erro-zero, tal como proposto por Medeiros e outros [13].

REFERÊNCIAS

- [1] S. Imre and F. Balazs, *Quantum Computing and Communications - An Engineering Approach*. John Wiley & Sons, 2005.
- [2] R. A. C. Medeiros, "Zero-error capacity of quantum channels," Ph.D. dissertation, Universidade Federal de Campina Grande – TELECOM Paris Tech, 2008.
- [3] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8–19, 1956.
- [4] J. Körner and A. Orlitsky, "Zero-error information theory," *IEEE Transactions on Information Theory*, vol. 44, pp. 2207–2229, 1998.
- [5] R. A. C. Medeiros and F. M. de Assis, "Quantum zero-error capacity," *International Journal of Quantum Information*, vol. 3, no. 1, pp. 135–139, 2005.
- [6] R. Duan, S. Severini, and A. Winter, "Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovász ϑ function," 2011, in IEEE International Symposium on Information Theory. Disponível em arxiv:quant-ph/1002.2514.
- [7] E. B. Guedes and F. M. de Assis, "Quantum zero-error secrecy capacity," in *Workshop School of Quantum Computation and Information*, 2012, pp. 1–8.
- [8] P. Dirac, *The principles of Quantum Mechanics*, 4th ed. Oxford University Press, 1982.
- [9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2006.
- [10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Bookman, 2010.
- [11] C. H. Bennett and P. W. Shor, "Quantum information theory," *IEEE Transactions on Information Theory*, vol. 44, no. 6, 1998.
- [12] L. Lovász, "On the Shannon capacity of a graph," *IEEE Trans. Info. Theory*, vol. 25, no. 1, pp. 1–7, 1979.
- [13] R. Medeiros, R. Alleaume, G. Cohen, and F. M. de Assis, "Zero-error capacity of quantum channels and noiseless subsystems," in *IEEE International Telecommunications Symposium*, 2006, pp. 900–905.