

Códigos Simplex Descrevem Estados Quânticos com Máximo Emaranhamento Global

Wanessa C. Gazzoni e Reginaldo Palazzo Jr.

Resumo—A proposta deste trabalho é mostrar que códigos *simplex* n -dimensionais geram estados de máximo emaranhamento global em sistemas com mais de dois *qubits* segundo a medida de Meyer-Wallach.

Palavras-Chave—Códigos *simplex*, estados com máximo emaranhamento global.

Abstract—The purpose of this paper is to show that in a multiparticle system composed of *simplex* code states the maximum global entanglement is achieved under the Meyer-Wallach measure.

Keywords—*Simplex* code, maximum global entangled states.

I. INTRODUÇÃO

O estudo do emaranhamento quântico é fundamental para as aplicações em informação e computação quântica, tais como a codificação superdensa [1], o teletransporte [2] e a criptografia quântica [3]. Em muitos contextos de pesquisas este fenômeno têm sido abordado. Em particular, propostas de uma caracterização matemática dos estados quânticos emaranhados e de medidas adequadas para assim classificá-los foram apresentadas em muitos trabalhos, como por exemplo, [4] - [8]. Num outro contexto, os trabalhos como os de [9] a [12], entre outros, apresentaram propostas de formalização das medidas dos diferentes tipos de emaranhamento.

O objetivo deste trabalho é mostrar que em um sistema com mais de dois *qubits*, se um estado puro tem as amplitudes todas iguais e é composto por *kets* cujas representações correspondem a palavras-código de um código *simplex* n -dimensional, então o máximo emaranhamento global é alcançado, de acordo com a medida de Meyer-Wallach, [10]. Tal resultado foi verificado a partir da identificação entre as representações dos *kets* de um estado quântico com n *qubits* e os vértices de um n -cubo unitário. Considerando a n -esfera que circunscribe este cubo, temos que o problema de descrever as combinações de *kets* que compõem um estado quântico arbitrário é equivalente ao problema de descrever conjuntos de pontos na superfície desta esfera. Sob esta interpretação, temos que determinar as configurações de um estado puro de máximo emaranhamento global é equivalente a determinar um código de Slepian sob a condição de que o canal é Gaussiano aditivo, sem restrição de faixa e com símbolos equiprováveis na entrada do canal. Este trabalho está organizado da seguinte forma. Na Seção II apresentamos uma interpretação geométrica para estados puros arbitrários. Na Seção III mencionamos alguns conceitos

acerca da teoria de projetos de sinais e justificamos a respectiva utilização no contexto do trabalho. Decorrente desse estudo, apresentamos na Seção IV os códigos de Reed-Muller e os códigos *simplex*. Na Seção V, definimos os operadores que referentes à medida de emaranhamento global de Meyer-Wallach e, na Seção VI, apresentamos os resultados obtidos por esta proposta e algumas implicações desta interpretação no contexto de medidas de emaranhamento mais gerais. Finalmente, na Seção VII, as conclusões são mencionadas.

II. INTERPRETAÇÃO GEOMÉTRICA PARA ESTADOS PUROS COM n *qubits*

Um estado puro arbitrário com três *qubits* $|\psi\rangle_3$ pode ser representado como

$$|\psi\rangle_3 = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle, \quad (1)$$

onde $\alpha_i \in \mathbb{C}$, $i \in \{0, \dots, 7\}$, tais que $\sum_{i=0}^7 |\alpha_i|^2 = 1$. Tal estado pode ser interpretado geometricamente de forma que as representações binárias dos *kets* estejam associadas aos vértices de um cubo unitário no espaço discreto definido por todas as sequências binárias de comprimento três, [13]. Tal espaço é denominado *espaço de Hamming* e denotado por \mathcal{H}_2^3 .

Mais explicitamente, os *kets* que compõem o estado $|\psi\rangle_3$ são representados pelos vértices $v_0 = (000)$, $v_1 = (001)$, $v_2 = (010)$, $v_3 = (011)$, $v_4 = (100)$, $v_5 = (101)$, $v_6 = (110)$ e $v_7 = (111)$ do cubo unitário, conforme é apresentado na Fig. 1. Desta forma, temos que o estado $|\psi\rangle_3$ é representado como uma combinação de vértices deste cubo.

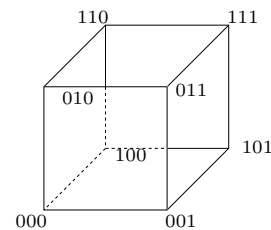


Fig. 1. Cubo unitário que representa o estado $|\psi\rangle_3$.

Esta interpretação geométrica pode ser generalizada para estados puros com n *qubits*. Neste caso, as representações binárias que compõem os *kets* do estado são identificadas com os vértices de um n -cubo unitário definido no espaço de Hamming, \mathcal{H}_2^n .

Nos espaços de Hamming, a medida usual de distância é definida da seguinte forma. Dadas duas representações binárias $s, t \in \mathcal{H}_2^n$, a *distância de Hamming* entre s, t , denotada por $d_H(s, t)$, consiste no número de coordenadas diferentes entre tais representações.

Embora a interpretação geométrica relativa aos estados puros com n qubits seja definida no espaço de Hamming, a mesma pode ser também descrita no espaço Euclidiano, considerando que, neste espaço, a distância usual é a Euclidiana. As distâncias de Hamming e Euclidiana são equivalentes e esta equivalência é definida pelo fato de que *distância de Hamming é igual ao quadrado da distância Euclidiana*.

Considerando a representação do n -cubo unitário no espaço Euclidiano, é possível definir uma esfera n -dimensional que circunscreve o n -cubo. Como os vértices deste n -cubo estão associados às representações que definem os *kets* de um estado puro arbitrário, temos que esses *kets* podem ser vistos como pontos na superfície da esfera n -dimensional, que, sob esta interpretação, tem característica similar a n -esfera de Bloch.

Uma vez estabelecida a equivalência entre as interpretações no espaço de Hamming e no espaço Euclidiano, podemos considerar o problema de determinar a combinação de *kets* que compõem um estado quântico puro com n qubits equivalente ao problema de determinar conjuntos de pontos na superfície da esfera n -dimensional que circunscreve o n -cubo unitário.

Dado um conjunto de pontos na superfície na n -esfera separados pelo máximo valor do quadrado da distância Euclidiana, ou, de forma equivalente, pela maior distância de Hamming possível, é conhecido que este conjunto maximiza a entropia (clássica) de Shannon no sistema representado pelos vértices do n -cubo.

Baseados neste fato, o objetivo deste trabalho é mostrar que o conjunto de pontos com esta característica descrevem estados de máximo emaranhamento global. Para verificar que tais associações são válidas, uma vez determinados os conjuntos de pontos que satisfazem a condição anteriormente apresentada, escrevemos os estados quânticos representados no n -cubo por tais configurações e utilizamos a medida de emaranhamento global de Meyer-Wallach, Q , para mostrar que tais estados são, de fato, estados de máximo emaranhamento global.

Na próxima seção, apresentamos uma forma de determinar os conjuntos dos pontos separados pelo máximo valor da distância de Hamming na superfície da n -esfera. Tal problema refere-se a uma questão importante para projetos de sistemas de comunicações e, por isso, será abordado neste contexto.

III. PROJETO DE CONSTELAÇÕES DE SINAIS

Um dos problemas mais relevantes em sistemas de comunicação é projetar constelações de sinais que sejam adequadas aos efeitos do canal de transmissão tal que a probabilidade de erro seja minimizada. Mais especificamente, conhecidos o modelo do canal e a cardinalidade do conjunto de sinais a serem transmitidas, utilizando o teste de hipóteses e um critério de decisão é possível determinar o receptor que decidirá corretamente pelo sinal transmitido, mesmo que este tenha sido distorcido por interferências introduzidas pelo canal de transmissão.

Como as mensagens podem ser representadas por sinais no domínio do tempo, e estes por sua vez podem ser representados geometricamente como pontos em um espaço de dimensão apropriada, resulta que o conjunto de pontos assim caracterizados forma a constelação de sinais. Como consequência do estabelecimento do critério de decisão é possível realizar o particionamento do espaço de sinais em regiões de decisão através da distância resultante da caracterização estatística do canal. Cada região de decisão está associada a uma única mensagem (sinal ou ponto) e a união dessas regiões recobre o espaço das mensagens.

Uma *constelação de sinais* é um conjunto de vetores $\{\mathbf{x}_i = (x_{i1}, x_{i2}, \dots, x_{in}) : x_{ij} \in \mathbb{R}, 1 \leq i \leq M \text{ and } 1 \leq j \leq n\}$ tal que a energia associada ao i -ésimo sinal é dada pelo produto escalar $\mathbf{x}_i \cdot \mathbf{x}_i$ e que a energia total da constelação é $E_T = \sum_{i=1}^M E_i$.

Se considerarmos constelações de sinais ortogonais, isto é, $\mathbf{x}_i = (0, 0, \dots, 1, \dots, 0, 0)$, com “1” na i -ésima posição e “0” nas demais $(n - 1)$ posições, então temos que $\mathbf{x}_i \cdot \mathbf{x}_j = \delta_{ij}$. Porém, se o objetivo é minimizar a energia total, constelações de sinais ortogonais não satisfazem esta condição, [14]. Devemos então buscar uma isometria que alcance tal objetivo. Seja α a translação a ser efetuada no conjunto de sinais, isto é, $\{\mathbf{y}_i\} = \{\mathbf{x}_i - \alpha\}$. Então, não é difícil mostrar que a energia total é minimizada quando $\alpha = (1/n, 1/n, \dots, 1/n)$. O conjunto de sinais resultante $\{\mathbf{y}_i\}$ é chamado *conjunto de sinais simplex*.

Exemplo 1: Considere o conjunto de sinais ortogonais $\{\mathbf{x}_1 = (1, 0, 0, 0), \mathbf{x}_2 = (0, 1, 0, 0), \mathbf{x}_3 = (0, 0, 1, 0), \mathbf{x}_4 = (0, 0, 0, 1)\}$. Os sinais desse conjunto transladados por $\alpha = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ conduzem ao conjunto de sinais *simplex regular* dado por $\{\mathbf{y}_1 = (\frac{3}{4}, \frac{-1}{4}, \frac{-1}{4}, \frac{-1}{4}), \mathbf{y}_2 = (\frac{-1}{4}, \frac{3}{4}, \frac{-1}{4}, \frac{-1}{4}), \mathbf{y}_3 = (\frac{-1}{4}, \frac{-1}{4}, \frac{3}{4}, \frac{-1}{4}), \mathbf{y}_4 = (\frac{-1}{4}, \frac{-1}{4}, \frac{-1}{4}, \frac{3}{4})\}$.

Considerando que os sinais são equiprováveis, que o canal é o Gaussiano aditivo e que não existe restrição da faixa de transmissão, um resultado conhecido e demonstrado por Weber, [15], é que a constelação de sinais ótima no espaço Euclidiano é a *simplex regular*. Tal constelação é definida a seguir.

Definição 1: O conjunto de $(n + 1)$ pontos equidistantes no espaço Euclidiano n -dimensional estabelece uma constelação de sinais do tipo *simplex regular* n -dimensional, ou um n -*simplex*.

É conhecido que existe uma correspondência entre uma constelação de sinais em um espaço Euclidiano e um *código*, definido no espaço de Hamming. Tal correspondência decorre da equivalência entre as medidas destes dois espaços e é estabelecida de forma que os pontos (sinais) da primeira são vistos como as palavras-código do segundo.

Em particular, os códigos associados às constelações de sinais do tipo *simplex regular* são denominados *códigos simplex*, cujas palavras-código preservam as mesmas propriedades dos pontos da constelação.

Exemplo 2: Note que no Exemplo 1 o conjunto de sinais *simplex regular* é caracterizado pelo fato que $d_E^2(\mathbf{x}_i, \mathbf{x}_j) = 2$, para todo i, j tal que $i \neq j$. Como $d_E^2 = d_H$, segue que o código *simplex* associado à constelação referida é definido

por um conjunto de palavras satisfazendo a distância de Hamming igual a 2. Desta forma, um código *simplex* associado à constelação do Exemplo 1 é dado por

$$\mathcal{C} = \{000, 011, 101, 110\}.$$

Uma vez mencionada a correspondência entre as constelações de sinais *simplex* e os códigos *simplex*, apresentamos na próxima seção um breve resumo das propriedades dessa classe de códigos.

IV. CÓDIGOS REED-MULLER $RM(1, m)$ E CÓDIGOS SIMPLEX

Neste trabalho, consideramos apenas os códigos *simplex* binários, contendo esta família códigos lineares e não-lineares. Os códigos *simplex* lineares são descritos em função dos códigos Reed-Muller de primeira ordem. Todavia, salientamos que esta não é a única forma de descrevê-los, como pode ser visto em [16].

O código de Reed-Muller de primeira ordem e comprimento $n = 2^m$, denotado por $RM(1, m)$, é o conjunto de todos os vetores \mathbf{f} , onde $\mathbf{f}(\mathbf{v})$ é uma função Booleana, isto é, um polinômio cujo grau é no máximo 1, e $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m) \in \mathcal{H}_2^{2^m}$, o conjunto de todas as 2^m -uplas binárias, [16].

Como exemplo, considere $m = 2$. Então, as palavras-código do código $RM(1, 2)$ são dadas pela composição

$$a_0 \cdot \mathbf{1} + a_1 \cdot \mathbf{v}_1 + a_2 \cdot \mathbf{v}_2, \quad a_i = 0 \text{ ou } 1$$

onde $\mathbf{1} = 1111$, $\mathbf{v}_2 = 0011$ e $\mathbf{v}_1 = 0101$.

Os parâmetros do código $RM(1, m)$ são dados por $n = 2^m$, $k = 1 + \binom{m}{1}$ e $d_H = 2^{m-1}$, para $m \geq 2$.

Disso segue que a matriz geradora do código $RM(1, m)$ consiste em

$$\begin{bmatrix} G_0 \\ G_1 \end{bmatrix},$$

onde $G_0 = [\mathbf{1}]$, $G_1^T = [\mathbf{v}_m \ \mathbf{v}_{m-1} \ \dots \ \mathbf{v}_1]$ e $\mathbf{v}_j = 2^{m-j}$ termos do tipo $\{0^{2^{j-1}} \ 1^{2^{j-1}}\}$, para $1 \leq j \leq m$.

O código dual do código $RM(1, m)$ com parâmetros $(2^m, m+1, 2^{m-1})$ é o código de Hamming estendido $(2^m, 2^m - m - 1, 4)$.

Note que a submatriz G_0 gera um código de repetição $(2^m, 1, 2^m)$. Este código constitui um código *simplex trivial*, ou ainda, um código *simplex* 1-dimensional.

Por outro lado, se considerarmos a submatriz G_1 , excluída sua primeira coluna, temos uma matriz onde cada coluna é a decomposição binária do número inteiro correspondente àquela coluna. Esta matriz caracteriza um código *simplex* linear com parâmetros $(2^m - 1, m, 2^{m-1})$. O código dual é o código de Hamming com parâmetros $(2^m - 1, 2^m - m - 1, 3)$.

Uma outra forma de denotarmos os parâmetros de um código *simplex* binário n -dimensional consiste em

$$(n, M, d) = \left(n, n+1, \frac{n+1}{2} \right),$$

onde $n \equiv 3 \pmod{4}$. Utilizamos esta notação no desenvolvimento da proposta.

Um exemplo de um código *simplex* é o código \mathcal{C} apresentado no Exemplo 2. Observe que \mathcal{C} satisfaz a condição de linearidade e é tal que $n = 3$, $M = 4$ e $d_H = 2$ para todos os pares de palavras-código.

Um exemplo de código *simplex* não-linear é o código de Hadamard \mathcal{A}_{12} com parâmetros $(11, 12, 6)$, cujas palavras-código são $\{0000000000, 11011100010 + \text{deslocamentos cíclicos}\}$.

De acordo com a interpretação geométrica apresentada na Seção II, as representações binárias dos *kets* de um estado puro arbitrário foram identificadas com os vértices de um n -cubo definido em \mathbb{Z}_2^n . Alguns desses vértices foram associados a pontos das constelações de sinais *simplex regulares* e estes, às palavras de um código *simplex*.

Reciprocamente, uma vez definido um código *simplex*, podemos associar um estado quântico. Cada palavra-código é identificada com uma representação binária que define um *ket*. Repetindo o processo para todas as palavras-código, temos definida a composição de *kets* do estado.

Como os pontos de uma constelação *simplex* definem uma combinação de vértices do n -cubo unitário inscrito na esfera n -dimensional e como cada vértice será rotulado por uma palavra-código do código *simplex*, então um estado quântico (puro) arbitrário poderá ser descrito como a composição das correspondentes palavras-código.

A amplitude de cada um dos *kets* será associada à raiz quadrada da probabilidade de ocorrência do respectivo ponto na constelação de sinais *simplex*. Como os sinais são considerados equiprováveis, temos que as amplitudes associadas aos *kets* são iguais entre si. Como as palavras-código foram obtidas de pontos equiprováveis de uma constelação de sinais *simplex* regular, então todas as amplitudes associadas aos *kets* são iguais. Como a probabilidade de cada ponto em uma constelação *simplex* n -dimensional consiste do valor $1/(n+1)$, decorre que as amplitudes assumem o valor $1/\sqrt{n+1}$, onde $(n+1)$ refere-se à cardinalidade da constelação, segundo a Definição 1.

Baseados nestas justificativas, temos que o estado associado ao código *simplex* linear mencionado no Exemplo 2 é dado por

$$|\varphi\rangle = \frac{1}{\sqrt{4}} (|000\rangle + |011\rangle + |101\rangle + |110\rangle). \quad (2)$$

Seja $|\xi\rangle$ um estado puro com n qubits caracterizado pela igualdade entre as amplitudes de valor $1/\sqrt{n+1}$ e pela composição de *kets* cujas representações sejam estabelecidas pelo conjunto de palavras de um código *simplex* n -dimensional, com parâmetros $(n, M, d) = (n, n+1, (n+1)/2)$, $n \equiv 3 \pmod{4}$. Na Seção VI demonstramos que os estados $|\xi\rangle$ satisfazem as condições que os classificamos como estados de máximo emaranhamento global, segundo a medida de Meyer-Wallach, que é definida a seguir.

V. MEDIDA DE EMARANHAMENTO GLOBAL DE MEYER-WALLACH

A medida de emaranhamento global definida por Meyer e Wallach, [10], e denotada por Q , pode ser aplicada a estados quânticos puros arbitrários. Tal medida é definida como segue, [11].

Para cada $j = 1, \dots, n$ representando as posições nos *kets* e $b \in \{0, 1\}$, os possíveis valores para os *qubits*, definimos a função linear $\iota_j(b) : (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n-1}$ através da respectiva ação na base do produto, a saber,

$$\begin{aligned} \iota_j(b) (|x_1\rangle \otimes \dots \otimes |x_n\rangle) &= \delta_{bx_j} |x_1\rangle \otimes \dots \otimes |x_{j-1}\rangle \otimes \\ &\otimes |x_{j+1}\rangle \otimes \dots \otimes |x_n\rangle, \end{aligned}$$

onde $x_i \in \{0, 1\}$.

Definição 2: Dado um estado quântico puro arbitrário com n *qubits* $|\psi\rangle$, a *medida de emaranhamento global de Meyer-Wallach* consiste em

$$Q(|\psi\rangle) \equiv \frac{4}{n} \sum_{j=1}^n D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle), \quad (3)$$

onde

$$\begin{aligned} D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle) &= \langle \psi | \iota_j(0), \iota_j(0) | \psi \rangle \langle \psi | \iota_j(1), \iota_j(1) | \psi \rangle \\ &- |\langle \psi | \iota_j(0), \iota_j(1) | \psi \rangle|^2, \end{aligned} \quad (4)$$

para todo $j \in \{1, \dots, n\}$.

Q é invariante sob transformações unitárias locais e tal que $0 \leq Q \leq 1$, com $Q(|\psi\rangle) = 0$ se, e somente se, $|\psi\rangle$ é um estado separável, ou, um estado da forma produto, e, se $Q(|\psi\rangle) = 1$, então temos que $|\psi\rangle$ é um *estado puro de máximo emaranhamento global*, [10].

Uma vez definida a medida de emaranhamento global a ser utilizada para a classificação dos estados $|\xi\rangle$, apresentamos o estudo que justifica a proposta do trabalho.

VI. RESULTADOS

Segundo [16], os códigos *simplex* são códigos auto-ortogonais e puros. Uma vez que as palavras destes códigos foram identificadas com as representações que compõem os *kets* de um estado $|\xi\rangle$, podemos afirmar que tais representações mantêm as propriedades de auto-ortogonalidade e de equidistância que caracterizam as palavras dos códigos *simplex* associados.

Tais propriedades resultam em uma consideração importante acerca do operador $D(\iota_j(0)|\xi\rangle, \iota_j(1)|\xi\rangle)$, conforme apresentado a seguir.

Lema 1: Para os estados quânticos puros obtidos a partir de códigos *simplex* n -dimensionais, $D(\iota_j(0)|\xi\rangle, \iota_j(1)|\xi\rangle) = 1/4$, para todo $j, j \in \{1, \dots, n\}$.

Demonstração: Primeiramente, considere os estados obtidos a partir do código de repetição (código *simplex* trivial). A amplitude associada aos *kets* é $1/\sqrt{2}$. Fixado um $j, j \in \{1, \dots, n\}$, temos que os estados $\iota_j(0)|\xi\rangle$ e $\iota_j(1)|\xi\rangle$ são constituídos somente de zeros e uns, respectivamente. Como consequência,

$$\langle \xi | \iota_j(0), \iota_j(1) | \xi \rangle = 0, \quad (5)$$

$$\langle \xi | \iota_j(0), \iota_j(0) | \xi \rangle = \langle \xi | \iota_j(1), \iota_j(1) | \xi \rangle = (1/\sqrt{2})^2 = 1/2. \quad (6)$$

De (5) e (6), decorre que, para todo j fixo, $D(\iota_j(0)|\xi\rangle, \iota_j(1)|\xi\rangle) = 1/4$.

Considere agora, o caso dos estados obtidos a partir de códigos *simplex* n -dimensionais. A amplitude associada a cada um dos *kets* é $1/\sqrt{n+1}$. Como consideramos apenas os códigos *simplex* lineares, uma propriedade decorrente desta linearidade é o fato de que há exatamente $(n+1)/2$ palavras-código com “0” e $(n+1)/2$ palavras-códigos com “1” na j -ésima posição, para cada j fixo. Sejam esses dois conjuntos de $(n+1)/2$ palavras-código representados, respectivamente por $p_1, p_2, \dots, p_{(n+1)/2}$ e $q_1, q_2, \dots, q_{(n+1)/2}$. Fixando j e considerando $p_i^0, 1 \leq i \leq \frac{n+1}{2}$, como as palavras-código obtidas pela exclusão do dígito “0” da j -ésima posição das palavras $p_i, 1 \leq i \leq (n+1)/2$, e q_i^1 as palavras-código obtidas pela exclusão do dígito “1” da j -ésima posição das palavras q_i , temos que

$$\iota_j(0)|\xi\rangle = \frac{1}{\sqrt{n+1}} (|p_1^0\rangle + |p_2^0\rangle + |p_3^0\rangle + \dots + |p_{(n+1)/2}^0\rangle)$$

e

$$\iota_j(1)|\xi\rangle = \frac{1}{\sqrt{n+1}} (|q_1^1\rangle + |q_2^1\rangle + |q_3^1\rangle + \dots + |q_{(n+1)/2}^1\rangle).$$

Assim, podemos escrever, para $K = \left(\frac{1}{\sqrt{n+1}}\right)^2$,

$$\begin{aligned} \langle \xi | \iota_j(0), \iota_j(0) | \xi \rangle &= K (\langle p_1^0 | p_1^0 \rangle + \dots + \langle p_1^0 | p_{(n+1)/2}^0 \rangle + \dots \\ &+ \langle p_{(n+1)/2}^0 | p_1^0 \rangle + \dots + \langle p_{(n+1)/2}^0 | p_{(n+1)/2}^0 \rangle). \end{aligned}$$

De acordo com as propriedades do produto interno, são diferentes de zero apenas os termos na forma $\langle p_i^0 | p_i^0 \rangle, i \in \{1, \dots, (n+1)/2\}$. Portanto, para j fixo, decorre que

$$\langle \xi | \iota_j(0), \iota_j(0) | \xi \rangle = \left(\frac{1}{\sqrt{n+1}}\right)^2 \cdot \left(\frac{n+1}{2}\right) = 1/2, \quad (7)$$

De acordo com os mesmo argumentos, segue que

$$\langle \xi | \iota_j(1), \iota_j(1) | \xi \rangle = 1/2. \quad (8)$$

No caso de $\langle \xi | \iota_j(0), \iota_j(1) | \xi \rangle$, temos,

$$\begin{aligned} \langle \xi | \iota_j(0), \iota_j(1) | \xi \rangle &= K \cdot (\langle p_1^0 | q_1^1 \rangle + \dots + \langle p_1^0 | q_{(n+1)/2}^1 \rangle + \dots \\ &+ \langle p_{(n+1)/2}^0 | q_1^1 \rangle + \dots + \langle p_{(n+1)/2}^0 | q_{(n+1)/2}^1 \rangle). \end{aligned}$$

Pode-se verificar que, para cada j fixo, não existe i e i' ($i, i' \in \{1, \dots, (n+1)/2\}$), tais que $p_i^0 = q_{i'}^1$, donde concluímos que, para cada j fixo,

$$\langle \xi | \iota_j(0), \iota_j(1) | \xi \rangle = 0. \quad (9)$$

Portanto, de acordo com (7), (8) e (9), para cada j fixo, $j \in \{1, \dots, n\}$, decorre que $D(\iota_j(0)|\xi\rangle, \iota_j(1)|\xi\rangle) = 1/4$, o que conclui a verificação do Lema 1 ■

Como consequência, decorre o seguinte resultado.

Teorema 1: Estados quânticos puros com n *qubits* obtidos a partir de códigos *simplex* n -dimensionais com amplitudes

identicamente distribuídas e iguais a $\frac{1}{\sqrt{n+1}}$ são estados puros de máximo emaranhamento global.

Demonstração: De acordo com o Lema 1, temos que

$D(\iota_j(0)|\xi, \iota_j(1)|\xi) = 1/4$, para cada j fixo. Então, segue que

$$\begin{aligned} Q(|\xi\rangle) &\equiv \frac{4}{n} \sum_{j=1}^n D(\iota_j(0)|\xi, \iota_j(1)|\xi) \\ &= \frac{4}{n} \cdot n \cdot D(\iota_j(0)|\xi, \iota_j(1)|\xi) = 1. \end{aligned} \quad (10)$$

Portanto, todos os estados obtidos a partir de códigos *simplex* n -dimensionais com amplitudes equiprováveis, são estados de máximo emaranhamento global segundo a medida de Meyer-Wallach. ■

Seguem alguns exemplos dos cálculos referentes à medida Q de Meyer-Wallach.

Exemplo 3: Um código *simplex* trivial de parâmetros $(n, M, d) = (3, 2, 3)$ é definido pelas palavras-código $\{000, 111\}$. O estado associado a este código é denominado estado *GHZ* e é representado na forma

$$|\delta\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle). \quad (11)$$

De acordo com os operadores definidos na Seção V, temos que

$$\begin{aligned} \iota_1(0)|\delta\rangle &= \iota_2(0)|\delta\rangle = \iota_3(0)|\delta\rangle = \frac{1}{\sqrt{2}}(|00\rangle) = \iota_j(0)|\delta\rangle, \\ \iota_1(1)|\delta\rangle &= \iota_2(1)|\delta\rangle = \iota_3(1)|\delta\rangle = \frac{1}{\sqrt{2}}(|11\rangle) = \iota_j(1)|\delta\rangle, \end{aligned}$$

para $j = 1, 2$ e 3 . A substituição destas expressões em (4) resulta em

$$\begin{aligned} D &= \langle \delta | \iota_j(0), \iota_j(0) | \delta \rangle \langle \delta | \iota_j(1), \iota_j(1) | \delta \rangle - |\langle \delta | \iota_j(0), \iota_j(1) | \delta \rangle|^2 \\ &= \left(\frac{1}{\sqrt{2}} \right)^2 \langle 00 | 00 \rangle \left(\frac{1}{\sqrt{2}} \right)^2 \langle 11 | 11 \rangle - \left(\frac{1}{\sqrt{2}} \right)^2 |\langle 00 | 11 \rangle|^2 \\ &= \left(\frac{1}{\sqrt{2}} \right)^4 (\langle 0 | 0 \rangle \langle 0 | 0 \rangle (\langle 1 | 1 \rangle \langle 1 | 1 \rangle) - \left(\frac{1}{\sqrt{2}} \right)^2 (\langle 0 | 1 \rangle \langle 0 | 1 \rangle) \\ &= \left(\frac{1}{\sqrt{2}} \right)^4 = 1/4, \end{aligned}$$

para $j = 1, 2$ e 3 . Com base neste valor obtido, decorre de (3) que

$$Q(|\delta\rangle) = \frac{4}{3} \sum_{j=1}^3 D(\iota_j(0)|\delta, \iota_j(1)|\delta) = \frac{4}{3} \sum_{j=1}^3 \frac{1}{4} = 1.$$

Exemplo 4: O estado obtido do código *simplex* 3-dimensional apresentado no Exemplo 2 é representado por

$$|\varphi\rangle = \frac{1}{\sqrt{4}} (|000\rangle + |011\rangle + |101\rangle + |110\rangle).$$

De acordo com os operadores que definem a medida Q , temos que

$$\begin{aligned} \iota_1(0)|\varphi\rangle &= \iota_2(0)|\varphi\rangle = \iota_3(0)|\varphi\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |11\rangle), \\ \iota_1(1)|\varphi\rangle &= \iota_2(1)|\varphi\rangle = \iota_3(1)|\varphi\rangle = \frac{1}{\sqrt{4}}(|10\rangle + |01\rangle), \end{aligned}$$

para $j = 1, 2$ e 3 . Pela substituição destas expressões em (4), obtemos que

$$\begin{aligned} D &= \left(\frac{1}{\sqrt{4}} \right)^4 (\langle 00 | \langle 11 |, |00\rangle + |11\rangle) (\langle 10 | + \langle 01 |, |10\rangle + |01\rangle) \\ &\quad - \left(\frac{1}{\sqrt{4}} \right)^2 |\langle 00 | \langle 11 |, |10\rangle + |01\rangle|^2 \\ &= \left(\frac{1}{\sqrt{4}} \right)^2 (\langle 00 | 00 \rangle + \langle 00 | 11 \rangle + \langle 11 | 00 \rangle + \langle 11 | 11 \rangle) \cdot \\ &\quad \cdot \left(\frac{1}{\sqrt{4}} \right)^2 (\langle 10 | 10 \rangle \langle 10 | 01 \rangle + \langle 01 | 10 \rangle + \langle 01 | 10 \rangle) \\ &\quad - \left(\frac{1}{\sqrt{4}} \right)^2 |\langle 00 | 10 \rangle + \langle 00 | 01 \rangle + \langle 11 | 10 \rangle + \langle 11 | 01 \rangle|^2 \\ &= 4 \left(\frac{1}{\sqrt{4}} \right)^4 = 1/4. \end{aligned}$$

para $j = 1, 2, 3$. Substituindo este valor em (3), obtemos que

$$Q(|\varphi\rangle) = \frac{4}{3} \sum_{j=1}^3 \frac{1}{4} = 1.$$

Exemplo 5: O código dual ao código de Hamming é um código *simplex* de parâmetros $(n, M, d) = (7, 8, 4)$. O estado quântico puro com sete *qubits* associado a este código consiste em

$$\begin{aligned} |\psi_{Ham}\rangle &= \frac{1}{\sqrt{8}} (|0000000\rangle + |0110011\rangle + |0001111\rangle \\ &\quad + |0111100\rangle + |1010101\rangle + |1100110\rangle \\ &\quad + |1011010\rangle + |1101001\rangle). \end{aligned}$$

Desenvolvendo os cálculos estabelecidos na Seção V como nos exemplos anteriores, concluímos que $Q = 1$, donde decorre que $|\psi_{Ham}\rangle$ também é um estado de máximo emaranhamento global.

Exemplo 6: A partir do código *simplex* trivial de parâmetros $(n, M, d) = (n, 2, n)$, para todo $n \in \mathbb{N}$, é possível definir uma classe de estados de máximo emaranhamento global conhecidos como *estados GHZ generalizados*. Tais estados são representados na forma

$$|\psi_{GHZg}\rangle = \frac{1}{\sqrt{2}} \left(\underbrace{|00 \dots 0\rangle}_n + \underbrace{|11 \dots 1\rangle}_n \right)$$

e são entendidos como uma generalização dos estados *EPRs*. Os estados *GHZ* generalizados, assim como os estados *EPR*, são utilizados para a execução de tarefas como a codificação superdensa, criptografia quântica e teletransporte quântico, [17].

Os Exemplos 5 e 6 explicitam a consistência da interpretação que nos permite associar a descrição de estados de máximo emaranhamento global, assim classificados segundo a medida de Meyer-Wallach, e os códigos *simplex* n -dimensionais.

Salientamos, porém, que as condições sob as quais os códigos de Slepian são determinados (conforme descrito na Seção I) são similares às descrições de estados puros emaranhados em um sistema *multipartite*, quando a medida de emaranhamento entre os subsistemas é a entropia de von Neumann dos operadores reduzidos. Segundo pode ser visto em [11], a medida de Meyer-Wallach é uma particularidade desta medida, podendo ser reescrita na forma

$$Q(|\mu\rangle) = 2 \left(1 - \frac{1}{n} \sum_{k=1}^n \text{tr}(\rho_k)^2 \right), \quad (12)$$

onde ρ_k é o operador densidade reduzido sobre o k -ésimo qubit.

Neste contexto, a interpretação sugerida neste trabalho auxilia na descrição de estados satisfazendo condições de máximo emaranhamento global, considerando não apenas o emaranhamento no sistema biparticionado, como é o caso da medida de Meyer-Wallach, mas sim entre os diversas partes de um sistema multipartite.

VII. CONCLUSÕES

Neste trabalho mostramos que existe uma forma sistemática de obter estados puros arbitrários de máximo emaranhamento global. Esta forma sistemática consiste em considerar que as representações dos *kets* sejam as palavras-código de um código *simplex* n -dimensional com parâmetros $(n, n+1, \frac{n+1}{2})$, para $n \equiv 3 \pmod{4}$ e associar a cada um desses *kets* a amplitude igual a $\frac{1}{\sqrt{n+1}}$. A interpretação sugerida neste trabalho pode ser associada a medidas de emaranhamento global mais gerais, o que nos permite descrever também estados de máximo emaranhamento global em sistemas multipartites. Tais fatos indicam que muitos outros resultados podem ser obtidos a partir da associação de medida de emaranhamento e conceitos de teoria clássica de informação, principalmente no contexto de propostas de medidas de emaranhamento.

AGRADECIMENTOS

Os autores agradecem o suporte financeiro das agências CAPES, CNPq e FAPESP durante o período desta pesquisa e ao colega Rodrigo Gusmão Cavalcante pelas sugestões no texto.

REFERÊNCIAS

- [1] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.* **69**, pp. 2881-2884 (1992).
- [2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, "Teleporting an Unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.* **70**, pp.1895-1899 (1993).
- [3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, pp. 661-663 (1991).
- [4] R. Mosseri and R. Dandoloff, "Geometry of entangled states, Bloch spheres and Hopf fibrations," (2001). Disponível em www.arXiv.org/quant-ph/0108137.
- [5] I. Bengtsson and J. Brännlund, " CP^n , or, entanglement illustrated," (2001). Disponível em www.arXiv.org/quant-ph/0108064.
- [6] N. Linden and S. Popescu, "On multi-particle entanglement," (1997). Disponível em www.arXiv.org/quant-ph/9711016.
- [7] W. K. Wootters, "Quantum entanglement as a quantifiable resource," *Phil. Trans. R. Soc. London A* **356**, pp. 1717-1731 (1998).
- [8] D. Bruß, "Characterizing entanglement," *J. Math. Phys.* **43**, pp. 4237-4251 (2002).
- [9] V. Coffman, J. Kundu and W. K. Wootters, "Distributed entanglement," *Phys. Rev. A* **61**, pp. 052306-052311 (1999).
- [10] D. A. Meyer, and N. R. Wallach "Global entanglement in multiparticle systems," *Journal of Mathematical Physics* **43**, Number **9**, 2002, pp. 4273-4278 (2002).
- [11] A. J. Scott, "Multipartite entanglement, quantum error-correcting codes, and entangling power of quantum evolution," *Physical Review A* **69**, pp. 052330 (2004).
- [12] T. C. Wei and P. M. Goldbart, "Geometric measure of entanglement and applications to bipartite and multipartite quantum states," *Physical Review A* **68**, pp. 042307 (2003).
- [13] C. S. Yu and H. S. Song, "Global entanglement of multipartite quantum states," *Physical Review A* **73**, pp. 022325 (2005).
- [14] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering*. New York, NY: John Wiley and Sons, 1965.
- [15] C. L. Weber, *Elements of Detection and Signal Design*. New York, NY: Springer-Verlag, 1987.
- [16] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, Netherlands: North-Holland Publishing Company, 1977.
- [17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, MA: Cambridge University Press, 2000.