Capacidade erro-zero de canais quânticos com medições coletivas

Rex A. C. Medeiros[†§], Francisco M. de Assis[§], Romain Alléaume[†] e Gérard Cohen[†]

***Resumo*— A capacidade erro-zero de um canal quântico foi definida como sendo o supremo das taxas em que informação clássica pode ser transmitida através de um canal quântico, considerando uma probabilidade de erro igual a zero. Neste artigo, o valor da capacidade é analisado para o caso em que medições entrelaçadas são permitidas na saída do canal. É mostrado que medições coletivas podem aumentar a capacidade erro-zero dos canais quânticos. É também mostrado um exemplo de um canal quântico para o qual a capacidade erro-zero é alcançada usando uma família de estados quânticos não ortogonais na entrada do canal.**

***Palavras-Chave*— Canais quânticos, capacidade erro-zero, medições entrelaçadas.**

***Abstract*— The zero-error capacity of a quantum channel was defined as the least upper bound of rates at which classical information can be transmitted without error through a noisy quantum channel. This paper investigates the behavior of the quantum zero-error capacity when entangled measurements between several channel outputs are allowed. It is shown that collective measurements may increase the channel capacity. We also show an example of a quantum channel for which the zero-error capacity is reached using an ensemble of non-orthogonal input states.**

***Keywords*— Quantum channels, zero-error capacity, collective measurements.**

I. INTRODUÇÃO

A teoria da informação quântica, assim como a teoria da informação clássica, geralmente propõe soluções assintóticas para o problema da determinação da capacidade de canais, em que uma probabilidade de erro arbitrariamente pequena existe mesmo quando se faz uso do melhor esquema de codificação. Ao que concerne a transmissão de informação clássica através de um canal quântico, se encaixam nesta categoria:

1) a capacidade de Holevo-Schumacher-Westrmoreland (HSW), definida como a taxa assintótica máxima na qual a informação clássica pode ser transmitida confiavelmente, usando codificação e decodificação quânticas [1], [2];
2) a capacidade auxiliada por entrelaçamento C_E, que é o supremo das taxas para transmissão de informação clássica através de um canal quântico quando uma quantidade ilimitada de entrelaçamento está disponível entre o transmissor e o receptor [3];
3) a capacidade adaptativa de Shor [4], em que o sistema de medição dos estados quânticos na saída do canal pode variar segundo o resultado de medições passadas.

Nos casos 1) e 2) o protocolo de comunicação restringe à entrada do canal a produtos tensoriais de estados quânticos, enquanto que as medições na saída são entrelaçadas entre vários usos do canal. A capacidade de Shor prevê medições individuais para cada estado quântico recebido.

Recentemente, Medeiros e Assis [5] generalizaram a capacidade erro-zero de canais clássicos discretos sem memória [6], [7] para canais quânticos. A capacidade erro-zero quântica (CEZQ) foi definida como o supremo das taxas para a transmissão de informação clássica através de um canal quântico ruidoso, com a restrição de que a probabilidade de erro deve ser igual a zero. Quanto ao protocolo, as entradas são restritas a produtos tensoriais e as medições são tomadas individualmente na saída do canal. Vários foram os desenvolvimentos feitos em torno da CEZQ [8], [9]. Em particular, foi demonstrado que a capacidade HSW é um limitante superior para a CEZQ [10], bem como conexões com a teoria de subsistemas quânticos sem ruído e subespaços livres de decoerência[11].

Neste trabalho será analisado o que acontece com o valor da capacidade erro-zero quântica quando são permitidas medições entrelaçadas entre várias saídas do canal. Como no caso da capacidade HSW, é mostrado que tais medições podem contribuir para aumentar o valor da capacidade erro-zero de canais quânticos. Nesta abordagem, uma maximização sobre as medições (POVM) torna-se desnecessária, contrariamente ao caso em que a capacidade erro-zero é calculada considerando medições individuais [12]. Por último, será mostrado um exemplo de um canal quântico tal que sua CEZQ é alcançada usando um subconjunto de estados quânticos não-ortogonais na entrada do canal. Ainda, este canal quântico dá origem ao pentágono como grafo característico, de forma que a CEZQ pode ser precisamente calculada e um código atingindo a capacidade explicitado.

O artigo está organizado como segue. A Seç. II apresenta um resumo da definição da capacidade erro-zero quântica, bem como desenvolvimentos necessários à compreensão do restante do artigo. As várias formas de definir capacidades erro-zero para a transmissão de informação clássica através de canais quânticos são discutidas na Seç. III. Na Seç. IV a capacidade erro-zero é analisada para o caso onde são consideradas medições coletivas na saída do canal. Finalmente, a Seç. V mostra um exemplo de um canal quântico cuja capacidade é alcançada para estados não-ortogonais na entrada do canal. As conclusões são tecidas na Seç. VI.

[†] Département Informatique et Réseaux, École Nationale Supérieure des Télécommunications, Paris, France

[§] Departamento de Engenharia Elétrica, Universidade Federal de Campina Grande, Campina Grande, Brazil.

Emails: medeiros@enst.fr, fmarcos@dee.ufcg.edu.br, alleaume@enst.fr e cohen@enst.fr

II. CAPACIDADE ERRO-ZERO DE CANAIS QUÂNTICOS

Com o objetivo de facilitar a leitura deste trabalho, será apresentada nesta seção um resumo da capacidade erro-zero de canais quânticos tal como ela foi definida em [5].

Seja $\mathcal{E}$ um canal quântico definido num espaço de Hilbert $\mathcal{H}$ de dimensão d. Tal canal quântico pode ser modelado por um operador linear, completamente positivo e que preserva o traço dos operadores de densidade na entrada do canal, $\mathcal{E} \equiv \{E_a\}$, em que E_a são operadores de Kraus em $\mathcal{H}$ satisfazendo $\sum_a E_a^\dagger E_a = \mathbb{1}$ [13]. A saída do canal para uma entrada ρ_i é dada por

$$\mathcal{E}(\rho_i) = \sum_a E_a \rho_i E_a^\dagger. \tag{1}$$

O canal quântico $\mathcal{E}$ é dito ser sem memória se o mesmo não produz entrelaçamento na saída quando produtos tensoriais de estados quânticos são colocados na entrada. Neste caso, n usos do canal quântico para a transmissão de um estado $\overline{\rho}_i = \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}$ produz uma saída $\mathcal{E}(\overline{\rho}_i)$ que é dada por

$$\begin{aligned} \mathcal{E}(\overline{\rho}_i) &= \mathcal{E}(\rho_{i_1}) \otimes \cdots \otimes \mathcal{E}(\rho_{i_n}) \\ &= \bigotimes_{j=1}^{n} \mathcal{E}(\rho_{i_j}). \end{aligned} \tag{2}$$

O protocolo de comunicação originalmente proposto pode ser resumido como segue. É definido um subconjunto finito de estados quânticos de entrada $\mathcal{S} = \{\rho_1, \ldots, \rho_l\}$, em que cada estado $\rho_i \in \mathcal{S}$ reside num espaço de Hilbert de entrada $\mathcal{H}_E$ de mesma dimensão que $\mathcal{H}$. As palavras-código de um código quântico de erro-zero de comprimento n são produtos tensoriais de estados em $\mathcal{S}$, $\overline{\rho}_i = \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}$, os quais são definidos num espaço produto $\mathcal{H}_E^{\otimes n}$ de dimensão d^n. Por sua vez, um código de bloco quântico de erro-zero e de comprimento n é um mapeamento de K_n mensagens clássicas (que podem ser representadas por índices $1, \ldots, K_n$) em um subconjunto de palavras-código de comprimento n. Claramente, a taxa deste código é dada por $R = \frac{1}{n} \log K_n$.

Na recepção, as seqüências recebidas são medidas usando um POVM (*Positive Operator-Valued Measurements*), $\mathcal{P} = \{M_1, \ldots, M_m\}$, em que M_i são operadores no espaço de Hilbert de saída $\mathcal{H}_S$ de dimensão d. Isto implica que o protocolo emprega medições individuais, ou seja, cada estado $\mathcal{E}(\rho_{i_j})$ da palavra-código de saída $\mathcal{E}(\overline{\rho}_i) = \mathcal{E}(\rho_{i_1}) \otimes \cdots \otimes \mathcal{E}(\rho_{i_n})$ é medido individualmente. Neste caso, a medição de $\mathcal{E}(\overline{\rho}_i)$ produz uma de *palavra de saída*, $w_n \in \{1, \ldots, m\}^n$.

O esquema de decodificação para um código de bloco quântico de comprimento n é uma função que associa univocamente cada palavra de saída a inteiros de 1 a K_n que representam as mensagens clássicas. A *probabilidade de erro* para este código é maior do que zero se o sistema de decodificação identifica na saída uma mensagem diferente daquela enviada.

A Fig. 1 ilustra o diagrama de blocos de um sistema de comunicações para a transmissão de mensagens clássicas através de um canal quântico usando o protocolo de erro-zero descrito. Inicialmente é escolhido um índice i que representa uma das K_n mensagens clássicas. Em seguida, o codificador mapeia i numa palavra-código de comprimento n. A seqüência é então transmitida através de um canal quântico ruidoso. Na recepção, são realizadas medições individuais definidas pelo POVM $\mathcal{P}$ composto por operadores em $\mathcal{H}_S$. De posse da palavra de saída w_n, o decodificador deve decidir, *sem erro*, em um dos índices $1, \ldots, K_n$ que representa a mensagem realmente transmitida.

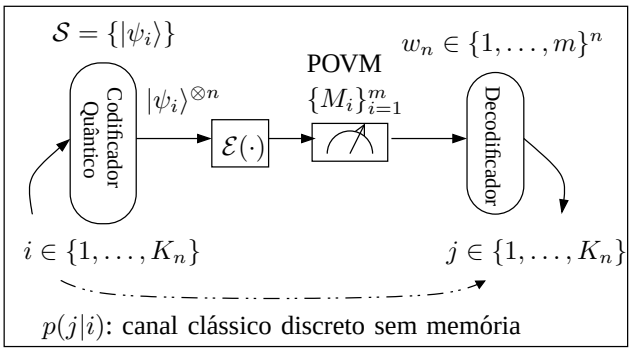

Fig. 1. Representação geral de um sistema de comunicações quântico para a transmissão de mensagem clássicas.

Originalmente, a capacidade erro-zero de um canal quântico foi definida como segue [5]:

Definição 1 *Seja $\mathcal{E}$ um canal quântico representado por um operador linear, completamente positivo e que preserva o traço. A capacidade erro-zero de $\mathcal{E}$, denotada por $C^{(0)}(\mathcal{E})$, é o supremo de todas as taxas alcançáveis com probabilidade de erro igual a zero. Isto é,*

$$C^{(0)}(\mathcal{E}) = \sup_n \frac{1}{n} \log K_n, \tag{3}$$

em que K_n é o número máximo de mensagens clássicas que o sistema pode transmitir sem erro, quando um código de bloco quântico de comprimento n é usado.

A. Equivalente clássico

A Definição 1 não faz menção sobre como a capacidade erro-zero de um canal quântico pode ser calculada. Medeiros e Assis [14] propuseram um procedimento geral para este cálculo, o qual é descrito a seguir.

Considere um canal quântico $\mathcal{E}$. Para uma escolha de um subconjunto $\mathcal{S} = \{\rho_i, \ldots, \rho_l\}$ de estados quânticos de entrada e de um POVM $\mathcal{P} = \{M_1, \ldots, M_m\}$, é possível definir um canal clássico discreto sem memória como segue:

- O alfabeto de entrada X do canal discreto sem memória é composto pelos índices dos estados quânticos de entrada, ou seja, $X = \{1, \ldots, l\}$.
- O alfabeto de saída Y é dado pelos índices dos operadores de medição, $Y = \{1, \ldots, m\}$.
- Os elementos da matriz estocástica do canal equivalente clássico são dados por

$$p(y|x) = \operatorname{tr}\left[\mathcal{E}(\rho_x) M_y\right]. \tag{4}$$

Desta forma, para cada par $(\mathcal{S}, \mathcal{P})$ é possível definir um canal clássico discreto sem memória equivalente. Evidentemente, cada um desses canais equivalentes possui uma capacidade erro-zero (clássica) $C_0(\mathcal{S}, \mathcal{P})$. Foi mostrado [14], [5] que a capacidade erro-zero do canal quântico $\mathcal{E}$ é igual ao supremo

das capacidades erro-zero clássicas $C_0(\mathcal{S},\mathcal{P})$ sobre todos os pares $(\mathcal{S},\mathcal{P})$ possíveis, ou seja,

$$C^{(0)}(\mathcal{E}) = \sup_{(\mathcal{S},\mathcal{P})} C_0(\mathcal{S},\mathcal{P}). \quad (5)$$

O par $(\mathcal{S},\mathcal{P})$ que alcança o supremo na Eq. (5) é chamado de *ótimo*.

Para um canal quântico $\mathcal{E}$ e uma escolha de um par $(\mathcal{S},\mathcal{P})$, dois estados $\rho_i,\rho_j \in \mathcal{S}$ são ditos ser adjacentes *com relação* ao POVM $\mathcal{P}$ se, e somente se, tr $[\mathcal{E}(\rho_i)M_k] > 0$ e tr $[\mathcal{E}(\rho_j)M_k] > 0$ para ao menos um $M_k \in \mathcal{P}$. Caso contrário, ρ_i e ρ_j são denominados não-adjacentes. É fácil verificar que se ρ_i e ρ_j são não-adjacentes com relação a $\mathcal{P}$, então é possível distinguir perfeitamente entre $\mathcal{E}(\rho_i)$ e $\mathcal{E}(\rho_j)$. Medeiros e Assis mostraram que um canal quântico possui capacidade erro-zero positiva se, e somente se, existir um par $(\mathcal{S},\mathcal{P})$ tal que pelo menos dois estados em $\mathcal{S}$ são não-adjacentes com relação ao POVM $\mathcal{P}$ [5].

Seguindo uma construção sugerida por Shannon [6], [7], o método de cálculo da capacidade erro-zero de canais quânticos via equivalente clássico pode ser reformulado usando elementos da teoria de grafos. Considere um canal quântico $\mathcal{E}$. Para um dado par $(\mathcal{S},\mathcal{P})$ é possível construir um grafo característico $\mathcal{G}$ como segue. O conjunto de vértices é formado pelos índices de $\mathcal{S}$, $V(\mathcal{G}) = \{1,\ldots,l\}$, e dois vértices $i,j \in V(\mathcal{G})$ são conectados em $\mathcal{G}$ se os respectivos estados quânticos $\rho_i,\rho_j \in \mathcal{S}$ são não-adjacentes com relação ao POVM $\mathcal{P}$. A Eq. (5) pode ser então reescrita como [5], [11]:

$$C^{(0)}(\mathcal{E}) = \sup_{(\mathcal{S},\mathcal{P})} \sup_n \frac{1}{n} \log \omega(\mathcal{G}^n), \quad (6)$$

em que $\omega(\mathcal{G})$ é o número de cliques [15] do grafo $\mathcal{G}$, e $\mathcal{G}^n$ é o $n-$ésimo produto de $\mathcal{G}$ como definido em [7].

III. Formas de definir a capacidade erro-zero

Como indicado na introdução, existem várias maneiras de definir capacidades de canais quânticos. Somente capacidades para transmissão de mensagens clássicas serão discutidas aqui. Com relação à capacidade erro-zero, existem quatro protocolos principais que podem originar valores diferentes de capacidades:

1) palavras-código são restritas a produtos tensoriais de estados quânticos de entrada, e medições são feitas individualmente na saída do canal;
2) entrelaçamento entre vários usos do canal é permitido, enquanto que medições são feitas individualmente na saída do canal;
3) palavras-código são restritas a produtos tensoriais de estados quânticos de entrada, enquanto que medições entrelaçadas entre várias saídas do canal são permitidas;
4) entrelaçamento entre vários usos do canal é permitido, como também medições entrelaçadas entre várias saídas.

A capacidade erro-zero na Def. 1 corresponde ao caso 1). Um dos problemas em aberto na teoria da informação é o da aditividade da capacidade HSW. Holevo conjeturou [2] que o uso de entrelaçamento na entrada não aumenta a capacidade HSW de canais quânticos sem memória[1]. Embora não tenham formalmente provado, Medeiros e Assis [8] mostraram vários indícios de que a aditividade de Holevo também pode ser válida para a capacidade erro-zero.

Com relação às medições, é sabido que medidas entrelaçadas entre várias saídas do canal podem aumentar a informação mútua entre a entrada e a saída do canal quântico, sendo essenciais para atingir a capacidade HSW [13]. Desta forma, o protocolo do item 3) é de particular interesse e será discutido ao longo deste artigo. Será mostrado na próxima seção que o uso de medições entrelaçadas pode aumentar a capacidade $C^{(0)}(\mathcal{E})$ da Def. 1. Para este protocolo, será mostrado que não é necessária uma maximização sobre as medições $\mathcal{P}$, contrariamente ao caso da capacidade erro-zero com medições individuais, cujo valor é dado pelas Eqs. (5) e (6).

IV. Capacidade erro-zero com medições coletivas

De maneira análoga à Sec. II, considere um canal quântico $\mathcal{E}$ num espaço de Hilbert $\mathcal{H}$ de dimensão d. Considere o protocolo do item 3) da Sec. III, descrito em detalhes abaixo:

- o alfabeto do código quântico de erro-zero é um subconjunto $\mathcal{S} = \{\rho_1,\ldots,\rho_l\}$ de estados quânticos pertencentes ao espaço de Hilbert de entrada $\mathcal{H}_E$ de dimensão d;
- para serem transmitidas através do canal quântico, as mensagens clássicas são mapeadas em palavras-código quânticas que são produtos tensoriais de estados em $\mathcal{S}$;
- são permitidas medições POVM entrelaçadas entre várias saídas do canal.

Antes de definir a capacidade, é necessário definir o esquema de (de)codificação:

Definição 2 *Um código erro-zero de bloco (K_n^∞, n) para um canal quântico $\mathcal{E}$ é composto de:*

1) *um conjunto de índices $\{1,\ldots,K_n^\infty\}$, em que cada índice está associado a uma mensagem clássica;*
2) *uma função de codificação*

$$X^n : \{1,\ldots,K_n^\infty\} \to \mathcal{S}^{\otimes n}, \quad (7)$$

que mapeia mensagens clássicas em palavras-código $\overline{\rho}_1 = X^n(1),\ldots,\overline{\rho}_{K_n^\infty} = X^n(K_n^\infty)$;
3) *uma função de decodificação*

$$g : \{1,\ldots,m\} \to \{1,\ldots,K_n^\infty\}, \quad (8)$$

que associa, de maneira determinística, a cada saída $y \in \{1,\ldots,m\}$ de uma medição POVM $\mathcal{P} = \{M_1,\ldots,M_m\}$ um índice $\{1,\ldots,K_n^\infty\}$ representando uma mensagem clássica. A função de decodificação possui a seguinte propriedade:

$$Pr\ (g(Y=y) \neq i | X^n = X^n(i)) = 0 \ \forall\ i \in \{1,\ldots,K_n^\infty\}. \quad (9)$$

A taxa do código da Def. 2 é ainda $R = \frac{1}{n}\log K_n^\infty$. A diferença fundamental entre tal código e o definido na

[1]No entanto, o uso de estados entrelaçados entre vários usos do canal é mostrado aumentar a capacidade HSW de canais quânticos com memória [16].

Seç. II é que aqui os elementos do POVM $\mathcal{P}$ são matrizes M_k num espaço de Hilbert de dimensão d^n. A definição da capacidade é essencialmente a mesma da Def. 1, exceto pelo uso do protocolo e do código acima descritos. Para evitar confusão, a capacidade erro-zero para o caso em que medições entrelaçadas são permitidas será denotada por $C_\infty^{(0)}(\mathcal{E})$. Visto que o protocolo de $C^{(0)}(\mathcal{E})$ emprega medições individuais, é de se esperar que

$$C_\infty^{(0)}(\mathcal{E}) \geq C^{(0)}(\mathcal{E}). \tag{10}$$

Antes de mostrar a desigualdade na Eq. (10), serão tecidas algumas considerações acerca da ortogonalidade/não-adjacência dos estados quânticos em $\mathcal{S}$. Na Seç. II, a adjacência entre estados quânticos em $\mathcal{S}$ foi definida com relação a um determinado POVM $\mathcal{P}$. Dois estados $\rho_i, \rho_j \in \mathcal{S}$ foram ditos ser não-adjacentes com relação a $\mathcal{P}$ se fosse possível distinguir perfeitamente entre $\mathcal{E}(\rho_i)$ e $\mathcal{E}(\rho_j)$ usando $\mathcal{P}$. Dos fundamentos da mecânica quântica [13], é sabido que dois estados quânticos são perfeitamente distinguíveis se, e somente se, eles pertencem a subespaços de Hilbert ortogonais. Isto implica dizer que é possível definir uma relação de adjacência entre estados em $\mathcal{S}$ independentemente da escolha do POVM $\mathcal{P}$: dois estados quânticos $\rho_i, \rho_j \in \mathcal{S}$ são ditos não-adjacentes se, e somente se, o subespaço de Hilbert gerado pelos autovetores no suporte de $\mathcal{E}(\rho_i)$ é ortogonal ao subespaço de Hilbert gerado pelos autovetores no suporte de $\mathcal{E}(\rho_j)$. Neste caso denota-se $\rho_i \pm_\mathcal{E} \rho_j$. A notação $\pm_\mathcal{E}$ é para lembrar que a ortogonalidade é com relação aos estados na saída do canal quântico $\mathcal{E}$. A mesma noção pode ser aplicada a um estado produto tensorial. Seja $\mathcal{S} = \{\rho_i, \ldots, \rho_l\}$ um subconjunto finito de estados quânticos de entrada para $\mathcal{E}$. Considere todas as seqüências de produtos tensoriais de comprimento n, $\mathcal{S}^{\otimes n}$. Duas seqüências $\hat{\rho}_i = \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}$ e $\hat{\rho}_j = \rho_{j_1} \otimes \cdots \otimes \rho_{j_n}$ são ditas ser não-adjacentes se, e somente se, os subespaços de Hilbert gerados pelos autovetores nos suportes de $\mathcal{E}(\hat{\rho}_i)$ e $\mathcal{E}(\hat{\rho}_j)$ são ortogonais. Novamente, denota-se $\hat{\rho}_i \pm_\mathcal{E} \hat{\rho}_j$.

Para um determinado canal quântico $\mathcal{E}$, escolha um subconjunto $\mathcal{S} = \{\rho_i, \ldots, \rho_l\}$ de estados quânticos e considere seqüências de comprimento n, $\mathcal{S}^{\otimes n}$. Fazendo uso de tais seqüências, é fácil verificar que o número máximo de mensagens clássicas que se pode transmitir sem erro através de $\mathcal{E}$ é igual ao número máximo de seqüências $\overline{\rho}_i \in \mathcal{S}^{\otimes n}$ que são duas-a-duas não-adjacentes. Supondo que existem K_n^∞ dessas seqüências, a capacidade erro-zero do canal quântico é dada por

$$C_\infty^{(0)}(\mathcal{E}) = \sup_\mathcal{S} \sup_n \frac{1}{n} \log K_n^\infty. \tag{11}$$

Suponha que a capacidade seja alcançada para um determinado subconjunto $\mathcal{S}$ e um comprimento de código n. Isto implica na existência de um código de erro-zero quântico contendo K_n^∞ palavras-código

$$\overline{\rho}_1, \overline{\rho}_2, \ldots, \overline{\rho}_{K_n^\infty}; \overline{\rho}_i \pm_\mathcal{E} \overline{\rho}_j, i \neq j.$$

Em outras palavras, os subespaços de Hilbert gerados pelos autovetores no suporte de cada

$$\begin{aligned}
\mathcal{E}(\overline{\rho}_1) &= \underbrace{\mathcal{E}(\rho_{1_1}) \otimes \mathcal{E}(\rho_{1_2}) \otimes \cdots \otimes \mathcal{E}(\rho_{1_n})}_{P_1} \\
\mathcal{E}(\overline{\rho}_2) &= \underbrace{\mathcal{E}(\rho_{2_1}) \otimes \mathcal{E}(\rho_{2_2}) \otimes \cdots \otimes \mathcal{E}(\rho_{2_n})}_{P_2} \\
&\vdots \\
\mathcal{E}(\overline{\rho}_{K_n^\infty}) &= \underbrace{\mathcal{E}(\rho_{K_{n_1}^\infty}) \otimes \mathcal{E}(\rho_{K_{n_2}^\infty}) \otimes \cdots \otimes \mathcal{E}(\rho_{K_{n_n}^\infty})}_{P_{K_n^\infty}}
\end{aligned} \tag{12}$$

são mutuamente ortogonais, em que P_i denota o projetor sobre o subespaço de Hilbert gerado pelos autovetores no suporte de $\mathcal{E}(\overline{\rho}_i)$. É fácil verificar que estes estados são completamente distinguíveis na saída do canal. Ainda, uma medição de von Neumann permitindo a distinção é dada por

$$\mathbb{P} = \{P_1, \ldots, P_{K_n^\infty}, P_{K_n^\infty+1}\}, \tag{13}$$

em que $P_{K_n^\infty+1} = \mathbb{1} - \sum_{i=1}^{K_n^\infty} P_i$.

A diferença na definição das capacidades $C_\infty^{(0)}(\mathcal{E})$ e $C^{(0)}(\mathcal{E})$ aparece de forma clara quando o conjunto de Eqs. (12) é observado. Claramente vê-se que as medições que permitem alcançar a capacidade devem ser definidas num espaço de Hilbert de dimensão d^n. No caso do protocolo de $C^{(0)}(\mathcal{E})$ descrito na Seç. II, as medições simultâneas em n estados de saída estão limitadas a

$$\mathbb{P}' = \mathcal{P}^{\otimes n}, \tag{14}$$

em que $\mathcal{P}$ é um POVM cujos operadores pertencem a um espaço de Hilbert de dimensão d.

O resultado a seguir permite verificar a desigualdade na Eq. (10).

Proposição 1 *Seja $\mathcal{S}$ um subconjunto de estados quânticos de entrada para $\mathcal{E}$ e $\hat{\rho}_i, \hat{\rho}_j \in \mathcal{S}^{\otimes n}$. Então $\hat{\rho}_i \pm_\mathcal{E} \hat{\rho}_j$ se, e somente se, existir pelo menos um $1 \leq k \leq n$ tal que $\rho_{i_k} \pm_\mathcal{E} \rho_{j_k}$.*

Demonstração: A não-adjacência $\hat{\rho}_i \pm_\mathcal{E} \hat{\rho}_j$ implica que

$$\begin{aligned}
\text{tr}\left[\mathcal{E}(\hat{\rho}_i)\mathcal{E}(\hat{\rho}_j)\right] &= \text{tr}\left[\left(\bigotimes_{k=1}^n \mathcal{E}(\rho_{i_k})\right)\left(\bigotimes_{k=1}^n \mathcal{E}(\rho_{j_k})\right)\right] \\
&= \prod_{k=1}^n \text{tr}\left[\mathcal{E}(\rho_{i_k})\mathcal{E}(\rho_{j_k})\right] \\
&= 0
\end{aligned} \tag{15}$$

se, e somente se, $\rho_{i_k} \pm_\mathcal{E} \rho_{j_k}$ para ao menos um $1 \leq k \leq n$. A prova do inverso é trivial. ■

O resultado da Prop. 1 é ilustrado na Fig. 2. Essencialmente, a proposição afirma que duas seqüências de n produtos tensoriais em $\mathcal{S}$ são não-adjacentes (e portanto completamente distinguíveis na saída do canal) se, e somente se, existir pelo menos uma posição k nas seqüências tal que os estados $\rho_{i_k}, \rho_{j_k} \in \mathcal{S}$ são distinguíveis. Em outras palavras, a distinguibilidade de quaisquer duas seqüências de n produtos tensoriais de $\mathcal{S}$ na saída do canal quântico depende somente das relações de não-adjacência dos estados quânticos em $\mathcal{S}$.

$$\begin{aligned}\mathcal{E}(\overline{\rho}_i) &= \mathcal{E}(\rho_{i_1})\otimes\cdots\otimes\mathcal{E}(\rho_{i_k})\otimes\cdots\otimes\mathcal{E}(\rho_{i_n})\\ \mathcal{E}(\overline{\rho}_j) &= \mathcal{E}(\rho_{j_1})\otimes\cdots\otimes\mathcal{E}(\rho_{j_k})\otimes\cdots\otimes\mathcal{E}(\rho_{j_n})\end{aligned}$$

Fig. 2. Duas seqüências de n produtos tensoriais de estados quânticos $\mathcal{S}$ que são não-adjacentes.

Para provar a desigualdade na Eq. (10) é necessário mostrar que $C_\infty^{(0)}(\mathcal{E})$ nem sempre pode ser alcançada usando medições individuais.

A distinguibilidade de estados quânticos é uma área bastante estudada em teoria da informação quântica. Uma de suas vertentes consiste na distinção de estados quânticos ortogonais e multi-particionados (*multipartite*), em que cada parte do sistema quântico está fisicamente separada [17], [18]. Neste caso, o problema consiste em decidir sobre a ortogonalidade dos estados produtos tensoriais através da realização de medições locais e comunicação clássica entre as partes. Este problema, por sua vez, pode ser abordado de duas formas: os estados multi-particionados são entrelaçados [18] ou são produtos tensoriais como os estados da Eq. (12) [17]. Bennett *et. al.* [19] mostraram a existência de um conjunto de estados quânticos ortogonais, produtos tensoriais de duas partículas de três estados, em que quaisquer dois estados do conjunto, embora globalmente ortogonais, *não* podem ser distinguidos usando pares de medições individuais, mesmo se os observadores são autorizados a realizar qualquer tipo de operação local e comunicação clássica.

Retornando ao problema de distinguir perfeitamente entre as seqüências da Eq. (12), se medições individuais forem consideradas, fica claro que o protocolo de medição empregado é um caso particular do protocolo do exemplo de Bennett *et. al.*, em que além da restrição de medições individuais impõe-se ainda o fato de que estados do produto tensorial devem ser medidos usando um mesmo POVM $\mathcal{P}$. Isto deve-se ao fato de que, embora quaisquer duas palavras-código na saída do canal, digamos $\mathcal{E}(\overline{\rho}_i)$ e $\mathcal{E}(\overline{\rho}_j)$, sejam ortogonais, os estados $\mathcal{E}(\rho_{i_{k'}})$ e $\mathcal{E}(\rho_{j_{k'}})$ não necessariamente os são, visto que a Prop. 1 obriga a ortogonalidade em pelo menos uma posição k mas não em todas.

Dessa forma, fica evidente que nem sempre é possível distinguir perfeitamente entre estados de um conjunto de seqüências de estados quânticos ortogonais usando medições individuais. Portanto, a capacidade erro-zero usando medições coletivas pode ser maior do que a capacidade erro-zero como definida na Ref. [5] e a Eq. (10) é assim verificada.

V. Capacidade erro-zero com estados quânticos não-ortogonais

Será discutido nesta seção um exemplo de um canal quântico cuja capacidade erro-zero quântica é calculada de maneira não trivial. O termo não trivial quer dizer que o supremo na Eq. (3) é alcançado para $n > 1$ e que subconjuntos $\mathcal{S}$ que alcançam o supremo contenham estados quânticos não ortogonais entre si. O canal quântico do exemplo a seguir não possui interpretação física, embora ele corresponda a algum processo físico. Além da não trivialidade no cálculo da capacidade, este canal dá origem ao pentágono como grafo característico para o subconjunto $\mathcal{S}$ que atinge a capacidade.

Seja $\mathcal{E}$ o canal quântico cujos operadores de Kraus $\{E_1, E_2, E_3\}$ são dados por

$$E_1 = \begin{bmatrix} 0.5 & 0 & 0 & 0 & \frac{\sqrt{49902}}{620} \\ 0.5 & -0.5 & 0 & 0 & 0 \\ 0 & 0.5 & -0.5 & 0 & 0 \\ 0 & 0 & 0.5 & -\frac{\sqrt{457}}{50} & \frac{\sqrt{457}}{50} \\ 0 & 0 & 0 & -0.62 & -\frac{289}{1550} \end{bmatrix},$$

$$E_2 = \begin{bmatrix} 0.5 & 0 & 0 & 0 & -\frac{\sqrt{49902}}{620} \\ 0.5 & 0.5 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & \frac{\sqrt{457}}{50} & -\frac{\sqrt{457}}{50} \\ 0 & 0 & 0 & 0.5 & 0.5 \end{bmatrix}, \qquad E_3 = 0.3|4\rangle\langle 4|,$$

em que a base computacional para o espaço de Hilbert de dimensão 5 é denotada por $\beta = \{|0\rangle, \ldots, |4\rangle\}$. É fácil verificar que $\sum_{a=1}^{3} E_a^\dagger E_a = \mathbb{1}$, significando que $\mathcal{E} \equiv \{E_a\}$ é um operador linear, positivo e que preserva o traço, de forma a representar um determinado processo físico.

O canal $\mathcal{E}$ foi obtido usando a ferramenta MATLAB, onde foi a imposta a restrição de que $\mathcal{E}$ deveria possuir *no máximo* dois estados mutuamente não-adjacentes.

Neste caso, a capacidade erro-zero do canal é alcançada pelo subconjunto

$$\mathcal{S} = \left\{ |v_1\rangle = |0\rangle, |v_2\rangle = |1\rangle, |v_3\rangle = |2\rangle, |v_4\rangle = |3\rangle, |v_5\rangle = \frac{|3\rangle + |4\rangle}{\sqrt{2}} \right\}. \tag{16}$$

O conjunto $\mathcal{S}$ alcança o supremo na Eq. (5) pelo seguinte motivo. Dentre os grafos característicos com até 5 vértices e tendo número de clique menor ou igual a dois, o grafo que fornece a maior capacidade é o pentágono [6]. É fácil verificar que o conjunto $\mathcal{S}$ dá origem ao pentágono como grafo de adjacência. Para isso, basta explicitar as relações de não-adjacência entre os estados de $\mathcal{S}$:

$$|v_1\rangle \pm_{\mathcal{E}} |v_3\rangle \qquad |v_1\rangle \pm_{\mathcal{E}} |v_4\rangle \qquad |v_2\rangle \pm_{\mathcal{E}} |v_4\rangle$$

$$|v_2\rangle \pm_{\mathcal{E}} |v_5\rangle \qquad |v_3\rangle \pm_{\mathcal{E}} |v_5\rangle.$$

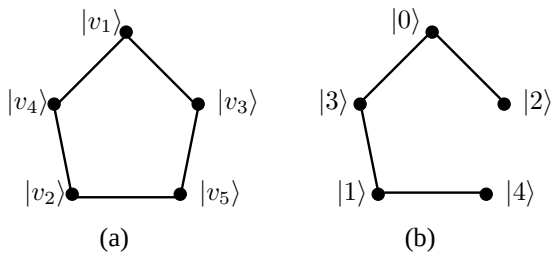

Fig. 3. (a) Grafo característico $\mathcal{G}$ para o subconjunto $\mathcal{S}$ que alcança a capacidade erro-zero. (b) Grafo característico para o caso em que o estado $|v_5\rangle \in \mathcal{S}$ é substituído pelo estado $|4\rangle$.

O grafo característico é mostrado na Fig. 3(a). Note que no caso em que as palavras-código são de comprimento um só é possível transmitir no máximo duas mensagens clássicas sem erro através do canal quântico, por exemplo, escolhendo $|v_1\rangle$ e $|v_3\rangle$ ou $|v_2\rangle$ e $|v_4\rangle$. Entretanto, seguindo a construção

inicialmente feita por Shannon [6], é possível construir um código contendo cinco palavras-código não adjacentes:

$$\overline{\rho}_1 = |v_1\rangle|v_1\rangle, \quad \overline{\rho}_2 = |v_2\rangle|v_3\rangle, \quad \overline{\rho}_3 = |v_3\rangle|v_5\rangle$$
$$\overline{\rho}_4 = |v_4\rangle|v_2\rangle, \qquad \overline{\rho}_5 = |v_5\rangle|v_4\rangle. \tag{17}$$

A capacidade do pentágono foi determinada por Lovász [20], e é alcançada quando o canal é usado duas ou mais vezes. Logo, a capacidade erro-zero do canal quântico $\mathcal{E}$ é dada por:

$$C_\infty^{(0)}(\text{pentagon}) = \frac{1}{2}\log 5 \approx 1,16 \text{ bits por uso.}$$

Portanto, $C_\infty^{(0)}(\text{pentagon})$ é a máxima taxa em que informação clássica pode ser transmitida através do canal $\mathcal{E}$ com uma probabilidade de erro igual a zero.

É interessante notar que se ao invés de $\mathcal{S}$ fosse escolhida a base computacional acima, então uma adjacência entre os $|2\rangle$ e $|4\rangle$ é verificada, de forma que o grafo característico para β é mostrado na Figura 3(b). Claramente este grafo possui capacidade igual a um e portanto inferior à capacidade do pentágono.

VI. Conclusões

Na forma em que foi inicialmente definida, a capacidade erro-zero de canais quânticos previa o uso de medições individuais na saída do canal quântico. Neste artigo foi verificado o comportamento do valor da capacidade para o caso em que medições entrelaçadas entre várias saídas do canal são permitidas. Foi mostrado que tais medições podem aumentar a capacidade erro-zero dos canais quânticos. A razão para tal reside no fato de que todas as palavras-código de um código de bloco de erro-zero devem ser completamente distinguíveis na saída do canal, e esta distinguibilidade depende somente da distinguibilidade dos estados quânticos do alfabeto do código, como demonstrado na Prop. 1. Entretanto, Bennett *et. al.* mostraram que nem sempre é possível distinguir estados produtos tensoriais de um conjunto de estados quânticos ortogonais usando medições individuais. Foi observado também que não é necessária uma maximização sobre as medições para o cálculo da capacidade com medições coletivas.

Finalmente, foi mostrado um exemplo de um canal quântico cuja capacidade é não trivialmente calculada, ou seja, a capacidade é alcançada por um conjunto de estados quânticos não ortogonais e o canal requer duas ou mais utilizações para que a capacidade $C_\infty^{(0)}(\mathcal{E})$ seja atingida.

Agradecimentos

Os autores gostariam de agradecer o Programa Alβan, Programa de bolsas de alto nível da União Europeia para América Latina, bolsa nº E05D051893BR, bem como o CNPq (CT-INFO Quanta, contrato # 552254/02-9), pelo apoio financeiro. Este trabalho foi fincanciado em parte pelo projeto Europeu SECOQC (contrato # IST-2003-506813).

Referências

[1] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56(1):131–138, 1997.

[2] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Info. Theory*, 44(1):269–273, 1998.

[3] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. *Phys. Rev. Lett.*, 83:3081–3084, 1999.

[4] P. W. Shor. The adaptive classical capacity of a quantum channel, or information capacities of three symmetric pure states in three dimensions. *IBM. J. Res. & Dev.*, 48(1):115–137, 2004.

[5] R. A. C. Medeiros and F. M. de Assis. Quantum zero-error capacity. *Int. J. Quant. Inf.*, 3(1):135–139, 2005.

[6] C. E. Shannon. The zero error capaciy of a noisy channel. *IRE Trans. Inform. Theory*, IT-2(3):8–19, 1956.

[7] J. Köner and A. Orlitsky. Zero-error information theory. *IEEE Trans. Info. Theory*, 44(6):2207–2229, 1998.

[8] R. A. C. Medeiros and F. M. de Assis. Capacidade erro-zero de canais quânticos e estados puros. In *Anais do XXII Simpósio Brasileiro de Telecomunicações*, XXII Simpósio Brasileiro de Telecomunicações - SBrT'05, Campinas-PB, Brazil, 2005.

[9] R. A. C. Medeiros, R. Alléaume, F. M. de Assis, and G. Cohen. Quantum state characterization for the zero-error capacity. In *Proceeding of the IEEE Information Theory Winter School 2007*, page 19, France, 2007.

[10] R. A. C. Medeiros and F. M. de Assis. Quantum zero-error capacity and HSW capacity. In *Proceedings of the The Seventh International Conference on Quantum Communication, Measurement and Computing QCMC'04*, volume 734 of *AIP Conference Proceedings*, pages 52–54. American Institute of Physics, 2004.

[11] R. A. C. Medeiros, R. Alléaume, G. Cohen, and F. M. de Assis. Zero-error capacity of quantum channel and noiseless subsystems. In *IEEE International Telecommunications Symposium ITS2006*, Brazil, 2006.

[12] R. A. C. Medeiros, R. Alléaume, G. Cohen, and F. M. de Assis. quant-ph/0611042.

[13] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[14] R. A. C. Medeiros and F. M. de Assis. Zero-error capacity of a quantum channel. In *Proceedings of the 11th International Conference on Telecommunications*, volume 3124 of *Lecture Notes in Computer Science*, pages 100–105, Heidelberg, 2004. Springer-Verlag Heidelberg.

[15] B. Bollobás. *Modern graph theory*. Springer-Verlag New York, Inc., New York, 1998.

[16] C Macchiavello and G. M. Palma. Entanglement-enhanced information transmission over a quantum channel with correlated noise. *Phys. Rev. A*, 65(5):050301, Apr 2002.

[17] W. K. Wootters. Distinguishing unentangled states with an unentangled measurement. *quant-ph/0506149*, 2005.

[18] J. Walgate, A. J. Short, L. Hardy, and V. Vedral. Local distinguishability of multipartite orthogonal quantum states. *quant-ph/0007098*, 2000.

[19] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A*, 59(2):1070–1091, Feb 1999.

[20] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Info. Theory*, 25(1):1–7, 1979.