Qubits Fatoráveis em Quaterbits

Delano Klinger Alves de Souza e José Cláudio do Nascimento

***Resumo*—In this paper we investigate whether some not factorable qubit can be written as the product of two quaterbits. As verification criteria we use the concurrence deduced by Wooters from the entropy of von Neumann of a special hermitian matrix.**

***Index Terms*—Qubits, quaterbits, von Neumann entropy, quaternions.**

I. INTRODUÇÃO

A entropia de von Neumann, $S(\rho) = -\text{tr}\left[\rho\log(\rho)\right]$ é uma extensão da entropia de Gibbs que se reduz a entropia de Shannon, $H(\lambda) = -\Sigma_{i=1}^{n}\lambda_i\log(\lambda_i)$, em que λ_i são os autovalores da matriz hermitiana ρ. Essa entropia é útil na avaliação de sistemas que estão correlacionados. Por exemplo, valores da entropia de von Neumann em estados especiais dizem o quão capaz um estado de dois sistemas é útil para a teleportação [1] e protocolos de criptografia [2,3].

No cálculo proposicional de Birkhoff e von Neumann [4], estados de um sistema quântico poderiam ser definidos num espaço de Hilbert sobre qualquer álgebra associativa. Os conjuntos sugeridos incluem os reais, $\mathbb{R}$, os complexos, $\mathbb{C}$, e os quatérnios, $\mathbb{H}$. Atualmente, todo estado ρ, matriz hermitiana, definido no reais é chamado de rebit, nos complexos, qubit, e nos quatérnios, quaterbit. Definimos

$$\tilde{\rho} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \bar{\rho} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

em que $\bar{\rho}$ é o complexo conjugado de ρ, e $R = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$. Se $S(R) = -\text{tr}\left[R\log(R)\right] = 0$, então ρ é fatorável num produto de Kronecker (tensorial) de dois estados, $\rho = \rho_A \otimes \rho_B$ [7].

Algumas investigações sobre a separabilidade nesses três conjuntos de estados têm sido de interesse para a Mecânica Quântica e a Teoria da Informação. Por exemplo, a probabilidade de um rebit, qubit e quaterbit, ser separável é variável [5]. Caves demonstrou que existem rebits não separáveis que são qubits separáveis. Ele também verificou que a medida de separabilidade varia entre os rebits e os qubits [6]. Caves e Wooters [6,8] perguntam se essa diferença entre as separabilidades também poderia acontecer entre os qubits e quaterbits.

Neste trabalho decidimos investigar se algum qubit não fatorável pode ser escrito como o produto de dois quaterbits. Decidimos testar essa hipótese primeiro para estados puros fatoráveis. Considerando $\mathbb{C} \subset \mathbb{H}$, investigamos as condições para que o produto de quaterbits, $|\phi_{12}\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \in \mathbb{H}^2 \times \mathbb{H}^2$, resulte num qubit, $|\tilde{\phi}_{12}\rangle \in \mathbb{C}^2 \times \mathbb{C}^2$. Usando a concurrência, $S(R) = -\text{tr}\left[R\log(R)\right]$, como critério de separabilidade, mostramos que $|\tilde{\phi}_{12}\rangle$ é separável, ou seja, o produto tensorial de dois quaterbits puros não geram um qubit puro bipartido não separável.

II. PRELIMINARES

Os quatérnios denotado por $\mathbb{H}$, foram desenvolvido por William Rowan Hamilton em 1843 como uma generalização dos números complexos representado por quatro componentes reais $q = (q_0, q_1, q_2, q_3)$. Um quatérnio q pode ser definido pela soma: $q = q_0 + \mathbf{q}$, onde $\mathbf{q} = \mathbf{i}q_1 + \mathbf{j}q_2 + \mathbf{k}q_3$ e $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ é a base canônica do espaço tridimensional $\mathbb{R}^3$, que é ortonormal, ou seja $\mathbf{i} = (1,0,0)$, $\mathbf{j} = (0,1,0)$ e $\mathbf{k} = (0,0,1)$. Dizemos que respectivamente q_0 e $\mathbf{q}$ são as partes real e vetorial do quatérnio. A soma de dois quatérnios é análoga ao dos complexos, enquanto o produto de dois quatérnios devemos ter mais atenção devido a não comutatividade. O produto de dois quatérnios deve atender aos produtos especiais fundamentais:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1. \tag{1}$$

O conjugado de um quatérnio $q = q_0 + \mathbf{q}$ será o quatérnio $\overline{q} = q_0 - \mathbf{q}$. A conjugação complexa quaterniônica induz uma norma multiplicativa $\|\cdot\| : \mathbb{H} \to \mathbb{R}$, via A norma de um quatérnio q, será denotada por $\|q\|$. Usando a definição de produto quaterniônico, junto com o fato de que, para qualquer vetor $\mathbf{q}$, temos $\mathbf{q} \times \mathbf{q} = 0$, pode-se provar que $\|q\| = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$. A norma do produto de dois quatérnios p e q é o produto das normas individuais, ou seja,$\|pq\| = \|p\|\|q\|$. Outro resultado interessante é que podemos escrever um quatérnio qualquer na forma:

$$q = z_1 + z_2\mathbf{j}, \tag{2}$$

com z_1, z_2 complexos. Para isso basta escrever $q = q_0 + q_1\mathbf{i} + (q_2 + \mathbf{i}q_3)\mathbf{j}$. Para finalizar, considere o lema: se z é um número complexo então $\mathbf{j}z = \overline{z}\mathbf{j}$. De fato, sendo $z = a + b\mathbf{i}$, com a, b reais, temos sucessivamente:

$$\mathbf{j}z = \mathbf{j}(a+b\mathbf{i}) = \mathbf{j}a + \mathbf{j}b\mathbf{i} = a\mathbf{j} + b(-\mathbf{ij}) = a\mathbf{j} - b\mathbf{ij} = (a - b\mathbf{i})\mathbf{j} = \overline{z}\mathbf{j}.$$

III. QUATERBITS PUROS NÃO GERAM QUBITS NÃO SEPARÁVEL

Sejam os estados puros quânticos quaterbits $|\varphi_1\rangle = a|0\rangle + b|1\rangle, a, b \in \mathcal{H}$ e $|\varphi_2\rangle = c|0\rangle + d|1\rangle, c, d \in \mathcal{H}$. Fazendo o produto tensorial entre eles, temos:

$$|\varphi_1\rangle \otimes |\varphi_2\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle. \tag{3}$$

Sabemos que um quatérnio q pode ser escrito na forma de singleto $q = z_1 + z_2\mathbf{j}$, onde $z_1, z_2 \in \mathbb{C}$. Logo para os quatérnios: a, b, c, d, teremos:

$$\begin{aligned} a &= \alpha_1 + \alpha_2\mathbf{j} \\ b &= \beta_1 + \beta_2\mathbf{j} \\ c &= \gamma_1 + \gamma_2\mathbf{j} \\ d &= \delta_1 + \delta_2\mathbf{j}. \end{aligned} \tag{4}$$

onde $\mathbf{j}^2 = -1$ da álgebra quaterniônica e os demais parâmetros são números complexos e são obedecidas nos dois quaterbits

$$\sum_{i=1}^{2} \|\alpha_i\|^2 + \|\beta_i\|^2 = 1 \quad \text{e} \quad \sum_{i=1}^{2} \|\gamma_i\|^2 + \|\delta_i\|^2 = 1. \tag{5}$$

Cada amplitude do quaterbit como produto entre os quatérnios pode ser reescrito por

$$\begin{aligned} ac &= (\alpha_1\gamma_1 - \alpha_2\overline{\gamma_2}) + (\alpha_1\gamma_2 + \alpha_2\overline{\gamma_1})\mathbf{j} \\ ad &= (\alpha_1\delta_1 - \alpha_2\overline{\delta_2}) + (\alpha_1\delta_2 + \alpha_2\overline{\delta_1})\mathbf{j} \\ bc &= (\beta_1\gamma_1 - \beta_2\overline{\gamma_2}) + (\beta_1\gamma_2 + \beta_2\overline{\gamma_1})\mathbf{j} \\ bd &= (\beta_1\delta_1 - \beta_2\overline{\delta_2}) + (\beta_1\delta_2 + \beta_2\overline{\delta_1})\mathbf{j}. \end{aligned} \tag{6}$$

Por simplicidade de notação, parametrizamos as quatro expressões anteriores:

$$\begin{aligned} \alpha_1\gamma_1 - \alpha_2\overline{\gamma_2} &= \tilde{A} \\ \alpha_1\delta_1 - \alpha_2\overline{\delta_2} &= \tilde{B} \\ \beta_1\gamma_1 - \beta_2\overline{\gamma_2} &= \tilde{C} \\ \beta_1\delta_1 - \beta_2\overline{\delta_2} &= \tilde{D} \end{aligned} \tag{7}$$

e

$$\begin{aligned} \alpha_1\gamma_2 + \alpha_2\overline{\gamma_1} &= A \\ \alpha_1\delta_2 + \alpha_2\overline{\delta_1} &= B \\ \beta_1\gamma_2 + \beta_2\overline{\gamma_1} &= C \\ \beta_1\delta_2 + \beta_2\overline{\delta_1} &= D. \end{aligned} \tag{8}$$

Podemos definir critérios para que os termos em $\mathbf{j}$ no produto tensorial $|\varphi_1\rangle \otimes |\varphi_2\rangle$ se anule. Dessa forma o estado quântico resultante estará presente na mecânica quântica complexa. Para isso devemos ter $A = B = C = D = 0$, de modo que:

$$\begin{aligned} \alpha_1\gamma_2 = -\alpha_2\overline{\gamma_1}, \alpha_1\delta_2 = -\alpha_2\overline{\delta_1} \\ \beta_1\gamma_2 = -\beta_2\overline{\gamma_1} \quad \text{e} \quad \beta_1\delta_2 = -\beta_2\overline{\delta_1}. \end{aligned} \tag{9}$$

Considerando a primeira e terceira equações podemos concluir que $\alpha_1\beta_2 - \alpha_2\beta_1 = 0$. As quatro equações acima nos leva ao estado qubit bipartite:

$$|\varphi_1\rangle \otimes |\varphi_2\rangle = \tilde{A}\,|00\rangle + \tilde{B}\,|01\rangle + \tilde{C}\,|10\rangle + \tilde{D}\,|11\rangle\,. \tag{10}$$

Como trata-se de qubit, então podemos usar o critério de Wooters [7] para verificar se esse estado é ou não separável. Pode-se verificar que para estados puros a concurrência é:

$$S(R) = -\mathrm{tr}\,[R\log(R)] = 2|\tilde{A}\tilde{D} - \tilde{B}\tilde{C}|. \tag{11}$$

Para um desenvolvimento mais detalhado apresentamos:

$$\tilde{A}\tilde{D} = (\alpha_1\gamma_1 - \alpha_2\overline{\gamma_2})(\beta_1\delta_1 - \beta_2\overline{\delta_2}) \tag{12}$$

e

$$\tilde{B}\tilde{C} = (\alpha_1\delta_1 - \alpha_2\overline{\delta_2})(\beta_1\gamma_1 - \beta_2\overline{\gamma_2}) \tag{13}$$

de modo que

$$\tilde{A}\tilde{D} = \alpha_1\gamma_1\beta_1\delta_1 - \alpha_1\gamma_1\beta_2\overline{\delta_2} - \alpha_2\overline{\gamma_2}\beta_1\delta_1 + \alpha_2\overline{\gamma_2}\beta_2\overline{\delta_2} \tag{14}$$

e

$$\tilde{B}\tilde{C} = \alpha_1\delta_1\beta_1\gamma_1 - \alpha_1\delta_1\beta_2\overline{\gamma_2} - \alpha_2\overline{\delta_2}\beta_1\gamma_1 + \alpha_2\overline{\delta_2}\beta_2\overline{\gamma_2}. \tag{15}$$

Alguns termos já reconhecidos como iguais já podem ser cancelados. Então:

$$S(R) = 2|(\delta_1\overline{\gamma_2} - \gamma_1\overline{\delta_2})(\alpha_1\beta_2 - \alpha_2\beta_1)| \tag{16}$$

Lembrando do fato que $\alpha_1\beta_2 - \alpha_2\beta_1 = 0$, logo a concurrência é nula. Mostrando que esse estado também é separável nos complexos.

IV. CONCLUSÃO

Propomos verificar se o produto de um par de quaterbits puros pode ser um qubit não fatorável. Para verificar essa hipótese, definimos dois quaterbits arbitrários na forma de singletos e em seguida fizemos o produto tensorial. A partir do resultado desse produto, estabelecemos as condições necessárias para que o estado resultante esteja somente nos complexos, ou seja, o produto de quaterbits gera um qubit bipartido. Então, verificamos que o qubit bipartido resultante ainda continua infatorável. Concluindo que o produto tensorial de dois quaterbits puros não geram um qubit puro bipartido não fatorável.

Para investigação futura, deve-se avaliar se essa característica se mantêm numa mistura de estados. E avaliar o impacto desse resultados sob alguns protocolos de comunicação que possuem a separabilidade ou não de estados como engrenagem principal de funcionamento.

REFERÊNCIAS

[1] M. Nielsen and I. Chuang, *Quantum Information and Computation*, first ed. 2000.

[2] A. Zeilinger, *Long-Distance Quantum Cryptography with Entangled Photons.*, International Society for Optics and Photonics Optics East, 2007.

[3] W. Tittel et al, *Quantum Cryptography Using Entangled Photons in Energy-Time Bell States*, Physical Review Letters 2000.

[4] G. Birkhoff and J. Von Neumann, *The Logic of Quantum Mechanics*, Annals of mathematics 1936.

[5] F. Jianjia and R. Joynt, *Numerical Computations of Separability Probabilities*, 2014.

[6] M. C. Caves, C. A. Fuchs, and P. Rungta. *Entanglement of Formation of an Arbitrary State of Two Rebits* Foundations of Physics Letters 2001

[7] W. K. Wootters, *Entanglement of Formation of an Arbitrary State of Two Qubits*, Physical Review Letters, (1998): 2245.

[8] W. K. Wootters, *Entanglement of Formation and Concurrence* Quantum Information and Computation 2001.