Capacidade erro-zero de canais clássicos-quânticos

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

***Resumo*— A capacidade erro-zero de canais quânticos é definida como sendo o supremo das taxas com que informação clássica é transmitida *sem erro* através de um canal quântico ruidoso. Neste trabalho, é feito um estudo da capacidade erro-zero de uma classe importante de canais: os canais clássicos-quânticos. Mais especificamente, é mostrado que o cálculo da capacidade erro-zero de tais canais é um problema puramente clássico, equivalente ao cálculo da capacidade erro-zero de um canal clássico discreto sem memória específico.**

***Palavras-Chave*— Capacidade erro-zero, canais quânticos, canais clássicos-quânticos.**

***Abstract*— The zero-error capacity of quantum channels has been defined as the supremum of the rates at which classical information can be transmitted through a noisy quantum channel with a zero probability of error. In this work, we study the quantum zero-error capacity of an important class of quantum channels, the so-called classical-quantum channels. More specifically, it is shown that the problem of finding the quantum zero-error capacity of such channels is purely classical, in the sense that it is equivalent to the problem of finding the zero-error capacity of a given classical discrete memoryless channel.**

***Keywords*— Zero-error capacity, quantum channels, classical-quantum channels**

I. INTRODUÇÃO

Um dos principais objetos de estudo da teoria da informação clássica [1] e da teoria da informação quântica [2] é o cálculo da capacidade de canais. A capacidade de canais clássicos é um número que indica a taxa assintótica com que a informação pode ser transmitida confiavelmente através do canal. Por sua vez, os canais quânticos possuem diversas capacidades dependendo do tipo de informação a ser transmitida (clássica ou quântica), dos recursos físicos empregados e do protocolo de comunicação. Para a transmissão de informação clássica, estão definidas na literatura:

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 [3], [4];
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 [5];
3) a capacidade adaptativa de Shor [6], em que o sistema de medição dos estados quânticos na saída do canal pode variar segundo o resultado de medições passadas.

Todas estas capacidades prevêem uma probabilidade de erro assintoticamente baixa (porém maior do que zero) para códigos cujas taxas se aproximam da capacidade do canal, mesmo para o melhor esquema de codificação.

Recentemente, Medeiros e Assis definiram a capacidade erro-zero de canais quânticos [7], que é a taxa máxima em que informação clássica pode ser transmitida através de um canal quântico com uma probabilidade de erro igual a zero. A capacidade erro-zero quântica (CEZQ) é uma generalização da capacidade erro-zero de canais discretos sem memória, definida por Shannon em 1956 [8].

Desde a sua definição, a CEZQ vem despertando um interesse crescente junto à comunidade científica. Recentemente, Beigi e Shor [9] estudaram a complexidade algorítmica do cálculo da capacidade erro-zero de canais quânticos, mostrando que a mesma pertence a classe de problemas QMA-completo. Num outro trabalho, Duan e Shi [10] estudaram a CEZQ para o caso em que n transmissores desejam se comunicar com m receptores. Os autores mostraram uma característica inédita da capacidade erro-zero de canais quânticos que não se verifica no caso clássico. Para $n = m = 2$, foi mostrado um canal quântico em que era possível transmitir informação *sem erro* a uma taxa não nula desde que fossem feitos dois ou mais usos do canal, enquanto que com apenas um uso do canal nenhuma informação poderia ser transmitida.

Neste artigo será estudada a CEZQ de uma classe importante de canais quânticos, os canais clássicos-quânticos, que por sua vez é um caso particular dos canais de quebra de emaranhamento [11]. Será mostrado que o problema de encontrar a CEZQ de tais canais é puramente clássico, e equivalente a calcular a capacidade erro-zero de um determinado canal clássico discreto sem memória. O artigo está organizado como segue. Na Sec. II é feita uma revisão dos principais conceitos relacionados à CEZQ. Os canais clássicos-quânticos, bem como algumas de suas propriedades, são considerados na Sec. III. A contribuição deste artigo está na Sec. IV, onde a CEZQ de canais clássicos-quânticos é estudada. Por fim, as conclusões são apresentadas na Sec. V.

II. CAPACIDADE ERRO-ZERO DE CANAIS QUÂNTICOS

Para facilitar a leitura deste trabalho, será feito nesta seção um resumo das principais definições e resultados sobre a capacidade erro-zero de canais quânticos, os quais são importantes à compreensão deste trabalho [7], [12].

Seja $\mathcal{E}$ um canal quântico definido num espaço de Hilbert $\mathcal{H}$ de dimensão d. Tal canal quântico pode ser modelado por um

[†] Département Informatique et Réseaux, TELECOM ParisTech, Paris, France

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

Emails: rex@ee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br, alleaume@telecom-paristech.fr, randriam@telecom-paristech.fr e cohen@telecom-paristech.fr

mapeamento linear, completamente positivo e que preserva o traço dos operadores de densidade, $\mathcal{E} \equiv \{E_a\}$, 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

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

O canal $\mathcal{E}$ é sem memória quando não produz entrelaçamento entre várias saídas do canal, mesmo para entradas entrelaçadas entre vários usos. Assim, a saída do canal para uma entrada do tipo $\overline{\rho}_i = \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}$, em que são feitos n usos do canal, é dada por

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

O protocolo de comunicação associado à capacidade erro-zero é resumido como segue. Define-se um subconjunto finito $\mathcal{S}$ de estados quânticos no espaço de Hilbert $\mathcal{H}$ de dimensão d, $\mathcal{S} = \{\rho_i, \ldots, \rho_l\}$. Estes estados serão, na verdade, o alfabeto de um código quântico de erro zero. O conjunto das palavras-códigos de comprimento n é um subconjunto das seqüências de n produtos tensoriais de estados de $\mathcal{S}$, denotado por $\mathcal{S}^{\otimes n}$, ou seja, a i-ésima palavra-código é dada por $\overline{\rho}_i = \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}$, em que $\rho_{i_j} \in \mathcal{S}$. Na saída do canal, Bob pode efetuar medições *coletivas* (entrelaçadas). Isto significa que Bob espera a chegada dos n estados correspondentes à palavra-código atualmente transmitida e efetua uma medição nos n estados usando para isto um POVM (*Positive Operator-Valued Measurement*) $\{M_m\}$, em que cada operador de medição M_i é um operador no espaço de Hilbert de dimensão d^n. Em resumo, o protocolo de comunicação empregado aqui é semelhante ao protocolo de Holevo-Schumacher-Westmoreland [3], [4], em que palavras-códigos entrelaçadas entre diversos usos do canal não são permitidas.

Antes de definir a capacidade erro-zero de canais quânticos, é conveniente a definição de um código. Um código de blocos de erro zero quântico (K_n, n) de comprimento n e alfabeto $\mathcal{S}$ é definido como sendo composto de:

1) um conjunto de índices $\{1, \ldots, K_n\}$, em que cada índice está associado a uma mensagem clássica;
2) uma função de codificação $X^n : \{1, \ldots, K_n\} \to \mathcal{S}^{\otimes n}$, que associa a cada uma das K_n mensagens clássicas uma palavra código de n produtos tensoriais de estados de $\mathcal{S}$;
3) uma função de decodificação $g : \{1, \ldots, m\} \to \{1, \ldots, K_n\}$, que associa deterministicamente e univocamente cada saída $y \in \{1, \ldots, m\}$ de uma medição POVM $\{M_1, \ldots, M_m\}$ a uma mensagem clássica, com a seguinte propriedade:

$$\Pr\left(g(Y = y) \neq i | X^n = X^n(i)\right) = 0 \; \forall \; i \in \{1, \ldots, K_n\}. \quad (3)$$

É fácil verificar que a taxa de um código (K_n, n) é dada por

$$R = \frac{1}{n} \log K_n \text{ bits/uso}. \quad (4)$$

Desta forma:

Definição 1: Seja $\mathcal{E}(\cdot)$ um canal quântico num espaço de Hilbert de dimensão d. A capacidade erro-zero quântica (CEZQ) de $\mathcal{E}$, denotada por $C^{(0)}(\mathcal{E})$, é o supremo das taxas alcançáveis com probabilidade de erro igual a zero, isto é,

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_{n} \frac{1}{n} \log K_n, \quad (5)$$

em que K_n é o número máximo de mensagens clássicas que o sistema pode transmitir sem erro, quando um código de bloco de erro-zero (K_n, n) com alfabeto $\mathcal{S}$ é usado.

Uma propriedade fundamental de estados quânticos é a distinguibilidade. Dois estados quânticos são distinguíveis se, e somente se, os espaços de Hilbert definidos pelos suportes dos respectivos estados são ortogonais. Dois estados quânticos $\rho_1, \rho_2 \in \mathcal{S}$ são ditos *não-adjacentes* se $\mathcal{E}(\rho_1)$ e $\mathcal{E}(\rho_2)$ são distinguíveis. Neste caso, denota-se $\rho_1 \perp_{\mathcal{E}} \rho_2$. Se não for possível distinguir $\mathcal{E}(\rho_1)$ de $\mathcal{E}(\rho_2)$, então ρ_1 e ρ_2 são ditos ser *adjacentes*. Para um canal quântico dado, a CEZQ é maior que zero se, e somente se, existir pelo menos dois estados não-adjacentes. Um resultado importante que concerne os estados em $\mathcal{S}$ é que o supremo na Eq. (1) pode sempre ser alcançado usando um conjunto $\mathcal{S}$ composto somente de estados puros.

Dado um conjunto de estados $\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_l\rangle\}$ para um canal quântico $\mathcal{E}$, as relações de adjacência entre os estados de $\mathcal{S}$ permitem construir um grafo característico $\mathcal{G}$ como segue:

$$V(\mathcal{G}) = \{1, \ldots, l\} \quad (6)$$

$$E(\mathcal{G}) = \{(i, j); |\psi_i\rangle \perp_{\mathcal{E}} |\psi_j\rangle; i \neq j; i, j \in \mathcal{S}\}. \quad (7)$$

Isto é, dois vértices estão conectados em $\mathcal{G}$ se os estados quânticos correspondentes em $\mathcal{S}$ são não-adjacentes. É fácil verificar que o número máximo de mensagens que pode ser transmitidas sem erro usando uma transmissão é dado pelo número de clique de $\mathcal{G}$, $K_1 = \omega(\mathcal{G})$, isto é, a cardinalidade do maior sub-grafo completo de $\mathcal{G}$. De maneira em geral, se produtos tensoriais de n estados de $\mathcal{S}$ são considerados, a CEZQ pode ser escrita da seguinte forma:

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_{n} \frac{1}{n} \log \omega(\mathcal{G}^n), \quad (8)$$

em que $\mathcal{G}^n$ é o grafo n-ésimo produto de Shannon de $\mathcal{G}$, definido por:

$$V(\mathcal{G}^n) = \{1, \ldots, l\}^n \quad (9)$$

$$E(\mathcal{G}^n) = \{(i_1 \ldots i_n, j_1 \ldots j_n); |\psi_{i_k}\rangle \perp_{\mathcal{E}} |\psi_{j_k}\rangle \text{ para ao menos um } 1 \leq k \leq n; |\psi_{i_k}\rangle, |\psi_{j_k}\rangle \in \mathcal{S}\}. \quad (10)$$

III. Canais clássicos-quânticos

Em teoria da informação quântica, um canal quântico $\mathcal{E}$ para o qual estado $(\mathbb{1} \otimes \mathcal{E})(\Gamma)$ é sempre separável (mesmo para um Γ entrelaçado) é chamado de canal de quebra de entrelaçamento (*entanglement breaking channels*). Horodecki *et. al* [14] mostraram que canais de quebra de entrelaçamento podem ser escritos como:

$$\mathcal{E}(\rho) = \sum_i \sigma_i \text{tr}\left[\rho X_i\right], \quad (11)$$

em que $\{\sigma_i\}$ é uma família fixa de estados quânticos e $\{X_i\}$ define uma medição POVM. O canal $\mathcal{E}$ é chamado de *clássico-quântico* (c-q) se $X_i = |\psi_i\rangle\langle\psi_i|$, em que $\{|\psi_i\rangle\}$ é uma base

ortonormal, i.e., os operadores do POVM são projetores de dimensão um. Por outro lado, se $\sigma_i = |\psi_i\rangle\langle\psi_i|$ então o canal é chamado de *quântico-clássico* (q-c).

Canais clássicos-quânticos possuem a propriedade que superposições na entrada do canal nunca são destruídas na saída. Para visualizar isto, considere o canal c-q definido pela família $\{\sigma_i\}$ e pelo POVM com operadores $X_i = |\psi_i\rangle\langle\psi_i|$. Suponha que o estado em superposição $|v\rangle = \sum_i v_i|\psi_i\rangle$ é enviado através do canal. O operador de densidade na entrada do canal é dado por $\rho_v = \sum_{ij} v_i v_j^*|\psi_i\rangle\langle\psi_j|$. O estado se saída será:

$$\begin{aligned}\mathcal{E}(\rho_v) &= \sum_i \sigma_i \text{tr}\,[\rho_v|\psi_i\rangle\langle\psi_i|] \\ &= \sum_i \langle\psi_i|\rho_v|\psi_i\rangle\sigma_i \\ &= \sum_i\sum_{jk}\langle\psi_i|v_j v_k^*|\psi_j\rangle\langle\psi_k||\psi_i\rangle\sigma_i \\ &= \sum_i ||v_i||^2\sigma_i. \end{aligned} \quad (12)$$

Outra propriedade interessante do canal c-q, é que a saída do mesmo dado que a entrada é um dos estados $|\psi_i\rangle$ é:

$$\begin{aligned}\mathcal{E}(|\psi_i\rangle) &= \sum_i \sigma_i \text{tr}\,[|\psi_i\rangle\langle\psi_i||\psi_i\rangle\langle\psi_i|] \\ &= \sigma_i, \end{aligned} \quad (13)$$

sendo portanto igual ao σ_i correspondente no modelo do canal.

IV. Capacidade erro-zero de canais clássicos-quânticos

Nesta seção, será estudada a capacidade erro-zero de canais clássicos quânticos. Antes de enunciar o resultado principal deste trabalho, é importante lembrar que, no contexto de erro-zero quântico, o supremo na Eq. (8) pode ser sempre alcançado usando um conjunto $\mathcal{S}$ de estados quânticos puros. O principal resultado deste trabalho é:

Proposição 1: Seja $\mathcal{E}_{cq}$ um canal clássico-quântico num espaço de Hilbert de dimensão d, definido pela família $\{\sigma_i\}$ e pelo POVM $\{X_i = |\psi_i\rangle\langle\psi_i|\}_{i=1}^d$, em que $\{|\psi_i\rangle\}$ é uma base ortonormal para o espaço. Então, a capacidade erro-zero do canal c-q pode ser sempre alcançada pelo conjunto

$$\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}. \quad (14)$$

A conseqüência principal da Proposição 1 é que o problema de encontrar a capacidade erro-zero quântica de um canal c-q é, na verdade, um problema clássico. Este problema se resume a encontrar as relações de adjacência entre os estados do conjunto $\{|\psi_i\rangle\}$ para o qual o canal c-q é definido, montar em seguida o grafo característico $\mathcal{G}$ associado, e por fim calcular a capacidade de Shannon [15] de tal grafo, que é dada por $C_0 = \sup_n \frac{1}{n}\log\omega(\mathcal{G}^n)$, em que o produto $\mathcal{G}^n$ é tal como definido anteriormente.

A idéia usada para provar tal resultado é de mostrar, num primeiro momento, que a maior *taxa de transmissão* sem erro usando um código quântico de erro-zero de alfabeto $\mathcal{S}_k = \{|v_1\rangle \ldots, |v_k\rangle\}$, $k \leq d$, é alcançada usando o conjunto $\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$. Por fim, é mostrado que não é possível ir além desta taxa pelo uso (inclusão) de mais estados no conjunto $\mathcal{S}$. Antes de provar o primeiro fato, é conveniente redefinir a CEZQ em termos da taxa de transmissão de informação.

Dado um conjunto arbitrário $\mathcal{S}$ de estados de entrada (alfabeto do código) para um canal quântico $\mathcal{E}$, é possível construir um grafo característico $\mathcal{G}$. A *taxa máxima de transmissão de informação sem erro* $R_\mathcal{S}$ usando um código de erro-zero com alfabeto $\mathcal{S}$ é dada por:

$$R_\mathcal{S} = \sup_n \frac{1}{n}\log\omega(\mathcal{G}^n). \quad (15)$$

De forma direta, a capacidade erro-zero quântica de $\mathcal{E}$ é dada por:

$$C_0(\mathcal{E}) = \sup_\mathcal{S} R_\mathcal{S}. \quad (16)$$

A primeira parte da demonstração da Proposição 1 refere-se a prova da seguinte proposição.

Proposição 2: Para um canal c-q de dimensão d, definido por $\{\sigma_i\}$ e $\{X_i = |\psi_i\rangle\langle\psi_i|\}_{i=1}^d$,

$$\sup_{\mathcal{S};|\mathcal{S}|\leq d} R_\mathcal{S} \quad (17)$$

pode sempre ser alcançado pelo conjunto

$$\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}. \quad (18)$$

É importante lembrar, que se um dado estado $|\psi_i\rangle \in \mathcal{S}$, então $\mathcal{E}_{cq}(|\psi_i\rangle) = \sigma_i$, enquanto que se $|v\rangle$ é uma combinação linear de $\{|\psi_i\rangle\}$, então a saída é dada pela Eq. (12). Lembre-se também que dois vértices u e v estão conectados no grafo característico se, e somente se, tr $[\mathcal{E}(|u\rangle)\mathcal{E}(|v\rangle)] = 0$, i.e., os estados quânticos correspondentes na saída do canal possuem suportes ortogonais.

Demonstração: (da Proposição 2). O resultado é obtido por construção. Seja k o número máximo de estados dois a dois ortogonais no conjunto $\{\sigma_i\}$, e.g., $\{\sigma_1, \ldots, \sigma_k\}$, $k \leq d$. Devido à Eq. (13), a taxa máxima R_{S_k} para qualquer código com $|\mathcal{S}| \leq k$ é alcançada pelo conjunto $\mathcal{S}_k = \{|\psi_1\rangle, \ldots, |\psi_k\rangle\}$, visto que o grafo característico $\mathcal{G}_k$ correspondente a $\mathcal{S}_k$ é um grafo completo. Se $k < d$, é conveniente adicionar estados puros $|v\rangle$ a $\mathcal{S}_k$ até se ter $k = d$. O fato de adicionar um estado a $\mathcal{S}_k$ implica em adicionar um vértice a $\mathcal{G}_k$. As arestas que serão adicionadas dependem das relações de adjacência entre o novo estado $|v\rangle$ e os estados em $\mathcal{S}_k$. Desta forma, o estado a ser adicionado a $\mathcal{S}_k$ deve ser tal que uma quantidade máxima de vértices seja adicionada ao conjunto $E(\mathcal{G}_k)$, ou seja, o grafo G_{k+1} deve ter o máximo número de vértices conectados. Em outras palavras, $\mathcal{E}(|v\rangle)$ deve ter seu suporte ortogonal com o máximo número possível de $\sup\ \sigma_i$, $i \leq k$. Suponha que $|v\rangle$ é uma combinação linear de $\{|\psi_i\rangle\}$. Então, $\mathcal{E}(|v\rangle) = \sum_i p_i\sigma_i$. Se $p_i > 0 \forall i$, então $|v\rangle$ é adjacente a todos os estados em $\mathcal{S}_k$. Devido ao fato de que interferências causadas por superposições de estados $\{|\psi_i\rangle\}$ nunca são destruídas na saída do canal, o estado a ser adicionado, $|v\rangle$, deve ser um dos estados remanescentes $|\psi_m\rangle$, $m > k$, pertencente a $\mathcal{S}\backslash\mathcal{S}_k$, tal que o conjunto $\{j; |\psi_m\rangle\perp_\mathcal{E}|\psi_j\rangle; 1 \leq j \leq k\}$ tenha cardinalidade máxima, já que $E(G_{k+1}) = E(G_k) \cup \{(i,j); |\psi_i\rangle\perp_\mathcal{E}|\psi_j\rangle; 1 \leq j \leq k\}$.

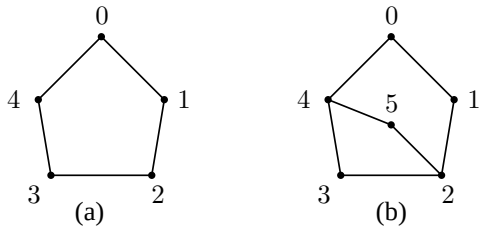

Fig. 1. (a) Um grafo G. (b) O grafo 3-clonado G'

O novo conjunto será $\mathcal{S}_{k+1} = \{|\psi_1\rangle, \ldots, |\psi_{k+1}\rangle\}$, em que o estado adicionado $|\psi_m\rangle$ possui índice $k+1$ em $\mathcal{S}_{k+1}$. Claramente, $R_{\mathcal{S}_{k+1}} \geq R_{\mathcal{S}_k}$. Repetindo este processo, obtem-se $\mathcal{S}_d = \mathcal{S}$. ∎

Antes da demonstração da Proposição 1 ser apresentada, faz-se necessário enunciar um resultado bastante interessante tanto para a teoria de erro-zero clássica quanto para a quântica.

Seja $G = (V, E)$ um grafo não direcionado tal que $V = \{1, \ldots, d\}$ e $E \subseteq \{(i,j); i,j \in V; i \neq j\}$. Para cada vértice $i \in V(G)$, denote por $N(i)$ o conjunto de vértices aos quais i está conectado:

$$N(i) = \{j \in V(G); (i,j) \in E(G)\}. \tag{19}$$

O conjunto $N(i)$ é conhecido como a *vizinhança* de i.

Seja $\omega(G^n)$ o número de clique de G^n , i.e., a cardinalidade do maior sub-grafo completo de G^n, em que G^n é o n-ésimo produto de Shannon do grafo G.

Definição 2 (Grafo k-clonado de G [16], [17]): O grafo k-clonado de G, denotado por G', é um grafo com $d+1$ vértices obtido de G através da *clonagem* do vértice k de G:

1) $V(G') = \{1, \ldots, d, d+1\}$, em que $d+1$ é o rótulo do vértice clonado.
2) $E(G') = E(G) \cup \{(d+1, j); j \in N(k)\}$, i.e, ambos os vértices $d+1$ e k possuem os mesmos vizinhos, $N(d+1) = N(k)$.

Como exemplo, seja G o grafo ilustrado na Fig. 1(a). Note que no grafo 3-clonado G' da Fig. 1(b), o vértice original 3 possui os mesmos vizinhos do vértice clonado 5.

Teorema 1 ([16], [17]): Para todo n, $\omega(G^n) = \omega(G'^n)$.

O teorema implica que a capacidade erro-zero (clássica ou quântica) associada com o grafo G' é igual a capacidade erro-zero do canal associado com G.

Corolário 1 ([16], [17]): Seja $V_k \subseteq N(k)$. Se o conjunto de arestas do gráfo k-clonado for tal que $E(G') = E(G) \cup \{(d+1, j); j \in V_k)\}$, então para todo n, $\omega(G^n) = \omega(G'^n)$.

O corolário afirma que no caso em que os vizinhos do vértice $d+1$ em G' formam um subconjunto dos vizinhos do vértice k em G, o resultado do Teorema 1 não se altera. Neste ponto, uma prova da Proposição 1 pode ser escrita:

Demonstração: (da Proposição 1). Devido ao resultado da Proposição 2, a demonstração se resume a mostrar que a adição de um estado ao conjunto $\mathcal{S}$ não aumenta $R_{\mathcal{S}}$.

Seja $\mathcal{G} = (V, E)$ o grafo característico associado a $\mathcal{S}$. Se i é o vértice associado com o estado $|\psi_i\rangle$, então

$$\begin{aligned} V(\mathcal{G}) &= \{1, \ldots, d\} && (20)\\ E(\mathcal{G}) &= \{(i,j); i,j \in V(\mathcal{G}); i \neq j; \text{tr}\,[\sigma_i \sigma_j] = 0\}. && (21) \end{aligned}$$

Denote por $|\psi_{d+1}\rangle$ o estado puro a ser adicionado a $\mathcal{S}$. Desde que $\{|\psi_i\rangle\}$ é uma base ortonormal para o espaço de Hilbert de dimensão d, pode-se considerar, sem perda de generalidade, que $|\psi_{d+1}\rangle$ é uma combinação linear dos primeiros k estados de $\mathcal{S}$: $|\psi_{d+1}\rangle = a_1|\psi_1\rangle + \cdots + a_k|\psi_k\rangle$. Então,

$$\mathcal{E}_{cq}(|\psi_{d+1}\rangle) = \sum_{i=1}^{k} ||a_i||^2 \sigma_i, \qquad a_i \neq 0. \tag{22}$$

As relações de adjacência entre o estado $|\psi_{d+1}\rangle$ e os estados de $\mathcal{S}$ podem ser obtidas como segue. Seja $|\psi_i\rangle \in \mathcal{S}$. Então,

$$\begin{aligned} \text{tr}\,[\mathcal{E}_{cq}(|\psi_{d+1}\rangle)\mathcal{E}_{cq}(|\psi_i\rangle)] &= \text{tr}\left[\left(\sum_{j=1}^{k} ||a_j||^2 \sigma_j\right)\sigma_i\right] \\ &= \sum_{j=1}^{k} ||a_j||^2 \text{tr}\,[\sigma_j \sigma_i]\,. \end{aligned} \tag{23}$$

É fácil ver que se $1 \leq i \leq k$, pelo menos um termo do lado direito da Eq. (23) é diferente de zero (o termo em que $j = i$). Então, $|\psi_{d+1}\rangle$ é adjacente a todo $|\psi_i\rangle$, $1 \leq i \leq k$. Uma análise mais detalhada mostra que

$$\begin{aligned} V(\mathcal{G}') &= \{1, \ldots, d+1\} && (24)\\ E(\mathcal{G}') &= E(\mathcal{G}) \cup \{(i, d+1); i \in V(\mathcal{G}); k < i \leq d; \\ &\qquad \text{tr}\,[\sigma_1 \sigma_i] = \cdots = \text{tr}\,[\sigma_k \sigma_i] = 0\}. && (25) \end{aligned}$$

A Eq. (25) possui uma interpretação interessante. Ela diz que o vértice adicionado $d+1$ está conectado ao vértice i se, e somente se, $|\psi_i\rangle$ é não-adjacente a todos os estados $|\psi_1\rangle, \ldots, |\psi_k\rangle$. Conseqüentemente, o novo vértice $d+1$ de $\mathcal{G}'$ pode ser visto como sendo o vértice clonado no sentido do Corolário 1, em que o vértice original no grafo $\mathcal{G}$ pode ser qualquer um dos vértices $1, \ldots, k$ de $\mathcal{G}$. Pelo Corolário 1, $\omega(\mathcal{G}'^n) = \omega(\mathcal{G}^n)$. ∎

Uma conseqüência imediata da Proposição 1 é que, calcular a CEZQ de um canal c-q definido por $\{\sigma_i\}$ e $\{X_i = |\psi_i\rangle\langle\psi_i|\}_{i=1}^{d}$ é equivalente a encontrar a capacidade erro-zero clássica [8] do canal clássico discreto sem memória (DSM) com alfabetos de entrada e saída $\mathcal{X} = \mathcal{Y} = \{1, \ldots, d\}$ e matriz de adjacência $A = [a_{ij}]$ [8], em que

$$a_{ij} = \begin{cases} 0, & \text{se tr}\,[\sigma_i \sigma_j] = 0 \\ 1, & \text{se tr}\,[\sigma_i \sigma_j] \neq 0. \end{cases} \tag{26}$$

De fato, o grafo característico de um canal DSM [15] é tal que os vértices são símbolos do alfabeto de entrada, e dois vértices i, j estão conectados se, e somente se, $a_{ij} = 0$. Note que o grafo característico do canal DSM acima é igual ao grafo característico associado ao conjunto $\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$, ou seja, ambos possuem a mesma capacidade de Shannon.

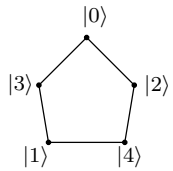

Fig. 2. Grafo característico correspondente ao conjunto $\mathcal{S}$ que alcança a capacidade erro-zero do canal c-q.

A. Um exemplo

Como exemplo, considere o canal clássico-quântico $\mathcal{E}_{cq}$ num espaço de Hilbert de dimensão 5, definido por:

$$|\sigma_i\rangle = \frac{|i\rangle + |i+1 \mod 5\rangle}{\sqrt{2}}, \sigma_i = |\sigma_i\rangle\langle\sigma_i| \qquad (27)$$

e

$$X_i = |i\rangle\langle i|, \quad 0 \leq i \leq 4, \qquad (28)$$

em que $\{|0\rangle, \ldots, |4\rangle\}$ é a base computacional do espaço de Hilbert de dimensão 5.

Pela Proposição 1, o conjunto $\mathcal{S}$ que alcança o supremo na Eq. (8) é dado por:

$$\mathcal{S} = \{|0\rangle, \ldots, |4\rangle\}. \qquad (29)$$

As saídas correspondentes às entradas em $\mathcal{S}$ são:

$$\begin{aligned} \mathcal{E}(|i\rangle) &= \sum_{j=0}^{4} \sigma_j ||\langle i|j\rangle||^2 \\ &= \sigma_i. \end{aligned} \qquad (30)$$

As relações de adjacência podem ser explicitadas: o estado $|0\rangle$ é não-adjacente a $|2\rangle$ e $|3\rangle$. Para ver isto, note que

$$\mathcal{E}(|0\rangle) = \sigma_0 = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right) \qquad (31)$$

$$= \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) \qquad (32)$$

e

$$\mathcal{E}(|2\rangle) = \sigma_2 = \left(\frac{|2\rangle + |3\rangle}{\sqrt{2}}\right)\left(\frac{\langle 2| + \langle 3|}{\sqrt{2}}\right) \qquad (33)$$

$$= \frac{1}{2}(|2\rangle\langle 2| + |2\rangle\langle 3| + |3\rangle\langle 2| + |3\rangle\langle 3|) \qquad (34)$$

possuem suporte ortogonal, como também $\mathcal{E}(|0\rangle)$ e $\mathcal{E}(|3\rangle)$:

$$|0\rangle \perp_{\mathcal{E}} |2\rangle \qquad |0\rangle \perp_{\mathcal{E}} |3\rangle.$$

De forma direta, pode-se verificar que

$$|1\rangle \perp_{\mathcal{E}} |3\rangle \qquad |1\rangle \perp_{\mathcal{E}} |4\rangle \qquad |2\rangle \perp_{\mathcal{E}} |4\rangle.$$

O grafo característico com relação a $\mathcal{S}$ é mostrado na Fig. 2. Como pode ser visto, o conjunto $\mathcal{S}$ que alcança a CEZQ dá origem ao pentágono como grafo característico. Portanto, a capacidade do canal $\mathcal{E}_{cq}$ é dada pela capacidade de Shannon do pentágono [18]:

$$C^{(0)}(\mathcal{E}_{cq}) = C_0(\text{pentágono}) = \frac{1}{2}\log 5 \text{ bits/uso}. \qquad (35)$$

Baseado numa construção de Shannon [8], é possível escrever um código quântico de erro-zero que atinge a capacidade de $\mathcal{E}_{cq}$:

$$\begin{aligned} \overline{\rho}_1 = |0\rangle|0\rangle, \quad \overline{\rho}_2 = |1\rangle|2\rangle, \quad \overline{\rho}_3 = |2\rangle|4\rangle \\ \overline{\rho}_4 = |3\rangle|1\rangle, \qquad \overline{\rho}_5 = |4\rangle|3\rangle. \end{aligned} \qquad (36)$$

Note que, embora a CEZQ tenha sido obtida usando estados dois a dois ortogonais para a sinalização (alfabeto do código), são necessários dois ou mais usos do canal para que a capacidade erro-zero seja alcançada.

V. Conclusões

Neste trabalho foi estudada a capacidade erro-zero quântica dos canais clássicos-quânticos (c-q). Foi mostrado que, para um determinado canal c-q num espaço de Hilbert de dimensão d, definido pela família $\{\sigma_i\}$ e pelo POVM $\{X_i = |\psi_i\rangle\langle\psi_i|\}$, a capacidade erro-zero quântica pode sempre ser alcançada pelo conjunto $\mathcal{S} = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$, que corresponde a uma base ortonormal do espaço de Hilbert no qual o canal está definido.

A conseqüência imediata deste fato, é que o cálculo da CEZQ de um canal c-q reduz-se a encontrar a capacidade erro-zero clássica de um canal DSM cuja matriz de adjacência foi explicitada. Por fim, foi mostrado um exemplo de um canal c-q para o qual são necessários dois ou mais usos de canal para que a capacidade seja atingida. Um código de bloco quântico de erro-zero atingindo a capacidade foi construído.

Agradecimentos

Os autores gostariam de agradecer ao CNPq (CT-INFO Quanta, contrato # 552254/02-9) pelo apoio financeiro. Este trabalho foi financiado em parte pelo projeto Europeu SECOQC (contrato # IST-2003-506813).

Referências

[1] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons Inc., New York, 1991.
[2] C. H. Bennett and P. W. Shor. Quantum information theory. *IEEE Trans. Info. Theory*, 44(6):2724–2755, October 1998.
[3] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56(1):131–138, 1997.
[4] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Info. Theory*, 44(1):269–273, 1998.
[5] 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.
[6] 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.
[7] R. A. C. Medeiros and F. M. de Assis. Quantum zero-error capacity. *Int. J. Quant. Inf.*, 3(1):135–139, 2005.
[8] C. E. Shannon. The zero error capaciy of a noisy channel. *IRE Trans. Inform. Theory*, IT-2(3):8–19, 1956.
[9] S. Beigi and P. W. Shor. On the complexity of computing zero-error and holevo capacity of quantum channels. *quant-ph/0709.2090v2*, 2007.
[10] Runyao Duan and Yaoyun Shi. Entanglement between two uses of a noisy multipartite quantum channel enables perfect transmission of classical information, 2007.
[11] A. S. Holevo. Coding theorems for quantum channels. *quant-ph/9809023*, 1998.
[12] R. A. C. Medeiros, F. M. de Assis, R. Alléaume, and G. Cohen. Capacidade erro-zero de canais quânticos com medições coletivas. In *in: Anais do XXV Simpósio Brasileiro de Telecomunicações - SBrT 2007*, pages 1–6, Recife-PE, 2007.

[13] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
[14] M. Horodecki, P. W. Shor, and M. B. Ruskai. Entanglement breaking channels. *Rev. Math. Phys*, 15:629–641, 2003.
[15] J. Köner and A. Orlitsky. Zero-error information theory. *IEEE Trans. Info. Theory*, 44(6):2207–2229, 1998.
[16] R. A. C. Medeiros, R. Alléaume, H. Randriam, F. M. de Assis, and G. Cohen. On the zero-error capacity of entanglement breaking channels. *In preparation*, 2008.
[17] R. A. C. Medeiros. *Zero-Error Capacity of Quantum Channels*. PhD thesis, Universidade Federal de Campina Grande, 2008.
[18] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Info. Theory*, 25(1):1–7, 1979.