Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação
Departamento de Telemática

Estudo do Emaranhamento Quântico com base na Teoria da Codificação Clássica

Autora: Wanessa Carla Gazzoni

Orientador: Prof. Dr. Reginaldo Palazzo Júnior
(DT-FEEC/UNICAMP)

Co-Orientador: Prof. Dr. Carlile Lavor
(DMA-IMECC/UNICAMP)

Banca Examinadora:

Prof. Dr. Reginaldo Palazzo Júnior	**DT-FEEC/UNICAMP**
Prof. Dr. Amir Ordacgi Caldeira	**DFMC-IFGW/UNICAMP**
Dr. Antonio Carlos Aido de Almeida	**Intelekto Consultoria**
Prof. Dr. Henrique Lazari	**IGCE/UNESP-Rio Claro**
Prof. Dr. Marcelo Firer	**DM-IMEEC/UNICAMP**
Prof. Dr. Carlos Eduardo Câmara	**FCC/USF** (suplente)
Prof. Dr. Max Henrique Machado Costa	**FEEC/UNICAMP** (suplente)
Prof. Dr. Romis Ribeiro Faissol Attux	**FECC/UNICAMP** (suplente)

Tese apresentada na Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica.

Campinas - SP
15 de Agosto de 2008

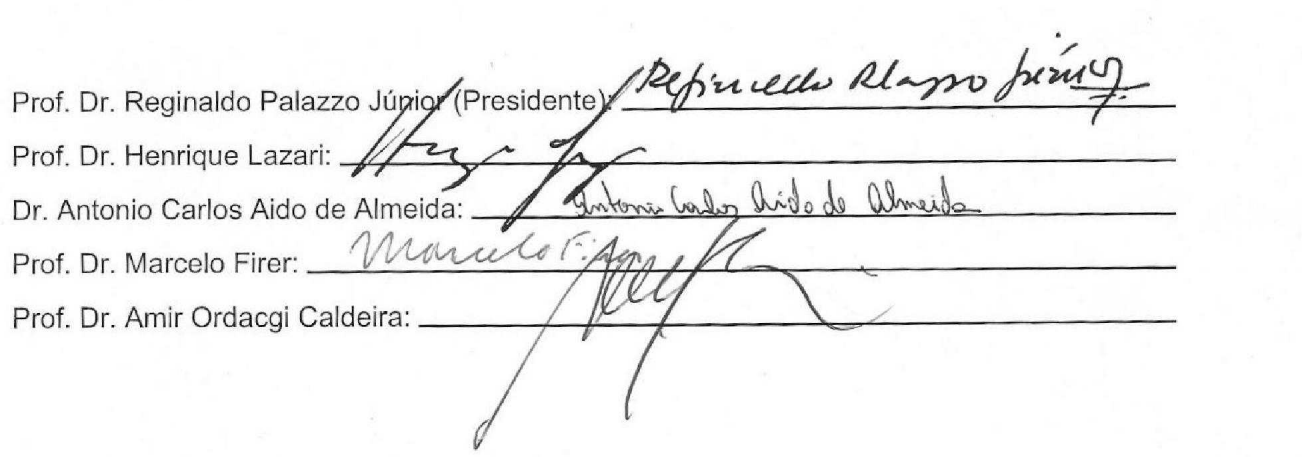
FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA
DA ÁREA DE ENGENHARIA E ARQUITETURA- BAE - UNICAMP

G259e	Gazzoni, Wanessa Carla Estudo do Emaranhamento Quântico com base na Teoria da Codificação Clássica / Wanessa Carla Gazzoni. – Campinas, SP: [s.n.], 2008. Orientadores: Reginaldo Palazzo Júnior; Carlile Lavor. Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação. 1. Emaranhamento quântico. 2. Teoria da codificação. 3. Códigos de controle de erros (Teoria da informação). I. Palazzo Júnior, Reginaldo. II. Lavor, Carlile. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título

Título em Inglês:	Analysis of quantum entanglement based on classical coding theory.
Palavras-chave em Inglês:	Separability criterion, Entangled states, Classical coding theory, Information error protection.
Área de concentração:	Telecomunicações e Telemática
Titulação:	Doutor em Engenharia Elétrica
Banca Examinadora:	Henrique Lazari, Antonio Carlos Aido de Almeida, Marcelo Firer e Amir Ordacgi Caldeira.
Data da defesa:	15/08/2008
Programa de Pós-Graduação:	Engenharia Elétrica

Estudo do Emaranhamento Quântico com base na Teoria da Codificação Clássica

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Wanessa Carla Gazzoni e aprovada pela banca examinadora. Campinas, 15 de agosto de 2008.



Tese apresentada na Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica.

Campinas - SP
Agosto de 2008

Resumo

Este trabalho apresenta algumas contribuições para um melhor entendimento do emaranhamento quântico e suas aplicações. Com o propósito de obter a classificação de estados quânticos puros arbitrários em separáveis ou emaranhados, apresentamos um critério de separabilidade do qual tal classificação decorre. Este critério está baseado em uma interpretação homológica-geométrica, que nos permitiu formalizar algumas conclusões acerca da quantificação do emaranhamento em estados puros arbitrários com três qubits. A partir desta interpretação, foi possível também associar a descrição do conteúdo dos *kets* de um estado puro arbitrário a conceitos de teoria da codificação clássica. Tendo como base esta associação, propomos uma forma bastante simplificada para determinar a descrição matemática de estados puros arbitrários que satisfazem o máximo emaranhamento global. De acordo com conceitos da teoria da codificação, analisamos os estados de máximo emaranhamento global com relação à proteção contra erros que esses estados possuem. Neste contexto, apresentamos uma nova classe de estados que ainda não havia sido mencionada na literatura.

Palavras-chave: estados quânticos puros arbitrários, critério de separabilidade, máximo emaranhamento global, teoria da codificação clássica, proteção de informação contra ação de erros.

Abstract

In this thesis we present some contributions to a better understanding of quantum entanglement and its applications. With the purpose of obtaining a classification of the arbitrary pure quantum states as separable or entangled, a separability criterion is presented. This criterion is based on an homologic-geometric interpretation which allowed us to formalize some conclusions on the entanglement quantification of arbitrary pure states with three qubits. From this interpretation, it was possible to associate a description of the kets' content of an arbitrary pure state with the concepts of the classical coding theory. Based on this association, we propose a simplified form to determine a mathematical description of arbitrary quantum states satisfying the maximum global entanglement. From the concepts of coding theory we considered the states of maximum global entanglement with respect to its inherent error protection. In this context, we present a new class of states satisfying all the previous properties and which were not known in the open literature.

Keywords: arbitrary pure quantum states, separability criterion, maximally entangled states, classical coding theory, information error protection.

Aos que se esforçam a entender o significado real da palavra paciência ao longo da vida. Aos que percebem a grandeza de ser e conviver com o humano, demasiado humano.

Agradecimentos

Como bem disse o escritor Antonio Machado: “Não há caminho; caminho se faz ao andar”. Esses agradecimentos referem-se às pessoas estiveram ao meu lado nesta caminhada.

Ao meu orientador, Reginaldo Palazzo Júnior, que me ensinou o caminho da pesquisa, confiando a mim sua dedicação e seus conhecimentos. Agradeço de coração esta confiança no nosso trabalho, por me dar tantas oportunidades de cada vez mais aprender e por tudo o que me ensinou em nossas tantas conversas.

Ao meu co-orientador, Carlile Lavor, que também dedicou a este projeto parte de sua atenção. Ao professor Amir Caldeira que nos deu a oportunidade de apresentar partes desse trabalho nos encontros do grupo de pesquisa por ele chefiado sobre Informação Quântica... E pelos famosos “alvarás estendidos”.

Aos membros da banca que constituíram a comissão julgadora e ao professor Romis Attux pelas sugestões e críticas que apresentaram com relação a esta proposta, contribuindo, desta forma, para que a versão final deste trabalho fosse aprimorada.

Ao irmão e aos pais maravilhosos que tenho, cujo apoio nunca me faltou. A eles eu devo uma lição que muitas vezes apliquei durante o desenvolvimento do trabalho: *realização vem do trabalho de todos os dias e da constante perseverança*.

Ao meu namorado Eduardo pelo carinho e atenção com o qual tem me acompanhado neste percurso e pela pessoa melhor que sou desde que chegou.

A minha amiga Ana Monteiro por constituir definitivamente uma parte da minha família aqui em Campinas.

Ao meu grande amigo Rodrigo Gusmão Cavalcante por ter estado sempre ao meu lado. Nunca vou esquecer de tudo o que compartilhamos no LTIA e fora dele. Ao também amigo Giuliano La Guardia pelo carinho e zêlo com o qual me estendeu os braços tantas vezes.

As minhas amigas Andréa, Luzinete e Clarice por tudo: por se darem ao trabalho de compreender minhas maluquices e respeitá-las, pelos milhões de telefonemas e cafés, pelos tantos conselhos sempre tão valiosos, pelas boas risadas, pelos choros tão sentidos e por, em total confiança, me emprestarem um pouquinho o Henrique e o Gustavo para eu brincar de *tia*.

Ao apoio financeiro da bolsa de estudos prestado pela CAPES e pela ajuda financeira para a participação em eventos cedida pela CNPq e FAPESP. E, finalmente, aos que trabalharam e trabalham de forma séria e honesta para o desenvolvimento da UNICAMP.

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução Geral do Trabalho

Este trabalho tem como objetivo contribuir para um melhor entendimento dos estados quânticos emaranhados, no que se refere à descrição matemática.

A primeira questão abordada neste contexto consiste em classificar os estados quânticos em separáveis e emaranhados. Para isso, propusemos um critério de separabilidade a partir do qual estados puros arbitrários com n *qubits* podem ser assim classificados.

Contudo, reconhecer quais estados são emaranhados não é suficiente para uma descrição matemática completa desta classe de estados. Observamos que as tarefas de processamento de informação executadas de forma eficiente, somente no contexto da mecânica quântica, estão fundamentadas em estados quânticos emaranhados que satisfazem também as condições quanto ao máximo emaranhamento global, segundo a medida estabelecida por Meyer-Wallach.

De acordo com interpretações decorrentes do critério de separabilidade proposto, estabelecemos uma nova descrição para esta medida. Com base nesta proposta, apresentamos uma forma sistemática de descrever matematicamente estados arbitrários de máximo emaranhamento global, que está diretamente relacionada à definição de códigos binários lineares e algumas classes de códigos binários não-lineares.

Considerando as várias classes de estados de máximo emaranhamento global que podem ser obtidos segundo esta condição, retornamos ao contexto das tarefas de processamento da informação fundamentadas nos estados de emaranhamento global máximo. Nestas tarefas, a informação a ser transportada ou armazenada é associada aos conjuntos de *kets* do estado, escolhido para esta aplicação. A transmissão de um estado através de um canal é um processo suscetível a erros, de forma que podemos estabelecer que um estado mais eficiente quanto à execução de alguma tarefa é aquele que apresenta maior proteção à informação contra erros que possam vir a ocorrer. Neste contexto, uma questão interessante consiste em determinar se há estados de máximo emaranhamento global ou classes desses que sejam mais eficientes.

Uma vez estabelecido que as seqüências que compõem os *kets* que definem o estado de máximo emaranhamento global escolhido decorrem da definição de um código binário linear (os códigos não-lineares foram desconsiderados neste estudo), então determinar a classe de estados mais eficientes quanto à proteção de erros é um problema similar à definição de códigos binários

clássicos com boa capacidade de correção de erros.

De acordo com tais considerações e conceitos de teoria da codificação, obtivemos justificativas acerca da vasta utilização dos estados quânticos conhecidos como estados *GHZ* generalizados e destacamos uma nova classe de estados de máximo emaranhamento global que executam as tarefas de processamento de forma eficiente e que ainda não haviam sido destacadas na literatura.

Salientamos que havia um interesse pré-estabelecido quanto aos estados de máximo emaranhamento global. Como pode ser encontrado na literatura, essa característica é verificada apenas para os estados puros, donde decorre o estudo restrito a estados quânticos desta classe.

1.1 Estrutura da Tese

Este trabalho está organizado na seguinte forma. No Capítulo 2, apresentamos os conceitos matemáticos da física quântica que são necessários para o entendimento da proposta. Além disso, mencionamos um pouco da história do estudo do emaranhamento e das primeiras e principais contribuições acerca de suas aplicações. No Capítulo 3, apresentamos um resumo das propostas encontradas na literatura quanto à classificação e quantificação do emaranhamento. No Capítulo 4, propomos um critério de separabilidade para estados quânticos puros com três *qubits* e apresentamos uma interpretação homológica-geométrica para o conjunto de equações que definem este critério. Com base nesta interpretação, propomos no Capítulo 5 um critério de separabilidade para estados quânticos puros com n *qubits* e a respectiva implementação computacional.

A partir de algumas constatações obtidas pela análise do critério de separabilidade e as devidas associações, descrevemos no Capítulo 6 a nossa interpretação acerca dos estados com três *qubits* de máximo emaranhamento global e esboçamos a decorrente generalização para estados puros arbitrários com n *qubits*. Tal generalização está fundamentada em conceitos de teoria da codificação que, por esse motivo, são mencionados no Capítulo 7. Decorrente das associações e fundamentos mencionados, apresentamos no Capítulo 8 uma nova medida de máximo emaranhamento global e uma forma sistemática de descrever matematicamente estados puros arbitrários de máximo emaranhamento global. De acordo com essses resultados, analisamos quais são os estados que oferecem maior proteção à informação que transportam ou armazenam contra a ação de erros durante a execução de uma tarefa de processamento.

Capítulo 2

Fundamentos

Penso em minha vida na física como dividida em três períodos. No primeiro período, trabalhei com a impressão de que Tudo são Partículas. Chamo meu segundo período de Tudo são Campos...Agora fui tomado por uma nova visão, a de que Tudo são Informações.

John Archibald Wheeler

Entre todos os questionamentos que esta reflexão de John Wheeler pode gerar, um desses pode ser resumido da seguinte forma: "Podemos pensar então que partículas, campos ... 'Tudo' são informações?"

Eis uma questão intrigante, se pensarmos na riqueza, em termos da cardinalidade, deste "Tudo".

Se a inquietação for demasiada ao ponto de buscarmos o total convencimento a respeito, encontraríamos ainda a afirmação de Rolf Landauer de que *a informação é física*, [71], donde poderíamos concluir que todo e qualquer *ente* físico pode representar *informação*. Ou seja, o "Tudo" de Wheeler está de volta às nossas mentes!

Mas como definimos *informação*? Na busca pela resposta, nossa mente clássica exibirá muitos dos exemplos já vastamente apresentados pela literatura: cara ou coroa, lâmpada acesa ou apagada, seta apontando para cima ou para baixo, uma esfera girando para direita ou para a esquerda, entre tantos outros. Todas essas têm o mesmo princípio: qualquer escolha entre duas possibilidades igualmente prováveis consiste de uma informação. No caso do *jogo de cara ou coroa*, quando jogamos uma moeda para o alto, o resultado só pode ser cara ou coroa. Temos, portanto, duas possibilidades igualmente prováveis. Quando a moeda cai e observamos qual lado está para cima, descobrimos qual das possibilidades se concretizou. Esta forma de descoberta consiste de uma *informação*. Na linguagem usual da computação, esta descoberta consiste de *um bit*.

Em termos do "Tudo" do Universo, a classe de exemplos apresentados é bastante reduzida. Todos consistem de *entes* físicos do mundo clássico, que satisfazem perfeitamente as regras da mecânica Newtoniana, ou, simplesmente, mecânica clássica.

Contudo, uma vez que a *informação é física*, é instrutivo considerar o que as teorias físicas têm a nos dizer sobre informação. Estas teorias, porém, vão além da mecânica clássica. Sabemos que o nosso Universo é regido fundamentalmente pelas leis da mecânica quântica e, neste contexto, as possibilidades de *entes* físicos que podem representar informação passa a ser, fundamentalmente, o "Tudo" do Universo.

Desde os primórdios da teoria quântica, ficou claro que as idéias clássicas sobre a informação precisavam ser revistas sob este novo contexto, cujos princípios são radicalmente diferentes dos da mecânica clássica. Por exemplo, os átomos e seus componentes, agora passíveis de representar informação, não obedecem às leis da mecânica Newtoniana, que até então descrevia o comportamento de tudo que tinha característica física, ou seja, de tudo o que representa informação, donde fica claro que a descrição acerca da informação precisava ser reformulada.

Esta reformulação leva em consideração algumas propriedades da mecânica quântica que desafiam o senso clássico comum, de forma tal que, segundo Schumacher, um especialista na área de Informação Quântica, *é sempre divertido aprender algo de novo a respeito da mecânica quântica*.

Entre outras propriedades próprias de estranheza ao senso clássico, citamos:

1. a informação quântica, de forma geral, não pode ser copiada com perfeita fidelidade (teorema da não-clonagem, que pode ser encontrado em [121]);

2. o ato de adquirir informação acerca de um sistema físico inevitavelmente o destruirá;

3. dois estados quânticos podem compartilhar a propriedade de *emaranhamento*. Dados estados com tal propriedade, o resultado da medida sobre um desses interfere no resultado da medida efetuada sobre o outro, ainda que esses estejam separados por uma longa distância [81].

O emaranhamento, a propriedade mais interessante da mecânica quântica, tem sido tema de muitas pesquisas, como veremos no Capítulo 3, embora um completo entendimento deste fenômeno e suas aplicações ainda não esteja estabelecido. Entretanto, por se tratar da propriedade que caracteriza o espaço no qual as informações serão descritas, as implicações do emaranhamento neste contexto também devem ser incorporadas. Para isso, é necessário que se defina como a *informação quântica* é representada e quais são as regras do jogo no mundo da mecânica quântica. Tais considerações são apresentadas na próxima seção.

2.1 Conceitos Iniciais

O objetivo deste seção é apresentar a descrição matemática da informação quântica. O primeiro passo é, então, definir a unidade básica desta informação, que denominaremos *qubit*[1].

[1]Outras formas admitidas para a tradução do inglês são *q-bit* ou qbit.

2.1.1 Os *qubits*

Os *bits quânticos* ou *qubits* podem ser entendidos como estados de um sistema físico e são definidos a partir do seguinte postulado:

A qualquer sistema físico isolado existe um espaço vetorial complexo associado com produto interno definido (espaço de Hilbert), conhecido como espaço de estados do sistema, [81].

Desta informação é possível concluir que dois estados de um sistema físico podem ser associados a vetores (unitários) no espaço de Hilbert. Sendo este espaço complexo, dois vetores que formam uma *base* (no sentido de que todos os vetores do espaço podem ser descritos em função desses) podem ser representados por

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.1}$$

Tais representações vetoriais foram resumidas nas formas $|0\rangle$ e $|1\rangle$, conhecidas como notação de Dirac[2], e essas constituem a base para a representação dos *qubits*. Um exemplo usual de *qubits* são os dois estados de um elétron orbitando em um átomo. Um deles é o estado fundamental, denotado por $|0\rangle$ e o outro o estado excitado, representado por $|1\rangle$.

Pela característica vetorial do espaço onde são definidos os estados, podemos afirmar que, escolhidos os estados $|0\rangle$ e $|1\rangle$, então a combinação linear entre esses gera um outro estado que também está definido neste espaço.

Explicitamente, um estado na forma[3]

$$|\psi\rangle_1 = a|0\rangle + b|1\rangle, \tag{2.2}$$

onde a e $b \in \mathbb{C}$ e $|a|^2 + |b|^2 = 1$ também pode representar um *qubit* .

Como $|a|^2 + |b|^2 = 1$, podemos reescrever a equação (2.2) na forma

$$|\psi\rangle_1 = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle, \tag{2.3}$$

onde θ e φ são números reais. Tais números definem um ponto sobre a superfície de uma esfera de raio unitário no espaço de Hilbert, $\mathbb{C}^2$. Esta esfera é geralmente denominada *esfera de Bloch* e é apresentada na Figura 2.1.

De acordo com esta interpretação, podemos concluir que *todos* os pontos na superfície desta esfera representam estados quânticos com um *qubit* [81]. Ou seja, há uma quantidade *contínua* de possíveis representações para estados de um *qubit*!

A propriedade que garante que esta quantidade contínua de estados na forma de (2.2) sejam definidos e representem informação é conhecida como *princípio da superposição*. A interpretação

[2] A forma $|.\rangle$ é chamada *ket*.

[3] O índice i em $|.\rangle_i$ indica o número de *qubits* que constituem o estado.

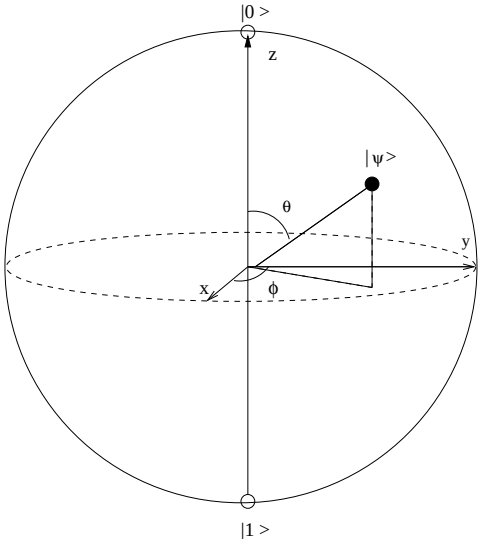


Figura 2.1: Representação de um *qubit* na esfera de Bloch.

para uma superposição de estados é estabelecida da seguinte forma. Um *qubit* definido como em (2.2) está no estado $|0\rangle$ com probabilidade $|a|^2$ e no estado $|1\rangle$ com probabilidade $|b|^2$. Ou seja, até que se efetue uma *medida*, *a priori* um estado superposto pode estar no estado $|0\rangle$, no estado $|1\rangle$ ou em uma combinação destes dois estados, simultaneamente.

Como foi visto, embora o *bit clássico* também represente estados de um sistema, as possibilidades para esses estados são denotadas por "0" ou "1", e são mutuamente exclusivas (ou "0 " ou "1"), o que faz das implicações do princípio da superposição sobre estados de um *qubit* absolutamente inusitadas quanto às perspectivas até então estabelecidas pelo mundo clássico[4].

O princípio da superposição quando aplicado a sistemas com mais de um *qubit* (sistemas compostos) implica em outras propriedades ainda mais intrigantes do mundo quântico. A principal dessas é o *fenômeno de emaranhamento*. De forma pouco precisa, estando dois estados emaranhados, qualquer operação (como a de medida, por exemplo) efetuada sobre um é induzida sobre o outro, ainda que os estados tenham sido separados por uma distância qualquer. É por esta característica que o emaranhamento é chamado de uma *fantasmagórica ação à distância* [42].

[4]Uma comparação interessante entre a informação clássica e a quântica foi estabelecida em [81]: que quantidade de informação clássica pode ser armazenada em um *qubit* de forma que ela possa ser extraída e utilizada. *A priori*, podemos deduzir que essa quantidade é infinita. Isso porque para especificarmos um estado quântico temos que definir sua latitude e longitude correspondente à representação na superfície da esfera de Bloch. Estes números codificam uma cadeia longa de bits. Por exemplo, 011101101... poderia ser codificado como sendo um estado com latitude 01 grau 11 minutos e 01101... segundos. Utilizamos então infinitos bits 0 e 1 nesta descrição e concluímos que o *qubit* carrega uma quantidade de informação clássica infinita. Embora pareça correto, o raciocínio não o é. Podemos codificar uma quantidade infinita de informação clássica em um único *qubit*, mas não há como extrair essa informação. A mais simples tentativa de "ler" o estado do *qubit*, que seria uma medida usual direta, resultaria em $|0\rangle$ ou $|1\rangle$. Esta medida compararia a probabilidade associada ao *qubit* de estar no estado $|0\rangle$ e à de estar no estado $|1\rangle$. A maior probabilidade indica o estado final do *qubit*. Entretanto, qualquer medida adotada "apaga" todas as informações contidas no *qubit*, com exceção daquela que de fato revela. *É como se o qubit contivesse informações ocultas que podemos manipular, mas não podemos acessar diretamente.*

Como veremos na Seção 2.2, o emaranhamento sempre causou muita discussão na comunidade científica desde 1935, com o artigo [42] de Einstein, Podolsky e Rosen, quando o fenômeno foi, pela primeira vez, abordado. Os questionamentos, as teorias, a busca por aplicações e a tentativa da verificação experimental destas nunca mais cessou. E, em nossos dias, a busca pelo completo entendimento do emaranhamento, suas aplicações e particularidades continua a passos firmes.

Como foi mencionado anteriormente, o emaranhamento é definido sobre sistemas com mais de um *qubit*. Mas, como descrever matematicamente *sistemas compostos*? Tal definição é dada por um postulado da mecânica quântica, que é apresentado a seguir.

O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas físicos individuais. Se os sistemas forem numerados de 1 até n e o sistema i for representado por $|\psi_i\rangle$*, decorre que o estado do sistema composto será* $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$, [81].

A operação de produto tensorial citada é uma forma de se *juntar* espaços vetoriais para formar espaços vetoriais maiores [81]. A definição e principais propriedades do produto tensorial são apresentadas na próxima subseção.

2.1.2 Produto tensorial

Suponha que V e W sejam espaços vetoriais de dimensões m e n, respectivamente, e que ambos sejam espaços de Hilbert. Assim, $V \otimes W$ (leia-se *V tensor W*) é um espaço vetorial de dimensão mn. Antes de iniciarmos o estudo de $V \otimes W$, é necessário que se apresentem algumas propriedades de V e W.

Sendo V um espaço de Hilbert, então existe um produto interno associado a este espaço pela própria definição. Tal produto será denotado na forma $\langle\varphi|\psi\rangle$ e satisfaz as condições a seguir, para $a, b \in \mathbb{C}$ e $|\varphi\rangle, |\psi\rangle, |u\rangle, |v\rangle \in V$, [81].

1. $\langle\psi|\varphi\rangle = \langle\varphi|\psi\rangle^*$, onde $*$ é o complexo conjugado,
2. $\langle\varphi|(a|u\rangle + b|v\rangle)\rangle = a\langle\varphi|u\rangle + b\langle\varphi|v\rangle$,
3. $\langle\varphi|\varphi\rangle > 0$ se $|\varphi\rangle \neq 0$.

A norma de um vetor $|\varphi\rangle$ é dada por

$$||\varphi\rangle|| = \sqrt{\langle\varphi|\varphi\rangle}.$$

A notação $\langle\varphi|$ é utilizada para o vetor dual do vetor $|\varphi\rangle$ e é definida de forma que

$$\langle\varphi|(|v\rangle) = \langle\varphi|v\rangle, \quad \forall\ |v\rangle \in V.$$

Se $|\varphi\rangle = a|0\rangle + b|1\rangle$ e $|\psi\rangle = c|0\rangle + d|1\rangle$, então as matrizes que representam o produto interno e o transposto deste são, respectivamente,

$$\langle\varphi|\psi\rangle = \begin{bmatrix} a^* & b^* \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = a^*c + b^*d,$$

$$|\varphi\rangle\langle\psi| = \begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} c^* & d^* \end{bmatrix} = \begin{bmatrix} ac^* & ad^* \\ bc^* & bd^* \end{bmatrix}.$$

Apresentada a caracterização dos espaços de Hilbert V e W, a partir dos quais se define o produto tensorial $V \otimes W$, passamos a descrever as propriedades desta operação.

Os elementos de $V \otimes W$ são combinações lineares dos produtos tensoriais $|v\rangle \otimes |w\rangle$, que satisfazem as seguintes condições, para $z \in \mathbb{C}, |v\rangle, |v_1\rangle, |v_2\rangle \in V$ e $|w\rangle, |w_1\rangle, |w_2\rangle \in W$, [81].

- $z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$,
- $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = (|v_1\rangle \otimes |w\rangle) + (|v_2\rangle \otimes |w\rangle)$,
- $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = (|v\rangle \otimes w_1\rangle) + (|v\rangle \otimes |w_2\rangle)$.

Utilizamos as notações $|v\rangle|w\rangle$ ou $|vw\rangle$ para o produto tensorial $|v\rangle \otimes |w\rangle$. Note que o produto tensorial é não comutativo e, por isso, a notação deve preservar a ordem.

Em termos de praticidade, o produto tensorial entre dois espaços é representado matricialmente e definido em termos de dois operadores lineares definidos nestes espaços. Dados dois operadores lineares A e B definidos sobre os espaços V e W, respectivamente, o operador linear $A \otimes B$ em $V \otimes W$ é descrito por

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle, \tag{2.4}$$

onde $|v\rangle \in V$ e $|w\rangle \in W$. A matriz que representa $A \otimes B$ é dada por

$$A \otimes B = \begin{bmatrix} A_{11}B & . & . & . & A_{1m}B \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ A_{m1}B & . & . & . & A_{mm}B \end{bmatrix},$$

onde A e B são matrizes de ordem m e n, respectivamente, donde decorre que a matriz $A \otimes B$ tem ordem mn.

Por exemplo, dadas as matrizes

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

o produto tensorial $A \otimes B$ é

$$A \otimes B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Apesar da generalidade de casos nos quais se pode definir esta operação, o que é de nosso interesse é o produto tensorial entre dois ou mais estados que, como já vimos, estão associados vetores unitários.

Por exemplo, se considerarmos os estados $|0\rangle$ e $|1\rangle$, o resultado do produto tensorial $|0\rangle \otimes |1\rangle$ é

$$|0\rangle \otimes |1\rangle = |01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

O estado representado por $|0\rangle \otimes |1\rangle$ é um estado quântico com dois *qubits* e, portanto, consiste de um sistema composto. Um estado com dois *qubits* arbitrário é definido pela forma

$$|\psi\rangle_2 = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle,$$

com a restrição

$$|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1.$$

Observe que $|\psi\rangle_2$ é um vetor de um espaço complexo 4-dimensional.

A operação de produto tensorial pode ser definida entre mais de dois estados, por exemplo,

$$|0\rangle \otimes |1\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

que é um vetor de um espaço complexo 8-dimensional. Indutivamente, temos que um estado com n *qubits* é um elemento do espaço vetorial complexo 2^n- dimensional [81].

Tendo como base os conceitos e definições apresentados, é possível descrever de forma mais específica o *emaranhamento*. O objetivo das próximas seções é apresentar um pouco da história e da literatura associada ao tema[5], bem como as principais aplicações para os estados emara-

[5]Há uma grande quantidade de contribuições acerca do entendimento do emaranhamento quântico na literatura. Os contextos de tantos trabalhos, como é evidente, são absolutamente variados, de forma que é uma tarefa não passível de realização, uma abordagem tão vasta. Algumas referências interessantes são [17, 52, 67, 73, 79, 114].

nhados. Como foi especificado no Capítulo 1, nosso interesse reduz-se ao emaranhamento entre estados puros e, por esse motivo, este estudo refere-se apenas a esta subclasse[6].

2.2 Um Pouco de História

A caracterização do contexto que resultou na definição do fenômeno que, *a posteriori* foi denominado *entanglement*, foi pela primeira vez abordada no belíssimo artigo de Einstein, Podolsky e Rosen publicado em 1935, [42], que formou a base para as primeiras comprovações teóricas [7] e experimentais [2].

Motivado pelo trabalho de Einstein e seus colaboradores, Schrödinger descreve em [96] uma situação interessante e que proporciona uma idéia clara das facetas às quais estamos sujeitos quando consideramos as propriedades do mundo quântico e analisamos as suas implicações sob o ponto de vista clássico.

Imaginemos o seguinte experimento: dentro de uma caixa absolutamente fechada há uma gata que pode estar *viva* ou *morta*. Juntamente com a gata, sabe-se que há na caixa um átomo *instável* que pode ter se tornado *estável*, resultando desta transição uma energia suficiente para ativar algum mecanismo ou desarranjo no ambiente interno da caixa que resultaria em uma morte rápida para a gata. A única informação que conhecemos é a probabilidade de o átomo em questão sofrer tal transição, não sendo possível estimar *quando* isso acontece.

Podemos pensar neste experimento macroscópico no contexto quântico. Neste caso, teríamos os estados $|viva\rangle$ e $|morta\rangle$ e $|\text{instável}\rangle$ e $|\text{estável}\rangle$, num sistema formado por duas partes: a gata e o átomo. Considerando que a probabilidade do átomo se tornar estável seja b e de ser estável seja a e assumindo o princípio da superposição, podemos dizer que o estado superposto

$$a|\text{instável}\rangle|viva\rangle + b|\text{estável}\rangle|morta\rangle \tag{2.5}$$

existe e deve ser considerado.

Em outras palavras, de acordo com este experimento imaginário, a gata poderia estar *viva* e *morta* ao mesmo tempo, o que, em termos de teorias comprovadas cientificamente, é uma conclusão eloqüente.

Ao *paradoxo da gata*, descrito pela equação (2.5), Schrödinger batizou como *entanglement*, que, traduzido para a nossa língua, resultou em *emaranhamento*.

Mais do que causar dúvidas, na década de 90 surgiram as primeiras considerações que tratavam o emaranhamento como um recurso disponível na Natureza [18]. Nesta época, também foram apresentadas as primeiras discussões que tratavam o emaranhamento como ferramenta eficiente para a realização de tarefas associadas ao processamento de informações que não podiam ser implementadas com recursos clássicos. Exemplos destas tarefas são a *codificação superdensa*,

[6] Além dos estados puros, temos os estados quânticos mistos. Tais estados constituem uma combinação estatística de estados puros e são considerados mais gerais do que os primeiros. Alguns detalhes dos estados quânticos mistos serão apresentados no Capítulo 3.

discutida na Seção 2.4.2 a seguir, o teletransporte e a criptografia quântica. Ainda nos anos 90, surgiram as primeiras contribuições no contexto de *algoritmos quânticos*, tais como o algoritmo de Shor para a fatoração [99] e o algoritmo de Grover para efetuar buscas em listas de dados não ordenadas [54], também discutidas a seguir na Seção 2.4.1.

Dado um breve resumo do panorama inicial das pesquisas acerca do emaranhamento, iniciamos na próxima seção a formalização de alguns conceitos.

2.3 Estados Puros Emaranhados

Embora o interesse seja definir estados emaranhados, o que se observa na literatura é a definição de estados *não-emaranhados* ou *estados separáveis*. Também assim o faremos, justificando em um ponto oportuno do texto o porquê desta abordagem.

Definição 1 *Um estado puro arbitrário com n qubits* $|\psi\rangle_n$ *representado por*

$$|\psi\rangle_n = \alpha_0|00\cdots0\rangle + \alpha_1|00\cdots1\rangle + \cdots + \alpha_{2^n-2}|11\cdots0\rangle + \alpha_{2^n-1}|11\cdots1\rangle, \tag{2.6}$$

onde $\alpha_0, ..., \alpha_{2^n-1} \in \mathbb{C}$ *e* $\sum_{s=0}^{2^n-1} |\alpha_s|^2 = 1$ *é dito separável se puder ser escrito como* $|\psi\rangle_n = |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 \otimes \cdots \otimes |\varphi_n\rangle_1$*, onde* $|\varphi_1\rangle_1, |\varphi_2\rangle_1, \cdots, |\varphi_n\rangle_1$ *são estados puros com 1 qubit.*

Assim, qualquer estado que não admitir exatamente esta decomposição é considerado um estado *emaranhado*. Por exemplo, um estado com três *qubits* que só admite decomposição em um produto tensorial entre dois estados com um e dois *qubits*, respectivamente, não satisfaz a condição da Definição 1 e, por isso, é um estado emaranhado.

Seguem alguns exemplos de estados quânticos e as respectivas classificações.

Exemplo 1 *O estado* $|\delta\rangle_2 = |01\rangle$ *é um estado separável, uma vez que admite a seguinte decomposição* $|0\rangle_1 \otimes |1\rangle_1$*.*

Exemplo 2 *O estado*

$$|\xi\rangle_2 = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

pode ser reescrito na forma $|\xi\rangle_2 = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ *e, por isso, é classificado como um estado separável.*

Exemplo 3 *O estado*

$$|\psi_{EPR}\rangle_2 = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

não admite decomposição alguma, donde decorre que este é um estado emaranhado. Em particular, este estado é um representante da classe chamada EPR (Einstein-Podolsky-Rosen) ou estados de Bell que é muito citada na literatura desde que foi introduzida em [42]. Estados desta classe são estados de máximo emaranhamento.

Exemplo 4 *O estado*

$$|\mu\rangle_3 = \frac{1}{\sqrt{2}}\left(|001\rangle + |010\rangle\right)$$

admite a seguinte decomposição

$$|\mu\rangle_3 = \frac{1}{\sqrt{2}}|0\rangle \otimes \left(|01\rangle + |10\rangle\right).$$

Como esta descrição tem a forma $|\varphi_1\rangle_1 \otimes |\varphi_2\rangle_2$, então esta não satisfaz a condição explicitada na Definição 1 e, por isso, $|\mu\rangle_3$ é classificado como emaranhado.

Exemplo 5 *O estado*

$$|\psi_{GHZ}\rangle_3 = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

não admite decomposição alguma e é também um estado emaranhado. Este é um representante da classe de estados emaranhados com três qubits conhecida como GHZ [53] e é, tais como os pares EPR's,um estado de máximo emaranhamento.

Exemplo 6 *Outra classe de estados emaranhados com três qubits é representada pelo estado conhecido como W [116], dado por*

$$|\psi_W\rangle_3 = \frac{1}{\sqrt{3}}\left(|011\rangle + |101\rangle + |110\rangle\right).$$

Exemplo 7 *Os estados emaranhados do tipo GHZ do Exemplo 5 podem ser generalizados pela forma*

$$|\psi_{GHZ}\rangle_n = \frac{1}{\sqrt{2}}\left(|00\cdots0\rangle + |11\cdots1\rangle\right).$$

Todos os estados com n qubits na forma de $|\psi_{GHZ}\rangle_n$ são estados emaranhados. Mais do que isso, trata-se de uma classe, conhecida como GHZ generalizada, que contém estados de máximo emaranhamento.

Embora o conceito de estados de *máximo emaranhamento* ainda não tenha sido definido, salientamos esta propriedade das classes de estados *EPR*, *GHZ* e *GHZ* generalizado pois esta caracterização será estudada em detalhes nos Capítulos 6 e 8.

Observando os exemplos apresentados, temos dois fatos a ressaltar. O primeiro diz respeito à justificativa do porquê definir estados separáveis ao invés de estados emaranhados. Quando o número de *qubits* é maior que dois, a análise e descrição das possibilidades de haver emaranhamento entre os *qubits* tornam-se trabalhosas. Considere, por exemplo, que, para estados com três *qubits*, podemos ter emaranhamento na forma de um *EPR* nos dois primeiros *qubits*, admitindo a separação do terceiro *qubit* com relação ao primeiro grupo. Estados satisfazendo essa descrição são emaranhados, mas de uma forma distinta dos estados que não admitem decomposição de nenhum de seus *qubits*, como definido no Exemplo 5. Uma análise completa a respeito das classes de emaranhamento em estados com três *qubits* foi apresentada em [122], do

qual decorreu a verificação de que há dois tipos distintos de emaranhamento para estes estados. Considerações interessantes acerca do emaranhamento em estados com três *qubits* também podem ser encontradas nas referências [25, 29, 34, 74, 104], entre outras. O estudo das diferentes classes de emaranhamento para estados com quatro *qubits* foi apresentada em [112], no qual se encontra o resultado que, para estes estados, há nove formas distintas de emaranhamento. Um estudo generalizado para as classes de emaranhamentos para estados com maior número de *qubits* pode ser encontrado em [40]. Com isso, concluímos que uma definição acerca de *estados emaranhados* deveria estabelecer, de acordo com o número de *qubits* no estado, as condições para que cada uma das classes distintas de emaranhamento fossem determinadas, o que, sem dúvida, tornaria tal definição muito menos precisa em relação à Definição 1.

Um segundo ponto que também diz respeito ao aumento do número de *qubits* no estado é acerca da complexidade (em termos de operações) para determinar se um estado pode ser completamente decomposto. Este é um problema de complexidade $O(2^n)$, onde n é o número de *qubits* no estado. Cálculos deste tipo são complicados para a computação clássica e, por isso, há um conjunto de contribuições na literatura que apresentam sugestões de formas alternativas de verificar a separabilidade de um dado estado. Tais *algoritmos* são denominados *critérios de separabilidade*.

No Capítulo 3, apresentamos as principais propostas de critérios de separabilidade da literatura, assim como as propostas referentes à diferenciação entre as formas de emaranhamento em estados puros e a quantificação dessas.

Finalizamos este capítulo apresentando as principais aplicações dos estados emaranhados. Os formalismos associados aos problemas e desenvolvimentos descritos podem ser encontrados nas referências indicadas. Vamos omiti-los a fim de proporcionar ao leitor uma leitura de curiosidades e questionamentos.

2.4 O Emaranhamento e suas Aplicações

2.4.1 Paralelismo e algoritmos quânticos

As vantagens da computação quântica e a consequente pesquisa acerca da construção do computador, softwares e internet quânticos causam grande repercussão na sociedade [12, 38]. A relação entre a computação quântica e o emaranhamento ocorre, precisamente, pelo fato de um computador quântico criar uma complexa distribuição de estados emaranhados em seus registradores de memória (*qubits*) ao executar qualquer algoritmo quântico [7]. Desta forma, o significado do emaranhamento fica estabelecido pelo fato de que, sem utilizar estados emaranhados, os algoritmos quânticos não apresentam a eficiência especificada quando comparados à computação clássica [4].

[7] Maiores argumentos a respeito desta afirmação exigem estudo das portas-quânticas, que pode ser encontrado em [81].

A idéia de associar o emaranhamento quântico às realizações de tarefas computacionais, segundo a literatura, seguiu um caminho bastante longo. O surgimento dos primeiros questionamentos acerca da suficiência dos conceitos clássicos da ciência da computação para descrever processos da Natureza ocorreu a partir dos primeiros desafios à tese forte de Church-Turing:

Qualquer processo algorítmico pode ser simulado eficientemente usando uma máquina de Turing.[8]

O primeiro desses desafios surgiu na década de 1970, quando Solovay e Strassen mostraram que é possível testar se um número inteiro é primo ou composto utilizando um algoritmo aleatório [101]. Ou seja, o teste de Solovay-Strassen tem como aspecto essencial a aleatoriedade. O algoritmo não determinava se um inteiro era primo ou composto com certeza, mas determinava se um número era *provavelmente* primo ou *provavelmente* composto. Repetindo o teste algumas vezes, era possível determinar quase com certeza se o número era primo ou composto. Logo, havia o fato de que computadores com acesso a geradores de números aleatórios seriam capazes de realizar tarefas computacionais sem solução eficiente em uma máquina de Turing [81].

Tal situação expôs a comunidade a uma nova dúvida. Existe uma forma de determinar um único modelo de computação que com garantia simule de forma eficiente qualquer modelo de computação?

Anos depois, o potencial do fenômeno quântico na computação foi sugerido por Richard Feynman na *Primeira Conferência sobre Física da Computação*, realizada em 1981. Feynman observou que parecia ser impossível simular, de maneira eficiente, a evolução de um sistema quântico num computador clássico [45].

Foi esta questão que levou Deutsch em 1985 a aliar propriedades da mecânica quântica a conceitos da ciência da computação, resultando na proposta de que um computador quântico devidamente projetado seria capaz de executar cálculos em *mundos* paralelos ao mesmo tempo [36]. É uma forma de *processamento paralelo*, cujo princípio já não era inédito na época e cuja eficiência era comprovada, uma vez que é evidente que mil processadores trabalhando simultaneamente podem resolver problemas mais depressa que um único processador [100].

O paralelismo de Deutsch, ou *paralelismo quântico*, porém, vai um pouco além disso, conduzindo a resultados bem mais impressionantes. Considere o caso de mil processadores elementares e suponha que cada um seja capaz de representar um bit de informação. Neste caso, o número de combinações de 0s e 1s que se pode obter é igual a 2^{1000}, ou, 1 seguido por 301 zeros. Para contar todas essas combinações, à razão de um trilhão de combinações por segundo, seria necessário um tempo de 10 bilhões de vezes a idade do Universo. Evidentemente, nenhum computador comum seria capaz de explorar todas as combinações obtidas. Em outras palavras, haveria muitos problemas que um computador comum com mil processadores operando em paralelo não poderia resolver em tempo útil. Entretanto, se os processadores comuns fossem substituídos por processadores quânticos, cada um capaz de representar um *qubit* de informação, todas as

[8] Em termos genéricos, *uma máquina de Turing é capaz de computar qualquer coisa que seja calculável.*

possíveis combinações de zeros e uns seriam representadas simultaneamente. Isso equivale a dizer que um computador com mil processadores quânticos em paralelo seria 2^{1000} vezes mais rápido do que o computador clássico com processadores comuns [100].

Embora Deutsch e Jozsa tenham proposto em [37] um problema que ilustrava a capacidade da computação quântica (ou seja, de operações realizadas em computadores com processadores quânticos), uma aplicação que de fato expressava a utilidade desta computação só foi apresentada por Shor, em 1996.

O algoritmo proposto por Shor em [99] é capaz de fatorar eficientemente números inteiros com centenas de dígitos, quando aplicado a um computador com processadores quânticos. A vantagem deste algoritmo sobre os clássicos é impressionante: para decompor um número inteiro com 500 dígitos em fatores primos, o melhor algoritmo clássico necessitaria de 5×10^{24} passos ou cerca de 150 mil anos na velocidade de um terahertz. Empregando as propriedades da mecânica quântica presentes nos supostos processadores, o algoritmo proposto por Shor necessitaria de 5×10^{10} passos, ou menos de um segundo na velocidade de um terahertz. Ou seja, o algoritmo quântico de Shor resolve este problema de fatoração em tempo polinomial, enquanto os algoritmos clássicos teriam um custo exponencial.

Há um comentário de Vazirani, responsável pelos avanços na área da matemática da computação quântica que precederam o trabalho de Shor, que resume muito bem o resultado da proposta de Shor quando aplicado a um número com 2000 dígitos.

Não é apenas o fato de que todos os computadores (clássicos) que existem no mundo, trabalhando juntos, não conseguiriam fatorar este número... Mesmo que todas as partículas do Universo conhecido fossem computadores (clássicos) e dispusessem de um tempo igual à idade estimada do Universo, este tempo não seria suficiente para fatorar este número.

A proposta de Shor aplicada a um computador quântico ameaça os esquemas utilizados em nossos dias para proteger informações eletrônicas, como o sistema *RSA* que é freqüentemente utilizado na segurança das informações bancárias. O sistema *RSA* baseia-se, exatamente, na impossibilidade de computadores clássicos fatorarem números inteiros com centenas de dígitos em pouco tempo [81]. Porém, para que a ameaça se torne completa, falta ainda um grande passo: a construção de computadores quânticos em escala capaz de atender, pelo menos, às grandes corporações. Por enquanto, não se tem notícias concretas que possibilitem acreditarmos que estamos às vésperas de tal situação. Entretanto, a proposta de Shor fez com que a computação quântica se tornasse um tema de pesquisa merecedor de altos investimentos e se espalhasse pelo complexo industrial-militar, levando, por exemplo, a IBM e a NASA a entrarem na corrida da computação quântica. Tanto que, em 1998, a NASA patrocinou uma conferência para discutir ou averiguar os progressos na área. Uma das novidades mais interessantes foi a descoberta de uma maneira de executar computações quânticas usando o método de ressonância magnética nuclear (NMR), o mesmo empregado para obtenção de imagens do interior do corpo humano. Nesta abordagem, a informação quântica está contida nos spins dos núcleos atômicos, que são afetados

por campos magnéticos. A alteração de tais campos resulta na possibilidade de manipulação das informações armazenadas nos núcleos [32]. Nesta ocasião, a IBM apresentou um protótipo de um computador NMR com dois *qubits*, que, programada por Chuang e Gershenfeld, realizou uma busca em um banco de dados que continha quatro elementos. Maiores detalhes sobre esta aplicação podem ser encontrados em [31].

Tal rotina corresponde a uma versão simplificada do problema formulado por Grover, que tinha por objetivo mostrar que um computador quântico seria capaz de localizar um item em uma lista não ordenada mais depressa do que computadores convencionais, [54, 55]. Supondo que a busca se referisse a um nome numa lista de um milhão deles, a busca convencional necessitaria de, em média, meio milhão de tentativas, ou seja, a metade do comprimento da lista. Grover mostrou que a busca quântica necessitaria de um número de operações aproximadamente igual à raiz quadrada do número de elementos da lista, que, neste caso, são mil operações, o que mostra a vantagem da versão quântica.

O algoritmo de Grover foi utilizado para atacar o sistema criptográfico clássico *DES (Data Encryption Standard)* que apresenta $2^{56} = 7 \times 10^{16}$ caminhos possíveis. Se um computador clássico, operando com um algoritmo clássico puder checar 1 milhão de caminhos por segundo, levará 100 anos para descobrir o caminho correto, enquanto, pelo algoritmo de Grover, obtém-se tal resultado em menos de quatro minutos [81]. Por este motivo, o algoritmo de Grover também causou certo impacto nas pesquisas acerca da computação quântica.

Uma outra aplicação bastante especulativa para o emaranhamento em computação, refere-se às *generalizações quânticas para a teoria de jogos* [77]. A expansão de operações físicas realizáveis no contexto quântico, quando comparada ao clássico, e a consequente realização de problemas que eram inacessíveis pelas abordagens clássicas favorecem as pesquisas em teoria de jogos. Por exemplo, tornou-se possível obter o equilíbrio de Nash em alguns casos utilizando estratégias de jogos quânticos [39] e, da mesma forma, o *dilema do prisioneiro* [41]. O que é importante salientar destes exemplos é que existe uma tendência bastante forte em descobrir aplicações para o emaranhamento em muitos campos (clássicos) da ciência [4].

As aplicações de estados emaranhados em tarefas de processamento de informação não estão restritas à possibilidade de ataque às chaves de criptografia *RSA* pelo algoritmo de Shor ou de Grover. Muito mais que isso, a utilização do emaranhamento favorece novas propostas na área de teoria da informação e aplicações. Segue um breve estudo a este respeito.

2.4.2 Teoria da informação quântica

O desenvolvimento da teoria da informação clássica baseia-se no estudo do problema do envio de informação clássica (letras de um alfabeto, textos, seqüências de bits, por exemplo) através de canais de comunicação, que operam de acordo com as leis da física clássica. O que mudaria nesta descrição se pudéssemos construir canais quânticos de informação? Essa redefinição de um *canal de comunicação* nos remete às questões que motivaram a teoria da informação clássica,

em busca de novas respostas que nos levam à *teoria da informação quântica*. Como a mecânica quântica inclui, com relação à mecânica Newtoniana, muitas classes adicionais de processos estáticos e dinâmicos elementares, é possível dizer que a teoria da informação quântica é mais rica do que a clássica. A primeira contém todos os processos clássicos já familiares e outros absolutamente novos, como o emaranhamento.

Em [81], podemos encontrar muitos resultados da teoria da informação clássica generalizados para o contexto quântico. Por não ser o principal objetivo deste trabalho, não entraremos em detalhes acerca dos avanços nesta área, embora alguns desses sejam citados a seguir[9].

Uma das questões fundamentais em teoria da informação clássica é o estudo da *capacidade de canal*. No contexto quântico, isso também é verificado: a necessidade de um estudo bem fundamentado acerca da *capacidade de canal para informações quânticas*. Este problema tem, pelo menos, dois aspectos. O primeiro concentra-se em considerar a capacidade de um canal quântico com respeito à transmissão de informação clássica. Mensagens clássicas podem ser codificadas utilizando-se estados quânticos, cuja base seja $\{|0\rangle, |1\rangle\}$. O principal resultado neste contexto foi demonstrado em [59, 62]. O outro aspecto considera o problema da capacidade de canais para informação quântica, ou seja, aquele que transmite de fato informações quânticas [118]. A sutileza desta abordagem consiste do fato de que os estados transmitidos devem preservar qualquer correlação que venham a possuir com outros sistemas, isto é, devem preservar o emaranhamento [97]. É exatamente esta propriedade que torna possível as aplicações referentes a tarefas de processamento de informação quântica. Os avanços na área de transmissão de informação clássica e quântica por canais quânticos apresentados introduziram o conceito de *informação coerente* [5, 6] e alguns métodos para o cálculo desta em vários sistemas.

Dentre todas as generalizações necessárias para adaptar a teoria da informação clássica para a aplicação no contexto quântico, salientamos a questão do *grupo de erros*. Isso porque toda informação que é enviada através de um *canal ruidoso* pode sofrer a ação de um erro, introduzido pelo canal, que pode, como resultado final da transmissão, fornecer ao receptor da mensagem enviada uma letra ou sequência de *qubits* que não corresponde à original. Este estudo em geral se baseia nas características do canal utilizado na transmissão.

No caso clássico, uma informação pode ser representada por "0" ou "1", somente. Supondo que tenha sido adotada a representação "0" para uma determinada informação, a única forma de que um erro seja verificado é que a representação "0" tenha sido modificada para a representação "1". Em outras palavras, o único *erro clássico* é definido por um operador Er, cuja ação na base $\{0, 1\}$ é dada por

$$Er(0) = 1 \qquad \text{ou} \qquad Er(1) = 0.$$

No mundo quântico, porém, a descrição dos erros é mais complexa. Os operadores de erros quânticos são denotados por I, X, Z e Y e representados matricialmente pela ação nos elementos

[9] Aos leitores não adaptados aos conceitos da teoria da informação, sugerimos as referências [35] e [98] que tratam do contexto clássico. Uma comparação muito bem estabelecida deste com o contexto quântico pode ser encontrada em [81].

da base $\{|0\rangle, |1\rangle\}$, pelas respectivas formas

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{e} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{2.7}$$

Os erros representados por X e Z são chamados *erros bit flip* e *phase flip*, respectivamente. Considerando a representação vetorial de (2.1), observamos, que

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle,$$

da mesma forma que $X|1\rangle = |0\rangle$. Disso é possível concluir que o erro *bit flip* quântico tem ação análoga ao erro clássico.

Quanto ao erro Z, observamos que

$$Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|1\rangle,$$

enquanto que $Z(|0\rangle) = |0\rangle$. Tal ação não tem análogo clássico e representa a *inversão de fase* do estado, que consiste em considerar em (2.3) um ângulo $\theta' = -\theta$.

A respeito do erro Y, observamos que

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = iXZ,$$

donde concluímos que Y pode ser obtido pela composição dos erros X e Z. Ou seja, Y substitui $|0\rangle$ por $|1\rangle$ (e vice-versa) e inverte a fase do estado inicial.

Mais do que um conjunto de erros, $\{I, X, Z, Y\}$ constitui um *grupo* no sentido algébrico e é conhecido como *grupo de Pauli* [119]. A partir deste grupo é possível obter todas as matrizes unitárias definidas num espaço de Hilbert [56]. Sabendo que a *evolução temporal de um sistema quântico é regida por operações unitárias* [81], temos então que a definição dos operadores de erros quânticos e, conseqüentemente, do grupo de Pauli é fundamental não só para o melhor entendimento da teoria da informação quântica, mas para entender todo o contexto da *informação quântica* e suas aplicações.

O processo de *transmitir informação quântica* viabiliza a realização de tarefas de processamento de informação próprias do mundo quântico. Entre essas, há a possibilidade de novas propostas de protocolos de *criptografia*, chamada, em geral, de *criptografia quântica*. Em tais protocolos é sempre possível detectar um invasor. Esta propriedade deriva do fato que os *qubits*, ao contrário do bits clássicos, não podem ser copiados [121]. O primeiro protocolo de criptografia quântica foi proposto em 1982 [10] e, depois de muitos trabalhos comprovando a realização experimental com estados emaranhados, declarou-se que a criptografia quântica é, de fato, comercialmente viável. Outras referências, onde detalhes da criptografia quântica podem ser encontrados, são [8, 43].

Além da criptografia quântica, o estudo de canais de informações quânticas está relacionado com a viabilização do *teletransporte quântico*. De forma resumida, a essência do teletransporte

consiste em transferir um estado quântico de um objeto físico para outro sem que haja a interação desses [11, 19]. Um estado emaranhado, tal como um par de Bell ou *EPR* e um canal clássico de comunicação são necessários para realizar tal tarefa, de forma que a informação essencial sobre o estado transportado é codificada como uma mensagem clássica e esta é transmitida por um canal também clássico. Cada *qubit* transportado é codificado em dois bits clássicos e, a partir desses, as características do estado teletransportado serão reconstruídas. Sob o ponto de vista da teoria da informação quântica, o teletransporte quântico é somente um canal de informação quântica que age sem ruído, de forma a transmitir perfeitamente os *qubits* de um sistema para outro. Embora pareça ingênuo, a conexão entre o teletransporte e a teoria da informação quântica tornou possível a verificação de muitos teoremas importantes sobre a capacidade de canal de informações quânticas [9].

O problema oposto ao do teletransporte é a *codificação superdensa*, que consiste em enviar uma grande quantidade de informação clássica por um canal quântico fazendo uso, para isso, de estados emaranhados. Seguem maiores detalhes desta aplicação.

Codificação Superdensa

A codificação superdensa foi proposta por Bennett e Wiesner em 1992 [16], e o protocolo descrito foi, em seguida, parcialmente verificado experimentalmente por Mattle, Weinfurter, Kwiat e Zeilinger em 1996 [76]. Trata-se de uma aplicação surpreendente da mecânica quântica elementar, que combina de forma não-trivial todos os ingredientes básicos desta teoria e, por isso, é um bom exemplo de tarefa de processamento que pode ser realizada utilizando os conceitos da mecânica quântica. Um esquema de codificação superdensa envolve dois parceiros, conhecidos como Alice e Bob que se encontram separados por uma grande distância. O objetivo é transmitir informação clássica de Alice para Bob, mas utilizando conceitos de informação quântica, como descrito a seguir.

Suponha que Alice queira enviar dois bits clássicos para Bob utilizando apenas um *qubit* e que ambos compartilhem, inicialmente, um par de *qubits* em um estado emaranhado, descrito na forma

$$|\psi\rangle_2 = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

O primeiro *qubit* e o segundo *qubit* estão, respectivamente, em posse de Alice e Bob. Ao enviar o seu *qubit* para Bob, Alice pode enviar dois bits clássicos se adotar o seguinte procedimento:

- se Alice deseja enviar a sequência 00, deve enviar o seu *qubit* sem alterá-lo, ou, aplicar o operador I de (2.7);
- se a sequência que Alice deseja enviar é 01, então ela deve modificar seu *qubit* através de um operador Z, definido em (2.7);

- se a sequência 10 é a que deve ser transmitida por Alice, então ela deve modificar o seu *qubit* através da ação do operador X, também definido em (2.7);

- se Alice deseja enviar a sequência 11, então o seu *qubit* deve ser modificado pela ação do operador iY, definido pela seguinte matriz de representação,

$$iY = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Pela característica do emaranhamento presente no estado $|\psi\rangle_2$, pelo que foi mencionado anteriormente acerca das propriedades de estados emaranhados, sabemos que as operações que Alice aplicar sobre o seu *qubit* automaticamente serão aplicadas ao *qubit* em posse de Bob, uma vez que os *qubits* estavam em um estado emaranhado antes da separação. Por isso, as escolhas de Alice representam a aplicação do operador associado não só ao *qubit* em sua posse, mas sim no estado total. De forma resumida, temos as seguintes possibilidades:

$$00 : |\psi\rangle_2 \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$01 : |\psi\rangle_2 \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$10 : |\psi\rangle_2 \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$$
$$11 : |\psi\rangle_2 \rightarrow \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Todos esses estados apresentados são chamados *estados de Bell* ou *pares EPR*. Todos são *estados emaranhados* [7]. Além disso, é possível verificar que tais estados formam uma base no espaço dos estados quânticos com dois *qubits* e, segundo as leis da mecânica quântica, por isso podem ser distinguidos por meio de uma medida apropriada [81]. Uma vez que Alice envia o seu *qubit*, Bob, com a posse dos dois *qubits* novamente, ou seja, do estado total, pode realizar esta medida apropriada e verificar qual dentre os estados descritos acima está em sua posse. Porém, se isso for determinado, Bob conhece então qual dentre as quatro sequências foi enviada por Alice.

Resumindo, manipulando apenas um *qubit*, Alice é capaz de enviar dois bits de informação clássica. Observe que dois *qubits* estão envolvidos no protocolo, mas apenas um foi manipulado por Alice, uma tarefa impossível de ser realizada com bits clássicos.

No contexto da codificação superdensa, torna-se evidente a utilização do estados emaranhados e as respectivas propriedades para assegurar o funcionamento ótimo do processo. Sob o nosso ponto de vista, foi exatamente este protocolo que despertou o interesse por *códigos corretores de erros quânticos*, uma das áreas em teoria da informação quântica mais pesquisadas e com maior número de contribuições. Esta teoria pode ser vista em detalhes em [51], que foi um dos

pioneiros na pesquisa de códigos que fizeram uso das propriedades do emaranhamento para implementar códigos com boa taxa de correção de erros. Outras contribuições muito interessantes podem ser encontradas em [1, 13, 26, 27, 28, 68, 102, 103].

Além das aplicações citadas, os conceitos de teoria da informação quântica têm aplicações também em termos da *medida de emaranhamento*, ou, mais precisamente, no contexto de exibir quantificadores de emaranhamento. Exemplos destas aplicações podem ser encontrados em [9, 14, 15, 30, 82], sendo que algumas destas propostas serão abordadas no Capítulo 3.

Com base no que foi apresentado até este ponto, observamos que, tanto para garantir a otimalidade dos algoritmos quânticos como para executar tarefas de processamento de informação não realizáveis no contexto clássico com eficiência, os estados com a propriedade de emaranhamento são fundamentais.

Neste contexto, é de suma importância que se possa decidir, com base em algum algoritmo, se um dado estado é emaranhado e, *a posteriori*, exibir a *quantidade de emaranhamento deste estado*. No Capítulo 3, apresentamos algumas das propostas para resolver o problema de classificação e quantificação do emaranhamento apresentados na literatura.

Capítulo 3

Critérios de Separabilidade e Medidas de Emaranhamento

O objetivo deste capítulo é apresentar uma revisão das propostas de *critérios de separabilidade* e *quantificadores de emaranhamento* encontradas na literatura. Estudamos com mais detalhes as propostas mais utilizadas e as que contribuíram diretamente para o desenvolvimento deste trabalho. Este Capítulo está organizado da seguinte forma. Na Seção 3.1, apresentamos algumas propostas de critérios de separabilidade encontradas na literatura, tais como *as desigualdades de Bell* e a *decomposição de Schmidt*, descritas nas Subseções 3.1.1 e 3.1.2, respectivamente. Na Subseção 3.1.3, mencionamos a proposta denominada *critério de Peres* e, na Subseção 3.1.4, o que pode ser entendido como uma generalização desta, conhecida como *critério dos Horodeckis*. Na Subseção 3.1.5, apresentamos um breve resumo da proposta de Nielsen e Kempe. A Seção 3.2 consiste de um resumo das propostas de *medidas de emaranhamento*. Mencionamos, na Subseção 3.2.1, a medida de emaranhamento descrita a partir da *entropia de von Neumann*, e, na Subsecção 3.2.2, mencionamos o *emaranhamento de formação* e a *concorrência*. Os operadores *tangles* são defininidos na Subseção 3.2.3 e a Subseção 3.2.4 menciona o quantificador de emaranhamento definido como *entropia relativa de emaranhamento* e outros a este associado. Por fim, na Seção 3.3, nos referimos às propostas de medidas de *emaranhamento global*, destacando entre as propostas existentes a medida de *Meyer-Wallach* na Subseção 3.3.1.

3.1 Propostas de Critério de Separabilidade para Estados Puros

A determinação de um critério de separabilidade que seja implementável para qualquer que seja o número de *qubits* no estado ainda é um problema em aberto, exatamente porque a análise de estados com um número grande de *qubits* é problemática e não apresenta uma sistemática definida. Como pode ser notado a seguir, as propostas existentes são bastante divergentes quanto ao contexto de formalização matemática, e muitas dessas, não têm interpretação física

alguma [93].

3.1.1 Desigualdades de Bell

Considerando apenas os estados puros com dois *qubits*, o primeiro resultado que temos quanto à análise da separabilidade de um dado estado está baseada nas *desigualdades de Bell*, cujos argumentos podem ser vistos em detalhes no trabalho [7]. Resumidamente, tal resultado é estabelecido da seguinte forma: como visto no Capítulo 2, uma medida adequada sobre um *qubit* apresenta uma resposta que é absolutamente independente da resposta da mesma medida aplicada a qualquer outro *qubit*, donde se obtem uma relação entre os resultados da medida conjunta dos dois *qubits* e das medidas de cada um dos *qubits*.

Porém, como foi mencionado também no Capítulo 2, dois *qubits* em um estado emaranhado são caracterizados pelo fato de que a medida de um interfere no resultado da medida do segundo, ainda que estejam separados por longas distâncias. Ainda que sem detalhes formais, que podem ser encontrados em [33], podemos inferir que a relação estabelecida no parágrafo anterior não é válida quando se analisa estados emaranhados. De acordo com esta idéia, o primeiro critério de separabilidade sugere que *todo estado puro emaranhado viola uma desigualdade de Bell* [7].

Uma demonstração interessante, porém bastante complexa para este teorema, pode ser vista em [93]. Para entender um pouco melhor a importância das desigualdades de Bell para caracterizar o emaranhamento, uma boa referência é [117].

O estudo das medidas as quais se refere tal resultado é um campo bastante árduo, o que associa a este teorema um processo de classificação pouco sistemático e, conseqüentemente, não implementável.

A segunda proposta é descrita em termos de conceitos de álgebra linear e propriedades dos espaços de Hilbert, conforme pode ser visto a seguir.

3.1.2 Decomposição de Schmidt

Assim como a análise em termos das desigualdades de Bell para classificar emaranhamento, a decomposição de Schmidt também só é válida para estados puros. Contudo, a decomposição de Schmidt pode ser aplicada a estados com um número arbitrário de *qubits*, desde que esses sejam analisados em dois conjuntos. Em outras palavras, tal decomposição só é válida para sistemas analisados em bipartições. Um sistema particionado desta forma é chamado *sistema bipartite, de duas partes* ou, *biparticionado*.

A *decomposição de Schmidt* de um estado puro biparticionado é apresentada a seguir.

Teorema 1 *[88] Seja U um espaço de Hilbert, tal que $U = V \otimes W$, com $dim(W) = m$ e $dim(V) = n$, $m \leq n$, sem perda de generalidade.Dado um vetor unitário (estado quântico)*

arbitrário $|\varphi\rangle \in U$*, existem bases ortonormais* $\{|v_i\rangle\}$ *de* V *e* $\{|w_j\rangle\}$ *de* W*, tais que*

$$|\varphi\rangle = \sum_{k=1}^{l} \lambda_k |v_k\rangle \otimes |w_k\rangle, \tag{3.1}$$

onde $\lambda_k > 0$ *e* $\sum {\lambda_k}^2 = 1$.

Os coeficientes λ_k são chamados *coeficientes de Schmidt* e as bases $\{|v_i\rangle\}$ e $\{|w_j\rangle\}$ são *bases de Schmidt* para o estado $|\varphi\rangle$. O número de coeficientes necessários para descrever um estado puro é chamado *número de Schmidt*.

Uma vez definida a decomposição de Schmidt associada a um estado puro, descrevemos no Teorema 2 a proposta de critério de separabilidade baseada em tal conceito.

Teorema 2 *[44] Um estado puro é separável se, e somente se, o número de Schmidt associado à sua decomposição é 1.*

Embora esta proposta seja extremamente elegante, sabe-se que não é possível generalizá-la para um sistema com mais de duas partes [93].

Existem critérios de verificação de separabilidade para estados puros com duas partes que têm como base um ponto de vista geométrico, definido por [23]. Esta proposta envolve projeções do espaço de estados (ou de um espaço de Hilbert) e conceitos da geometria algébrica como o *produto de Segre*, devidamente definido em [57]. Embora tal proposta não seja abordada com detalhes neste trabalho, gostaríamos de sugerir a leitura das contribuições citadas para os interessados no tópico.

Há propostas de critérios de separabilidade estabelecidos para *estados mistos*. De forma simplificada, os *estados mistos são uma combinação estatística de um conjunto de estados puros*, donde decorre que os estados puros podem ser vistos como uma versão simplificada desses primeiros. Optamos, desta forma, em apresentar também esses resultados, porém com as devidas adaptações referentes ao interesse restrito a estados puros. Antes disso, porém, é necessário que se defina o *operador de densidade* associado a um estado quântico.

Definição 2 *[81] O operador densidade* ρ *associado a um estado quântico puro* $|\psi\rangle$ *consiste em*

$$\rho = |\psi\rangle\langle\psi|. \tag{3.2}$$

A representação deste operador na base adequada é chamada *matriz densidade*.

Apresentamos em seguida alguns exemplos de estados quânticos e os operadores e matrizes densidade a esses associados.

Exemplo 8 *O operador densidade associado ao estado* $|\psi\rangle_1 = \alpha|0\rangle + \beta|1\rangle$ *é dado por*

$$\begin{aligned} \rho &= (\alpha|0\rangle + \beta|1\rangle)\,(\alpha|0\rangle + \beta|1\rangle)^\dagger = (\alpha|0\rangle + \beta|1\rangle)\,(\alpha^*\langle 0| + \beta^*\langle 1|) \\ &= |\alpha|^2|0\rangle\langle 0| + \alpha\beta^*|0\rangle\langle 1| + \alpha^*\beta|1\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|. \end{aligned}$$

Considerando a base $\{|0\rangle, |1\rangle\}$ *para a representação, a matriz densidade associada é dada por*

$$\rho = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}.$$

Exemplo 9 *Considerando o estado com dois qubits*

$$|\psi\rangle_2 = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

temos que o operador densidade é dado por

$$\begin{aligned} \rho &= \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) \\ &= \frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}. \end{aligned} \tag{3.3}$$

Considerando a base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ *para a representação matricial, temos que*

$$\rho = \begin{bmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{bmatrix}.$$

Quando consideramos sistemas com mais de um *qubit*, há mais um conceito a ser definido, que, para a análise de emaranhamento, é fundamental. Trata-se do *operador densidade reduzido*.

Suponha que se tenha dois sistemas A e B, cujo estado total seja descrito pelo operador densidade denotado por ρ^{AB}.

Definição 3 *[81] O operador reduzido para o sistema A é definido por*

$$\rho^A = tr_B\left(\rho^{AB}\right),$$

onde tr_B *é a operação conhecida como traço parcial sobre* B *e é definida por*

$$tr_B\left(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|\right) = |a_1\rangle\langle a_2|\ tr_B\left(|b_1\rangle\langle b_2|\right), \tag{3.4}$$

onde $tr_B\left(|b_1\rangle\langle b_2|\right) = \langle b_2|b_1\rangle$*, que, por sua vez, foi definida no Capítulo 2.* $|a_1\rangle$ *e* $|a_2\rangle$ *são quaisquer dois vetores do espaço* A *e* $|b_1\rangle$ *e* $|b_2\rangle$ *são quaisquer dois vetores do espaço* B*.*

Exemplo 10 *Considerando o estudo apresentado no Exemplo 9, temos que, realizando o traço sobre o segundo qubit, determina-se o operador densidade reduzido do primeiro qubit,* ρ'*,*

$$\begin{aligned} \rho' &= tr_2(\rho) = \frac{tr_2(|00\rangle\langle 00|) + tr_2(|11\rangle\langle 00|) + tr_2(|00\rangle\langle 11|) + tr_2(|11\rangle\langle 11|)}{2} \\ &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \\ &= \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} = \frac{I}{2}. \end{aligned}$$

O conceito de operador reduzido (e, conseqüentemente, de matriz densidade reduzida) é fundamental para definirmos uma *matriz separável*.

Definição 4 *[81] Dada uma matriz densidade ρ associada a um estado $|\psi\rangle$, dizemos que ρ é matriz separável se puder ser escrita como produto tensorial das matrizes de traço reduzido sobre cada qubit do sistema composto.*

Por exemplo, no caso de um sistema com duas partes, A e B, a matriz densidade que representa o sistema total ρ^{AB} é separável se, e somente se,

$$\rho^{AB} = \rho^A \otimes \rho^B,$$

onde ρ^A e ρ^B são as matrizes de traço reduzido sobre os sistemas B e A, respectivamente.

Pode-se demonstrar que todo estado associado a uma matriz densidade separável é um *estado separável*, valendo também a recíproca [107].

Exemplo 11 *Considere o estado*

$$|\xi\rangle_2 = \frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right) = \frac{1}{\sqrt{2}}|0\rangle \otimes \left(|0\rangle + |1\rangle\right),$$

que, pela Definição 1, é classificado como separável.

A matriz densidade ρ associada a este estado é dada por

$$\begin{bmatrix} 1/2 & 1/2 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

As matrizes de traço reduzido são dadas por

$$\rho^A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad e \quad \rho^B = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix},$$

donde segue que

$$\rho^{AB} = \begin{bmatrix} 1/2 & 1/2 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = \rho^A \otimes \rho^B.$$

Um último conceito a ser comentado é o de *transposta parcial de uma matriz densidade ρ^{AB}*.

Definição 5 *[81] A matriz transposta parcial sobre o primeiro qubit da matriz densidade do sistema total ρ^{AB} é denotada por ρ_1^{AB} e definida como*

$$\rho_1^{AB} = \left(\rho^A\right)^\dagger \otimes \rho^B.$$

Da mesma forma, denotamos por ρ_2^{AB} e definimos como $\rho_2^{AB} = \rho^A \otimes \left(\rho^B\right)^\dagger$ a matriz de transposição parcial do sistema total sobre o segundo *qubit*.

Tendo como base nestas novas definições, retornamos à apresentação das propostas de critério de separabilidade.

3.1.3 Critério de Peres

A proposta de Peres, apresentada em [89], refere-se diretamente ao conceito de matriz separável que definimos. Salientando que denominamos por *matriz positiva semidefinida* toda matriz com autovalores não negativos, segue a condição de separabilidade proposta por Peres.

Teorema 3 *[89] Se alguma matriz transposta parcial de ρ não for positiva semidefinida, então ρ é emaranhado.*

Ao apresentar sua proposta, Peres conjecturou que a condição exibida era necessária e suficiente para sistemas compostos por um número arbitrário de *qubits*, porém analisados sobre a condição da bipartição. Contudo, um grupo de pesquisadores conhecido como *família Horodecki* mostrou que a suficiência não se verificava para tais análises generalizadas [93].

Vejamos os argumentos desta justificativa e a condição suficiente para garantir a separabilidade de estados que decorreu desta discussão.

3.1.4 Critério da família Horodecki

Em [64], a familía Horodecki mostrou que era necessário um operador mais forte do que a *transposição parcial* utilizada por Peres para garantir a determinação de uma condição de separabilidade para estados biparticionados quaisquer. Para resolver esta questão, o operador *mapa* foi introduzido.

Um *mapa* $\mathcal{M}$ é um operador que age nos espaços dos operadores, ou seja, se $\mathbf{A}$ é um operador, então $\mathcal{M}\mathbf{A}$ também o é. Dizemos que *um mapa é positivo quando leva operadores positivos em operadores positivos.* De acordo com esses conceitos, podemos concluir que a transposição utilizada por Peres é um *mapa positivo*, uma vez que esta ação não modifica o conjunto dos autovalores de uma matriz.

Esta propriedade, sob o ponto de vista de análise funcional da familia Horodecki não era suficiente, uma vez que foi verificado que, se ρ não é uma matriz separável, então existe um mapa positivo $\mathcal{M}$ tal que $\mathcal{M}\rho$ não é positivo [107]. Neste contexto, os Horodecki apresentaram uma condição necessária e suficiente para garantir a separabilidade em sistemas de duas partes, conforme descreve o próximo teorema.

Teorema 4 *[64] Seja ρ uma matriz densidade associada a um estado biparticionado. Então, ρ é separável se, e somente se, para qualquer mapa positivo $\mathcal{M}$, $\mathcal{M}\rho$ é positivo.*

Em termos de conceitos de análise funcional, o estudo apresentado em [64], do qual deriva o Teorema 4 é muito rico, o que implica em uma enorme quantidade de detalhes que aqui serão omitidos. Algumas referências sobre o desenvolvimento desta proposta são, também, [63, 65, 66].

3.1.5 Critério de Nielsen e Kempe

Uma abordagem bastante diferente acerca de determinar formas de decidir se um dado estado é ou não emaranhado foi apresentada por Nielsen e Kempe em [82]. A motivação deve-se à observação de que, classicamente, se um sistema tem duas partes, a *desordem* do sistema total é maior ou igual a desordem de cada parte. A forma usual de quantificar a desordem de um sistema é através do uso de medidas entrópicas. No contexto clássico, a entropia utilizada é a *entropia de Shannon*, denotada por $H(X)$ e definida por

$$H(X) \equiv H(p_1, \cdots, p_n) = -\sum_i p_i \log_2 p_i,$$

onde $X = (X_1, \cdots, X_n)$ pode ser entendido como o conjunto das partes (ou das variáveis aleatórias) do sistema, associadas às probabilidades $p_1, \cdots, p_n$, respectivamente, [98].

No contexto quântico, a entropia mais utilizada é a *entropia de von Neumann*, denotada por S [80]. A entropia de um estado representado pela matriz densidade ρ é definida por

$$S(\rho) = -tr\left[\rho \log_2(\rho)\right],$$

onde tr denota a função traço usual de matrizes.

Escolhida uma medida de entropia $Ent(X)$, pode-se definir a entropia condicional entre duas partes X e Y como

$$Ent(X|Y) = Ent(X,Y) - Ent(Y),$$

onde $Ent(X,Y)$ denota a entropia do sistema total, constituído por X e Y. A entropia condicional pode ser entendida como a *entropia de X dado que a parte Y é conhecida.*

Classicamente, $Ent(X|Y)$ é sempre não negativa. Isto significa que a entropia de Shannon satisfaz

$$H(X,Y) \geq H(X) \quad \text{e} \quad H(X,Y) \geq H(Y).$$

Quanto ao contexto quântico e a respectiva condição considerando-se a entropia de von Neumann, em [82], podemos encontrar a demonstração de que, para estados separáveis, a seguinte condição é satisfeita,

$$S(\rho^{AB}) \geq S(\rho^A) \quad \text{e} \quad S(\rho^{AB}) \geq S(\rho^B).$$

A partir desta análise, decorre que *se $S(A|B) = S(\rho^{AB}) - S(\rho^B) < 0$, então o estado representado pela matriz ρ^{AB} é um estado emaranhado.*

Embora a idéia do critério proposto por Nielsen e Kempe seja basicamente essa, o resultado apresentado em [82] é descrito em termos da *teoria de majoração*. A relação de *ordem* entre os estados depende somente dos autovalores dos respectivos operadores de densidade. Dados dois estados representados por matrizes ρ e ρ', calculando e ordenando de forma não-crescente os respectivos autovalores nos vetores r_i e r'_i, nesta ordem, dizemos que r_i é *majorado* por r'_i ($r_i \preceq r'_i$) quando

$$\sum_{i=0}^{k} r_i \leq \sum_{i=0}^{k} r'_i,$$

para todo k tal que $1 \leq k \leq n-1$, onde n é o número de estados no sistema, sendo considerada a multiplicidade dos autovalores.

Nestes termos, segue o critério proposto por Nielsen e Kempe.

Teorema 5 *[82] Se um estado de duas partes, associado à matriz ρ^{AB}, é separável, então*

$$\lambda(\rho^A) \preceq \lambda(\rho^{AB}) \quad e \quad \lambda(\rho^B) \preceq \lambda(\rho^{AB}),$$

onde $\lambda(\rho^{AB})$, $\lambda(\rho^A)$ e $\lambda(\rho^B)$ representam os vetores contendo os autovalores das respectivas matrizes em ordem não-crescente.

A idéia de Nielsen e Kempe de medir com *uma* entropia a desordem de um sistema de estados quânticos, é, sob o nosso ponto de vista, muito interessante. Entre outras razões, esta proposta utiliza conceitos de teoria de informação, que foram definidos no Capítulo 2. Além disso, intuitivamente, este é o critério que induz mais diretamente a quantificação do emaranhamento. Uma justificativa para esta afirmação poderá ser vista em detalhes nos Capítulos 6 e 8.

Uma vez abordada a questão da quantificação do emaranhamento, cabe-nos discorrer brevemente acerca de algumas questões interessantes no contexto do estudo deste fenômeno.

Como mencionado no Capítulo 2, quando analisamos o emaranhamento em estados com mais de dois *qubits*, observamos que a classificação de um estado arbitrário em *separável* ou *emaranhado* está longe de ser satisfatória. Isso porque há várias formas de se estabelecer emaranhamento, no sentido de que para estados com múltiplos *qubits*, há mais de uma possibilidade para os estados se *agruparem* em emaranhamento, sendo estas classes de emaranhamento distintas.

Obter um procedimento sistemático e eficiente que quantifique as distintas classes de emaranhamento e estabeleça um padrão de comparação em termos do *emaranhamento total* do estado é uma questão em aberto. Não se sabe responder definitivamente como fazer este cálculo, de forma que a resposta obtida reproduza, com total fidelidade, as configurações de um estado arbitrário. Ainda que sejamos menos exigentes e nos questionemos acerca da caracterização matemática dos estados emaranhados que satisfazem a um determinado tipo de emaranhamento, tampouco se pode exibi-la com total certeza da generalidade do resultado. De forma mais precisa, observemos que, para as aplicações em computação e informação quântica apresentadas no Capítulo 2, sempre havia referência não a um par emaranhado qualquer, mas a um estado do tipo *EPR*, que é um estado de máximo emaranhamento. Mais do que isso, em sistemas com dois *qubits*, tais estados determinam a *única* classe de estados de máximo emaranhamento.

A pergunta que motiva a próxima seção é: *O que podemos garantir quanto à quantificação do emaranhamento para estados puros com um número arbitrário de qubits?*

3.2 Medidas de Emaranhamento

Antes de iniciarmos o resumo das medidas e quantificadores de emaranhamento encontradas na literatura, salientamos que, quando tratamos de *medidas sobre sistemas biparticionados*, entendemos que a medida em questão só é válida para a análise do emaranhamento existente entre duas partes de um estado arbitrário.

3.2.1 Entropia de von Neumann das matrizes reduzidas

Uma das idéias pioneiras na quantificação do emaranhamento foi o uso da entropia de von Neumann [9]. Assim como foi estabelecido pelo critério de Nielsen e Kempe (veja Seção 3.1.5), a partir das matrizes reduzidas dos subsistemas é possível estudar também a *quantidade de emaranhamento* de um estado. Tal quantificação é especificada em termos da *entropia de emaranhamento*, denotada por E e definida a seguir.

Se $\rho = |\psi\rangle\langle\psi|$ é a matriz densidade que descreve o estado puro $|\psi\rangle$, a quantidade de emaranhamento de ρ é

$$E(\psi) = -tr\{\rho_1 log_2(\rho_1)\} = -tr\{\rho_2 log_2(\rho_2)\}, \tag{3.5}$$

onde $\rho_1 = tr_2\{\rho\}$ e $\rho_2 = tr_1\{\rho\}$ são as matrizes que representam os operadores de traço reduzidos do sistema de duas partes (veja Definição 3).

Escrevendo a decomposição de Schmidt de $|\psi\rangle$, conforme especificado na Seção 3.1.2, temos

$$|\psi\rangle = \sum_{i=1}^{n} c_i |u_i\rangle_A |v_i\rangle_B,$$

donde obtemos que

$$E(\psi) = -\sum_{i=1}^{n} c_i^2 log_2(c_i^2). \tag{3.6}$$

Por esta definição, é possível verificar que os estados *EPR*s, maximamente emaranhados com dois *qubits*, são caracterizados pelo valor igual a 1 desta medida de emaranhamento, enquanto que os estados separáveis estão associados ao valor nulo desta [93].

A utilização da *entropia de emaranhamento* para a quantificação foi generalizada para estados puros de múltiplas partes, embora o cálculo de (3.6) para sistemas com mais de duas partes seja computacionalmente complicado. Maiores detalhes desta generalização podem ser encontrados em [21], entre outros.

3.2.2 Emaranhamento de formação e concorrência

Uma outra contribuição importante em termos de apresentar um método prático de quantificar o emaranhamento foi a proposta de Hill e Wootters para estados com dois *qubits*, definida em [61] e [123].

A *concorrência* de um estado associado à matriz densidade ρ é definida como segue. Seja $\bar{\rho} = Y \otimes Y \rho^* Y \otimes Y$, onde Y é o operador definido na equação (2.7) do Capítulo 2 e ρ^* denota o complexo conjugado de ρ.

A *concorrência* de ρ é definida como

$$C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\},$$

onde λ_i representam as raízes quadradas dos autovalores em ordem descrescente da matriz $\rho\bar{\rho}$.

A quantificação dada por $C(\rho)$ é bastante simplificada e é definida da seguinte forma. Se $C(\rho) = 0$, então o estado representado por ρ é separável. Se $C(\rho) = 1$, então temos um estado de máximo emaranhamento.

O conceito de *emaranhamento de formação* é demasiadamente importante para a quantificação de estados mistos. Embora este não seja o objetivo do trabalho, mencionaremos brevemente este assunto.

Um estado misto consiste de uma combinação probabilística de estados puros[1]. Maiores detalhes acerca dos estados mistos ou misturados são encontrado em [81]. Em outras palavras, um estado misto pode der descrito na seguinte forma:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{3.7}$$

onde $\{p_i\}$ é uma distribuição de probabilidades.

Neste contexto, o emaranhamento de formação consiste, como a própria nomenclatura sugere, do cálculo da entropia de emaranhamento E de cada estado puro em (3.7) e tomar a média $\bar{E}$ desses valores, devidamente ponderados pelas probabilidades $\{p_i\}$, de forma que

$$\bar{E}(\{p_i, |\rho\rangle\}) = \sum_i p_i E(|\psi_i\rangle). \tag{3.8}$$

Como a descrição exibida em (3.7) não é única, há mais de um valor possível para $\bar{E}$. Formalmente, o emaranhamento de formação de um estado misto é definido como a minimização de $\bar{E}$ sobre todas as possíveis escolhas $\{p_i, |\psi_i\rangle\}$ que descrevem ρ [13]. Ou seja,

$$EoF(\rho) = inf_{\{p_i, |\psi_i\rangle\}} \bar{E}(\{p_i, |\psi_i\rangle\}). \tag{3.9}$$

Observe que, por causa do processo de minimização, o cálculo de EoF como dado em (3.9) torna-se inviável na maioria dos casos para sistemas gerais. Para o caso de estados com dois *qubits*, tendo como base o conceito de concorrência, uma forma analítica para o cálculo do emaranhamento de formação foi obtida. Tal forma consiste em

$$EoF(\rho) = H_2\left(\frac{1}{2} + \frac{1}{2}\sqrt{1 - C^2(\rho)}\right),$$

[1]Em termos gerais, diz-se que um estado misto é uma mistura estatística de estados puros.

onde H_2 indica a entropia (clássica e binária) de Shannon, definida por $H_2(x) = -xlog_2x - (1-x)log_2(1-x)$.

Além de viabilizar o cálculo do emaranhamento de formação para estados com dois *qubits*[2], a definição da concorrência foi fundamental para a proposta de operadores *tangle* que quantificam o emaranhamento de estados puros com três *qubits* e outros sistemas mais gerais, analisados em termos da bipartição do conjunto de *qubits*. Apresentamos na próxima seção alguns comentários acerca destas propostas.

3.2.3 Operadores *tangle* como medida de emaranhamento

A definição dos operadores *tangle* como medidas de emaranhamento para estados com três *qubits* foi apresentada no trabalho [34] e formou a base para uma nova abordagem acerca dos operadores de medida do emaranhamento em sistemas biparticionados.

Considere um estado com três *qubits* representado na forma

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

e suponha que os subsistemas deste estado sejam denotados respectivamente por A, B e C. A primeira forma de emaranhamento possível é aquela que engloba os três *qubits*, ou seja, um emaranhamento na forma ABC. Uma segunda possibilidade é um emaranhamento restrito a apenas dois dos três *qubits*, nas formas AB, AC e BC, ou, ainda, nas formas $A(BC)$, $B(CA)$ e $C(AB)$, que indicam dois tipos diferentes de emaranhamento: um entre os pares denotados entre parênteses e um outro associado a este par (visto como um só *qubit*) e o terceiro. Tendo como base este conjunto de possibilidades, Coffman *et al.* definem um operador *tangle* para cada uma das formas de emaranhamento. Tais operadores são denotados por τ_{ABC}, τ_{AB}, τ_{AC}, τ_{BC}, $\tau_{A(BC)}$, $\tau_{B(CA)}$ e $\tau_{C(AB)}$, mantendo a ordem em que as possibilidades de emaranhamento foram apresentadas.

Uma informação importante no contexto é que os *tangles* geram uma quantificação do emaranhamento em um dado estado de uma forma bastante simplificada: os valores que um operador *tangle* pode assumir variam entre 0 e 1, inclusive. Por exemplo, se $\tau_{ABC} = 0$, então não há emaranhamento que envolva os três *qubits* do estado simultaneamente. Já no caso de $\tau_{ABC} = 1$, então temos emaranhamento máximo entre os três *qubits*.

O primeiro *tangle* a ser definido refere-se à medida do emaranhamento entre dois *qubits* do sistema, como se o terceiro fosse ignorado (formas AB, AC e BC). Tal medida é representada pela seguinte expressão

$$\tau_{AB} = tr(\rho_{AB}\bar{\rho}_{AB}) - 2\lambda_1\lambda_2, \tag{3.10}$$

[2] A concorrência está estreitamente relacionada a duas outras medidas de emaranhamento, conhecidas como *negatividade* e *negatividade logarítmica*, como pode ser visto em [111]. Tais medidas foram introduzidas nos trabalhos [113, 126], onde maiores detalhes podem ser encontrados.

onde ρ_{AB} é a matriz de traço parcial de ρ com relação a C,

$$\bar{\rho}_{AB} = (\sigma_y \otimes \sigma_y)\rho^*_{AB}(\sigma_y \otimes \sigma_y), \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

o asterisco denota o complexo conjugado na base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ e λ_1 e λ_2 são as raízes quadradas dos autovalores da matriz $\rho_{AB}\bar{\rho}_{AB}$. De forma análoga, temos que

$$\tau_{AC} = tr(\rho_{AC}\bar{\rho}_{AC}) - 2\lambda_1\lambda_2,$$

onde λ_1 e λ_2 são relativos à matriz $\rho_{AC}\bar{\rho}_{AC}$.

Em seguida, apresentamos o *tangle* que mede o emaranhamento entre um dos *qubits* e o outro subsistema com dois *qubits* (formas $A(BC)$, $B(CA)$ e $C(AB)$). Esta medida é representada pelo operador

$$\tau_{A(BC)} = 4det|\rho_A|, \tag{3.11}$$

onde ρ_A denota a matriz densidade associada ao *qubit* A. De forma análoga, definimos $\tau_{B(CA)} = 4det|\rho_B|$ e $\tau_{C(AB)} = 4det|\rho_C|$, onde ρ_B e ρ_C são as matrizes densidades associadas aos *qubits* B e C, respectivamente.

É importante salientar que existe uma *regra* quanto à distribuição do emaranhamento, apresentada em [34], que é

$$\tau_{AB} + \tau_{AC} \leq \tau_{A(BC)}. \tag{3.12}$$

Ou seja, o emaranhamento entre o *qubit* A e o par BC representa o máximo valor para a soma entre $\tau_{AB}+\tau_{AC}$. Para o caso de ocorrer a igualdade, define-se a classe dos *estados maximamente emaranhados aos pares*. Para o caso em que $\tau_{AB} + \tau_{AC} < \tau_{A(BC)}$, define-se o *emaranhamento residual*. Tal emaranhamento é medido pelo *tangle* τ_{ABC} dado pela seguinte forma

$$\tau_{ABC} = 4|d_1 - 2d_2 + 4d_3|, \tag{3.13}$$

onde $|\ .\ |$ denota o valor absoluto e

$$d_1 = \alpha_0^2\alpha_7^2 + \alpha_1^2\alpha_6^2 + \alpha_2^2\alpha_5^2 + \alpha_3^2\alpha_4^2,$$

$$d_2 = \alpha_0\alpha_7\alpha_3\alpha_4 + \alpha_0\alpha_7\alpha_5\alpha_2 + \alpha_0\alpha_7\alpha_6\alpha_1 + \alpha_3\alpha_4\alpha_5\alpha_2 + \alpha_3\alpha_4\alpha_6\alpha_1 + \alpha_5\alpha_2\alpha_6\alpha_1,$$

$$d_3 = \alpha_0\alpha_6\alpha_5\alpha_3 + \alpha_7\alpha_1\alpha_2\alpha_4.$$

Nas definições de d_1, d_2 e d_3, consideramos que $\alpha_0, \cdots, \alpha_7$ são números complexos que representam as amplitudes associadas a cada *ket* do estado arbitrário $|\psi\rangle_3$.

Os estados para os quais τ_{ABC} assume o valor máximo 1 formam uma outra classe de *estados de emaranhamento máximo*. Esta é a justificativa para o fato de haver duas classes de máximo *emaranhamento genuíno tripartite* para estados com três *qubits* [122].

Com o objetivo de exemplificar a utilização dos operadores *tangles*, observamos que os cálculos definidos com relação aos *tangles* para o estado $|\psi_{GHZ}\rangle_3 = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ resultam em $\tau_{AB} = 0$, $\tau_{AC} = 0$ e $\tau_{A(BC)} = 1$. Analisando as amplitudes de $|\psi_{GHZ}\rangle_3$, temos que $d_1 = 1/4, d_2 = d_3 = 0$, donde decorre que $\tau_{ABC} = 1$.

Considerando o estado $|\psi_W\rangle_3 = \frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |110\rangle)$, temos que $\tau_{AB} = \tau_{AC} = 4/9$ e $\tau_{A(BC)} = 8/9$. Por fim, $d_1 = d_2 = d_3 = 0$, o que implica que $\tau_{ABC} = 0$. Como há a igualdade em (3.12), trata-se de um exemplo da classe de *estados maximamente emaranhados aos pares*[3].

Esta proposta de Coffman *et al.* é bastante interessante porque nos permite dar um passo no entendimento do emaranhamento em estados com mais de dois *qubits*. Estes autores mostraram que, ao utilizar uma generalização da concorrência[4] como medida, o emaranhamento existente entre dois *qubits* limita o emaranhamento que esses podem estabelecer com o terceiro. Tal propriedade é explicitada pela expressão

$$\tau_{AB} + \tau_{AC} \leq \tau_{A(BC)}.$$

Decorrentes de conjecturas apresentadas em [34], mais recentemente as contribuições [87, 120, 124] apresentaram a forma generalizada de (3.12) para sistemas de duas partes, porém com número arbitrário de *qubits*. Tal expressão é dada por

$$\tau_{12} + \tau_{13} + \cdots + \tau_{1n} \leq \tau_{1:23\cdots n}, \tag{3.14}$$

onde $\tau_{1:23\cdots n}$ representa o emaranhamento referente à bipartição dos *qubits* na forma (1) e $(2\cdots n)$.

Ainda que em forma de conjectura na ocasião do trabalho de Coffmann, tal desigualdade despertou o interesse da comunidade de informação quântica, não só por se tratar de um tema sem análogo clássico, mas também porque tal resultado pode estar relacionado à segurança de certos protocolos criptográficos [94].

Baseadas na consideração explicitada em (3.12), surgiram comprovações de que a quantidade de emaranhamento em um sistema inibe não só o emaranhamento deste com os outros sistemas, mas também correlações clássicas entre esses [70]. Além disso, estudos relativos à distribuição de emaranhamento tornaram-se frequentes e, com as novas propostas, surgiram novos temas como o *compartilhamento* e a *monogamia do emaranhamento* em sistemas mais gerais. Não vamos abordar tais estudos neste trabalho, mas recomendamos as referências [24, 69, 106] aos leitores interessados.

Nas próximas subseções apresentamos medidas para sistemas analisados sob multi-partições, ou, simplesmente, *sistemas multipartites*.

3.2.4 Entropia relativa do emaranhamento

Este quantificador de emaranhamento multipartite faz uso da idéia de *distinguibilidade* de estados quânticos, que será abordada a seguir.

Um problema importante em protocolos de comunicação é o de distinguir duas distribuições de probabilidades. Suponha, por exemplo, que possuímos uma moeda viciada com distribuição

[3] Maiores detalhes dos cálculos que nos levaram a tais conclusões podem ser encontrados em [48].

[4] Os *tangles* podem ser vistos, simplesmente, como o quadrado da concorrência, de forma que $\tau_{AB} = C^2(\rho_{AB})$.

de probabilidades para "cara" e "coroa" dada por $f = (1/3, 2/3)$. Qual a probabilidade de que esta moeda seja confundida com uma moeda honesta, com distribuição de probabilidades $q = (1/2, 1/2)$?

Se as moedas forem atiradas um número n grande de vezes, a resposta é [81],

$$p(moeda\ viciada \rightarrow moeda\ honesta) = exp[-nS_{cl}(f \mid\mid q)],$$

onde

$$S_{cl}(f \mid\mid q) = 1/3 \ln (1/3) + 2/3 \ln (2/3) - 1/3 \ln (1/2) - 2/3 \ln (1/2) .$$

S_{cl} denota a divergência das duas distribuições [60] e é tal que, se $n \rightarrow \infty$ e $p \rightarrow 0$, então podemos distinguir com certeza a moeda viciada da honesta. Tal resultado é válido para quaisquer duas distribuições de probabilidades $P(x)$ e $Q(x)$, de forma que

$$S_{cl}(P(x) \mid\mid Q(x)) = \sum_i p_i \ln p_i - p_i \ln q_i. \tag{3.15}$$

Tal resultado foi generalizado no trabalho [108] no seguinte contexto: a probabilidade de não distinguir dois estados quânticos representados pelas matrizes ρ e σ, após n medições apropriadas, é

$$p(\rho \rightarrow \sigma) = exp[-nS(\sigma \mid\mid \rho)],$$

onde

$$S(\sigma \mid\mid \rho) := tr[\sigma ln\sigma - \sigma ln\rho]$$

é a entropia relativa quântica.

Vedral *et al.* propuseram em [109, 110] que a entropia relativa poderia ser utilizada para quantificar emaranhamento multipartite. Sob esta interpretação, a idéia é quantificar quão bem um estado ρ pode ser distinguido de um estado separável. Em outras palavras, o objetivo é obter $S(\sigma \mid\mid \rho)$ quando σ é um estado separável.

A *entropia relativa de emaranhamento de um estado* ρ é definida como

$$E_R(\rho) = min_{\{\sigma separavel\}} S(\sigma \mid\mid \rho), \tag{3.16}$$

ou seja, a entropia relativa de emaranhamento de ρ é dada pela minimização de ρ com relação a todos os estados separáveis.

Apesar da clara intepretação da distinguibilidade, observamos que o cálculo de E_R não é operacional devido ao processo de minimização para estados arbitrários. Tal quantificador pode ser utilizado somente para estados com alguma característica especial que facilite o processo de minimização. Em [115], por exemplo, os autores apresentam uma forma analítica para o cálculo de E_R para estados puros completamente simétricos com n *qubits*.

Uma outra abordagem para a quantificação do emaranhamento em sistemas multipartites que também se baseia no conceito de entropia foi apresentada em [15, 105].

Mais recentemente propostos, temos em [20] e [92] os quantificadores denominados *emaranhamento testemunhado* e *emaranhamento de teletransporte*, respectivamente.

O *emaranhamento testemunhado* consiste em comparar (em termos de um conceito parecido com a distância entre espaços) um estado arbitrário a um *estado testemunha*. De acordo com a quantidade de emaranhamento desta *testemunha* e da "distância" estabelecida entre os estados, é possível quantificar o emaranhamento do segundo estado. Associado a este quantificador, temos o conceito de *robustez de emaranhamento*, que nos permite uma interessante visualização geométrica desta proposta de quantificação. Maiores detalhes podem ser encontrados nas contribuições [58, 126]. Por sua vez, o *emaranhamento de teletransporte* consiste em utilizar como medida de emaranhamento de um estado a eficiência deste para teletransportar estados quânticos arbitrários (veja alguns detalhes do teletransporte quântico na Seção 2.4.2). Todos os detalhes desta nova e interessante abordagem podem ser encontrados também em [93].

Apresentadas algumas propostas de quantificadores de emaranhamento, salientamos que, como mencionado no Capítulo 1, o objetivo deste trabalho é estudar a quantificação do *emaranhamento global* em estados puros arbitrários. Por isso, destacamos, na próxima seção, algumas das propostas de quantificação deste emaranhamento que serão fundamentais para o desenvolvimento da nossa proposta.

3.3 Quantificação do Emaranhamento Global

A definição de *emaranhamento global* é, basicamente, a existência de emaranhamento em um estado, ou a existência de correlação quântica entre os *qubits* do estado.

A primeira medida que vamos apresentar só é capaz de identificar, em um estado de muitos *qubits*, emaranhamento entre duas partes. Segue a definição deste quantificador conforme proposto em [78].

3.3.1 Medida de Meyer-Wallach

Seja $|\psi\rangle$[5] um estado puro arbitrário com n *qubits* descrito na forma

$$|\psi\rangle = \alpha_0|00\cdots0\rangle + \alpha_1|00\cdots1\rangle + \cdots + \alpha_{2^n-2}|11\cdots0\rangle + \alpha_{2^n-1}|11\cdots1\rangle, \tag{3.17}$$

onde $\alpha_0, ..., \alpha_{2^n-1} \in \mathbb{C}$ e $\sum_{s=0}^{2^n-1} |\alpha_s|^2 = 1$.

A medida de emaranhamento global para estados quânticos puros, denotada por Q, dada por Meyer-Wallach em [78], é definida da seguinte forma.

Seja $\mathbf{x} = x_1 \cdots x_n$ uma n-upla binária associada ao conteúdo de um *ket* de $|\psi\rangle$, sendo x_j, $j = 1, \cdots, n$, cada coordenada de $\mathbf{x}$. Considere $\iota_j(b) : (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n-1}$ a função linear definida pela seguinte ação na base

$$\iota_j(b)\left(|x_1\rangle \otimes \cdots \otimes |x_n\rangle\right) = \delta_{bx_j}|x_1\rangle \otimes \cdots \otimes |x_{j-1}\rangle \otimes |x_{j+1}\rangle \otimes \cdots |x_n\rangle,$$

[5] Para definir operadores associados à medida de Meyer-Wallach e efetuar os cálculos, omitimos o índice i em $|\psi\rangle_i$ para simplificar a notação.

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

Proposição 1 *[95] Dado um estado quântico puro com n qubits $|\psi\rangle$, a medida de emaranhamento global de Meyer-Wallach é dada por*

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

onde

$$D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle) = \langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle\langle\psi|\iota_j(1), \iota_j(1)|\psi\rangle - |\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle|^2,$$

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

Q é invariante sob transformações unitárias locais e tal que $0 \leq Q \leq 1$. Assim, $Q(|\psi\rangle) = 0$ se, e somente se, $|\psi\rangle$ é um estado separável, e $Q(|\psi\rangle) = 1$ se, e somente se, $|\psi\rangle$ é um estado puro de máximo emaranhamento global[6]*.*

A proposta de Meyer-Wallach é interessante no sentido de permitir uma sistematização para os cálculos. Veremos adiante a nossa proposta de uma forma alternativa de expressá-la, que, considerando conceitos de teoria de informação e codificação clássica, resulta em uma simplificação desses cálculos.

Porém, embora a medida de Meyer-Wallach tenha sido utilizada neste trabalho, sabe-se que esta não é o único quantificador para emaranhamento global em sistemas de duas partes da forma $(qubit\ k)(qubit\ 1 \cdots (k-1)\ (k+1) \cdots n)$. Uma outra proposta para este mesmo contexto é o trabalho de Pope e Milburn [90], cujos detalhes podem ser encontrados nesta referência.

Ainda com relação à medida de Meyer-Wallach, o trabalho de Brennen [22] mostrou que esta pode ser vista como a entropia linear dos subsistemas que constituem o estado, de forma que

$$Q(|\psi\rangle) = 2\left(1 - \frac{1}{n}\sum_{k=1}^{n} tr\rho_k^2\right), \tag{3.18}$$

onde ρ_k é a matriz do operador densidade reduzido sobre o k-ésimo *qubit*.

Tendo como base esta simplificação proposta por Brennen, foi possível generalizar a medida de Meyer-Wallach para estados de *multiqudits*, $|\psi\rangle \in (\mathbb{C}^D) \otimes n$, e para todas as possíveis bipartições dos n *qubits*. A forma generalizada de Q é descrita em [95] e consiste em

$$Q_m(|\psi\rangle) = \frac{D^m}{D^m - 1}\left(1 - \frac{m!(n-m)!}{n!}\sum_{|S|=m} tr\rho_S^2\right), \tag{3.19}$$

para $D \geq 2$, $m = 1, \cdots, \lfloor n/2 \rfloor$, $S \subset \{1, \cdots, n\}$, $\rho_S = tr_{S'}|\psi\rangle\langle\psi|$ denota o operador densidade reduzido sobre os elementos que não foram incluídos em S e $\lfloor k \rfloor$ denota a parte inteira de k.

[6] Observe que se um estado puro $|\xi\rangle$ é tal que $Q(|\xi\rangle) \neq 0$ e $Q(|\xi\rangle) \neq 1$, então podemos afirmar apenas que $|\xi\rangle$ é um estado puro emaranhado.

Observe que Q_m, definida em (3.19), reduz-se à medida de Meyer-Wallach para $m = 1$ e $D = 2$.

Uma vez definida tal generalização, podemos encontrar em [95] muitas propriedades desta medida que, sem dúvida, muito contribuem na busca de um entendimento completo do emaranhamento em sistemas de muitos *qubits* (e *qudits*), com bipartições genéricas.

Mais recentemente, surgiram pesquisas que utilizam-se do conceito de *transição de fases quânticas* para desenvolver medidas para o emaranhamento global. Os resultados são, também, bastante gerais e consideram inclusive situações com multipartições do sistema. Indicamos as seguintes referências aos leitores interessados [83, 84, 85, 86].

Há muitas contribuições na literatura referentes à critérios de separabilidade e quantificadores de emaranhamento, principalmente quando nos restringimos a estados puros, como é o caso deste trabalho. Tal restrição decorre do fato do nosso interesse consistir em determinar a forma matemática de *estados de máximo emaranhamento*, e, uma vez sabido que esta propriedade só é verificada em estados puros [94], é desnecessário considerarmos os estados mistos.

Nos Capítulos 4 e 5, apresentamos uma proposta de critério de separabilidade para estados puros arbitrários à qual foi possível associar uma interpretação homológica-geométrica bastante simples. Foi a simplicidade desta interpretação que nos permitiu encontrar, além do critério de separabilidade, algumas propriedades que relacionam a determinação de estados de máximo emaranhamento global e resultados importantes da teoria de informação clássica, cuja discussão será apresentada nos Capítulos 6 e 8.

Capítulo 4

Critério de Separabilidade para Estados com Três *Qubits*

Conforme os comentários apresentados no capítulo de Introdução, o objetivo deste trabalho é contribuir em direção a uma descrição matemática para os estados puros emaranhados. Por isso, é importante exibir um critério a partir do qual, dado um estado puro arbitrário, seja possível classificá-lo em separável ou emaranhado. Como mencionado anteriormente, para o caso de estados puros com dois *qubits*, há algumas propostas na literatura. Entre essas, salientamos a de Peres, [88], pois através das idéias envolvidas nessa proposta é que determinamos a direção para definir critérios de separabilidade para estados puros com um número qualquer de *qubits*, o que implica na generalização do processo.

Este capítulo está organizado na seguinte forma. Na Seção 4.1, apresentamos o critério de separabilidade proposto por Peres para estados puros com dois *qubits*. Na Seção 4.2, descrevemos uma proposta de critério de separabilidade para estados puros com três *qubits*. Uma interpretação geométrica para as equações obtidas a partir desta proposta é apresentada na Seção 4.3, tal como considerações importantes que serão utilizadas para a generalização do critério.

4.1 Critério de Separabilidade para Estados com Dois *Qubits*

A condição que classifica estados separáveis foi apresentada na Definição 1, Capítulo 2. Mantendo a notação por ora estabelecida, tal definição, quanto a estados com dois *qubits*, pode ser reescrita como segue.

Definição 6 *Seja $|\psi\rangle_2$ um estado puro arbitrário com dois qubits dado por*

$$|\psi\rangle_2 = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle, \tag{4.1}$$

onde $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ e $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$. $|\psi\rangle_2$ é separável (ou não-emaranhado) se pode ser escrito como $|\psi\rangle_2 = |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1$, onde $|\varphi_1\rangle_1$ e $|\varphi_2\rangle_1$ são estados puros de um qubit.

Supondo que $|\varphi_1\rangle_1 = a|0\rangle + b|1\rangle$ e $|\varphi_2\rangle_1 = c|0\rangle + d|1\rangle$, onde $a, b, c, d \in \mathbb{C}$ com $|a|^2 + |b|^2 = 1$ e $|c|^2 + |d|^2 = 1$, apresentamos os seguintes resultados.

Lema 1 *Um estado puro com dois qubits $|\psi\rangle_2$, como em (4.1), é separável se, e somente se, as igualdades a seguir são simultaneamente satisfeitas*

$$\alpha_0 = ac, \tag{4.2}$$

$$\alpha_1 = ad, \tag{4.3}$$

$$\alpha_2 = bc, \tag{4.4}$$

$$\alpha_3 = bd. \tag{4.5}$$

Demonstração. Pela Definição 6, se $|\psi\rangle_2$ é separável, então este estado pode ser escrito como

$$|\psi\rangle_2 = |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle, \tag{4.6}$$

o que implica que $\alpha_0 = ac$, $\alpha_1 = ad$, $\alpha_2 = bc$ e $\alpha_3 = bd$. Por outro lado, assumindo que as igualdades dadas em (4.2), (4.3), (4.4), (4.5) são simultaneamente satisfeitas, temos que (4.1) pode ser reescrita como

$$\begin{aligned} |\psi\rangle_2 &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \\ &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle), \end{aligned}$$

o que implica que $|\psi\rangle_2$ é separável.

■

Lema 2 *Seja $|\psi\rangle_2$ um estado puro com dois qubits, como em (4.1). As equações (4.2), (4.3), (4.4) e (4.5) são simultaneamente satisfeitas se, e somente se,*

$$\alpha_0\alpha_3 = \alpha_1\alpha_2. \tag{4.7}$$

Demonstração. Se (4.2), (4.3), (4.4) e (4.5) são simultaneamente satisfeitas, então (4.7) também é satisfeita para quaisquer $a, b, c, d \in \mathbb{C}$. Agora, mostraremos que se α_0, α_1, α_2, e $\alpha_3 \in \mathbb{C}$ com $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$, então cada α_i pode ser escrito como o produto de dois números complexos satisfazendo também a restrição $\alpha_0\alpha_3 = \alpha_1\alpha_2$. Para isso, observamos dois casos.

a-) Suponha que $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}^*$, onde $\mathbb{C}^*$ denota o conjunto dos números complexos não nulos. Dado um $\beta_0 \in \mathbb{C}^*$, é possível determinar β_1, β_2 e $\beta_3 \in \mathbb{C}^*$ tais que

$$\begin{aligned} \alpha_0 &= \beta_0\beta_2, \\ \alpha_1 &= \beta_0\beta_3, \\ \alpha_2 &= \beta_1\beta_2. \end{aligned}$$

Assim, de (4.7), decorre que a única representação para α_3 é

$$\alpha_3 = \beta_1\beta_3.$$

b-) Considere a equação (4.7). Se $\alpha_0 = 0$, então $\alpha_1 = 0$ ou $\alpha_2 = 0$ ou $\alpha_1 = \alpha_2 = 0$. Quando $\alpha_1 = \alpha_2 = 0$, segue de (4.1) que $|\psi\rangle_2 = \alpha_3|11\rangle$, donde temos que $|\psi\rangle_2$ é separável. Desta forma, decorre do Lema 1 que (4.2), (4.3), (4.4) e (4.5) são simultaneamente verdadeiras. Por outro lado, sem perda de generalidade, considere $\alpha_1 = 0$ e $\alpha_2 \neq 0$. Se $\alpha_3 = 0$, então $|\psi\rangle_2 = \alpha_2|10\rangle$. Quando $\alpha_3 \neq 0$, $|\psi\rangle_2 = \alpha_2|10\rangle + \alpha_3|11\rangle = |1\rangle \otimes (\alpha_2|0\rangle + \alpha_3|1\rangle)$. Em ambos os casos $|\psi\rangle_2$ é separável e, novamente pelo Lema 1, temos que (4.2), (4.3), (4.4) e (4.5) são satisfeitas. O mesmo argumento se aplica no caso em que $\alpha_1 = 0$, $\alpha_2 = 0$ ou $\alpha_3 = 0$.

■

Como conseqüência dos Lemas 1 e 2, temos o seguinte resultado.

Teorema 6 *Um estado puro arbitrário com dois qubits $|\psi\rangle_2$, dado por*

$$|\psi\rangle_2 = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle,$$

onde $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ e $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$, é separável se, e somente se,

$$\alpha_0\alpha_3 = \alpha_1\alpha_2. \tag{4.8}$$

O Teorema 6 estabelece o critério de separabilidade apresentado por Peres, [88]. As demonstrações dadas pelo autor dos Lemas 1 e 2 foram modificadas para que pudessem ser utilizadas diretamente nas demonstrações dos critérios que serão definidos a seguir.

4.2 Critério de Separabilidade para Estados Puros com Três *Qubits*

A Definição 1, quando restrita a estados com três *qubits*, pode ser reescrita como segue.

Definição 7 *Seja $|\psi\rangle_3$ um estado puro arbitrário com três qubits, dado por*

$$|\psi\rangle_3 = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle, \tag{4.9}$$

onde $\alpha_0, ..., \alpha_7 \in \mathbb{C}$ e $\sum_{i=0}^{7} |\alpha_i|^2 = 1$. $|\psi\rangle_3$ é dito separável se pode ser escrito como $|\psi\rangle_3 = |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 \otimes |\varphi_3\rangle_1$, onde $|\varphi_1\rangle_1$, $|\varphi_2\rangle_1$ e $|\varphi_3\rangle_1$ são estados puros de um qubit.

Considerando que $|\varphi_1\rangle_1 = a|0\rangle + b|1\rangle$, $|\varphi_2\rangle_1 = c|0\rangle + d|1\rangle$ e $|\varphi_3\rangle_1 = e|0\rangle + f|1\rangle$, onde a, b, c, d, e, $f \in \mathbb{C}$, então

$$\begin{aligned} |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 \otimes |\varphi_3\rangle_1 \;=\; & ace|000\rangle + acf|001\rangle + ade|010\rangle + adf|011\rangle \\ & + bce|100\rangle + bcf|101\rangle + bde|110\rangle + bdf|111\rangle, \end{aligned} \tag{4.10}$$

com a restrição $|ace|^2 + |acf|^2 + |ade|^2 + |adf|^2 + |bce|^2 + |bcf|^2 + |bde|^2 + |bdf|^2 = 1$.

De acordo com estas considerações, seguem os resultados que, com base no processo apresentado para estados com dois *qubits*, resultam em uma proposta para o critério de separabilidade para estados com três *qubits*.

Lema 3 *Um estado puro arbitrário com três qubits $|\psi\rangle_3$, como em (4.9), é separável se, e somente se,*

$$\begin{array}{ll} \alpha_0 = ace & \alpha_4 = bce \\ \alpha_1 = acf & \alpha_5 = bcf \\ \alpha_2 = ade & \alpha_6 = bde \\ \alpha_3 = adf & \alpha_7 = bdf. \end{array}$$

Demonstração. Considerando que $|\psi\rangle_3 = |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 \otimes |\varphi_3\rangle_1$ e igualando os correspondentes coeficientes dos *kets* em (4.9) e (4.10), segue a verificação. Supondo agora que as igualdades apresentadas neste lema sejam simultaneamente satisfeitas, a substituição de cada uma dessas igualdades nas respectivas posições em (4.9) resulta em

$$\begin{aligned} |\psi\rangle_3 &= ace|000\rangle + acf|001\rangle + ade|010\rangle + adf|011\rangle + bce|100\rangle \\ &\quad + bcf|101\rangle + bde|110\rangle + bdf|111\rangle \\ &= a|0\rangle \otimes (ce|00\rangle + cf|01\rangle + de|10\rangle + df|11\rangle) + \\ &\quad + b|1\rangle \otimes (ce|00\rangle + cf|01\rangle + de|10\rangle + df|11\rangle) \\ &= a|0\rangle \otimes \{c|0\rangle \otimes (e|0\rangle + f|1\rangle) + d|1\rangle \otimes (e|0\rangle + f|1\rangle)\} + \\ &\quad + b|1\rangle \otimes \{c|0\rangle \otimes (e|0\rangle + f|1\rangle) + d|1\rangle \otimes (e|0\rangle + f|1\rangle)\} \\ &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \otimes (e|0\rangle + f|1\rangle) \\ &= |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 \otimes |\varphi_3\rangle_1, \end{aligned}$$

o que caracteriza $|\psi\rangle_3$ como separável.

■

Lema 4 *Todas as igualdades do Lema 3 são válidas se, e somente se,*

$$\begin{array}{ll} \alpha_0\alpha_3 = \alpha_1\alpha_2, & \alpha_1\alpha_7 = \alpha_3\alpha_5, \\ \alpha_0\alpha_5 = \alpha_1\alpha_4, & \alpha_0\alpha_7 = \alpha_2\alpha_5, \\ \alpha_2\alpha_7 = \alpha_3\alpha_6, & \alpha_0\alpha_7 = \alpha_1\alpha_6, \\ \alpha_4\alpha_7 = \alpha_5\alpha_6, & \alpha_0\alpha_7 = \alpha_3\alpha_4. \\ \alpha_0\alpha_6 = \alpha_2\alpha_4, & \end{array}$$

Demonstração. Supondo que as igualdades apresentadas no Lema 3 sejam simultaneamente satisfeitas, é fácil verificar que as equações propostas no Lema 4 são satisfeitas para quaisquer escolhas de $a, b, c, d, e, f \in \mathbb{C}$, tais que $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$ e $|e|^2 + |f|^2 = 1$. A recíproca decorre da mesma idéia utilizada na demonstração do Lema 2.

■

O teorema a seguir é uma conseqüência dos Lemas 3 e 4 e estabelece a proposta do critério de separabilidade para estados com três *qubits*.

Teorema 7 *Um estado puro arbitrário com três qubits $|\psi\rangle_3$, como em (4.9), é separável se, e somente se, todas as equações a seguir são simultaneamente satisfeitas*

$$\begin{aligned}
\alpha_0\alpha_3 &= \alpha_1\alpha_2,\\
\alpha_0\alpha_5 &= \alpha_1\alpha_4,\\
\alpha_0\alpha_6 &= \alpha_2\alpha_4,\\
\alpha_1\alpha_7 &= \alpha_3\alpha_5,\\
\alpha_2\alpha_7 &= \alpha_3\alpha_6,\\
\alpha_4\alpha_7 &= \alpha_5\alpha_6,\\
\alpha_0\alpha_7 &= \alpha_1\alpha_6,\\
\alpha_0\alpha_7 &= \alpha_2\alpha_5,\\
\alpha_0\alpha_7 &= \alpha_3\alpha_4.
\end{aligned}$$

Até este ponto, exibimos uma descrição algébrica para um critério de separabilidade para estados puros com 2 e 3 *qubits*, a partir da qual é possível observar que tal descrição torna-se demasiadamente trabalhosa à medida que o número de *qubits* nos estados aumenta. Como o objetivo é apresentar um procedimento a partir do qual se possa obter um critério de separabilidade para qualquer que seja o número de *qubits* no estado, tal abordagem não é a mais apropriada.

Com o objetivo de contornar este problema, apresentaremos na seção a seguir uma interpretação geométrica para os estados puros com três *qubits* proposta em [125]. Como conseqüência, dessa, propomos uma interpretação também para as equações do critério de separabilidade para estados com este número de *qubits*. Como será mencionado no Capítulo 5, tendo como base o contexto desta interpretação, exibiremos um procedimento do qual será possível obter a forma das equações que definirão o critério de separabilidade generalizado.

4.3 Interpretação Homológica-Geométrica para o Critério de Separabilidade Proposto

Dado um estado quântico puro arbritário com três *qubits*, (4.9), é possível associar a cada índice i dos coeficientes α_i's, $i \in \{0, 1, \cdots, 7\}$, uma sequência binária que se refere ao conteúdo do *ket* do qual α_i é coeficiente.

De acordo com [125], dado um estado puro com três *qubits*, os conteúdos dos *kets* que o definem podem ser geometricamente representados por vértices de um cubo de lado unitário

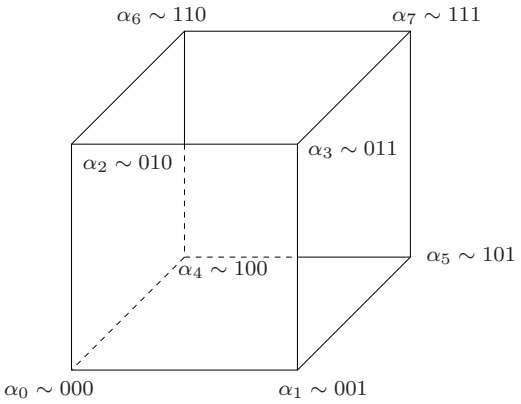


Figura 4.1: Cubo unitário em $\mathcal{H}_2^3$.

definido no espaço de todas as seqüências binárias de comprimento três. Este espaço é conhecido como o *espaço de Hamming* e denotado por $\mathcal{H}_2^3$. Este cubo, por sua vez, denota o grafo associado a este conjunto de coeficientes.

Desta forma, os *kets* que compõem o estado $|\psi\rangle_3$ são representados pelos vértices v_s, $s = 0, ..., 7$, a saber

$$v_0 = (000),\ v_1 = (001),\ v_2 = (010),\ v_3 = (011),$$
$$v_4 = (100),\ v_5 = (101),\ v_6 = (110),\ v_7 = (111).$$

Cada vértice v_s está associado a uma amplitude α_s, $s = 0, ..., 7$ (veja Fig. 4.1). Com o objetivo de simplificar a notação, denotamos por $\mathbf{s}$ a sequência binária que constitui o *ket* de $|\psi\rangle_3$ associado ao vértice v_s do cubo.

Decorrente desta interpretação geométrica, temos que a análise da combinação de *kets* que definem o estado $|\psi\rangle_3$ pode ser determinada pelo estudo do respectivo conjunto de vértices no cubo, definido no espaço de Hamming. Desta forma, faz-se necessário mencionar algumas das propriedades deste espaço.

Definição 8 *[75] A distância de Hamming entre duas seqüências binárias $\mathbf{s}, \mathbf{t} \in \{0,1\}^n$, denotada por $d_H(\mathbf{s}, \mathbf{t})$, é definida como o número de coordenadas em que tais seqüências diferem.*

Por exemplo, se $\mathbf{s} = (001)$ e $\mathbf{t} = (100)$, então $d_H(\mathbf{s}, \mathbf{t}) = 2$. A distribuição das distâncias de Hamming entre as representações de vértices do cubo unitário são apresentadas na Tabela 4.1.

Como mencionado, o cubo que representa $|\psi\rangle_3$ denota também o grafo associado ao conjunto de amplitudes deste estado. Propriedades da homologia de grafos que podem ser encontradas em [50] nos permitem algumas associações entre as amplitudes do $|\psi\rangle_3$, identificadas aos vértices deste grafo (cubo).

Se α_i e α_j são as amplitudes associadas aos vértices v_i e v_j, respectivamente, então associamos o produto dos números complexos α_i e α_j à diagonal (v_i, v_j), de forma que

$$(v_i, v_j) \leftrightarrow \alpha_i \alpha_j.$$

-	000	001	010	011	100	101	110	111
000	0	1	1	2	1	2	2	3
001	-	0	2	1	2	1	3	2
010	-	-	0	1	2	3	1	2
011	-	-	-	0	3	2	2	1
100	-	-	-	-	0	1	1	2
101	-	-	-	-	-	0	2	1
110	-	-	-	-	-	-	0	1
111	-	-	-	-	-	-	-	0

Tabela 4.1: Distribuição de distâncias de Hamming em $\mathcal{H}_2^3$.

Sejam v_i e v_j dois vértices quaisquer do cubo unitário, então (v_i, v_j) será 1-*diagonal* se $d_H(v_i, v_j) = 1$, 2-*diagonal*, se $d_H(v_i, v_j) = 2$, e 3-*diagonal*, se $d_H(v_i, v_j) = 3$. Se (v_i, v_j) e (v_k, v_l) são 2-*diagonais* da mesma face do cubo, então escrevemos que

$$\alpha_i\alpha_j = \alpha_k\alpha_l.$$

Tendo como base a Fig. 4.1 e a Tabela 4.1, segue a lista dos pares de 2-*diagonais* para cada face do cubo e as equações do critério de separabilidade associadas.

$$\begin{aligned}
(000, 011) \text{ e } (001, 010) &\longleftrightarrow \alpha_0\alpha_3 = \alpha_1\alpha_2,\\
(000, 101) \text{ e } (001, 100) &\longleftrightarrow \alpha_0\alpha_5 = \alpha_1\alpha_4,\\
(000, 110) \text{ e } (010, 100) &\longleftrightarrow \alpha_0\alpha_6 = \alpha_2\alpha_4,\\
(001, 111) \text{ e } (011, 101) &\longleftrightarrow \alpha_1\alpha_7 = \alpha_3\alpha_5,\\
(010, 111) \text{ e } (011, 110) &\longleftrightarrow \alpha_2\alpha_7 = \alpha_3\alpha_6,\\
(100, 111) \text{ e } (101, 110) &\longleftrightarrow \alpha_4\alpha_7 = \alpha_5\alpha_6.
\end{aligned}$$

Além dos pares de 2-*diagonais* nas faces do cubo, é necessário analisar também os pares de 3-*diagonais* e as respectivas equações associadas, a saber:

$$\begin{aligned}
(000, 111) \text{ e } (001, 110) &\longleftrightarrow \alpha_0\alpha_7 = \alpha_1\alpha_6,\\
(000, 111) \text{ e } (011, 100) &\longleftrightarrow \alpha_0\alpha_7 = \alpha_3\alpha_4,\\
(001, 110) \text{ e } (010, 101) &\longleftrightarrow \alpha_1\alpha_6 = \alpha_2\alpha_5,\\
(001, 110) \text{ e } (011, 100) &\longleftrightarrow \alpha_1\alpha_6 = \alpha_3\alpha_4,\\
(010, 101) \text{ e } (011, 100) &\longleftrightarrow \alpha_2\alpha_5 = \alpha_3\alpha_4.
\end{aligned}$$

Note que as últimas três equações podem ser obtidas das três primeiras. Assim, para eliminar a redundância deste conjunto, podemos considerar somente as seguintes associações:

$$\begin{aligned}
(000, 111) \text{ e } (001, 110) &\longleftrightarrow \alpha_0\alpha_7 = \alpha_1\alpha_6,\\
(000, 111) \text{ e } (010, 101) &\longleftrightarrow \alpha_0\alpha_7 = \alpha_2\alpha_5,
\end{aligned}$$

$$(000, 111) \text{ e } (011, 100) \quad \longleftrightarrow \quad \alpha_0\alpha_7 = \alpha_3\alpha_4.$$

Observando o conjunto de equações obtidas por esta interpretação homológica-geométrica, concluímos que o conjunto de pares de 2-*diagonais* na mesma face e os pares de 3-*diagonais* geram um conjunto de equações exatamente igual ao do critério de separabilidade proposto no Teorema 7 para estados puros arbitrários com três *qubits*.

Assim, uma forma de se resumir a interpretação do critério de separabilidade dado pelo Teorema 7 em termos das diagonais do cubo é: *um estado puro arbitrário com três qubits é separável se, e somente se, satisfaz as equações na forma* $\alpha_i\alpha_j = \alpha_k\alpha_l$, *onde os índices* i, j, k e l *satisfazem*

$$\begin{cases} d_H(v_i, v_j) = d_H(v_k, v_l) = 2, \\ \text{com} \quad d_H(v_i, v_k) = d_H(v_j, v_l) = 1 \quad \text{e} \quad d_H(v_i, v_l) = d_H(v_j, v_k) = 1, \end{cases}$$

ou

$$\begin{cases} d_H(v_i, v_j) = d_H(v_k, v_l) = 3, \\ \text{com} \quad d_H(v_i, v_k) = d_H(v_j, v_l) = 1 \quad \text{e} \quad d_H(v_i, v_l) = d_H(v_j, v_k) = 2, \end{cases}$$

onde v_i *é o vértice associado à amplitude* α_i, $i \in \{0, \cdots, 7\}$.

As condições adicionais dadas por $d_H(v_i, v_k) = d_H(v_j, v_l) = 1 \quad \text{e} \quad d_H(v_i, v_l) = d_H(v_j, v_k) = 1$ e $d_H(v_i, v_k) = d_H(v_j, v_l) = 1 \quad \text{e} \quad d_H(v_i, v_l) = d_H(v_j, v_k) = 2$ têm o objetivo de garantir que os pares de 2-*diagonais* estejam na mesma face e eliminar a redundância, respectivamente.

É importante salientar que esta interpretação pode ser aplicada também a estados puros arbitrários com dois *qubits*. Neste caso, as representações que formam os possíveis *kets* do estado são interpretados como vértices de um quadrado de lado unitário (veja Fig. 4.2). De acordo com as condições estabelecidas anteriormente, o critério de separabilidade consiste da associação do par de 2-*diagonais* do quadrado, resultando em

$$\alpha_0\alpha_3 = \alpha_1\alpha_2.$$

Este é o mesmo resultado como estabelecido no Teorema 6.

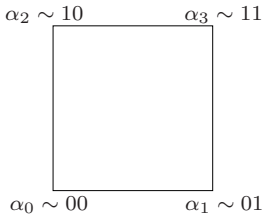


Figura 4.2: Quadrado unitário em $\mathcal{H}_2^2$.

A seguir, apresentamos alguns exemplos de classificação para estados puros arbitrários com três *qubits* segundo a interpretação homológica-geométrica considerada.

Exemplo 12 *Considere o estado*

$$|\psi\rangle_3 = \alpha_0|000\rangle + \alpha_7|111\rangle.$$

A interpretação homológica-geométrica referente a $|\psi\rangle_3$ *consiste em identificar os kets* 000 *e* 111 *aos vértices do cubo unitário* v_0 *e* v_7*, respectivamente, e associar com esses vértices as amplitudes não-nulas* α_0 *e* α_7*, nesta ordem. Todos os outros vértices estão associados a amplitudes nulas, o que implica que qualquer outra diagonal que não a* (v_0, v_7) *está identificada a um produto nulo. Assim, há equações do Teorema 7 que não são satisfeitas, o que implica na classificação deste estado como emaranhado. Explicitamente, as equações que não são satisfeitas por este estado são*

$$\begin{aligned} \alpha_0\alpha_7 &= \alpha_1\alpha_6, \\ \alpha_0\alpha_7 &= \alpha_2\alpha_5, \\ \alpha_0\alpha_7 &= \alpha_3\alpha_4. \end{aligned}$$

Observe a particularidade de que as equações que não são satisfeitas decorrem de associações entre 3*-diagonais.*

Para $\alpha_0 = \alpha_7 = \frac{1}{\sqrt{2}}$ *o estado* $|\psi\rangle_3$ *é o conhecido estado GHZ,* $|\psi_{GHZ}\rangle$*, representado na Fig. 4.3. Como mencionado no Exemplo 5 do Capítulo 2, este estado satisfaz a propriedade do máximo emaranhamento.*

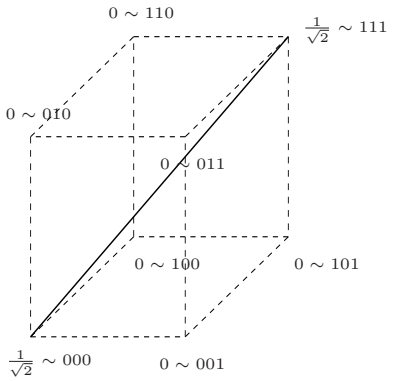


Figura 4.3: Interpretação homológica-geométrica do estado $|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

Exemplo 13 *Considere o estado*

$$|\xi\rangle_3 = \alpha_3|011\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle.$$

A interpretação homológica-geométrica de $|\xi\rangle_3$ *consiste em identificar os kets* 011*,* 101 *e* 110 *aos vértices do cubo unitário* v_3*,* v_5 *e* v_6*, respectivamente, e associar a esses vértices as amplitudes não-nulas* α_3*,* α_5 *e* α_6*, nesta ordem. Segundo o Teorema 7, este estado é classificado como*

emaranhado pois as seguintes equações não são satisfeitas

$$\begin{aligned} \alpha_1\alpha_7 &= \alpha_3\alpha_5, \\ \alpha_2\alpha_7 &= \alpha_3\alpha_6, \\ \alpha_4\alpha_7 &= \alpha_5\alpha_6. \end{aligned}$$

Neste caso, essas equações estão associadas a pares de 2-diagonais de uma mesma face do cubo unitário.

Para $\alpha_3 = \alpha_5 = \alpha_6 = \frac{1}{\sqrt{3}}$, o estado $|\xi\rangle_3$ é o estado W, $|\psi_W\rangle$, representado na Fig. 4.4 (veja Exemplo 6, Capítulo 2).

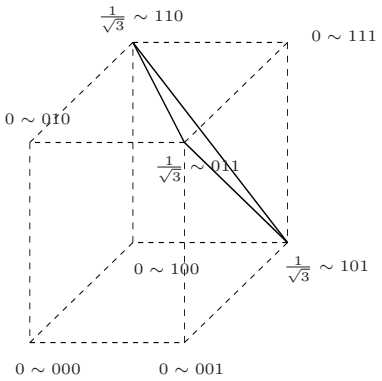


Figura 4.4: Interpretação homológica-geométrica do estado $|\psi_W\rangle = \frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |110\rangle)$.

A partir desta interpretação, exibimos em [46] todas as distribuições de vértices no cubo e quadrado unitário que resultam em estados puros emaranhados com três e dois *qubits*, respectivamente.

De acordo com que foi discutido nesta seção, existe uma forma sistemática de se obter o conjunto de equações que corresponde ao critério de separabilidade para estados puros arbitrários com três *qubits*. Este processo tem como base uma interpretação homológica-geométrica que consiste em identificar tais estados a um cubo de lado unitário em $\mathcal{H}_2^3$, de forma que as equações do critério sejam obtidas pelas combinações dos produtos das amplitudes associadas aos vértices que definem pares de 2-*diagonais* em uma face ou pares de 3-*diagonais*.

A interpretação homológica-geométrica, que consiste em representar o conteúdo dos *kets* que compõem um estado puro com três *qubits* como vértices de um cubo de lado unitário definido num espaço de Hamming pode ser generalizada sob o seguinte raciocínio. Dado um estado puro arbitrário com n *qubits*, os conteúdos dos *kets* que o compõem podem ser representados por vértices de um hipercubo n-dimensional, ou simplesmente, n-cubo, definido no espaço de Hamming, $\mathcal{H}_2^n$. Considerando tal interpretação e associando a amplitude de um dado *ket* ao vértice que representa o conteúdo deste *ket*, é possível repetir para estados com n *qubits* a

proposta de obter um conjunto de equações. Tais equações são estabelecidas pelo produto das amplitudes associadas aos vértices que definem diagonais do n-cubo.

Capítulo 5

Critério de Separabilidade para Estados Puros Arbitrários

O objetivo deste capítulo é apresentar uma proposta de critério de separabilidade para estados puros arbitrários. Além disso, pretende-se exibir uma rotina computacional que, sendo fornecidos a distribuição de amplitudes e as seqüências binárias que constituem o conjunto de *kets* de um estado puro, apresenta quais são as equações do critério de separabilidade que não são satisfeitas, estabelecendo, conseqüentemente, a classificação do referido estado.

Este capítulo está organizado da seguinte forma. Na Seção 5.1, exemplificamos como a forma das equações do conjunto candidato a critério de separabilidade é obtida, considerando estados puros com quatro *qubits*. Na Seção 5.2, explicitamos a construção deste conjunto candidato para estados puros arbitrários e a demonstração de que se trata de um critério de separabilidade generalizado. Na Seção 5.3, salientamos as particularidades da análise das condições referentes ao critério proposto quando a distribuição de amplitudes e o conjunto de *kets* de um estado particular. Tendo como base este estudo, na Seção 5.4, apresentamos as rotinas computacionais que permitem a classificação de estados puros arbitrários, sendo fornecidas as configurações (distribuição de amplitudes e conjunto de *kets*) destes. Finalmente, na Seção 5.5, mencionamos as principais características da proposta.

5.1 Critério de Separabilidade para Estados Puros com Quatro *Qubits*

Considere um estado puro arbitrário com quatro *qubits* representado na forma

$$|\psi\rangle_4 = \alpha_0|0000\rangle + \alpha_1|0001\rangle + \cdots + \alpha_{14}|1110\rangle + \alpha_{15}|1111\rangle, \tag{5.1}$$

onde $\alpha_0, ..., \alpha_{15} \in \mathbb{C}$ e $\sum_{s=0}^{15} |\alpha_s|^2 = 1$.

Como mencionado anteriormente, o conteúdo dos *kets* de um estado puro arbitrário pode ser interpretado geometricamente por vértices de um cubo de lado unitário definido no espaço de Hamming de dimensão adequada. Um estado puro com quatro *qubits* tem dezesseis possíveis

seqüências binárias para o conteúdo dos *kets*. Um hipercubo 4-dimensional tem exatamente este número de vértices. Como as seqüências são binárias e têm comprimento quatro, então este hipercubo é definido no espaço de Hamming $\mathcal{H}_2^4$.

Considerando tais argumentos, temos que as seqüências que constituem os *kets* de um estado puro arbitrário com quatro *qubits* podem ser interpretados como vértices um hipercubo unitário em $\mathcal{H}_2^4$ (veja Fig. 5.1). Para simplificar a notação, denotaremos tal hipercubo por 4-cubo.

De acordo com a proposta do Capítulo 4, um conjunto de equações pode ser obtido a partir das associações de produtos de amplitudes identificadas com vértices que definem diagonais do 4-cubo. Quanto aos conjuntos de diagonais, o 4-cubo possibilita a existência de 2-*diagonais*, 3-*diagonais* e também as 4-*diagonais*, definidas por pares de vértices (v_i, v_j) satisfazendo $d_H(v_i, v_j) = 4$.

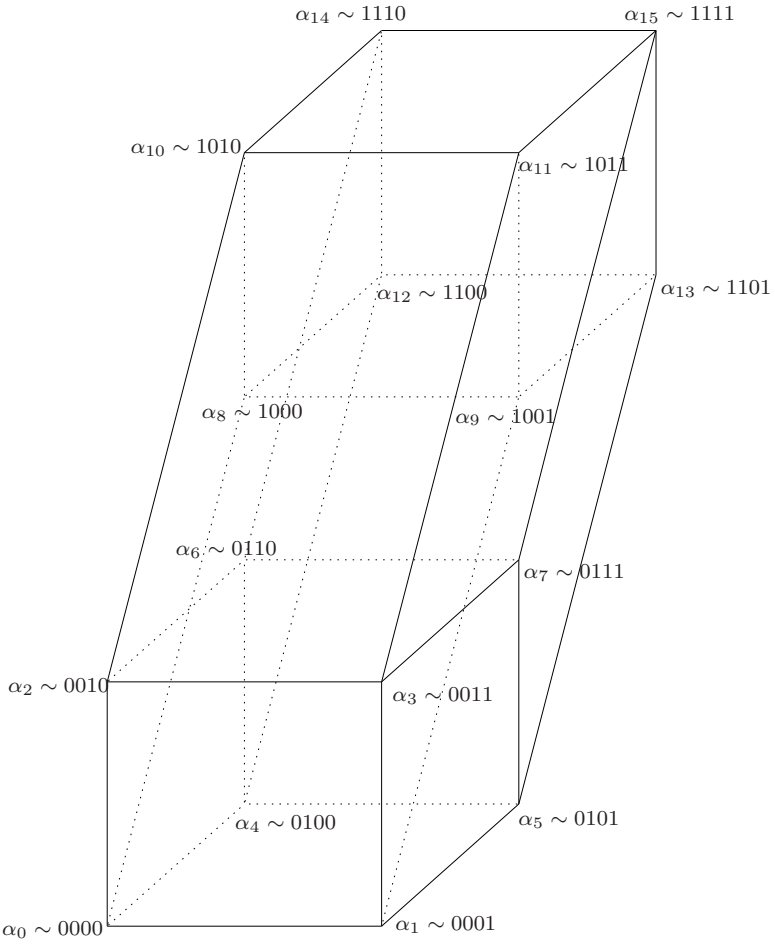


Figura 5.1: Hipercubo unitário em $\mathcal{H}_2^4$.

Desta forma, um conjunto de equações *candidato* ao critério de separabilidade para estados puros com quatro *qubits* é obtido por equações da forma $\alpha_i\alpha_j = \alpha_k\alpha_l$, tal que a escolha de i, j,

k e l satisfaça

$$\begin{cases} d_H(v_i,v_j) = d_H(v_k,v_l) = 2, \\ \text{com} \quad d_H(v_i,v_k) = d_H(v_j,v_l) = 1 \quad \text{e} \quad d_H(v_i,v_l) = d_H(v_j,v_k) = 1, \end{cases}$$

ou

$$\begin{cases} d_H(v_i,v_j) = d_H(v_k,v_l) = 3, \\ \text{com} \quad d_H(v_i,v_k) = d_H(v_j,v_l) = 1 \quad \text{e} \quad d_H(v_i,v_l) = d_H(v_j,v_k) = 2, \end{cases}$$

ou

$$\begin{cases} d_H(v_i,v_j) = d_H(v_k,v_l) = 4, \\ \text{com} \quad d_H(v_i,v_k) = d_H(v_j,v_l) = 1 \quad \text{e} \quad d_H(v_i,v_l) = d_H(v_j,v_k) = 3, \end{cases}$$

onde α_i é a amplitude associada ao vértice v_i, $i \in \{0, \cdots, 15\}$.

De acordo com as condições explicitadas acima e demais associações definidas, é possível obter um conjunto de equações candidato ao critério de separabilidade, como ocorreu para estados puros com três *qubits*. A demonstração de que o conjunto de equações obtido constitui um critério de separabilidade para estados com quatro *qubits* é apresentada a seguir.

5.2 Critério de Separabilidade para Estados Puros Arbitrários

Definição 9 *Seja $|\psi\rangle_n$ um estado puro arbitrário com n qubits dado por*

$$|\psi\rangle_n = \alpha_0|00\cdots0\rangle + \alpha_1|00\cdots1\rangle + \cdots + \alpha_{2^n-2}|11\cdots0\rangle + \alpha_{2^n-1}|11\cdots1\rangle, \tag{5.2}$$

onde $\alpha_0, ..., \alpha_{2^n-1} \in \mathbb{C}$ e $\sum_{s=0}^{2^n-1} |\alpha_s|^2 = 1$. $|\psi\rangle_n$ é dito separável se puder ser escrito como $|\psi\rangle_n = |\varphi_1\rangle_1 \otimes |\varphi_2\rangle_1 \otimes \cdots \otimes |\varphi_n\rangle_1$, onde $|\varphi_1\rangle_1, |\varphi_2\rangle_1, \cdots, |\varphi_n\rangle_1$ são estados puros com 1 qubit.

Considerando $|\delta\rangle_{n-1}$ como sendo um estado arbitrário com $(n-1)$ *qubits* que pode ser decomposto como o produto de $(n-1)$ estados de um *qubit* (ou seja, é um estado separável), então um estado com n *qubits* separável pode ser representado como $|\psi\rangle_n = |\varphi_1\rangle_1 \otimes |\delta\rangle_{n-1}$.

Da mesma forma que as representações contidas nos *kets* dos estados $|\psi\rangle_3$ e $|\psi\rangle_4$ foram identificados a vértices do 3-cubo e do 4-cubo nos respectivos espaços de Hamming, é possível identificar um estado arbitrário com n *qubits* $|\psi\rangle_n$ a um n-cubo unitário no espaço das seqüências binárias de comprimento n, $\mathcal{H}_2^n$. Um conjunto de equações pode ser obtido pelas associações das diagonais deste n-cubo, como especificado para estados puros com 2, 3 e 4 *qubits*.

Enquanto para esses casos era possível visualizar a definição das diagonais a partir dos vértices, para estados com n *qubits* isso não ocorre. Porém, como foi mencionado na Definição 8, a distância de Hamming nos possibilita descrever as diagonais com base apenas nas seqüências binárias que estão associadas aos vértices. Por isso, o critério de separabilidade para estados puros arbitrários é definido em função destas seqüências.

O objetivo do Teorema 8 é apresentar a forma geral para a obtenção destas equações, referentes às associações das diagonais, para qualquer que seja o número de *qubits* no estado e comprovar que este conjunto consiste, de fato, de um critério de separabilidade para os estados associados.

Teorema 8 *Um critério de separabilidade para estados puros arbitrários com n qubits, como em (5.2), é dado pelo conjunto de equações $\alpha_i\alpha_j = \alpha_k\alpha_l$, onde i, j, k e $l \in \{0, 1, \cdots, 2^n - 1\}$ são escolhidos de acordo com as seguintes condições*

$$d_H(\mathbf{i}, \mathbf{j}) = d_H(\mathbf{k}, \mathbf{l}) = t, \tag{5.3}$$

satisfazendo

$$d_H(\mathbf{i}, \mathbf{k}) = d_H(\mathbf{j}, \mathbf{l}) = 1 \quad e \quad d_H(\mathbf{i}, \mathbf{l}) = d_H(\mathbf{j}, \mathbf{k}) = t - 1, \tag{5.4}$$

onde $2 \leq t \leq n$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ e $\mathbf{l}$ são seqüências binárias de comprimento n associadas, respectivamente, às amplitudes α_i, α_j, α_k e α_k, nesta ordem.

As equações (5.3) e (5.4) apresentam a forma geral para condições que, impostas sobre os vértices cujas representações são $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ e $\mathbf{l}$, geram as 2-*diagonais*, 3-*diagonais*, $\cdots$, n-*diagonais*. Em particular, (5.4) garante que os pares de diagonais estejam na mesma face para $t \neq n$ e elimina a redundância das equações quando $t = n$.

Para demonstrar a validade deste resultado, utilizamos o princípio de indução finita sobre o número n de *qubits* dos estados. Isso porque, como mencionado anteriormente, as componentes do *kets* que definem um estado com n *qubits* estão associadas às seqüências binárias que definem o espaço de Hamming $\mathcal{H}_2^n$. É fácil verificar que as seqüências binárias de comprimento n podem ser obtidas a partir das seqüências de comprimento $(n-1)$ (veja Lema 5). Além disso, sabemos que no n-cubo pode-se definir todos os conjuntos de k-*diagonais*, onde $2 \leq k \leq n$. Disso decorre que as condições sob a distância entre as seqüências binárias de comprimento k, para $2 \leq k \leq (n-1)$, continuam válidas.

Como trata-se de uma demonstração longa, optamos por dividi-la entre resultados de demonstrações menos complexas e extensas. Esta divisão está baseada no padrão de apresentação dos resultados estabelecidos referentes a estados puros com dois e três *qubits*

De forma resumida, a demonstração do Teorema 8 decorrerá da seguinte forma. A Proposição 2 é uma generalização dos Lemas 1 e 3 e consiste em analisar as condições necessárias e suficientes sobre as quais as amplitudes de um estado arbitrário são iguais às correspondentes em um estado separável. Em seguida, a Proposição 3 estabelece as combinações na forma $\alpha_i\alpha_j = \alpha_k\alpha_l$ entre as amplitudes descritas na Proposição 2, que resultam em igualdade. Por outro lado, a Proposição 4 estabelece que se todas as combinações entre as amplitudes na forma $\alpha_i\alpha_j = \alpha_k\alpha_l$ são satisfeitas, então as decomposições de amplitudes do estado arbitrário propostas na Proposição 2 são também satisfeitas, donde decorre a separabilidade do estado[1]. Desta forma, podemos afirmar que as equações mencionadas na Proposição 4 constituem um critério de separabilidade. Entretanto, explicitamente, este conjunto de equações não está na forma das condições (5.3) e (5.4). Para verificar a validade do Teorema 8, temos que demonstrar que o conjunto de equações obtido a partir de (5.3) e (5.4) é equivalente ao conjunto de equações mencionado na Proposição 3. Este resultado é apresentado na Proposição 5.

[1]Observe que as Proposições 3 e 4 são generalizações do resultado apresentados pelos Lemas 2 e 4.

Estabelecido um resumo dos fundamentos da verificação do Teorema 8, em seguida, a apresentamos de fato.

Proposição 2 *Um estado puro arbitrário com n qubits* $|\psi\rangle_n$*, como em (5.2), é separável se, e somente se,*

$$\begin{array}{cc} \alpha_0 = a\theta_0 & \alpha_{2^{n-1}} = b\theta_0 \\ \alpha_1 = a\theta_1 & \alpha_{2^{n-1}+1} = b\theta_1 \\ \vdots & \vdots \\ \alpha_{2^{n-1}-1} = a\theta_{2^{n-1}-1} & \alpha_{2^{n-1}+(2^{n-1}-1)} = b\theta_{2^{n-1}-1}, \end{array}$$

onde θ_i*,* $i \in \{0, \cdots 2^{n-1}-1\}$*, são as amplitudes de um estado puro separável com* $(n-1)$ *qubits* $|\delta\rangle_{n-1}$*.*

Demonstração. Se $|\psi\rangle_n$ é separável, então $|\psi\rangle_n = |\varphi\rangle_1 \otimes |\delta\rangle_{n-1}$, onde $|\delta\rangle_{n-1}$ é um estado separável. Pela hipótese indutiva, temos que as amplitudes θ_i, $i \in \{0, \cdots, 2^{n-1}-1\}$, associadas ao estado $|\delta\rangle_{n-1}$ admitem as decomposições apresentadas. Assim, utilizando a propriedade distributiva do produto tensorial, decorre a validade das decomposições apresentadas. Supondo agora que as decomposições sejam válidas, podemos substituí-las em (5.2), e assim temos $|\psi\rangle_n = (a|0\rangle + b|1\rangle) \otimes |\delta\rangle_{n-1}$, donde segue que $|\psi\rangle_n$ é separável, pois, pela hipótese indutiva, $|\delta\rangle_{n-1}$ é separável, o que conclui a demonstração.

■

Proposição 3 *Se as decomposições apresentadas na Proposição 2 são simultaneamente verdadeiras, então são satisfeitas simultaneamente as equações obtidas a partir da decomposição das amplitudes de um estado puro arbitrário* $|\delta\rangle_{n-1}$*, e também as equações geradas pelas seguintes formas*

$$\begin{aligned} \alpha_x\alpha_{2^{n-1}+z} &= \alpha_{2^{n-1}+x}\alpha_z, \\ \alpha_{2^{n-1}+x}\alpha_{2^{n-1}+2^{n-2}+z} &= \alpha_{2^{n-1}+2^{n-2}+x}\alpha_{2^{n-1}+z}, \\ &\vdots \\ \alpha_{2^{n-1}+x}\alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+z} &= \alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+x}\alpha_{2^{n-1}+z}, \\ \alpha_{2^{n-1}+2^{n-2}+x}\alpha_{2^{n-1}+2^{n-2}+2^{n-3}+z} &= \alpha_{2^{n-1}+2^{n-2}+2^{n-3}+x}\alpha_{2^{n-1}+2^{n-2}+z}, \\ &\vdots \\ \alpha_{2^{n-1}+2^{n-2}+x}\alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+z} &= \alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+x}\alpha_{2^{n-1}+2^{n-2}+z}, \\ &\vdots \\ \alpha_{2^{n-1}+\cdots+2^{n-(n-2)}+x}\alpha_{2^{n-1}++\cdots+2^{n-(n-1)}+z} &= \alpha_{2^{n-1}+\cdots+2^{n-(n-1)}+x}\alpha_{2^{n-1}+\cdots+2^{n-(n-2)}+z}, \\ \alpha_x\alpha_{2^{n-1}+2^{n-2}+z} &= \alpha_{2^{n-1}+2^{n-2}+x}\alpha_z, \end{aligned}$$

$$\alpha_x\alpha_{2^{n-1}+2^{n-2}+2^{n-3}+z} = \alpha_{2^{n-1}+2^{n-2}+2^{n-3}+x}\alpha_z,$$
$$\vdots$$
$$\alpha_x\alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+z} = \alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+x}\alpha_z,$$

onde $x < z, x, z \in \{0, \cdots 2^{n-1}-1\}$.

Demonstração. Antes da demonstração propriamente dita, salientamos que o principal ponto desta proposição é obter as equações de separabilidade para estados com n *qubits*, sendo conhecido o critério de separabilidade para $(n-1)$ *qubits*. Como tais equações são definidas a partir do arranjo entre as amplitudes do estado com condições sobre os respectivos índices, o primeiro passo é obter os índices das amplitudes dos estados com n *qubits* a partir das amplitudes referentes a estados com $(n-1)$ *qubits*. Com base na interpretação geométrica e notação apresentadas, cada amplitude α_i, $i \in \{0, \cdots, 2^n-1\}$, é representada em $\mathcal{H}_2^n$ pela seqüência binária $\mathbf{i}$, que consiste da representação binária de i. Assim, o objetivo é obter uma forma de descrever as seqüências binárias de comprimento n a partir das de comprimento $n-1$. Segue um fato importante nesse contexto.

Lema 5 *Seja* $\mathbf{i}$ *a seqüência binária de comprimento* $(n-1)$ *associada à representação binária do número* i, $i \in \{0, \cdots, 2^{n-1}-1\}$. *Sem perda de generalidade, a seqüência binária de comprimento* n *de um número pertencente a* $\{0, \cdots, 2^n-1\}$ *pode ser obtida, a partir de* $\mathbf{i}$, *de duas formas, a saber:*

1. *Um dígito "0" é acrescentado à esquerda de* $\mathbf{i}$. *Neste caso, o número associado à seqüência binária de comprimento* n é também i, *que assume valores em* $\{0, \cdots, 2^{n-1}-1\}$.

2. *Um dígito "1" é acrescentado à esquerda de* $\mathbf{i}$. *Neste caso, o número associado à seqüência binária passa a ser* $i + 2^{n-1}$.

Observamos que os índices de amplitudes na forma $2^{n-1}+x$ para o caso com $(n-1)$ *qubits*, quando escritos para estados com n *qubits*, passam a ser $2^{n-1-1}+x$, ou seja, $2^{n-2}+x$.

Supondo que as decomposições da Proposição 2 sejam verdadeiras, temos que, para $n=2$, a única igualdade verdadeira é $\alpha_0\alpha_3 = \alpha_1\alpha_2$, que pode ser representada na forma $\alpha_x\alpha_{2^{n-1}+z} = \alpha_{2^{n-1}+x}\alpha_z$, para $x, z, 2^{n-1}+z, 2^{n-1}+x \in \{0, \cdots, 2^n-1\}$. A hipótese indutiva consiste em supor que a Proposição 3 seja verdadeira para estados com $(n-1)$ *qubits*. Supondo válidas as decomposições apresentadas na Proposição 2, pode-se verificar que todas as equações geradas pela forma $\alpha_x\alpha_{2^{n-1}+z} = \alpha_{2^{n-1}+x}\alpha_z$, com $x, 2^{n-1}+z, 2^{n-1}+x, z \in \{0, \cdots, 2^n-1\}, x < z$, são verdadeiras para quaisquer que sejam os valores de a, b e θ_i, $i \in \{0, \cdots, 2^{n-2}-1\}$, com a ressalva de que $\sum_{i=0}^{2^{n-2}-1} |\theta_i|^2 = 1$.

Todavia, outras igualdades podem ser obtidas da seguinte forma: dados os estados $|\varphi\rangle_1 = a|0\rangle + b|1\rangle$ e $|\delta\rangle_{n-1} = \theta_0|0\cdots0\rangle + \cdots + \theta_{2^{n-1}-1}|1\cdots1\rangle$, o produto tensorial $|\varphi\rangle_1 \otimes |\delta\rangle_{n-1}$ gera um estado de n *qubits* separável, para o qual valem as decomposições da Proposição 2. Analisando os arranjos entre as amplitudes do estado $|\psi\rangle_n$ resultante, de acordo com o Lema 5, temos:

- Para o caso $|\psi\rangle_n = a|0\rangle \otimes |\delta\rangle_{n-1}$, as amplitudes geram igualdades analisadas pela hipótese indutiva, uma vez que as seqüências binárias de comprimento n são caracterizadas como o item 1 do Lema 5.

- Para o caso $|\psi\rangle_n = b|1\rangle \otimes |\delta\rangle_{n-1}$, os índices das amplitudes são adicionados de 2^{n-1}, como foi explicitado no item 2 do Lema 5. Com isso, temos as seguintes igualdades para serem consideradas:

$$\alpha_{2^{n-1}+x}\alpha_{2^{n-1}+2^{n-2}+z} = \alpha_{2^{n-1}+2^{n-2}+x}\alpha_{2^{n-1}+z},$$
$$\vdots$$
$$\alpha_{2^{n-1}+2^{n-2}+x}\alpha_{2^{n-1}+2^{n-2}+2^{n-3}+z} = \alpha_{2^{n-1}+2^{n-2}+2^{n-3}+x}\alpha_{2^{n-1}+2^{n-2}+z},$$
$$\vdots$$
$$\alpha_{2^{n-1}+\cdots+2^{n-(n-2)}+x}\alpha_{2^{n-1}+\cdots+2^{n-(n-1)}+z} = \alpha_{2^{n-1}+\cdots+2^{n-(n-1)}+x}\alpha_{2^{n-1}+\cdots+2^{n-(n-2)}+z},$$

  para x e z tais que $x < z$ são índices de amplitudes pertencentes ao conjunto $\{0, \cdots, 2^n - 1\}$.

- Para o caso $|\psi\rangle_n = (a|0\rangle + b|1\rangle) \otimes |\delta\rangle_{n-1}$, pode-se verificar que os arranjos entre as amplitudes podem ser resumidos pela seguinte forma

$$\alpha_x\alpha_{2^{n-1}+2^{n-2}+z} = \alpha_{2^{n-1}+2^{n-2}+x}\alpha_z,$$
$$\vdots$$
$$\alpha_x\alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+z} = \alpha_{2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^{n-(n-1)}+x}\alpha_z,$$

  para $x < z$ e índices de amplitudes pertencentes a $\{0, \cdots, 2^n - 1\}$.

Considerando os quatro conjuntos de equações obtidos, concluímos a verificação da Proposição 3.

■

Note que a forma como as equações são apresentadas na Proposição 3 dificulta a descrição e a manipulação desses dados, embora satisfaçam o formato as equações que constituem o critério para estados com três *qubits* e sejam explícitas quanto a relação de comparação entre os produtos das amplitudes do estado.

Com o objetivo de amenizar o problema da manipulação dessas equações, apresentamos em seguida uma forma alternativa e mais concisa de expressá-las.

Para n fixo, correspondendo ao número de qubits de um estado puro arbitrário, consideramos todo k natural tal que $k \in \{0, \cdots n-2\}$. *A cada valor de k é associado um valor* m_k *tal que*

$$m_k = \begin{cases} 2^{n-1}, & \text{se } k = 0 \\ \text{soma de todas as potências de 2 maiores ou iguais a } 2^{(n-1)-k}, & \text{se } k \neq 0. \end{cases}$$

O primeiro conjunto descrevendo as igualdades obtidas a partir da decomposição das amplitudes do estado $|\psi\rangle_n$*, dadas pela Proposição 3, é da forma*:

$$\alpha_x \alpha_{m_k+z} = \alpha_{m_k+x} \alpha_z, \tag{5.5}$$

onde $x, m_k + z, m_k + x, z \in \{0, \cdots, 2^n - 1\}, x < z$.

A partir do conjunto de possibilidades para k*, definimos* g*, número natural,* $g \in \{1, \cdots, n-2\}$*, com* $k < g$*. Fixado* g*, associamos o valor* m_g *correspondente. O segundo conjunto, descrevendo as igualdades obtidas a partir da decomposição das amplitudes do estado* $|\psi\rangle_n$*, nas condições da hipótese, é dado por*

$$\alpha_{m_k+x} \alpha_{m_g+z} = \alpha_{m_g+x} \alpha_{m_k+z}, \tag{5.6}$$

para $k < g$, g *fixo, onde* $m_k + x, m_g + z, m_g + x, m_k + z \in \{0, \cdots, 2^n - 1\}, x < z$.

Podemos verificar que as equações (5.5) e (5.6) contêm redundância entre si e, ao contrário das equações (5.3) e (5.4), não existe uma interpretação geométrica que possibilite reduzi-la. Entretanto, tais expressões facilitam a descrição das equações apresentadas na Proposição 3. Passamos à Proposição 4, onde utilizaremos explicitamente as formas (5.5) e (5.6).

Proposição 4 *Se todas as igualdades apresentadas na Proposição 3 são simultaneamente satisfeitas, então as decomposições das amplitudes de* $|\psi\rangle_n$*, exibidas na Proposição 2, são simultaneamente satisfeitas.*

Demonstração. A idéia é demonstrar que, se são verdadeiras as igualdades da Proposição 3, então é possível decompor as amplitudes do estado puro com n *qubits* como o produto de dois números complexos e, em seguida, mostrar que uma das parcelas pode ser decomposta como o produto de $(n-1)$ números complexos (veja a demonstração do Lema 2, Capítulo 4). Supondo que as amplitudes sejam todas diferentes de zero, é possível escolher a seguinte decomposição para as amplitudes:

$$\alpha_0 = \beta_0 \gamma_0, \tag{5.7}$$
$$\alpha_1 = \beta_0 \gamma_1, \tag{5.8}$$
$$\alpha_2 = \beta_0 \gamma_2, \tag{5.9}$$
$$\vdots$$
$$\alpha_{2^{n-1}-1} = \beta_0 \gamma_{2^{n-1}-1}, \tag{5.10}$$
$$\alpha_{2^{n-1}} = \beta_1 \gamma_0, \tag{5.11}$$

para β_0 e β_1 números complexos fixos e não nulos e γ_v, $v \in \{0, \cdots 2^{n-1} - 1\}$, números complexos diferentes de zero, por conseqüência da escolha das amplitudes α_i's não nulas, $i \in \{0, \cdots, 2^n - 1\}$. Substituindo nas equações (5.5) e (5.6), obtemos a decomposição suposta e a unicidade desta para as demais amplitudes. No caso de haver ao menos uma amplitude nula, a substituição dessas nas equações (5.5) e (5.6) implica em condições com relação às outras amplitudes. Substituindo essas em (5.2), obtemos estados separáveis e, pela Proposição 2, decorrem as decomposições, o que conclui a demonstração da Proposição 4.

■

Segundo as Proposições 2, 3 e 4, as equações (5.5) e (5.6) são as formas gerais para o critério de separabilidade generalizado. Porém, como já foi discutido, tais equações são pouco intuitivas e geram um conjunto com mais redundância quando comparadas às formas (5.3) e (5.4).

O objetivo do Lema 6 e da Proposição 5 é mostrar a equivalência entre o conjunto de equações gerado pelas equações (5.3) e (5.4) e o obtido a partir das equações (5.5) e (5.6).

Lema 6 *Sejam α_i e α_j amplitudes de $|\psi\rangle_n$, com $i, j \in \{0, \cdots, 2^n - 1\}$, associadas às seqüências binárias* $\mathbf{i}$ *e* $\mathbf{j}$*, respectivamente. Então,*

$$d_H(\mathbf{i}, \mathbf{j}) = peso(\mathbf{i} + \mathbf{j}) = n \Longleftrightarrow i + j = 2^n - 1,$$

onde $peso(\mathbf{i} + \mathbf{j})$ indica o peso de Hamming, definido como sendo o número de componentes diferentes de zero da seqüência referente a $\mathbf{i} + \mathbf{j}$, onde + refere-se à operação de soma vetorial módulo 2.

Demonstração. Considerando que $d_H(\mathbf{i}, \mathbf{j}) = peso(\mathbf{i} + \mathbf{j}) = n$, por definição da distância de Hamming, as seqüências $\mathbf{i}$ e $\mathbf{j}$ diferem em todas as n posições. Em termos da notação utilizada para estados puros arbitrários com n *qubits*, dada em (5.2), isso ocorre nos *kets* em que as amplitudes têm índices, i e j, complementares quanto a $2^n - 1$, ou seja, $i + j = 2^n - 1$. Supondo agora que os índices i e j são tais que $i + j = 2^n - 1$, pela notação adotada em (5.2), temos que as seqüências binárias $\mathbf{i}$ e $\mathbf{j}$ diferem em todas as n posições, de forma que $d_H(\mathbf{i}, \mathbf{j}) = peso(\mathbf{i} + \mathbf{j}) = n$, donde decorre o Lema 6.

■

Segue a proposição final.

Proposição 5 *O conjunto das igualdades apresentadas na Proposição 3 é equivalente ao conjunto das equações geradas por (5.3) e (5.4).*

Demonstração. Como foi discutido, as equações da Proposição 3 podem ser descritas em termos das equações (5.5) e (5.6). Desta forma, o objetivo inicial é analisar se tais formas satisfazem as condições dadas pelas equações (5.3) e (5.4). Para isso, analisamos quais os possíveis valores da distância de Hamming entre as seqüências binárias $\mathbf{x}, \mathbf{m_k} + \mathbf{z}, \mathbf{m_k} + \mathbf{x}, \mathbf{z}$, referentes a (5.5), e $\mathbf{m_k} + \mathbf{x}, \mathbf{m_g} + \mathbf{z}, \mathbf{m_g} + \mathbf{x}, \mathbf{m_k} + \mathbf{z}$, referentes a (5.6), arranjados nas formas (5.3) e (5.4).

Os valores da distância obtidos para os arranjos de $\mathbf{x}, \mathbf{m_k} + \mathbf{z}, \mathbf{m_k} + \mathbf{x}, \mathbf{z}$ e $\mathbf{m_k} + \mathbf{x}, \mathbf{m_g} + \mathbf{z}, \mathbf{m_g} + \mathbf{x}, \mathbf{m_k} + \mathbf{z}$, na forma de (5.3), devem atingir o valor máximo n. No caso da forma $d_H(\mathbf{i}, \mathbf{l}) = d_H(\mathbf{j}, \mathbf{k})$, os valores devem estar limitados por $n - 1$ e, na forma, $d_H(\mathbf{i}, \mathbf{k}) = d_H(\mathbf{j}, \mathbf{l})$ deve admitir valor 1, onde $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ e $\mathbf{l} \in \{\mathbf{x}, \mathbf{m_k} + \mathbf{z}, \mathbf{m_k} + \mathbf{x}, \mathbf{z}, \mathbf{m_g} + \mathbf{z}, \mathbf{m_g} + \mathbf{x}\}$. Se estas três

condições forem satisfeitas, então verificamos que as equações (5.5) e (5.6) são caracterizadas pelas equações (5.3) e (5.4).

A equação (5.5) é dada por $\alpha_x\alpha_{m_k+z} = \alpha_{m_k+x}\alpha_z$, onde $k \in \mathbb{N}$, $k \in \{0, \cdots, n-2\}$, $m_k = 2^{n-1}$, se $k = 0$ ou m_k igual a soma de todas as potências de 2 maiores ou iguais a $2^{(n-1)-k}$, com $x, m_k + z, m_k + x, z \in \{0, \cdots, 2^N - 1\}, x < z$. Analisando tal equação na forma de (5.3), temos $d_H(\mathbf{x}, \mathbf{m_k} + \mathbf{z}) = peso(\mathbf{x} + \mathbf{m_k} + \mathbf{z}) = d_H(\mathbf{m_k} + \mathbf{x}, \mathbf{z})$. Como $z + m_k \leq 2^n - 1$, existe um z e um m_k tais que $z + m_k = 2^n - 1$. Considerando $x = 0$, temos que $x + z + m_k = 2^n - 1$, donde, pelo Lema 6, temos que $peso(\mathbf{x} + \mathbf{m_k} + \mathbf{z})$ assume todos os valores naturais menores ou iguais a n. Portanto, $d_H(\mathbf{x}, \mathbf{m_k} + \mathbf{z}) = d_H(\mathbf{m_k} + \mathbf{x}, \mathbf{z}) = t$, para $t \in \mathbb{N}, 2 \leq t \leq n$, e assim, concluímos a demonstração de que a equação (5.5) pode ser representada em termos de (5.3).

Quanto às condições dadas por (5.4), observamos que m_k é um número par e sua representação binária pode assumir, no máximo, peso de Hamming de valor $n - 1$. Como o caso de $m_k = 0$ está excluído, por definição, então a escolha de $peso(\mathbf{m_k}) = 1$ é possível de acordo com esta construção. Portanto, $d_H(\mathbf{x}, \mathbf{m_k} + \mathbf{x}) = d_H(\mathbf{z}, \mathbf{m_k} + \mathbf{z}) = 1$. Temos, também, que $d_H(\mathbf{x}, \mathbf{z}) = d_H(\mathbf{m_k} + \mathbf{z}, \mathbf{m_k} + \mathbf{x}) = peso(\mathbf{x} + \mathbf{z})$. Como é possível escolher $x = 2^{n-1} - 1$, decorre que $x + z = 2^{n-1} - 2 < 2^{n-1}$. Pelo Lema 6, temos que o máximo valor que a função $peso(\mathbf{x} + \mathbf{z})$ pode assumir é $n - 1$. Portanto, podemos escrever que $d_H(\mathbf{x}, \mathbf{z}) = d_H(\mathbf{m_k} + \mathbf{z}, \mathbf{m_k} + \mathbf{x}) = t - 1$, para $t \in \mathbb{N}$, tal que $2 \leq t \leq n$, o que conclui a verificação que a equação (5.5) satisfaz as condições de (5.3) e (5.4).

Analogamente, utilizamos o mesmo tipo de raciocínio para inferir com respeito a equação (5.6), o que completa a demonstração da primeira parte. Com os mesmos argumentos, demonstramos também que as equações obtidas pelas formas (5.3) e (5.4) podem ser reescritas nas formas de (5.5) e (5.6), completando então a demonstração da Proposição 5.

■

Analisando o conjunto de resultados desta seção, temos que as decomposições satisfeitas pelas amplitudes de estados puros separáveis apresentadas na Proposição 2 implicam em um conjunto de equações descritas pela Proposição 3. Tal conjunto, por sua vez, é equivalente ao gerado sob as restrições das equações (5.3) e (5.4), segundo a Proposição 5. Assim, concluímos que um estado quântico puro satisfaz as equações geradas sob as condições do Teorema 8. Por outro lado, se as equações geradas sob as condições de (5.3) e (5.4) são satisfeitas, então, pela Proposição 5, são satisfeitas as equações apresentadas na Proposição 3, o que implica, pela Proposição 4, que as decomposições da Proposição 2 são satisfeitas, donde resulta que o estado é separável. Em outras palavras, se as equações que definem o Teorema 8 são satisfeitas para um estado quântico puro, então este estado é separável. Disso concluímos que o Teorema 8 constitui um critério de separabilidade para estados quânticos puros com n *qubits*.

Como foi mencionado anteriormente, a demonstração do Teorema 8 decorre diretamente das proposições verificadas.

■

Concluímos esta seção salientando que o Teorema 8 estabelece um critério de separabilidade para estados quânticos puros arbitrários. Outras considerações sobre esta proposta podem ser encontradas em [49].

5.3 Particularidades da Classificação de Estados

Como mencionado na seção anterior, estabelecemos um procedimento a partir do qual é possível obter um critério de separabilidade para estados puros arbitrários.

A questão que queremos abordar nesta seção refere-se ao problema de classificar em emaranhado ou separável um estado quântico puro arbitrário. Embora a proposta mencionada no Teorema 8 seja suficiente para exibir esta resposta, podemos supor que o conhecimento das amplitudes e das seqüências binárias que compõem os *kets* de um estado implica em uma simplificação dos cálculos necessários para garantir a classificação desejada.

Como mencionado anteriormente, dado um estado puro arbitrário com n *qubits*, os conteúdos dos *kets* que definem este estado podem ser interpretados como vértices de um n-cubo unitário, que são representados por seqüências binárias de comprimento n. A amplitude associada a cada *ket* é então identificada ao respectivo vértice (veja Exemplos 12 e 13, Capítulo 4). Tendo como base o Teorema 8, a partir do conceito de distância de Hamming, é possível determinar condições necessárias e suficientes para a classificação do estado referido.

Dado o conjunto de seqüências binárias que constituem os *kets* de um estado puro arbitrário $|\psi\rangle_n$, é possível obter a distância de Hamming d_H entre todos os possíveis pares de seqüências. Considerando que $\mathcal{D} = \{d_1, d_2, \cdots, d_s\}$ seja o conjunto dos valores (distintos) de d_H obtidos, temos que, segundo o resultado do Teorema 8, as equações que garantem a classificação do estado $|\psi\rangle_n$ são obtidas a partir de produtos de amplitudes do estado $|\psi\rangle_n$. A forma como tais produtos são definidos depende das condições referentes à distância de Hamming entre as respectivas seqüências binárias. Como estabelecido por (5.3), esta distância pode assumir valores de 2 a n. Contudo, existe a possibilidade de que determinados valores de d_H entre 2 e n não estejam contidos no conjunto $\mathcal{D}$. Sendo esses valores denotados por $\bar{d}$, observe que, fixado um valor $\bar{d}$ para obtenção das equações do critério segundo (5.3) não há, por definição, seqüências binárias constituindo os *kets* de $|\psi\rangle_n$ satisfazendo esta condição.

mais especificamente, considere as equações na forma

$$\alpha_i \alpha_j = \alpha_k \alpha_l, \tag{5.12}$$

onde $\alpha_i, \alpha_j, \alpha_k, \alpha_l$ são as amplitudes associadas às seqüências binárias **i**, **j**, **k**, **l**, cuja ordenação decorre da condição

$$d_H(\mathbf{i}, \mathbf{j}) = d_H(\mathbf{k}, \mathbf{l}) = \bar{d}. \tag{5.13}$$

Como não há pares de seqüências binárias compondo os *kets* de $|\psi\rangle_n$ que satisfaçam as distâncias $\bar{d}$, então podemos afirmar que as seqüências que distam $\bar{d}$ entre si estão associados a amplitudes nulas. Logo, todas as equações na forma de (5.12) são igualdades do tipo "0=0".

Uma vez que as equações na forma de (5.12), obtidas sob a condição (5.13), são sempre satisfeitas, a análise das equações que resulta na classificação de um dado estado pode ser reduzida, como definido no próximo resultado.

Teorema 9 *Seja $|\psi\rangle_n$ um estado quântico puro arbitrário com n qubits e $\mathcal{D}$ o conjunto dos valores d assumidos pela distância de Hamming entre os pares de seqüências binárias que compõem os kets deste estado. A separabilidade de $|\psi\rangle_n$ é garantida se, e somente se, são satifeitas as equações $\alpha_i\alpha_j = \alpha_k\alpha_l$, onde α_i, α_j, α_k e α_l são as amplitudes associadas às seqüências* $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ *e* $\mathbf{l}$*, escolhidas de acordo com as condições*

$$d_H(\mathbf{i},\mathbf{j}) = d_H(\mathbf{k},\mathbf{l}) = d \tag{5.14}$$

e

$$d_H(\mathbf{i},\mathbf{k}) = d_H(\mathbf{j},\mathbf{l}) = 1 \quad e \quad d_H(\mathbf{i},\mathbf{l}) = d_H(\mathbf{j},\mathbf{k}) = d-1, \tag{5.15}$$

onde $2 \leq d \leq n$ *e* $i,j,k,l \in \{0,\cdots,2^n-1\}$.

Com base nesta simplificação do processo de análise de equações do qual resulta a classificação de um dado estado puro, apresentamos em seguida uma rotina computacional que implementa o resultado estabelecido pelo Teorema 9.

5.4 Implementação do Critério Proposto

Como foi mencionado na Seção 5.3, quando o objetivo é a classificação de um determinado estado puro, as respectivas configurações (amplitudes e seqüências binárias que compõem os *kets*) podem auxiliar no processo, simplificando a análise proposta pelo Teorema 8. Tendo como base este fato, a rotina computacional que será apresentada nesta seção foi desenvolvida de acordo com as idéias que fundamentaram o resultado mencionado no Teorema 9.

Fixado um estado puro arbitrário $|\psi\rangle_n$, o qual se deseja classificar em emaranhado ou separável, o primeiro passo do processo é definir computacionalmente quais são as características do estado referido.

A primeira rotina estabelece todas as possíveis seqüências binárias ($q = 2$) de comprimento n que podem constituir os *kets* de $|\psi\rangle_n$.

```
function [T]=P(n,q) for i=1:n
    k=0;
    for j=1:q^i
            T(k*q^(n-i)+1:(k+1)*q^(n-i),i)=rem(k,q);
            k=k+1;
    end
end
```

Uma vez que a classificação é descrita pela análise de equações obtidas sob condições acerca dos possíveis valores para a distância de Hamming d_H entre as seqüências que compõem os *kets* de $|\psi\rangle_n$, faz-se necessária a definição do conjunto $\mathcal{D}$ para este estado. Neste contexto, a segunda rotina apresenta a tabela de distribuição dos valores de distância de Hamming entre todas as possíveis seqüências binárias de comprimento n obtidas a partir da rotina anterior, agora denotada por B.

```
function [D]=distancia(B) m=max(size(B)); for i=1:m-1
    for j=i+1:m
        D(i,j)=sum(rem(B(i,:)+B(j,:),2));
        D(j,i)=D(i,j);
    end
end
```

Exemplo 14 *Para exemplificar a utilização das rotinas, temos que*

$$B = P(3,2) = \begin{matrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{matrix}$$

e

$$distancia(B) = \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline - & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ \hline 000 & 0 & 1 & 1 & 2 & 1 & 2 & 2 & 3 \\ \hline 001 & 1 & 0 & 2 & 1 & 2 & 1 & 3 & 2 \\ \hline 010 & 1 & 2 & 0 & 1 & 2 & 3 & 1 & 2 \\ \hline 011 & 2 & 1 & 1 & 0 & 3 & 2 & 2 & 1 \\ \hline 100 & 1 & 2 & 2 & 3 & 0 & 1 & 1 & 2 \\ \hline 101 & 2 & 1 & 3 & 2 & 1 & 0 & 2 & 1 \\ \hline 110 & 2 & 3 & 1 & 2 & 1 & 2 & 0 & 1 \\ \hline 111 & 3 & 2 & 2 & 1 & 2 & 1 & 1 & 0 \\ \hline \end{array}$$

Definidos os aspectos gerais de um estado puro arbitrário com n *qubits* $|\psi\rangle_n$, tais como comprimento das seqüências binárias que constituem os *kets* e a distribuição de valores para a distância de Hamming, iniciamos a apresentação dos dados que identificam um estado específico que se deseja classificar.

Com tal objetivo, definimos o vetor C por

$$C = [indices; \text{valores das amplitudes}]\,. \tag{5.16}$$

O conjunto *indices* refere-se à representação decimal de cada uma das seqüências binárias que constituem os *kets* de $|\psi\rangle_n$. Dada uma seqüência binária $\mathbf{v}$, o respectivo índice é obtido pela seguinte função

$$indice(\mathbf{v}) = \mathbf{v} \ * \ f',$$

onde

$$f = 2 \cdot \hat{} \, [2 - [0 : n - 1]],$$

n representa o número de *qubits* do estado e f' denota o transposto de f.

Uma vez fornecidos os dados referentes ao estado que se deseja classificar, exibimos a seguir a rotina *criterion(C,n)*, da qual resulta a classificação de $|\psi\rangle_n$. A rotina *criterion(C,n)* tem como variáveis de entrada o vetor C definido em (5.16) e o número de *qubits* n no estado $|\psi\rangle_n$.

```
function EQ=criterion(C,n) M=P(n,2); D=distancia(M); C=C+1;
k=max(size(C)); m=2^n; t=zeros(1,m); for(i=1:k)
    t(1,C(1,i))=C(2,i);
end h=1; V=zeros(1,5); N=zeros(2,n); S=N; for(i=1:k)
    for(j=1:m)
        if(D(C(1,i),j)!=0)
            for(l=1:m)
                if(l!=j && l!=C(1,i))
                    for(r=1:m)
                        if(D(C(1,i),j)==D(l,r))
                            if(D(C(1,i),l)==1 && D(j,r)==1)
                                if(D(C(1,i),r)==D(C(1,i),j)-1 && D(j,l)==D(C(1,i),j)-1)
                                    if(t(1,C(1,i))*t(1,j)!=t(1,l)*t(1,r))
                                        V(h,1)=C(1,i)-1;
                                        V(h,2)=j-1;
                                        V(h,3)=l-1;
                                        V(h,4)=r-1;
                                        V(h,5)=D(l,r);
                                        N(2,D(l,r))=N(2,D(l,r))+1;
                                        h=h+1;
                                    else
                                        S(2,D(l,r))=S(2,D(l,r))+1;
                                    end
                                end
                            end
                        end
                    end
                end
            end
        end
    end
end S(1,:)=1:n; N(1,:)=1:n; EQ=V(1,:); k=1; for(i=2:h-1)
    k=size(EQ,1);
    x=0;
    j=1;
    while(j<=k && x<1)
        if(V(i,1)==EQ(j,2) &&  V(i,2)==EQ(j,1) && V(i,3)==EQ(j,3) && V(i,4)==EQ(j,4))
            x=j;
        end
        if(V(i,1)==(j,2) &&  V(i,2)==EQ(j,1) && V(i,3)==EQ(j,4) && V(i,4)==EQ(j,3))
            x=j;
        end
        if(V(i,1)==EQ(j,1) &&  V(i,2)==EQ(j,2) && V(i,3)==EQ(j,4) && V(i,4)==EQ(j,3))
            x=j;
        end
        j=j+1;
    end
```

```
    if(x==0)
        EQ(k+1,:)=V(i,:);
    end
end
```

Mais do que a classificação de um estado puro arbitrário $|\psi\rangle_n$, a rotina *criterion(C,n)* apresenta como resultado combinações da forma

$$i\ j\ k\ l,\quad d \tag{5.17}$$

que identificam as equações

$$\alpha_i\alpha_j = \alpha_k\alpha_l,$$

obtidas segundo as especificações do Teorema 9, que não são satisfeitas pelo estado em análise. Além disso, esta rotina exibe, na variável especificada por d em (5.17), o valor da distância de Hamming que constituiu a condição para que a respectiva equação fosse obtida. Por curiosidade, as variáveis N e S resumem a quantidade de equações não satisfeitas e satisfeitas, respectivamente, para cada valor fixo de $d \in \mathcal{D}$.

Assim, muito mais do que classificar um estado puro arbitrário, a rotina proposta é capaz de apresentar o comportamento deste estado sob condições analisadas pelo critério de separabilidade mencionado no Teorema 9.

Em seguida, apresentamos alguns exemplos da classificação e alguns detalhes da análise definida pela rotina proposta.

Exemplo 15 *Considere o estado puro dado por*

$$|\psi_W\rangle = \frac{1}{\sqrt{3}}\left(|011\rangle + |101\rangle + |110\rangle\right).$$

Os índices deste estado são $3, 5$ *e* 6 *associados, respectivamente, às seqüências binárias dos kets* 011*,* 101 *e* 110*. Assim,* C *é representado da seguinte forma*

$$C = \left[3\ 5\ 6;\ \frac{1}{\sqrt{3}}\ \frac{1}{\sqrt{3}}\ \frac{1}{\sqrt{3}}\right].$$

Executando a rotina criterion(C,3), temos como resultado

```
3 5 1 7,  2
3 6 2 7,  2
5 6 4 7,  2
```

Como mencionado, estas representações referem-se, respectivamente, às equações

$$\alpha_3\alpha_5 = \alpha_1\alpha_7,$$

$$\alpha_3\alpha_6 = \alpha_2\alpha_7,$$

$$\alpha_5\alpha_6 = \alpha_4\alpha_7.$$

De acordo com a proposta, tais equações não são satisfeitas pelo estado $|\psi_W\rangle$, donde resulta na classificação deste como um estado emaranhado. Observe que todas essas equações referem-se à $d = 2$ na condição (5.3).

Exemplo 16 *Considerando o estado puro*

$$|\psi\rangle = \frac{1}{\sqrt{4}}\left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right),$$

este pode ser representado por

$$C = \left[0\ 3\ 5\ 6;\ \frac{1}{\sqrt{4}}\ \frac{1}{\sqrt{4}}\ \frac{1}{\sqrt{4}}\ \frac{1}{\sqrt{4}}\right],$$

A rotina criterion(C,3) para este estado apresenta as seguintes combinações de índices:

```
0 3 1 2 , 2
0 5 1 4,  2
0 6 2 4,  2
3 5 1 7,  2
3 6 2 7,  2
5 6 4 7,  2
```

As equações associadas a estas combinações são, respectivamente,

$$\alpha_0\alpha_3 = \alpha_1\alpha_2,$$

$$\alpha_0\alpha_5 = \alpha_1\alpha_4,$$

$$\alpha_0\alpha_6 = \alpha_2\alpha_4,$$

$$\alpha_3\alpha_5 = \alpha_1\alpha_7,$$

$$\alpha_3\alpha_6 = \alpha_2\alpha_7,$$

$$\alpha_5\alpha_6 = \alpha_4\alpha_7.$$

De acordo com a proposta, essas são as equações que não são satisfeitas pelo estado $|\psi\rangle$. Note que essas equações são obtidas também sob a condição de $d = 2$ em (5.3).

Exemplo 17 *Considerando o estado puro*

$$|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right),$$

este pode ser representado por $C = \left[0\ 7;\ \frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}}\right]$

A rotina criterion(C,3) para $|\psi_{GHZ}\rangle$ apresenta as seguintes respostas:

```
0 7 1 6,  3
0 7 2 5,  3
0 7 4 3,  3
```

As equações que não são satisfeitas foram obtidas sob a condição de $d = 3$ em (5.3).

Exemplo 18 *Considere o estado*

$$|\lambda\rangle = \frac{1}{\sqrt{2}}\left(|001\rangle + |011\rangle\right).$$

O vetor C associado é dado por $C = \left[1\ 3;\ \frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}}\right]$. A rotina criterion(C,3) não apresenta equações como resposta. Ou seja, este estado satisfaz todas as equações do critério, o que representa, pelo Teorema 9, que o estado é separável. De fato, $|\lambda\rangle$ pode ser reescrito na forma

$$|\lambda\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \left(|0\rangle + |1\rangle\right) \otimes |1\rangle\right),$$

o que, segundo a Definição 7, o classifica como separável.

O próximo exemplo, ao contrário dos anteriores, apresenta a análise de um estado puro arbitrário cujo desenvolvimento sem o auxílio das rotinas implementadas seria demasiadamente extenso.

Exemplo 19 *Considere o estado quântico com sete qubits na forma*

$$\begin{aligned}|\psi\rangle_7 \;=\; & \frac{1}{\sqrt{8}}\left(|0000000\rangle + |0110011\rangle + |0001111\rangle + |0111100\rangle + \right. \\ & \left. + |1010101\rangle + |1100110\rangle + |1011010\rangle + |1101001\rangle\right).\end{aligned}$$

De acordo com o conjunto de seqüências que constituem os kets e a distribuição de amplitudes, com o auxílio da função índice definida, temos que

$$C = \left[0\ 15\ 51\ 60\ 85\ 90\ 102\ 105;\ \frac{1}{\sqrt{8}}\ \frac{1}{\sqrt{8}}\ \frac{1}{\sqrt{8}}\ \frac{1}{\sqrt{8}}\ \frac{1}{\sqrt{8}}\ \frac{1}{\sqrt{8}}\ \frac{1}{\sqrt{8}}\ \frac{1}{\sqrt{8}}\right].$$

Aplicando a rotina emaran(C,7), temos que as seguintes equações não são satisfeitas pelo estado $|\psi\rangle_7$:

```
0 15 1 14, 4;        0 15 2 13, 4;        0 15 4 11, 4;        0 15 8 7, 4;
0 51 1 50, 4;        0 51 2 49, 4;        0 51 16 35, 4;       0 51 32 19, 4;
0 60 4 56, 4;        0 60 8 52, 4;        0 60 16 44, 4;       0 60 32 28, 4;
0 85 1 84, 4;        0 85 4 81, 4;        0 85 16 69, 4;       0 85 64 21, 4;
0 90 2 88, 4;        0 90 8 82, 4;        0 90 16 74, 4;       0 90 64 26, 4;
0 102 2 100, 4;      0 102 4 98, 4;       0 102 32 70, 4;      0 102 64 38, 4;
0 105 1 104, 4;      0 105 8 97, 4;       0 105 32 73, 4;      0 105 64 41, 4;
15 51 7 59, 4;       15 51 11 55, 4;      15 51 31 35, 4;      15 51 47 19, 4;
15 60 13 62, 4;      15 60 14 61, 4;      15 60 31 44, 4;      15 60 47 28, 4;
15 85 7 93, 4;       15 85 13 87, 4;      15 85 31 69, 4;      15 85 79 21, 4;
15 90 11 94, 4;      15 90 14 91,4;       15 90 31 74, 4;      15 90 79 26, 4;
```

```
15 102 7 110, 4;     15 102 14 103, 4;    15 102 47 70, 4;      15 102 79 38, 4;
15 105 11 109, 4;    15 105 13 107, 4;    15 105 47 73, 4;      15 105 79 41, 4;
51 60 49 62, 4;      51 60 50 61, 4;      51 60 55 56, 4;       51 60 59 52, 4;
51 85 19 117, 4;     51 85 49 87, 4;      51 85 55 81, 4;       51 85 115 21, 4;
51 90 19 122, 4;     51 90 50 91, 4;      51 90 59 82, 4;       51 90 115 26, 4;
51 102 35 118, 4;    51 102 50 103, 4;    51 102 55 98, 4;      51 102 115 38, 4;
51 105 35 121, 4;    51 105 49 107, 4;    51 105 59 97, 4;      51 105 115 41, 4;
60 85 28 117, 4;     60 85 52 93, 4;      60 85 61 84, 4;       60 85 124 21, 4;
60 90 28 122, 4;     60 90 56 94, 4;      60 90 62 88, 4;       60 90 124 26, 4;
60 102 44 118, 4;    60 102 52 110, 4;    60 102 62 100, 4;     60 102 124 38, 4;
60 105 44 121, 4;    60 105 56 109, 4;    60 105 61 104, 4;     60 105 124 41, 4;
85 90 81 94, 4;      85 90 84 91, 4;      85 90 87 88, 4;       85 90 93 82, 4;
85 102 69 118, 4;    85 102 84 103, 4;    85 102 87 100, 4;     85 102 117 70, 4;
85 105 69 121, 4;    85 105 81 109, 4;    85 105 93 97, 4;      85 105 117 73, 4;
90 102 74 118, 4;    90 102 82 110, 4;    90 102 94 98, 4;      90 102 122 70, 4;
90 105 74 121, 4;    90 105 88 107, 4;    90 105 91 104, 4;     90 105 122 73, 4;
102 105 98 109, 4;   102 105 100 107, 4;  102 105 103 104, 4;   102 105 110 97, 4;
```

As equações não satisfeitas contabilizam 112 e todas foram obtidas segundo a condição em (5.14) de $t = d_H = 4$, conforme fornece a variável N da rotina:

```
1 2 3  4  5 6 7

0 0 0 112 0 0 0
```

Para determinar o número de equações que foram verificadas, exibimos também o resultado da variável S da rotina, que estabelece o número de equações satisfeitas pelo estado em função do valor da distância sob as quais foram obtidas (primeira linha). A saber, S para o estado $|\psi\rangle_7$ é

```
1   2    3    4   5   6   7

0  168  420  448 420 168 28
```

É importante salientar que a rotina poderia ser bastante simplificada se o interesse fosse apenas exibir a classificação de um estado dado, o que seria suficiente, haja vista a proposta inicial. Porém, como o critério foi obtido a partir de uma interpretação homológica-geométrica, o objetivo era implementar uma rotina que, embora mais complexa, exibisse o comportamento das configurações iniciais do estado sob o ponto de vista geométrico da análise. Por isso, apresentamos a distribuição do número das equações satisfeitas e não satisfeitas pelo estado em função das distâncias d em (5.14) a partir da qual tais equações foram obtidas.

5.5 Visão Geral acerca do Critério de Separabilidade Generalizado

A partir da interpretação homológica-geométrica para o critério de separabilidade considerando estados puros arbitrários com três *qubits*, foi possível, pela utilização do princípio de

indução finita, obter o critério de separabilidade para estados puros arbitrários. Embora as demonstrações referentes a nossa proposta sejam extensas, são constituídas de idéias simples como, por exemplo, condições sobre os vértices para que as diagonais sejam definidas nos hipercubos unitários representados num espaço discreto de Hamming, donde resultou a utilização da distância usual deste espaço, denominada distância de Hamming.

É interessante salientar que o número de equações exibidas pela rotina para o estado do Exemplo 16 é maior quando comparado ao do Exemplo 15. Sob a condição na qual o critério foi construído, se um estado satisfaz um número maior de equações do critério com relação a um segundo estado, então o primeiro está mais próximo da separabilidade. Podemos inferir então que o estado $|\psi\rangle$ do Exemplo 16 é mais emaranhado que $|\psi_W\rangle$ do Exemplo 15?

As equações do critério de separabilidade são definidas a partir de condições sobre os valores da distância de Hamming no conjunto das seqüências binárias que compõem os *kets* de um estado. O valor de d utilizado em (5.14) do qual se obtém equações que não são satisfeitas por um estado implicam em alguma conclusão com respeito à quantificação deste? Em caso afirmativo, seria possível determinar do conjunto de seqüências binárias que não satisfazem a condição (5.14) para o valor d associado ao máximo emaranhamento. De acordo com as identificações propostas neste trabalho, a partir deste conjunto definimos os conteúdos dos *kets* de um estado e, por hipótese, teríamos um estado de máximo emaranhamento. No caso desta associção ser válida, existe alguma forma de sistematizar este processo?

Para que tais associações sejam verificadas, é necessário que se conheça quais são as classes de estados de máximo emaranhamento. Neste trabalho, nos restringimos aos estados de máximo emaranhamento global, assim classificados a partir da medida proposta por Meyer-Wallach em [78]. No próximo capítulo, estudamos os estados puros arbitrários com três *qubits* de acordo com esta medida e apresentamos algumas considerações acerca da associação entre os valores da distância de Hamming no conjunto das seqüências binárias que compõem os *kets* de um estado (e outros conceitos decorrentes) e a classificação desse como um estado de máximo emaranhamento global.

Capítulo 6

Emaranhamento Global para Estados com Três *Qubits*

Como mencionado no Capítulo 3, foram propostos vários critérios com relação à quantificação do emaranhamento de estados puros arbitrários. O objetivo deste capítulo é apresentar nosso entendimento sobre o emaranhamento quântico para estados com três *qubits* e a respectiva quantificação, tendo como base a medida de emaranhamento global proposta por Meyer-Wallach em [78].

6.1 Estados de Máximo Emaranhamento Global com Três *Qubits*

No caso de estados puros com dois *qubits*, não existe quantificação de emaranhamento. Tais estados são, simplesmente, emaranhados ou separáveis [61]. Conforme mencionado no Capítulo 3, Seção 3.2.3, há duas formas distintas de emaranhamento para estados com três *qubits*, uma denominada *emaranhamento tripartite*, que caracteriza a existência de emaranhamento entre os três *qubits* do estado, e o *emaranhamento aos pares*, que caracteriza o emaranhamento entre dois subsistemas do estado [40, 122].

De acordo com este resultado, há duas classes distintas de estados emaranhados com três *qubits*. O estado representante da classe associada ao emaranhamento tripartite é o estado *GHZ*, descrito como

$$|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right),$$

enquanto um representante para a classe dos estados emaranhados aos pares é o estado W, descrito como

$$|\psi_{W}\rangle = \frac{1}{\sqrt{3}}\left(|011\rangle + |101\rangle + |110\rangle\right).$$

Dados que estes dois estados representam as duas classes não equivalentes de emaranhamento em estados com três *qubits*, apresentamos a seguir a análise da quantificação do emaranhamento de $|\psi_{GHZ}\rangle$ e $|\psi_{W}\rangle$, com relação à medida proposta por Meyer-Wallach, Q, [78]. Segue um breve

resumo dos operadores associados. Maiores detalhes podem ser encontrados no Capítulo 3, Seção 3.3.1.

Seja $\mathbf{x} = x_1 \cdots x_n$ uma n-upla binária associada ao conteúdo de um *ket* de $|\psi\rangle$, sendo x_j, $j = 1, \cdots, n$, cada coordenada de $\mathbf{x}$. Considere $\iota_j(b) : (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n-1}$ a função linear definida pela seguinte ação na base

$$\iota_j(b)\left(|x_1\rangle \otimes \cdots \otimes |x_n\rangle\right) = \delta_{bx_j}|x_1\rangle \otimes \cdots \otimes |x_{j-1}\rangle \otimes |x_{j+1}\rangle \otimes \cdots |x_n\rangle, \tag{6.1}$$

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

Dado um estado quântico puro com n *qubits* $|\psi\rangle$[1], a *medida de emaranhamento global de Meyer-Wallach* é dada por

$$Q(|\psi\rangle) = \frac{4}{n}\sum_{j=1}^{n} D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle), \tag{6.2}$$

onde

$$D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle) = \langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle\langle\psi|\iota_j(1), \iota_j(1)|\psi\rangle - |\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle|^2, \tag{6.3}$$

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

Q é invariante sob transformações unitárias locais e tal que $0 \leq Q \leq 1$. Assim, $Q(|\psi\rangle) = 0$ se, e somente se, $|\psi\rangle$ é um estado separável, e $Q(|\psi\rangle) = 1$ se, e somente se, $|\psi\rangle$ é um *estado puro de máximo emaranhamento global*, [95].

Considerando o estado

$$|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right),$$

temos que os operadores mencionados em (6.1) satisfazem

$$\iota_1(0)|\psi_{GHZ}\rangle = \iota_2(0)|\psi_{GHZ}\rangle = \iota_3(0)|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|00\rangle),$$

$$\iota_1(1)|\psi_{GHZ}\rangle = \iota_2(1)|\psi_{GHZ}\rangle = \iota_3(1)|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|11\rangle).$$

Com o auxílio das propriedades da operação do produto tensorial mencionadas no Capítulo 2, Seção 2.1.2, é possível verificar que a substituição das expressões $\iota_j(0)|\psi_{GHZ}\rangle$ e $\iota_j(1)|\psi_{GHZ}\rangle$ em (6.3) resulta em

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

[1]Para simplificar a notação, omitimos o índice na representação $|\psi\rangle_n$, observando que $|\psi\rangle$ refere-se a um estado puro arbitrário.

para $j = 1, 2, 3$.

Com base neste valor obtido, decorre de (6.2) que

$$Q(|\psi_{GHZ}\rangle) = \frac{4}{3}\sum_{j=1}^{3} D\left(\iota_j(0)|\psi_{GHZ}\rangle, \iota_j(1)|\psi_{GHZ}\rangle\right) = \frac{4}{3}\sum_{j=1}^{3}\frac{1}{4} = 1,$$

donde concluímos que $|\psi_{GHZ}\rangle$ é um estado de máximo emaranhamento global.

Seguimos o mesmo procedimento para calcular o emaranhamento global do estado $|\psi_W\rangle$. De acordo com (6.1), temos

$$\iota_1(0)|\psi_W\rangle = \iota_2(0)|\psi_W\rangle = \iota_3(0)|\psi_W\rangle = \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle),$$

$$\iota_1(1)|\psi_W\rangle = \iota_2(1)|\psi_W\rangle = \iota_3(1)|\psi_W\rangle = \frac{1}{\sqrt{3}}(|00\rangle).$$

Pela substituição destas expressões em (6.3), obtemos

$$\begin{aligned}
D &= \left(1/\sqrt{3}\right)^2 \cdot \langle 01+10|01+10\rangle \left(1/\sqrt{3}\right)^2 \langle 00|00\rangle - \left(1/\sqrt{3}\right)^2 |\langle 01+10|00\rangle|^2 \\
&= \left(1/\sqrt{3}\right)^4 \left(\langle 01|01\rangle + \langle 01|10\rangle + \langle 10|01\rangle + \langle 10|10\rangle\right) \langle 00|00\rangle - \left(1/\sqrt{3}\right)^2 |\left(\langle 01|00\rangle + \langle 10|00\rangle\right)|^2 \\
&= \left(1/\sqrt{3}\right)^4 \left(\langle 0|0\rangle\langle 1|1\rangle + \langle 0|1\rangle\langle 1|0\rangle + \langle 1|0\rangle\langle 0|1\rangle + \langle 1|1\rangle\langle 0|0\rangle\right) \left(\langle 0|0\rangle\langle 0|0\rangle\right) + \\
&- \left(1/\sqrt{3}\right)^2 |\left(\langle 0|0\rangle\langle 1|0\rangle + \langle 1|0\rangle\langle 0|0\rangle\right)|^2 = 2\left(1/\sqrt{3}\right)^4 = 2/9.
\end{aligned}$$

para $j = 1, 2, 3$.

Substituindo este valor em (6.2), obtemos

$$Q(|\psi_W\rangle) = \frac{4}{3}\sum_{j=1}^{3} D|\left(\iota_j(0)|\psi_W\rangle, \iota_j(1)|\psi_W\rangle\right) = \frac{4}{3}\sum_{j=1}^{3}\frac{2}{9} = \frac{8}{9},$$

donde concluímos que $|\psi_W\rangle$ **não** é um estado de máximo emaranhamento global.

Como foi mencionado, os estados $|\psi_{GHZ}\rangle$ e $|\psi_W\rangle$ foram estudados quanto à quantidade de emaranhamento com respeito aos operadores de medida denominados *tangle* no Capítulo 3, Seção 3.2.3. Comparando esta análise com os resultados obtidos utilizando a medida de Meyer-Wallach, concluímos que esta medida não classifica o máximo emaranhamento entre duas partes do estado W como emaranhamento global. Há algumas discussões na literatura que justificam tal afirmação e são baseadas no fato de que as correlações entre os subsistemas do estado W são clássicas. Não mencionaremos esta discussão, mas sugerimos a leitura das referências [9, 117].

Retornando aos resultados obtidos quanto à quantidade de emaranhamento global para as classes de estados representadas por $|\psi_{GHZ}\rangle$ e $|\psi_W\rangle$, temos que apenas os estados contidos na primeira satisfazem a condição de máximo emaranhamento global segundo a medida de Meyer-Wallach. Será esta a única classe?

A resposta é não. É possível exibir mais uma classe de estados com três *qubits* satisfazendo a condição de máximo emaranhamento da medida Q. Conforme pode ser encontrado em [78],

por definição, a medida Q é invariante sob operações unitárias locais (aplicadas em cada uma das partes do estado separadamente). Ou seja, o resultado da medida Q de um estado não é modificada se este estado sofrer a ação de uma transformação unitária local.

O operador unitário local mais utilizado em informação quântica é conhecido como *operador de Hadamard*, geralmente denotado por Had. No espaço dos estados quânticos com 1 qubit, este operador é definido pela seguinte ação sobre a base

$$Had(|0\rangle) = 1/\sqrt{2}\,(|0\rangle + |1\rangle) \quad \text{e} \quad Had(|1\rangle) = 1/\sqrt{2}\,(|0\rangle - |1\rangle)\,.$$

A segunda classe de estados com três *qubits* de máximo emaranhamento global é obtida pela ação do operador de Hadamard sobre cada um dos *qubits* do estado *GHZ*, como descrito a seguir

$$\begin{aligned} |\psi_{HGHZ}\rangle &= Had^{\otimes 3}\left[1/\sqrt{2}\,(|000\rangle + |111\rangle)\right] \\ &= Had(|0\rangle) \otimes Had(|0\rangle) \otimes Had(|0\rangle) + Had(|1\rangle) \otimes Had(|1\rangle) \otimes Had(|1\rangle), \end{aligned}$$

onde $|\psi_{HGHZ}\rangle$ é um estado que representa esta nova classe de estados e é descrito na forma de combinações de *kets* como

$$|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}\,(|000\rangle + |011\rangle + |101\rangle + |110\rangle)\,. \tag{6.4}$$

Observe que o estado $|\psi_{HGHZ}\rangle$ foi estudado no Exemplo 16 do Capítulo 6. Geometricamente, este estado é representado por um tetraedro regular inscrito no cubo unitário, conforme ilustra a Fig. 6.1.

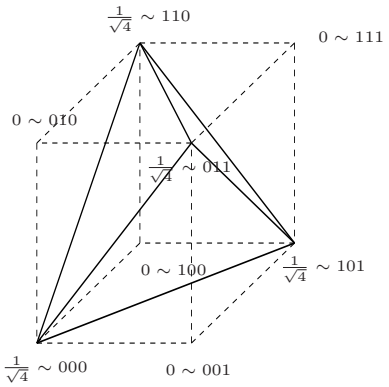


Figura 6.1: Interpretação do estado $|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}\,(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$.

Embora já esteja estabelecido por resultados teóricos que $|\psi_{HGHZ}\rangle$ é um estado de máximo emaranhamento global, desenvolvemos os cálculos referentes aos operadores que definem Q.

De acordo com (6.1), temos

$$\iota_1(0)|\psi_{HGHZ}\rangle = \iota_2(0)|\psi_{HGHZ}\rangle = \iota_3(0)|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |11\rangle),$$

$$\iota_1(1)|\psi_{HGHZ}\rangle = \iota_2(1)|\psi_{HGHZ}\rangle = \iota_3(1)|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|10+01\rangle).$$

Pela substituição destas expressões em (6.3), obtemos

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

para $j = 1, 2, 3$. Substituindo este valor em (6.2), obtemos

$$Q(|\psi_{HGHZ}\rangle) = \frac{4}{3}\sum_{j=1}^{3}\frac{1}{4} = 1,$$

donde decorre a classificação $|\psi_{HGHZ}\rangle$ como um estado de máximo emaranhamento global, como já era previsto.

Analisando os estados $|\psi_{HGHZ}\rangle$ e $|\psi_W\rangle$, temos que ambos têm a mesma distância de Hamming entre as seqüências binárias que constituem os *kets*. Contudo, esta condição não garantiu a classificação de $|\psi_W\rangle$ como estado de máximo emaranhamento global. Como o número de *kets* de $|\psi_{HGHZ}\rangle$ é maior com relação ao estado $|\psi_W\rangle$, poderíamos inferir que este é um fator que contribui para a classificação de $|\psi_{HGHZ}\rangle$ como um estado de máximo emaranhamento global. Note, porém, que os poucos *kets* que constituem o estado *GHZ* não impediram que este satisfizesse as condições definidas por Meyer-Wallach para o máximo emaranhamento global.

Assim, observamos a partir do estudo apresentado, que para estados puros arbitrários com três *qubits* de máximo emaranhamento global há uma certa *lei de compensação* entre o número de *kets* e a distância de Hamming no conjunto de seqüências binárias que determina o conteúdo desses *kets*.

Para que esta relação seja melhor entendida, retornemos à interpretação geométrica definida no Capítulo 4, Seção 4.3. De acordo com esta interpretação, um estado quântico com três *qubits* é representado por um cubo de lado unitário no espaço $\mathcal{H}_2^3$. Neste contexto, as representações binárias que compõem os *kets* são identificadas com os vértices deste cubo, que, por sua vez, também estão representados em termos de seqüências binárias de comprimento três.

Salientando que o espaço $\mathcal{H}_2^3$ é definido por todas as 2^3 seqüências binárias de comprimento três, temos que *o conjunto dos conteúdos dos kets de um estado $|\psi\rangle_3$ com três qubits pode ser entendido como um subconjunto de $\mathcal{H}_2^3$*. Denotemos por A_ψ este subconjunto.

Além da combinação dos *kets*, é necessário que se defina a distribuição de amplitudes associada a um estado puro para que este esteja completamente identificado. Neste contexto, restringimos nosso estudo apenas aos estados cujas amplitudes associadas aos *kets* sejam iguais entre si e correspondam ao valor $\frac{1}{\sqrt{M}}$, onde M é o número de *kets* do estado. Como a definição

das amplitudes depende da cardinalidade de A_ψ, a partir da determinação deste conjunto é possível identificar o estado $|\psi\rangle_3$.

No contexto das probabilidades associadas às amplitudes, essa escolha equivale a associar ao sistema (estado quântico) a máxima entropia (clássica) de Shannon. Este estudo foi apresentado em detalhes em [47].

De acordo com esta escolha com relação à distribuição de amplitudes no estado, temos que os estados

$$|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right), \quad |\psi_W\rangle = \frac{1}{\sqrt{3}}(|011\rangle + |101\rangle + |110\rangle)$$

e

$$|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}\left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right)$$

estão associados, respectivamente, aos conjuntos de

$$A_{\psi_{GHZ}} = \{000, 111\}, \quad A_{\psi_W} = \{011, 101, 110\} \quad \text{e} \quad A_{\psi_{HGHZ}} = \{000, 011, 101, 110\}.$$

Esta interpretação pode ser generalizada, de forma que um estado quântico puro $|\psi\rangle$ com n *qubits* e amplitudes iguais a $\frac{1}{\sqrt{M}}$, onde M o número de *kets* deste estado, pode ser identificado a partir de um subconjunto A_ψ de $\mathcal{H}_2^n$.

São subconjuntos de $\mathcal{H}_2^n$ que definem também *códigos binários* [75]. Dado o subconjunto de $\mathcal{H}_2^n$ que define um código $\mathcal{C}$, cada um de seus elementos é associado a uma *palavra-código*. Portanto, *pode ser estabelecida uma identificação entre as n-uplas binárias que compõem os kets de um estado quântico e as palavras-código de comprimento n de um código binário.*

Dentre os subconjuntos de seqüências binárias que definem os códigos, destacamos aqueles que satisfazem a propriedade de *fechamento*: se $\mathbf{a}$ e $\mathbf{b}$ são palavras de um código $\mathcal{C}$, então $\mathbf{a} + \mathbf{b} \in \mathcal{C}$. Os códigos definidos por subconjuntos com esta propriedade são denominados *códigos lineares*.

De acordo com o que foi apresentado, podemos concluir que os estados $|\psi_{GHZ}\rangle$ e $|\psi_{HGHZ}\rangle$, que são representantes das classes de estados com três *qubits* de máximo emaranhamento global, estão associados à codigos lineares, uma vez que $A_{\psi_{GHZ}}$ e $A_{\psi_{HGHZ}}$ satisfazem a propriedade de fechamento.

Já o conjunto A_{ψ_W} não apresenta a estrutura vetorial que decorre da propriedade do fechamento e, por isso, não pode ser associado a um código linear. Como mencionado, estado $|\psi_W\rangle$ não é classificado como um estado de máximo emaranhamento global segundo a medida de Meyer-Wallach.

Com base em tais considerações, afirmamos que há uma relação entre a existência de uma estrutura vetorial no conjunto A_ψ e a definição de um conjunto de *kets* que definem um estado com três *qubits* de máximo emaranhamento global. A questão que decorre é se esta relação é estabelecida entre códigos lineares e estados puros arbitrários de máximo emaranhamento global pode ser generalizada para estados puros arbitrários com n *qubits*. Este estudo será apresentado

no Capítulo 8. Antes disso, porém, apresentamos no Capítulo 7 alguns conceitos da teoria da codificação que são fundamentais para o desenvolvimento e descrição dos resultados.

Capítulo 7

Elementos de Teoria da Codificação

O objetivo deste capítulo é apresentar um breve resumo dos elementos de teoria da codificação, com enfoque em propriedades associadas aos códigos *binários e lineares* e contextualizar tais conceitos no desenvolvimento deste trabalho. Este capítulo está organizado da seguinte forma. Na Seção 7.1 apresentamos as propriedades dos códigos lineares, destacando os códigos de repetição, os códigos de Hamming, os códigos *simplex* e os códigos de Reed-Muller de primeira ordem. Na Seção 7.2, consideramos três classes de códigos binários não-lineares que serão destacados pelas respectivas propriedades no Capítulo 8. Na Seção 7.3, discutimos a importante questão de como escolher os códigos a serem utilizados em um processo de transmissão de informações para que a máxima segurança quanto à proteção de erros seja estabelecida.

7.1 Códigos Binários Lineares

Todo código binário $\mathcal{C}$ consiste de um subconjunto de $\mathcal{H}_2^n$, onde $\mathcal{H}_2^n$ representa o espaço vetorial definido pelas seqüências binárias de comprimento n.

Um código binário *linear* $\mathcal{C}$, denotado por (n, k), consiste de um subconjunto de 2^k n-uplas que definem um subespaço vetorial do espaço $\mathcal{H}_2^n$. Cada uma das 2^k n-uplas é denominada *palavra-código* e é denotada por $\mathbf{x}_i$, $i = 1, 2, \cdots, 2^k$. Dentre essas, é possível encontrar k palavras-código linearmente independentes, que são denotadas por $\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{k-1}$. De acordo com a estrutura vetorial do espaço, temos que toda palavra-código $\mathbf{x} \in \mathcal{C}$ é uma combinação linear de $\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{k-1}$, de forma que

$$\mathbf{x} = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \cdots u_{k-1}\mathbf{g}_{k-1},$$

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

Definindo uma matriz $k \times n$ cujas linhas correspondem às k palavras-código linearmente

independentes, obtemos a *matriz geradora* G associada ao código $\mathcal{C}$, descrita por

$$G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{01} & g_{02} & \cdots & g_{0,n} \\ g_{11} & g_{12} & \cdots & g_{1,n} \\ \vdots & \vdots & \vdots & \vdots \\ g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n} \end{bmatrix},$$

onde $\mathbf{g}_i = (g_{i1}, g_{i2}, \cdots, g_{i,n})$, para $0 \leq i \leq k-1$.

Exemplo 20 *Uma matriz geradora associada ao código definido pelo conjunto de palavras-código* $\{0000000, 0110011, 0001111, 0111100, 1010101, 1100110, 1011010, 1101001\}$ *é dada por*

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

A matriz G associa um processo sistemático quanto à descrição das palavras-código que definem o código associado. A saber, se $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$ é a mensagem a ser codificada, então a palavra-código $\mathbf{x}$ correspondente é obtida por

$$\mathbf{x} = \mathbf{u} * G.$$

Toda matriz geradora G associada a um código linear $\mathcal{C}$ pode ser representada na forma

$$G = [I_k | A], \tag{7.1}$$

onde I_k representa a matriz identidade de ordem k. Esta representação para a matriz geradora é denominada *forma sistemática* de G.

Por exemplo, a forma sistemática da matriz G do Exemplo 20 é dada por

$$G = [I_k | A] \left[\begin{array}{ccc|cccc} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right].$$

Um código linear $\mathcal{C}$ com parâmetros (n, k) pode ser representado também pela *matriz verificação de paridade* H.

Definição 10 *[75] Uma matriz H, com dimensões $(n-k) \times n$ é uma matriz verificação de paridade para um código linear $\mathcal{C}$ se, e somente se, para toda palavra $\mathbf{x}_i \in \mathcal{C}$, temos que $\mathbf{x}_i * H^t = 0$.*

Tendo como base a forma sistemática de representação para a matriz geradora G de um código $\mathcal{C}$, mencionada em (7.1), é conhecido que a matriz verificação de paridade H associada pode escrita na forma

$$H = [-A^t | I_{n-k}], \tag{7.2}$$

sendo A^t a matriz transposta de A em (7.1) e I_{n-k} a matriz identidade de ordem $(n-k)$.

As matrizes G e H associadas a um código $\mathcal{C}$ satisfazem as seguintes relações

$$G * H^t = 0 \quad \text{e} \quad H * G^t = 0.$$

Decorre desta propriedade a definição de *códigos duais*.

Definição 11 *[75] A matriz verificação de paridade H de um código $\mathcal{C}$ consiste da matriz geradora de um código denominado código dual de $\mathcal{C}$, denotado por $\mathcal{C}^{\perp}$.*

Além de n e k, é necessário um terceiro parâmetro para representar corretamente um código $\mathcal{C}$. Trata-se da *distância do código*, denotada por d.

Salientando que a distância de Hamming d_H entre duas palavras de um código $\mathcal{C}$ consiste no número de coordenadas em que essas diferem, a *distância de um código $\mathcal{C}$* é a mínima distância de Hamming entre todas as palavras de $\mathcal{C}$, ou seja,

$$d = min\{d_H(\mathbf{x}_i, \mathbf{x}_j) : \mathbf{x}_i \neq \mathbf{x}_j; \mathbf{x}_i, \mathbf{x}_j \in \mathcal{C}\}.$$

Um código linear com 2^k palavras-código de comprimento n e mínima distância de Hamming igual a d é representado na forma (n, k, d). Uma outra representação para códigos definida na literatura consiste na representação (n, M, d), onde M denota a cardinalidade do conjunto de palavras que definem o código.

Algumas propriedades associadas à estrutura dos códigos lineares, importantes para o desenvolvimento dos resultados deste trabalho, são mencionadas a seguir.

Lema 7 *[72] O número de palavras-código de um código binário linear é sempre da forma $M = 2^k$.*

Proposição 6 *[72] Considere um código binário linear $\mathcal{C}$ com parâmetros (n, M, d), definido pelo conjunto de palavras-código A, e uma posição j, $1 \leq j \leq n$, fixa para todas as palavras. Seja Z_j o subconjunto constituído por todas as palavras-código com "0" na posição j fixa. Então, Z_j tem cardinalidade igual a $z_j = M/2$, para qualquer que seja a escolha da posição j. A mesma afirmação é válida com relação ao subconjunto $\bar{Z}_j$, constituído por todas as palavras-código com "1" na posição j fixa.*

Omitimos as demonstrações de tais propriedades por serem extensas e pelo fato de que essas podem ser encontradas nas referências [72, 75], entre outras.

Destacamos algumas classes de códigos binários e lineares. A saber, discutimos em seguida os *códigos de repetição*, os *códigos de Hamming*, os *códigos simplex* e os *códigos de Reed-Muller de primeira ordem*.

7.1.1 Códigos de repetição

Os *códigos de repetição* são códigos lineares de representação bastante simples. Para qualquer valor n, tais códigos são definidos por duas palavras $\mathbf{x}_1$ e $\mathbf{x}_2$, tais que $d(\mathbf{x}_1, \mathbf{x}_2) = n$. Por exemplo,

$$\mathbf{x}_1 = \underbrace{00\cdots0}_{n} \quad \text{e} \quad \mathbf{x}_2 = \underbrace{11\cdots1}_{n}.$$

Para $n = 3$, as matrizes geradora e verificação de paridade do código de repetição de parâmetros $(n, M, d) = (3, 2, 3)$ são dadas, respectivamente, por

$$G = \left[\begin{array}{c|cc} 1 & 1 & 1 \end{array}\right] \quad \text{e} \quad H = \left[\begin{array}{c|cc} 1 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right].$$

7.1.2 Códigos de Hamming e códigos *Simplex*

Os *códigos de Hamming* constituem outra classe importante de códigos binários lineares e são representados pelos parâmetros $(n, M, d) = \left(2^m - 1, 2^{2^m - m - 1}, 3\right)$, $m \geq 2$.

Os códigos de Hamming podem ser facilmente descritos em termos das matrizes verificação de paridade associadas. Estas matrizes são constituídas de m linhas e $2^m - 1$ colunas e são caracterizadas pelo fato que os vetores colunas são todas as m-uplas possíveis excluindo a toda nula. Por exemplo, para $m = 3$, definimos um código de Hamming $\mathcal{C}_7$ com parâmetros $(n, M, d) = (7, 2^4, 3)$ a partir da seguinte matriz verificação de paridade

$$H_7 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Como mencionado na Definição 11, a matriz verificação de paridade H_7 do código de Hamming $\mathcal{C}_7$ consiste na matriz geradora do código dual $\mathcal{C}_7^{\perp}$. Os códigos duais dos códigos de Hamming de comprimento n, são denominados *códigos simplex lineares n-dimensionais* e são definidos para todo $n = 2^m - 1$, $m \geq 2$. Os códigos binários lineares *simplex* n-dimensionais) têm distância constante e igual a $\frac{n+1}{2}$, sendo $(n+1)$ a cardinalidade do conjunto de palavras-código associado [72]. Tais códigos são descritos pelos parâmetros

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

para n na forma $2^m - 1$, $m \geq 2$.

Exemplo 21 *Para $m = 2$, $n = 2^2 - 1 = 3$, a matriz verificação de paridade H_3 do código de Hamming $\mathcal{C}_3$ pode ser escolhida de forma que*

$$H_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Considerando que o código simplex 3-dimensional corresponde ao código dual de $\mathcal{C}_3$, então temos que a matriz H_3 apresentada consiste na matriz geradora do código simplex 3-dimensional,

de parâmetros $(n, M, d) = (3, 4, 2)$. *Este código simplex que é representado pelo seguinte conjunto de palavras-código*

$$\mathcal{C}_3^{\perp} = \{000, 011, 101, 110\}.$$

Os códigos *simplex* e de repetição podem ser definidos também em termos dos *códigos de Reed-Muller de primeira ordem*, conforme é apresentado a seguir.

7.1.3 Códigos Reed-Muller

Um código de Reed-Muller de primeria 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 $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m) \in \mathcal{H}_2^{2^m}$, o conjunto de todas as 2^m-uplas binárias [75].

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

$$a_0.\mathbf{1} + a_1.\mathbf{v}_1 + a_2.\mathbf{v}_2,$$

onde $a_i = 0$ ou 1, $\mathbf{1} = 1111$, $\mathbf{v}_2 = 0011$ e $\mathbf{v}_1 = 0101$.

Dessa forma, os parâmetros do código $RM(1, m)$ são dados por $n = 2^m$, $k = 1 + \begin{pmatrix} m \\ 1 \end{pmatrix}$ e $d = 2^{m-1}$, para $m \geq 2$.

Disso segue que a matriz geradora do código $RM(1, m)$ é dada por

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

onde $G_0 = [\mathbf{1}]$ e $G_1^t = [v_m \ v_{m-1} \cdots \ v_1]$, onde $v_j = 2^{m-j}$ termos do tipo $\{0^{2^{j-1}} \ 1^{2^{j-1}}\}$, para $1 \leq j \leq m$.

A submatriz G_0 gera um *código de repetição* com parâmetros $(n, M, d) = (2^m, 2, 2^m)$. Por outro lado, se considerarmos a submatriz G_1, excluída sua primeira coluna, temos uma matriz que consiste na matriz geradora de um código *simplex* linear n-dimensional com parâmetros $(n, M, d) = (2^m - 1, 2^m, 2^{m-1})$.

7.2 Códigos Binários Não-Lineares

Como mencionado na Seção 7.1, todo código binário $\mathcal{C}$ consiste de um subconjunto de $\mathcal{H}_2^n$, onde $\mathcal{H}_2^n$ representa o espaço vetorial definido pelas seqüências binárias de comprimento n.

Um código binário *linear* $\mathcal{C}$, denotado por (n, k), consiste de um subconjunto de 2^k n-uplas que definem um subespaço vetorial do espaço $\mathcal{H}_2^n$. Códigos que não satisfazem esta propriedade são denominados *códigos não-lineares*.

Ao contrário do que se verifica para códigos lineares, não existe uma forma sistemática de se representar códigos não-lineares. Sendo assim, muitas vezes são conhecidos apenas os

parâmetros de um código desta classe, sem nenhuma referência ao conjunto de palavras-código que o define. Porém, há alguns códigos não-lineares que permitem tal descrição. Apresentamos a seguir três exemplos de códigos com esta propriedade.

7.2.1 Códigos *Simplex* não-lineares

Os códigos *simplex* não-lineares são representados pelos parâmetros

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

e são definidos para todo $n \equiv 3\ mod 4$, $n \neq 2^m - 1$, $m \geq 2$. Não são muitos os códigos desta classe para os quais se conhece o conjunto de palavras-código associado. Dentre os quais tal descrição é conhecida, destacamos os *códigos de Hadamard*, denotados por $\mathcal{A}_{n+1}$.

Por exemplo, para $n = 11$ temos o código de Hadamard $\mathcal{A}_{12}$ com parâmetros $(n, M, d) = (11, 12, 6)$, cujo conjunto de palavras-código associado consiste de

$$\{00000000000, 11011100010 + \text{deslocamentos cíclicos}\}.$$

7.2.2 Código de Nordstrom-Robinson e códigos de Preparata

Um outro exemplo interessante de código não-linear cujo conjunto de palavras-código associado é conhecido trata-se do código de Nordstrom-Robinson, que é denotado por $\mathcal{N}_{16}$ e tem parâmetros $(n, M, d) = (16, 256, 6)$ [75].

Para descrever este código, considere a matriz G descrita por

$$G = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}.$$

Definimos $\mathcal{G}$ como sendo o conjunto constituído das linhas de G e das possíveis combinações entre essas (somadas módulo 2).

Seja $\mathbf{u}$ um elemento do conjunto $\{00000000, 11000000, 10100000, \cdots, 10000001\}$. O conjunto de palavras-código que define $\mathcal{N}_{16}$ consiste de toda seqüência binária $\mathbf{v}$ de comprimento 16 (ou, $\mathbf{v} \in \mathcal{H}_2^{16}$) que satisfaz a condição

$$\mathbf{uv} \in \mathcal{G},$$

onde $\mathbf{uv}$ representa a justaposição das seqüências $\mathbf{u}$ e $\mathbf{v}$.

Os *códigos de Preparata*, denotados por $\mathcal{P}_m$, podem ser entendidos como uma generalização do código de Nordstrom-Robinson, apresentando, tal como $\mathcal{N}_{16}$, uma forma sistemática de descrição. Os códigos $\mathcal{P}_m$ são definidos para todo m par, $m \geq 4$ e são caracterizados pelos parâmetros $(n, M, d) = (2^m, 2^{2^m-2m}, 6)$.

Devido à grande complexidade da notação envolvida na descrição dos códigos de Preparata, está será omitida. Porém, tal descrição pode ser encontrada com detalhes na referência [75].

É necessário salientar que os códigos *simplex* não-lineares, o código de Nordstrom-Robinson e os códigos de Preparata apresentam a propriedade mencionada na Proposição 6, embora não sejam lineares. Ou seja, dado o conjunto de palavras-código associado a um código pertencente a uma dessas classes, podemos garantir que, fixada uma posição j em todos os elementos deste conjunto, o número de palavras-código com "0" na j-ésima posição é igual ao número de palavras com "1" nesta posição, independentemente da escolha de j.

Esta propriedade é fundamental para o desenvolvimento de resultados que serão apresentados no Capítulo 8.

Há muitas outras classes de códigos lineares e algumas outras de códigos não-lineares dos quais se conhece o conjunto de palavras-código definidas na literatura [75]. Entretanto, todas essas classes foram propostas com o mesmo objetivo, que consiste em determinar códigos que tornem as transmissões de informação confiáveis quanto à proteção contra erros que possam ser introduzidos durante o processo.

Esta *confiabilidade* de um código $\mathcal{C}$ está associada à respectiva *capacidade de correção de erros*, que, por sua vez, está definida em função da distância de $\mathcal{C}$, conforme será mencionado pelo Teorema 10.

Na próxima seção, estudaremos quais são os códigos lineares com as maiores capacidades de correção de erros e as particularidades desta análise. Os códigos não-lineares não são considerados pela impossibilidade de analisá-los de forma geral, uma vez que não há uma estrutura matemática que os defina genericamente.

7.3 Proteção e Correção de Erros

O processo de transmissão da informação consiste, basicamente, de uma mensagem $\mathbf{u}$ sendo codificada na palavra-código $\mathbf{x}$, pertencente ao código $\mathcal{C}$ com parâmetros (n, M, d), e transmitida através de um canal. Este canal pode introduzir erro(s), ou seja, pode transformar a palavra-código $\mathbf{x}$ em uma outra n-upla $\mathbf{s}$. Ao receber $\mathbf{s}$, o receptor deve reconhecer se um erro ocorreu e, em caso afirmativo, reconstituir a palavra-código inicial $\mathbf{x}$.

Para isso, o receptor possui um esquema de decisão que consiste de uma partição do espaço das 2^n possíveis n-uplas enviadas em $M = 2^k$ regiões disjuntas $D_1, D_2, \cdots, D_M$, cada uma associada a uma palavra-código $\mathbf{x}_i$, para $1 \leq i \leq M$. Se considerarmos as palavras-código de um código (n, M, d) como um conjunto de pontos, o problema de codificação consiste no problema

de empacotar esferas contendo tantos pontos (n-uplas) quanto possível, mantendo, porém, uma certa distância entre essas esferas para garantir que as regiões associadas sejam disjuntas, [3]. Essas regiões são determinadas pelas *esferas de Hamming*. Uma esfera de Hamming de raio t e centro em $\mathbf{x}_i$ é definida pelo conjunto de n-uplas $\mathbf{z}$ que satisfazem

$$\{\mathbf{z} : d_H(\mathbf{x}_i, \mathbf{z}) \leq t\}. \tag{7.3}$$

O centro de uma esfera é a palavra-código associada à região. O raio das esferas associadas ao código $\mathcal{C}$ é dado pela capacidade de correção de erros que o caracteriza, estabelecida no teorema a seguir.

Teorema 10 *[75] Um código com distância d pode corrigir até* $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ *erros, onde* $\lfloor . \rfloor$ *indica o maior inteiro menor ou igual ao argumento. Se d é par, o código pode corrigir* $\frac{1}{2}(d-2)$ *erros e detectar* $d/2$ *erros simultaneamente.*

Considerando que o *peso de Hamming* de um vetor consiste no número de coordenadas diferentes de zero, o Teorema 10 estabelece que um código com distância d pode corrigir erros cujo peso de Hamming seja menor ou igual a $t = \left\lfloor \frac{d-1}{2} \right\rfloor$. Ou, no caso de d par, o código pode detectar a ocorrência de erros cujo peso seja menor ou igual a $\frac{d}{2}$.

Para exemplificar o processo de proteção e correção de erros no contexto dos códigos clássicos, suponha que uma palavra $\mathbf{x}_i$ de um código com distância d tenha sido transmitida através de um canal e que a palavra recebida seja $\mathbf{s} = \mathbf{x}_i + \mathbf{e}$.

O receptor tem o esquema de reconhecimento da informação estruturado da seguinte forma. A cada palavra-código $\mathbf{x}_i$ existe uma esfera de Hamming associada, de forma que

$$\{\mathbf{z} : d(\mathbf{x}_i, \mathbf{z}) < t = \left\lfloor \frac{d-1}{2} \right\rfloor, \mathbf{x}_i \neq \mathbf{z}\},$$

onde $\mathbf{z}$ consiste de uma das $(2^n - M)$ n-uplas que não são palavras-código de $\mathcal{C}$.

Se o peso de $\mathbf{e}$ for menor ou igual a t, então $\mathbf{s}$ corresponde a um *ponto* $\mathbf{z}$ no interior da esfera D_i e, portanto, $\mathbf{s}$ é reconhecida como a palavra-código $\mathbf{x}_i$. Caso o peso de $\mathbf{e}$ seja maior que t, então existe a possibilidade de $\mathbf{s}$ pertencer ao interior de uma esfera D_j e ser associada de forma equivocada à palavra $\mathbf{x}_j$.

De acordo com essas informações, é fácil identificar que um problema relevante neste contexto consiste em determinar uma partição do espaço das 2^n n-uplas para um código linear $\mathcal{C}$. Existe uma sistemática associada a este processo conhecida como *arranjo-padrão* [72], que é representado na forma de um tabela, como descrito a seguir.

$$\begin{array}{ccccccc}
\mathbf{x}_1 = \mathbf{0} & \mathbf{x}_2 & \cdots & \mathbf{x}_i & \cdots & \mathbf{x}_{2^k} \\
\mathbf{e}_1 & \mathbf{e}_1 + \mathbf{x}_2 & \cdots & \mathbf{e}_1 + \mathbf{x}_i & \cdots & \mathbf{e}_1 + \mathbf{x}_{2^k} \\
\mathbf{e}_2 & \mathbf{e}_2 + \mathbf{x}_2 & \cdots & \mathbf{e}_2 + \mathbf{x}_i & \cdots & \mathbf{e}_2 + \mathbf{x}_{2^k} \\
\vdots & & & & & \\
\mathbf{e}_l & \mathbf{e}_l + \mathbf{x}_2 & \cdots & \mathbf{e}_l + \mathbf{x}_i & \cdots & \mathbf{e}_l + \mathbf{x}_{2^k} \\
\vdots & & & & & \\
\mathbf{e}_{2^{n-k}-1} & \mathbf{e}_{2^{n-k}-1} + \mathbf{x}_2 & \cdots & \mathbf{e}_{2^{n-k}-1} + \mathbf{x}_i & \cdots & \mathbf{e}_{2^{n-k}-1} + \mathbf{x}_{2^k}
\end{array}$$

A primeira linha é constituída por todas as palavras-código $\mathbf{x}_i$, $i \in \{1, \cdots, M = 2^k\}$. Os $\mathbf{e}_j$'s denotam n-uplas distintas entre si, escolhidas com o menor peso possível, de forma que $\mathbf{e}_j \neq \mathbf{e}_z$ e $\mathbf{e}_j \neq \mathbf{e}_z + \mathbf{x}_i$, para $z < j$, $j \in \{1, \cdots, 2^{n-k} - 1\}$.

Cada uma das 2^{n-k} linhas define uma *classe lateral* de $\mathcal{C}$. O conjunto de todas essas classes laterais identifica a partição a ser utilizada. As colunas do arranjo-padrão estão associadas às esferas de Hamming de centro nas palavras-código $\mathbf{x}_i$ e raio $t = \left\lfloor \frac{d-1}{2} \right\rfloor$. Qualquer n-upla alocada na coluna sob a palavra-código $\mathbf{x}_i$ é associada a $\mathbf{x}_i$ pelo receptor. As n-uplas $\mathbf{e}_j$ definem os *padrões de erros* que o código pode corrigir. Por exemplo, um código de comprimento $n = 4$ pode corrigir todos os padrões de erros de peso 1 se $\mathbf{e}_1 = 0001$, $\mathbf{e}_2 = 0010$, $\mathbf{e}_3 = 0100$ e $\mathbf{e}_4 = 1000$. Se um código $\mathcal{C}$ pode corrigir qualquer padrão de erro de peso t, então é garantido pela construção do arranjo-padrão que todos os erros de peso t', $t' < t$ também são corrigidos. Maiores detalhes podem ser encontrados no Exemplo 27 do Capítulo 8.

Este comentário explicita a condição para que a proteção da informação contra erros seja estabelecida: quanto maior a distância associada ao código, maior a capacidade de correção e, conseqüentemente, maior a proteção contra erros estabelecida por tal código.

A maior distância possível em um código cujas palavras têm comprimento n é dada por $d = n$. Códigos com esta características são conhecidos como *códigos de repetição*. Conforme foi mencionado na Seção 7.1.1, as palavras-código que definem estes códigos são, em geral, representadas na forma $\underbrace{00\cdots0}_{n}$ e $\underbrace{11\cdots1}_{n}$.

Os códigos de repetição são uma particularidade de uma classe importante de códigos corretores de erros, denominada *códigos MDS*, do inglês, *maximal distance separable*, que é definida a seguir.

Definição 12 *[75] Um código binário $\mathcal{C}$ com parâmetros (n, M, d) é um código MDS se satisfaz a igualdade na expressão*

$$d \leq n - \log_2 M + 1. \tag{7.4}$$

Esta expressão é denominada *limitante de Singleton* [75]. Este limitante estabelece a maior distância possível, que denotaremos por d_{MDS}, para um código binário com parâmetros n e M.

De acordo com o estudo apresentado, se o objetivo é um processo de transmissão de informação que estabeleça a maior proteção quanto à ação de erros que possam ser introduzidos pelo canal, então o código a ser utilizado deve consistir em um código *MDS*.

As únicas classes de códigos binários *MDS* são dadas pelos parâmetros [75],

$$(n, M, d) = (n, 2, n) \quad (n, M, d) = (n, 2^n, 1) \quad \text{e} \quad (n, M, d) = (n, 2^{n-1}, 2).$$

Dentre esses, os que apresentam descrição mais simplificada, menor complexidade na decodificação e, para um n fixo, o maior valor de d associado, são os códigos de repetição.

Há, porém, uma ressalva quanto à utilização de códigos de repetição. Tais códigos são definidos apenas por duas palavras-código. A cardinalidade M do conjunto de palavras que define um código está associada à quantidade de símbolos (*bits*) de informação que podem ser transmitidos a partir deste código. Esta quantidade é descrita como $log_2 M$.

Para que a quantidade de informação transmitida a partir de um código seja grande, é necessário que o número de palavras-código também o seja. Entretanto, não é difícil mostrar que quanto maior a cardinalidade do conjunto de palavras, menor a distância de Hamming obtida, o que implica, segundo o Teorema 10, em uma menor proteção à informação contra erros que possam ser introduzidos no processo.

Observe que entre os códigos *MDS*, os que apresentam maior cardinalidade M são códigos com parâmetros $(n, M, d) = (n, 2^n, 1)$. O valor $d = 1$ associado implica que os códigos com esses parâmetros não detectam e nem corrigem erros, donde decorre a ausência total de proteção contra erros. Neste sentido, os códigos *MDS* representados por $(n, M, d) = (n, 2^{n-1}, 2)$ são melhores que os primeiros, pois ainda apresentam um valor grande para M e $d = 2$, donde é possível concluir que tais códigos podem, ao menos, detectar a ocorrência de erros de peso $t = 1$.

Todavia, apenas detectar erros de peso 1 para qualquer que seja n não é suficiente para garantir uma proteção confiável, a menos que o sistema esteja completamente isolado com relação à ocorrência de erros, o que, em geral não é observado. Com isso, concluímos que a classe dos códigos *MDS* binários não contém códigos que apresentem, para cada n, valores de M e d adequados, de forma que ambos sejam maximizados. Desta forma, é necessário determinar qual ou quais classes de códigos implicam nesta caracterização.

Uma relação bastante satisfatória neste sentido entre M e d pode ser estabelecida pelo *limitante de Plotkin* [75].

Definição 13 *Para todo código com parâmetros (n, M, d), com n e d tal que $n < 2d$, a seguite relação é satisfeita*

$$M \leq 2 \left\lfloor \frac{d}{2d - n} \right\rfloor \tag{7.5}$$

Se o objetivo é maximizar os valores de M e d, consideramos a igualdade na expressão (7.5), de forma a obtermos

$$M = 2 \left\lfloor \frac{d}{2d - n} \right\rfloor \tag{7.6}$$

Sem perda de generalidade, determinamos quais são os valores de d para cada n para os quais

$$\frac{d}{2d - n} = \beta,$$

$\beta \in \mathbb{Z}^*$. Esta condição implica que $M = 2\beta$.

Como consideramos neste estudo apenas códigos lineares, de acordo com o Lema 7, podemos assumir que $M = 2^k$, $k \geq 1$. Disso segue que

$$\frac{d}{2d - n} = 2^{k-1}.$$

Conseqüentemente, temos que d deve satisfazer, para cada n,

$$d = \frac{n2^{k-1}}{2^k - 1}.$$

Como d deve ser um número natural, temos que esta análise está restrita a valores de n, tais que $n = l(2^k - 1)$, o que resulta em $d = l(2^{k-1})$.

No caso de $\frac{d}{2d-n} = 1$, temos que $d = n$ e $k = 1$, donde resulta que $M = 2$. Ou seja, o menor valor para M está associado à maior distância possível ($d = n$) e pode ser obtido para qualquer valor de n. Esses são os *códigos de repetição*, que foram mencionados na Seção 7.1.1.

No caso de $l = 1$, para $k \geq 2$, temos uma classe de códigos com parâmetros $(n, M, d) = (2^k - 1, 2^k, 2^{k-1})$, que é conhecida como *códigos simplex n-dimensionais*, que foram mencionados na Seção 7.1.2. Esses códigos são facilmente descritos, uma vez que decorrem dos códigos de Reed-Muller de primeira ordem ou, simplesmente, consistem dos códigos duais dos códigos de Hamming.

Para os demais valores de n, múltiplos de $2^k - 1$, $k > 2$, os códigos associados são obtidos a partir de uma matriz geradora que consiste na *justaposição* da matriz geradora de um códigos *simplex*. Os parâmetros de códigos assim caracterizados são dados por

$$(n, M, d) = \left(n = l(2^k - 1), 2^k, d = l2^{k-1}\right). \tag{7.7}$$

Apresentamos a seguir um código cuja matriz geradora é uma justaposição da matriz geradora de um código *simplex* com o objetivo de exemplificar a construção de códigos com esta propriedade.

Exemplo 22 *Seja $\mathcal{C}_9$ o código de comprimento $n = 9$ descrito a partir de uma matriz geradora que é obtida da justaposição da matriz geradora do código simplex 3-dimensional $\mathcal{C}_3$ com parâmetros $(3, 4, 2)$ (veja Exemplo 21). De acordo com (7.7), para que $n = 9$, devemos considerar $l = 3$, de forma que os parâmetros do código $\mathcal{C}_9$ são $(n, M, d) = (9, 4, 6)$.*

Considerando que a matriz geradora do código simplex $\mathcal{C}_3$ consiste em

$$G_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

temos que a matriz geradora G_9 do código $\mathcal{C}_9$ é obtida a partir da repetição da matriz G_3 $l = 3$ vezes. Sob essas condições, temos que matriz geradora do código $\mathcal{C}_9$ é descrita por

$$G_9 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix},$$

donde decorre que o conjunto de palavras-código associado consiste em

$$\{000000000, 101101101, 011011011, 110110110\}.$$

Tendo como base os conceitos apresentados neste capítulo, retornaremos à questão de verificar se, de fato, existe uma relação entre o conjunto de seqüências binárias que definem os *kets* dos estados arbitrários de máximo emaranhamento global e os conjuntos de palavras associados a códigos binários e lineares. Tal estudo é apresentado no próximo capítulo.

Capítulo 8

Códigos Binários e Estados de Máximo Emaranhamento Global

O objetivo deste capítulo é apresentar que a identificação entre o conjunto de seqüências binárias que constituem os *kets* de um estado de máximo emaranhamento global e o conjunto de palavras de um código binário linear não é uma particularidade para estados com três *qubits*, como mencionado no Capítulo 6. Além disso, mostramos que determinados códigos binários não-lineares também satisfazem tal associação. A partir desta interpretação é possível descrever estados arbitrários de máximo emaranhamento global e estudar, tendo como base elementos de teoria da codificação, quais dentre todos os possíveis estados são os mais apropriados para serem empregados em tarefas de processamento de informação. Este capítulo está organizado da seguinte forma. Na Seção 8.1, apresentamos o resumo das principais identificações consideradas neste trabalho. Na Seção 8.2 propomos uma forma alternativa de descrever a medida de máximo emaranhamento global, denotada por Q, sugerida por Meyer-Wallach em [78]. Tendo como base esta nova descrição para a medida Q, explicitamos a condição que o conjunto de seqüências que definem os *kets* deve satisfazer para que o estado associado seja classificado como um estado de máximo emaranhamento global. Na Seção 8.3, reescrevemos tal condição no contexto de códigos binários. Dentre todos os estados de máximo emaranhamento global obtidos a partir da descrição estabelecida, estudamos na Seção 8.4 quais apresentam maior proteção às informações transmitidas ou armazenadas aos erros que possam ocorrer durante a execução de uma tarefa de processamento.

8.1 Revisão das Identificações Propostas

Seja $|\psi\rangle$ um estado puro arbitrário com n *qubits* descrito na forma

$$|\psi\rangle = \alpha_0|00\cdots0\rangle + \alpha_1|00\cdots1\rangle + \cdots + \alpha_{2^n-2}|11\cdots0\rangle + \alpha_{2^n-1}|11\cdots1\rangle,$$

onde $\alpha_0, ..., \alpha_{2^n-1} \in \mathbb{C}$ e $\sum_{s=0}^{2^n-1} |\alpha_s|^2 = 1$.

Considerando que o conjunto das seqüências binárias que constituem os *kets* de $|\psi\rangle$ é denotado por A_ψ, temos que este estado pode ser identificado a partir de A_ψ e da distribuição de amplitudes.

Como mencionado no Capítulo 6, este trabalho se restringe a estados com todas as amplitudes iguais a $\frac{1}{\sqrt{M}}$, onde M é a cardinalidade de A_ψ. Sendo assim, apenas a definição de um conjunto A_ψ é suficiente para a identificação de $|\psi\rangle$, de acordo com as restrições às quais este estado satisfaz.

Apresentamos a seguir a definição da medida de emaranhamento global Q proposta por Meyer-Wallach em [78].

Seja $\mathbf{x} = x_1 \cdots x_n$ uma n-upla binária associada ao conteúdo de um ket de $|\psi\rangle$, sendo x_j, $j = 1, \cdots, n$, cada coordenada de $\mathbf{x}$. Considere $\iota_j(b) : (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n-1}$ a função linear definida pela seguinte ação na base

$$\iota_j(b)\left(|x_1\rangle \otimes \cdots \otimes |x_n\rangle\right) = \delta_{bx_j}|x_1\rangle \otimes \cdots \otimes |x_{j-1}\rangle \otimes |x_{j+1}\rangle \otimes \cdots |x_n\rangle, \tag{8.1}$$

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

Proposição 7 *[95] Dado um estado quântico puro arbitrário com n qubits $|\psi\rangle$, a medida de emaranhamento global de Meyer-Wallach é dada por*

$$Q(|\psi\rangle) = \frac{4}{n}\sum_{j=1}^{n} D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle), \tag{8.2}$$

onde

$$D(\iota_j(0)|\psi\rangle, \iota_j(1)|\psi\rangle) = \langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle\langle\psi|\iota_j(1), \iota_j(1)|\psi\rangle - |\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle|^2, \tag{8.3}$$

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

Q é invariante sob transformações unitárias locais e tal que $0 \leq Q \leq 1$. Assim, $Q(|\psi\rangle) = 0$ se, e somente se, $|\psi\rangle$ é um estado separável, e $Q(|\psi\rangle) = 1$ se, e somente se, $|\psi\rangle$ é um estado puro de máximo emaranhamento global.

Tendo como base esta medida, apresentamos na próxima seção uma outra descrição para Q, que nos possibilita classificar estados com amplitudes iguais a $1/\sqrt{M}$ quanto à quantidade de emaranhamento global de forma bem mais simples do que a estabelecida em (8.2).

8.2 Nova Descrição para a Medida Q

Proposição 8 *Seja $|\psi\rangle$ um estado quântico puro com amplitudes iguais a $\frac{1}{\sqrt{M}}$ e tal que o conjunto A_ψ satisfaz $d > 1$. Nestas condições, a seguinte equivalência é estabelecida,*

$$Q(|\psi\rangle) \equiv Q'(|\psi\rangle) = \frac{4}{n}\frac{1}{M^2}\sum_{j=1}^{n} z_j \cdot (M - z_j), \tag{8.4}$$

onde z_j representa o número de n-uplas em A_ψ que têm 0 na j-ésima posição, para todo j, $j \in \{1, \cdots, n\}$, M denota a cardinalidade de A_ψ e d denota a mínima distância de Hamming neste conjunto.

Demonstração. Considere, para cada j fixo, as seguintes representações

$$\iota_j(0)|\psi\rangle = \frac{1}{\sqrt{M}}\left(|\mathbf{p}_1^0\rangle + |\mathbf{p}_2^0\rangle + \cdots + |\mathbf{p}_{L_0}^0\rangle\right)$$

e

$$\iota_j(1)|\psi\rangle = \frac{1}{\sqrt{M}}\left(|\mathbf{p}_1^1\rangle + |\mathbf{p}_2^1\rangle + \cdots + |\mathbf{p}_{L_1}^1\rangle\right),$$

onde $\mathbf{p}_l^0$ ($\mathbf{p}_l^1$) indicam as n-uplas em A_ψ com o dígito "0" ("1") excluído da posição j fixada. Os valores $L_0(j)$ e $L_1(j)$ indicam o número de n-uplas em A_ψ com "0" e "1", respectivamente, na j-ésima posição.

De acordo com esta notação, para cada j fixo, o produto $|\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle|^2$ representado em (8.3) pode ser reescrito como

$$\begin{aligned}\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle &= \left(\frac{1}{\sqrt{M}}\right)^2 \left(\langle\mathbf{p}_1^0|\mathbf{p}_1^1\rangle + \cdots + \langle\mathbf{p}_1^0|\mathbf{p}_{L_1}^1\rangle + \right.\\ &\quad \left. + \cdots + \langle\mathbf{p}_{L_0}^0|\mathbf{p}_1^1\rangle + \cdots + \langle\mathbf{p}_{L_0}^0|\mathbf{p}_{L_1}^1\rangle\right).\end{aligned}$$

Tendo como base as propriedades do produto interno, temos que $\langle\mathbf{p}|\mathbf{p}'\rangle$ são diferentes de zero se, e somente se, $\mathbf{p} = \mathbf{p}'$. Como $|\psi\rangle$ é tal que A_ψ satisfaz $d > 1$, então podemos garantir que não há duas n-uplas em A_ψ que diferem somente na posição j. Desta forma, podemos concluir que, fixada a posição j, não há possibilidade de que algum $\mathbf{p}^0$ seja igual a algum $\mathbf{p}^1$, donde decorre que todas as parcelas de $\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle$ satisfazem $|\langle\psi|\iota_j(0), \iota_j(1)|\psi\rangle|^2 = 0$.

Como o mesmo argumento vale para qualquer que seja a posição j, $j \in \{1, \cdots, n\}$, então (8.2) pode ser reduzida a

$$Q(|\psi\rangle) = \frac{4}{n}\sum_{j=1}^{n}\left(\langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle\langle\psi|\iota_j(1), \iota_j(1)|\psi\rangle\right). \tag{8.5}$$

Segundo a notação estabelecida, para $K = \left(\frac{1}{\sqrt{M}}\right)^2$, temos

$$\langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle = K\left(\langle\mathbf{p}_1^0|\mathbf{p}_1^0\rangle + \cdots + \langle\mathbf{p}_1^0|\mathbf{p}_{L_0}^0\rangle + \cdots + \cdots + \langle\mathbf{p}_{L_0}^0|\mathbf{p}_{L_0}^0\rangle\right). \tag{8.6}$$

Novamente, a condição $d > 1$ implica que, para cada j fixo, as n-uplas $\mathbf{p}^0$ são distintas entre si. Assim, só são diferentes de zero e iguais a 1 as parcelas de (8.6) na forma $\langle\mathbf{p}_l^0|\mathbf{p}_l^0\rangle$. Como l é limitado por L_0, há L_0 parcelas com esta característica, de forma que

$$\langle\psi|\iota_j(0), \iota_j(0)|\psi\rangle = L_0\left(\frac{1}{\sqrt{M}}\right)^2. \tag{8.7}$$

Salientando que as parcelas de $\iota_j(0)|\psi\rangle$ decorrem de n-uplas (distintas) do conjunto A_ψ, tais que a j-ésima posição contém um "0", temos que L_0 corresponde a z_j para cada j, conforme definido na Proposição 8.

As mesmas considerações garantem que

$$\langle\psi|\iota_j(1), \iota_j(1)|\psi\rangle = L_1 \left(\frac{1}{\sqrt{M}}\right)^2, \tag{8.8}$$

onde L_1 denota, para cada j, o número de n-uplas de A_ψ com "1" na j-ésima posição. Se a cardinalidade de A_ψ é M, segundo a definição de $L_0(j)$ e $L_1(j)$, decorre que $L_0(j) + L_1(j) = M$ e, conseqüentemente, $L_1(j) = M - L_0(j)$, ou $L_1(j) = M - z_j$, para cada $j \in \{1, \cdots, n\}$.

De acordo com (8.7) e (8.8), a equação (8.5) pode ser escrita na forma

$$Q(|\psi\rangle) = \frac{4}{n}\frac{1}{M^2}\sum_{j=1}^{n}(z_j \cdot (M - z_j)) \equiv Q'(|\psi\rangle), \tag{8.9}$$

o que conclui a demonstração do resultado.

■

Apresentamos a seguir algumas aplicações da medida Q' estabelecida.

Exemplo 23 *O estado* $|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ *é tal que* $A_\psi = \{000, 111\}$. *Disso decorre que* $M = 2$ *e* $z_1, z_2, z_3 = 1$. *Substituindo esses valores em (8.9), temos*

$$Q'(|\psi_{GHZ}\rangle) = \frac{4}{3}\frac{1}{2^2}\sum_{j=1}^{3}(1 \cdot (2 - 1)) = 1.$$

Exemplo 24 *O estado* $|\psi_W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ *está associado ao conjunto* $A_\psi = \{001, 010, 100\}$. *Disso segue que* $M = 3$ *e* $z_1, z_2, z_3 = 2$. *Substituindo em (8.9), temos como resultado*

$$Q'(|\psi_W\rangle) = \frac{4}{3}\frac{1}{3^2}\sum_{j=1}^{3}(2 \cdot (3 - 2)) = 8/9.$$

Exemplo 25 *O estado* $|\psi_{HGHZ}\rangle = \frac{1}{\sqrt{4}}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)$ *é tal que*

$$A_\psi = \{000, 011, 110, 101\},$$

donde decorre que $M = 4$ *e* $z_1, z_2, z_3 = 2$. *Substituindo em (8.9), temos como resultado*

$$Q'(|\psi_{HGHZ}\rangle) = \frac{4}{3}\frac{1}{4^2}\sum_{j=1}^{3}(2 \cdot (4 - 2)) = 1.$$

Tais valores para o emaranhamento global coincidem com os resultados obtidos a partir de Q, calculados em [78] e mencionados no Capítulo 6, Seção 6.1.

Esta nova descrição para a medida de Meyer-Wallach resulta em uma condição direta para a classificação e descrição de estados de máximo emaranhamento global, como é apresentado a seguir.

Salientando que z_j representa o número de n-uplas em A_ψ contendo "0" na j-ésima posição, para $j \in \{1, \cdots, n\}$, temos o seguinte resultado.

Teorema 11 *Seja $|\psi\rangle$ um estado quântico puro com amplitudes iguais a $\frac{1}{\sqrt{M}}$, cujo conjunto A_ψ associado satisfaz $d > 1$ e tem cardinalidade M. Então, $|\psi\rangle$ é um estado quântico puro de máximo emaranhamento global se, e somente se, $z_j = M/2$, para todo $j \in \{1, \cdots, n\}$.*

Demonstração. A primeira parte da demonstração consiste em determinar quais são as condições sobre A_ψ que implicam em $Q' = 1$. De acordo com (8.9), temos que

$$Q'(\psi) = \frac{4}{n}\frac{1}{M^2}\sum_{j=1}^{n}(z_j \cdot (M - z_j)) = 1 \Longrightarrow \sum_{j=1}^{n}(z_j \cdot (M - z_j)) = \frac{nM^2}{4}. \tag{8.10}$$

O objetivo é determinar quais são os possíveis valores de z_j para que (8.10) seja satisfeita. Para isso, observe que a expressão

$$\sum_{j=1}^{n}(z_j \cdot (M - z_j)) = \frac{nM^2}{4}$$

pode ser reescrita como

$$\sum_{j=1}^{n}\left(z_j^2 - Mz_j + \frac{M^2}{4}\right) = 0 \Longrightarrow \sum_{j=1}^{n}\left(z_j - \frac{M}{2}\right)^2 = 0.$$

Como a soma de parcelas não negativas resulta em zero se, e somente se, as parcelas forem todas nulas, então temos que os valores de z_j para os quais (8.10) é satisfeita são da forma

$$z_j = \frac{M}{2},$$

para todo $j \in \{1, \cdots, n\}$, onde M representa o número de *kets* do estado $|\psi\rangle$.

Considere um estado puro $|\psi\rangle$ com amplitudes iguais a $\frac{1}{\sqrt{M}}$, com A_ψ satisfazendo $d > 1$. A segunda parte da verificação consiste em mostrar que se A_ψ é tal que $z_j = M/2$, para todo $j = 1, \cdots, n$, então $|\psi\rangle$ é um estado de máximo emaranhamento global. Todavia, se A_ψ é tal que $z_j = M/2$, para todo $j = 1, \cdots, n$, então, por (8.9), temos que $Q'(|\psi\rangle) = 1$. Pela Proposição 8, temos que $Q(|\psi\rangle) = 1$, donde decorre a classificação de $|\psi\rangle$.

■

Portanto, dado um estado quântico puro $|\psi\rangle$ com amplitudes iguais a $\frac{1}{\sqrt{M}}$, composto por M *kets* e cujo conjunto A_ψ é caracterizado por $d > 1$, então este estado satisfaz $Q = 1$ se, e somente se, $z_j = M/2$, para todo $j \in \{1, \cdots, n\}$. De acordo com o resultado proposto por Meyer-Wallach, esta é a condição que nos permite classificar estados de máximo emaranhamento global.

O operador de medida Q' estabelecido em (8.9) é menos geral que a medida Q quanto à classificação de estados puros arbitrários, uma vez que só pode ser aplicada a estados com amplitudes iguais e tais que o conjunto A_ψ associado satisfaça $d > 1$. Por outro lado, a descrição mais direta, em termos de operadores, de Q' nos permite analisar quais são as condições que A_ψ deve satisfazer para que o estado associado atinja $Q' = 1$ e, conseqüentemente, seja classificado como um estado de máximo emaranhamento global.

Observe que a condição que o conjunto A_ψ deve satisfazer para que estados de máximo emaranhamento global sejam obtidos é bastante simples e facilmente implementável, donde resulta uma sistematização na descrição de estados com esta característica. Esta sistematização pode ser ainda mais refinada no contexto de teoria da codificação. Tal resultado é apresentado na próxima seção.

8.3 Códigos Lineares e Alguns Não-Lineares Descrevem Estados de Máximo Emaranhamento Global

Conforme mencionado no Capítulo 7, o conjunto A_ψ que contém as seqüências binárias que compõem os *kets* de um estado puro arbitrário com n *qubits* $|\psi\rangle$ consiste de um subconjunto de $\mathcal{H}_2^n$ (espaço consituído por todas as seqüências binárias de comprimento n). Uma vez que os códigos binários de comprimento n são definidos da mesma forma, estabelecemos uma identificação entre o conjunto de seqüências binárias A_ψ e o conjunto de palavras-código de um código binário. O resultado apresentado no Teorema 11 garante que $|\psi\rangle$ é um estado de máximo emaranhamento global se, e somente se, A_ψ satisfaz $z_j = M/2$. Com isso, determinar os conteúdos dos *kets* para que $|\psi\rangle$ seja um estado de máximo emaranhamento global equivale a determinar códigos cujo conjunto de palavras satisfaz $z_j = M/2$, para todo $j \in \{1, \cdots, n\}$.

De acordo com a propriedade apresentada na Proposição 6 do Capítulo 7, os códigos binários e lineares são caracterizados pelo conjunto de palavras-código satisfazendo $z_j = M/2$, para todo $j \in \{1, \cdots, n\}$. Desta forma, há uma relação estabelecida entre os conjuntos de palavras-código de códigos binários e lineares e o conjunto A_ψ que define as amplitudes e as seqüências binárias dos *kets* que descrevem estados de máximo emaranhamento global.

Todavia, salientamos que não só os códigos lineares satisfazem a propriedade estabelecida pelo Teorema 11. Como mencionado no Capítulo 7, Seção 7.2, os códigos *simplex* não-lineares, o código de Nordstrom-Robinson e os códigos de Preparata têm os respectivos conjuntos de palavras-código conhecidos e satisfazem a condição de $z_j = M/2$, para todo j. Portanto, temos

que os códigos não-lineares do tipo *simplex*, Nordstrom-Robinson e Preparata também definem estados de máximo emaranhamento global.

Com base em tais considerações, podemos reescrever o resultado apresentado no Teorema 11 na seguinte forma.

Teorema 12 *Seja $|\psi\rangle$ é um estado puro com amplitudes iguais a $\frac{1}{\sqrt{M}}$ e tal que A_ψ satisfaz $d > 1$. O estado $|\psi\rangle$ é um estado de máximo emaranhamento global se, e somente se, A_ψ corresponde a um conjunto de palavras de um código linear ou de um código não-linear satisfazendo a propriedade de $z_j = M/2$, para todo $j \in \{1, \cdots, n\}$, onde M corresponde à cardinalidade de A_ψ.*

Um exemplo da aplicação deste resultado consiste da análise do estado

$$|\psi_W\rangle = \frac{1}{\sqrt{3}} \left(|011\rangle + |110\rangle + |101\rangle \right).$$

Tal estado está associado ao conjunto $A_{\psi_W} = \{011, 110, 101\}$, que define um código não-linear, mas não satisfaz a condição $z_j = M/2$, para todo $j = 1, 2, 3$, e, portanto, $|\psi_W\rangle$ não é um estado de máximo emaranhamento global.

Como foi mencionado no Capítulo 7, nem sempre o conjunto de palavras-código de um código não-linear é conhecido, donde decorre que não é possível estabelecer o resultado de quais dentre esses códigos satisfazem a propriedade de $z_j = M/2$, para todo j. Tendo como base esta informação e o objetivo de apresentar a análise que segue de forma geral, optamos em considerar apenas os estados de máximo emaranhamento obtidos a partir de códigos binários lineares.

Dentre todos os estados de máximo emaranhamento global que podem ser descritos a partir de códigos lineares, o objetivo da próxima seção é determinar se há alguma classe dentre tais estados que apresente características diferenciadas quanto à realização de tarefas de processamento de informação.

8.4 Códigos *Simplex* e a Proteção de Estados Contra a Ação de Erros

Conforme mencionado no Capítulo 2, os estados emaranhados são fundamentais para a execução eficiente de tarefas de processamento da informação.

Para a realização destas tarefas, o que se faz é associar as informações a serem transmitidas e/ou armazenadas a estados quânticos. Durante a execução do processo, os estados podem sofrer alterações causadas pela ação do meio (do canal de transmissão, por exemplo). Como a informação é *armazenada* no conjunto das seqüências binárias que compõem os *kets* do estado utilizado, qualquer alteração nestes pode implicar que, ao receber o estado corrompido, a informação inicial não seja reconhecida corretamente, o que implica em um erro de transmissão.

Tais alterações podem modificar a seqüência de zeros e uns de um dos *kets* ou, ainda, alterar um determinado subsistema, modificando o *qubit* da k-ésima posição em todos os *kets* do estado, por exemplo.

Se as seqüências binárias que compõem os *kets* são escolhidas de forma adequada, um possível erro pode ser detectado pelo receptor e, então, corrigido. Neste caso, dizemos que o estado apresenta *proteção contra erros*. Como o conjunto de tais seqüências está associado ao conjunto de palavras de um código linear, podemos dizer que a determinação de um estado de máximo emaranhamento global que apresente proteção contra erros à informação que transporta ou armazena é equivalente a determinar um código com *capacidade de correção de erros*.

Tal questão foi discutida no Capítulo 7. Neste contexto, obtivemos que os códigos que apresentam maior proteção contra erros são aqueles cuja distância coincide com a distância estimada a partir do limitante de Singleton. Tais códigos são conhecidos como *MDS* e, dentre esse, destacamos os códigos de repetição, cujos parâmetros são $(n, M, d) = (n, 2, n)$ e as palavras são representadas por

$$\mathbf{x}_1 = \underbrace{00\cdots0}_{n} \quad \text{e} \quad \mathbf{x}_2 = \underbrace{11\cdots1}_{n}.$$

De acordo com as identificações propostas neste trabalho, aos códigos de repetição associamos estados de máximo emaranhamento global na forma

$$|\psi_{GHZ}\rangle_n = \frac{1}{\sqrt{2}}\left(|\underbrace{00\cdots0}_{n}\rangle + |\underbrace{11\cdots1}_{n}\rangle\right). \tag{8.11}$$

Tais estados, segundo a proposta deste trabalho, apresentam maior proteção à informação que transportam ou armazenam contra erros, e, por isso, são apropriados para a realização eficiente de tarefas de processamento.

De fato, os estados na forma de (8.11) são denominados *estados GHZ generalizados* e, segundo a literatura, todas as tarefas de processamento da informação realizáveis somente no contexto quântico, tais como o teletransporte, a codificação superdensa e a criptografia quântica estão baseadas em estados desta classe. Tal informação de alguma forma comprova a proposta de que esses são os estados que oferecem maior proteção a erros.

Há, porém, um ponto a ser observado. Os estados *GHZ generalizados* são restritos quanto ao número de *kets*. No caso da execução de uma tarefa cujo aumento da quantidade de *kets* seja necessária, ou simplesmente, torne sua execução mais eficiente, como no contexto do paralelismo quântico, seria interessante conhecer uma outra classe de estados que tivesse maior número de *kets*, mas que ainda apresentasse proteção confiável contra erros.

Conforme mencionado no Capítulo 6, uma classe de estados de máximo emaranhamento global importante é obtida a partir da aplicação do operador de Hadamard em todos os *qubits* do $|\psi_{GHZ}\rangle_n$, o que implica na definição dos estados do tipo *HGHZ* generalizados.

Em outras palavras, uma classe de estados com n *qubits* de máximo emaranhamento global

é representada por

$$|\psi_{HGHZ}\rangle_n = Had^{\otimes n}\left[\frac{1}{\sqrt{2}}\left(|\underbrace{00\cdots0}_{n}\rangle + |\underbrace{11\cdots1}_{n}\rangle\right)\right], \tag{8.12}$$

onde Had é o operador definido pela seguinte ação na base $\{|0\rangle, |1\rangle\}$:

$$Had(|0\rangle) = 1/\sqrt{2}\,(|0\rangle + |1\rangle) \quad \text{e} \quad Had(|1\rangle) = 1/\sqrt{2}\,(|0\rangle - |1\rangle)\,.$$

Com base nesta definição, temos que (8.12) pode ser reescrita como

$$|\psi_{HGHZ}\rangle_n = \frac{1}{\sqrt{2}}\left[\underbrace{Had(|0\rangle)\otimes\cdots\otimes Had(|0\rangle)}_{n} + \underbrace{Had(|1\rangle)\otimes\cdots\otimes Had(|1\rangle)}_{n}\right].$$

Pode-se verificar que, para todo n, o estado $|\psi_{HGHZ}\rangle_n$ está associado a um código linear cuja cardinalidade é dada por $M = 2^{n-1}$ e $d = 2$. Observe que tais parâmetros definem a classe dos códigos *MDS* na forma $(n, M, d) = (n, 2^{n-1}, 2)$.

Exemplo 26 *Para $n = 7$, temos que*

$$\begin{aligned}
|\psi_{HGHZ}\rangle_7 \;=\; 1/\sqrt{64}\;&(|0000000\rangle + |0000011\rangle + |0000101\rangle + |0000110\rangle\\
&+|0001001\rangle + |0001010\rangle + |0001100\rangle + |0001111\rangle\\
&+|0010001\rangle + |0010010\rangle + |0010100\rangle + |0010111\rangle\\
&+|0011000\rangle + |0011011\rangle + |0011101\rangle + |0011110\rangle\\
&+|0100001\rangle + |0100010\rangle + |0100100\rangle + |0100111\rangle\\
&+|0101000\rangle + |0101011\rangle + |0101101\rangle + |0101110\rangle\\
&+|0110000\rangle + |0110011\rangle + |0110101\rangle + |0110101\rangle\\
&+|0111001\rangle + |0111010\rangle + |0111100\rangle + |0111111\rangle\\
&+|1000001\rangle + |1000010\rangle + |1000100\rangle + |1000111\rangle\\
&+|1001000\rangle + |1001011\rangle + |1001101\rangle + |1001110\rangle\\
&+|1010000\rangle + |1010011\rangle + |1010101\rangle + |1010110\rangle\\
&+|1011001\rangle + |1011010\rangle + |1011100\rangle + |1011111\rangle\\
&+|1100011\rangle + |1100000\rangle + |1100101\rangle + |1100110\rangle\\
&+|1101001\rangle + |1101010\rangle + |1101100\rangle + |1101111\rangle\\
&+|1110001\rangle + |1110010\rangle + |1110100\rangle + |1110111\rangle\\
&+|1111000\rangle + |1111011\rangle + |1111101\rangle + |1111110\rangle).
\end{aligned}$$

Disso decorre que o conjunto A_ψ das seqüências binárias que compõem os kets de $|\psi_{HGHZ}\rangle_7$ satisfaz a propriedade de fechamento, tem cardinalidade $M = 64$ e distância mínima $d = 2$. Então, o código associado a $|\psi_{HGHZ}\rangle_7$ é linear e tem parâmetros $(n, M, d) = (7, 64, 2) = (n, 2^{n-1}, 2)$.

Embora o número de *kets* seja grande, segundo o Teorema 10, temos que códigos com distância $d = 2$ não corrigem erro, o que implica na ausência da proteção contra erros, contrariamente ao que os estados GHZ generalizados fazem. Disso decorre que tais estados podem

ser utilizados apenas em tarefas cujo ambiente seja o mais confiável possível, no sentido de não admitir interferências do meio.

Para que a proteção contra erros esteja de fato definida para situações mais gerais, é necessário que se determine estados com valores de M e d apropriados.

Tal questão também foi discutida no Capítulo 7, a partir do limitante de Plotkin, explicitado na Definição 13. Estabelecemos neste contexto que os códigos que apresentam os maiores valores para M e d, estando tais parâmetros condicionados entre si, são os códigos *simplex* n-dimensionais, definidos pelos parâmetros

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

para $n = 2^m - 1, m \geq 2$, e os códigos cujas matrizes geradoras são obtidas a partir da justaposição das matrizes geradoras dos primeiros, construídos como mencionado no Exemplo 22.

Apresentamos a seguir um exemplo de como a escolha de códigos *simplex* n-dimensionais como alternativa para transmissão de informações, considerando uma boa capacidade de correção de erros e um conjunto de *kets* com cardinalidade maior do que 2.

Exemplo 27 *Para $n = 7$ é possível definir um código simplex 7-dimensional, $\mathcal{C}_{simplex}$, cujos parâmetros são descritos por $(n, M, d) = (7, 8, 4)$. As palavras-código associadas são* $\{0000000, 0110011, 0001111, 0111100, 1010101, 1100110, 1011010, 1101001\}$.

Construindo o arranjo-padrão associado a este código, temos

		0000000	*0001111*	*0110011*	*0111100*	*1010101*	*1011010*	*1100110*	*1101001*
	0000001	*0000001*	*0001110*	*0110010*	*0111101*	*1010100*	*1011011*	*1100111*	*1101000*
	0000010	*0000010*	*0001101*	*0110001*	*0111110*	*1010111*	*1011000*	*1100100*	*1101011*
	0000100	*0000100*	*0001011*	*0110111*	*0111000*	*1010001*	*1011110*	*1100010*	*1101101*
$t = 1$	*0001000*	*0001000*	*0000111*	*0111011*	*0110100*	*1011101*	*1010010*	*1101110*	*1100001*
	0010000	*0010000*	*0011111*	*0100011*	*0101100*	*1000101*	*1001010*	*1110110*	*1111001*
	0100000	*0100000*	*0101111*	*0010011*	*0011100*	*1110101*	*1111010*	*1000110*	*1001001*
	1000000	*1000000*	*1001111*	*1110011*	*1111100*	*0010101*	*0011010*	*0100110*	*0101001*
	0000011	*0000011*	*0001100*	*0110000*	*0111111*	*1010110*	*1011001*	*1100101*	*1101010*
	0000101	*0000101*	*0001010*	*0110110*	*0111001*	*1010000*	*1011111*	*1100011*	*1101100*
	0000110	*0000110*	*0001001*	*0110101*	*0111010*	*1010011*	*1011100*	*1100000*	*1101110*
$t = 2$	*0010001*	*0010001*	*0011110*	*0100010*	*0101101*	*1000100*	*1001011*	*1110111*	*1111000*
	0010010	*0010010*	*0011101*	*0100001*	*0101110*	*1000111*	*1001000*	*1110100*	*1111011*
	0010100	*0010100*	*0011011*	*0100111*	*0101000*	*1000001*	*1001110*	*1110010*	*1111101*
	0011000	*0011000*	*0010111*	*0101011*	*0100100*	*1001101*	*1000010*	*1111110*	*1110001*
$t = 3$	*0010110*	*0010110*	*0011001*	*0100101*	*0101010*	*1000011*	*1001100*	*1110000*	*1111111*

Observe que $\mathcal{C}_{simplex}$ pode corrigir todos os erros de peso 1, reconhece a ocorrência de algumas classes de peso 2, representadas pelos erros 0000011*,* 0000101*,* 0000110*,* 0010001*,* 0010010*,* 0010100 *e* 0011000 *e de uma classe de erros de peso 3, cujo representante é* 0010110*. Isso implica que o código é capaz de corrigir ou detectar os erros que porventura ocorram na posição k das palavras onde há um dígito "1" nas n-uplas que estabelecem os padrões de erros. Por exemplo, o padrão de erro denotado por* 0000001 *indica que o código é capaz de corrigir erros introduzidos na sétima posição.*

O estado associado ao código $\mathcal{C}_{simplex}$ consiste de

$$|\psi_{simplex}\rangle = \frac{1}{\sqrt{8}}\left(|0000000\rangle + |0110011\rangle + |0001111\rangle + |0111100\rangle + \right.$$
$$\left. + |1010101\rangle + |1100110\rangle + |1011010\rangle + |1101001\rangle\right).$$

A caracterização do código $\mathcal{C}_{simplex}$ associado a este estado garante a proteção quanto a erros atuando nas mesmas posições em todos os kets do estado, o que corresponde ao caso de alguma transformação modificar um subsistema do estado. Como a distância do código é 4, pelo Teorema 10, temos que a capacidade de correção deste código consiste de $t = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$, exatamente o que nos explicita o arranjo-padrão. Com base na definição das colunas desta tabela, como as esferas de Hamming determinam a partição do estado, podemos concluir que se um erro corromper a informação codificada como $\mathbf{x}_i$ resultando em qualquer n-upla da coluna associada a tal palavra, então o receptor ainda vai reconhecê-la como a sequência original.

A distância d do código $\mathcal{C}_{simplex}$ pode ser comparada à distância ótima d_{MDS}, calculada a partir do limitante de Singleton, mencionado em (7.4). Tal limitante estabelece que $d_{MDS} = 7 - 3 + 1 = 5$, enquanto que $d = 4$. Com isso, podemos concluir que o código simplex $\mathcal{C}_{simplex}$ está apenas uma unidade, em termos da distância, abaixo do código ótimo, o que, sem dúvida, faz de $\mathcal{C}_{simplex}$ um código bom, o que é sempre verificado para códigos simplex n-dimensionais, para $n = 2^m - 1$, $m \geq 2$.

Com relação ao código de repetição com parâmetros $(n, M, d) = (7, 2, 7)$, temos que o código simplex $\mathcal{C}_{simplex}$ tem capacidade de correção três vezes menor, uma vez que a capacidade do primeiro é $t = \left\lfloor \frac{7-1}{2} \right\rfloor = 3$. No entanto, observe que o código $\mathcal{C}_{simplex}$ pode transmitir $log_2\ 8 = 3$ bits de informação, enquanto o código de repetição transmite apenas $log_2\ 2 = 1$ bit.

Com base neste estudo é possível determinar quais são as classes de estados de máximo emaranhamento global que devem ser utilizadas para execuções mais eficientes de tarefas de processamento da informação.

Em resumo, se a tarefa for executada em um meio suscetível à ação de erros, mas permitir que seja transmitida uma unidade de informação de cada vez, os estados adequados consistem dos *GHZ* generalizados, pois tais estados são obtidos a partir de códigos *MDS* com $d > 2$. Se o aumento dos símbolos de informação a serem enviados de cada vez pode tornar o processo mais eficiente, ainda que esteja sujeito a uma menor proteção contra erros, então os estados que devem ser utilizados são obtidos a partir de códigos *simplex* n-dimensionais ou códigos cujas matrizes geradoras são justaposição das matrizes geradoras dos primeiros. Por fim, se o meio onde a tarefa é executada consistir em um sistema isolado, então os estados do tipo *HGHZ* generalizados podem ser utilizados.

Desta forma, concluímos este capítulo salientando a verificação apresentada de que existe uma relação entre o conjunto de seqüências binárias que constituem os *kets* de um estado

quântico arbitrário de máximo emaranhamento global e o conjunto de palavras-código associado a um código binário e linear.

Utilizando conceitos de teoria da codificação foi possível identificar, dentre todos os estados de máximo emaranhamento global que podem ser obtidos de códigos lineares, quais apresentam maior proteção à informação (armazenada ou transmitida) contra erros que possam ocorrer durante a execução de uma tarefa de processamento da informação. Neste contexto, os códigos *simplex* foram destacados, resultado que ainda não havia sido mencionado na literatura.

Capítulo 9

Conclusões e Perspectivas de Pesquisa

Este trabalho propõe uma descrição matemática de estados quânticos puros emaranhados. Tais contribuições consistem em um critério de separabilidade para estados puros arbitrários e na definição de uma forma sistemática de se classificar e descrever estados quânticos puros arbitrários de máximo emaranhamento global.

No Capítulo 4, propusemos um critério de separabilidade para estados puros com três *qubits* e associamos uma interpretação homológica-geométrica às equações que o constituem.

Sendo esta interpretação suficientemente simples, pudemos generalizá-la e desta generalização obtivemos um conjunto de equações. No Capítulo 5, demonstramos que este conjunto constitui um critério de separabilidade para estados puros com n *qubits*. Como uma aplicação deste resultado, apresentamos como a classificação de estados puros é obtida de acordo com o critério proposto. A partir desta análise, desenvolvemos a rotina computacional que, muito mais do que classificar estados puros arbitrários, é capaz de explicitar o comportamento de um estado com relação às equações que constituem o critério. Destas análises, direcionamos o estudo quanto ao entendimento da quantificação do emaranhamento.

No Capítulo 6, propusemos uma interpretação acerca da quantificação do emaranhamento quanto a estados puros com três *qubits*. Com base nessas considerações, esboçamos a formalização desta interpretação quanto aos estados puros com n *qubits*.

No Capítulo 8, propusemos uma nova medida de emaranhamento global, equivalente à medida de Meyer-Wallach, que pode ser aplicada para estados puros e com distribuição idêntica de amplitudes. Esta nova medida, embora seja mais restritiva quanto aos estados para os quais está definida, resultou na determinação de condições bastante claras e simples que devem ser satisfeitas para que estados de máximo emaranhamento global sejam descritos matematicamente. Tendo como base este resultado, obtivemos justificativas teóricas para a utilização dos estados denominados *EPR*'s e *GHZ* generalizados na execução de tarefas de processamento da informação. Além disso, apresentamos a classe de estados obtida a partir de códigos *simplex* n-dimensionais como uma alternativa a ser considerada nesses processos. Tais considerações são resultados da associação entre a descrição matemática de estados puros arbitrários de máximo emaranharamento global e a teoria de códigos corretores de erros clássicos. Nesse contexto,

os estados do tipo *GHZ* e os obtidos de códigos *simplex* merecem destaque pelo fato que tais estados oferecem a maior proteção ou tolerância à informação que transportam ou armazenam contra erros durante a execução das tarefas especificadas.

9.1 Perspectivas de Pesquisa

Apresentamos nesta seção algumas avaliações acerca do trabalho desenvolvido e, decorrentes dessas, algumas sugestões para pesquisas futuras.

- A restrição quanto ao estudo apenas de estados puros baseia-se no interesse inicial em estados de máximo emaranhamento, que é uma propriedade verificada apenas por estados puros, [94]. Salientamos, porém, que a apresentação de um critério de separabilidade generalizado e que possa ser implemantável para estados mistos é uma contribuição importante e que merece destaque entre as sugestões para trabalhos futuros.

- No intuito de medir o emaranhamento global em estados puros, utilizamos a medida de Meyer-Wallach, [78]. Trata-se de uma proposta bastante restrita, no sentido que pode medir o emaranhamento apenas em sistemas biparticionados. Mesmo com esta restrição, escolhemos esta medida porque o objetivo era entender como o máximo emaranhamento se estabelece com relação à descrição matemática dos estados de forma geral. No entanto, é importante analisar os resultados apresentados neste trabalho com relação a medidas de emaranhamento global mais específicas, que considerem os estados em uma análise multipartite.

- Os *qubits* são representados em função de **dois** possíveis estados de um sistema. Ou seja, os estados $|0\rangle$ e $|1\rangle$ formam a base de representação para os *qubits*. É possível considerar que um sistema assume mais de dois estados. No caso de um sistema que assuma q estados, $q \geq 3$, temos que a base de representação para um estado quântico arbitrário é dada por $|0\rangle$, $|1\rangle$, $|2\rangle$, $\cdots$, $|q-1\rangle$. Os estados quânticos obidos a partir desta descrição são denominados *qudits*. Muito pouco se conhece a respeito dos *qudits*. Por isso, propomos o estudo desses estados e do respectivo emaranhamento. A associação entre as seqüências binárias que compõem os *kets* e códigos lineares mencionada este trabalho no contexto dos *qubits* pode auxiliar neste estudo, uma vez que há bons resultados em teoria da codificação quanto a códigos definidos em alfabetos q-ários.

- Estudo da proteção desigual em relação aos *qubits* associados aos subsistemas.

- Análise de emaranhamento em superfícies com gênero $g \geq 1$, ou seja, para estados quânticos que não sejam interpretados na superfície da esfera, mas em superfícies mais gerais. Neste contexto, a questão é se o conjunto de palavras-código associadas aos códigos denominados g-tóricos definem estados de máximo emaranhamento global.

9.2 Considerações Finais

Sabemos hoje que pesquisas relacionadas à informação quântica e suas aplicações são inevitáveis, irreversíveis e, principalmente, promissoras. Neste contexto, o entendimento do emaranhamento quântico é fundamental. Assim, a proposta de obter um critério de separabilidade e uma descrição matemática completa para estados de máximo emaranhamento global nos parece bastante relevante.

Além disso, acreditamos que a simplicidade dos conceitos e idéias nos quais se baseiam os resultados obtidos seja um diferencial deste trabalho. Isso decorre da escolha pela utilização da fundamentação matemática da teoria da codificacão, já estabelecida pela literatura. A análise de tal associação, sob variadas interpretações pode resultar em muitas outras pesquisas e, conseqüentemente, muitas outras contribuições.

Esperamos que este trabalho possa de alguma forma auxiliar essas novas pesquisas e outros pesquisadores que também se motivem a entender o fenômeno da informação quântica e suas aplicações.

Referências Bibliográficas

[1] A. C. A. de Almeida, *Códigos Convolucionais Quânticos Concatenados*. Tese de Doutorado, FEEC-UNICAMP, Campinas, SP, 2004.

[2] A. Aspect, J. Dalibard and G. Roger, "Experimental test of Bell's inequalities using time-varying analyzers," *Phys. Rev. Lett.* **49**, pp.1804 (1982).

[3] A. V. Balakrishnan, "A contribution to the Sphere-packing problems in communication theory," *J. Math. Anal. Appl.* **3**, n.03 (1961).

[4] I. V. Bargatin, B. A. Grishanin and V. N. Zadkov, "Entangled quantum states of atomic systems," *Physics* **44**, pp. 517 (2001).

[5] H. Barnum, E. Knill, M. A. Nielsen and B. Schumacher, "On quantum fidelities and channels capacities," *IEEE Trans. Inf. Theory* **46**, pp. 1317 (2000).

[6] H. Barnum, M. A. Nielsen and B. Schumacher, "Information transmission through a noisy quantum channel," *Phys. Rev. A* **57**, pp. 4153 (1998).

[7] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics* **1**, pp. 195 (1964).

[8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *J. Crypt.* **5**, pp. 3 (1992).

[9] C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, "Concentrating partial entanglement by local operations," *Phys. Rev. A*, **53**, pp. 2046 (1996).

[10] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore, Índia, 1984, pp. 175.

[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wotters, "Teleporting an Unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.* **70**, pp. 1895 (1993).

[12] C. H. Bennett and D. P. DiVicenzo, "Quantum information and computation," *Nature* **404**, pp. 247 (2000).

[13] C. H. Bennett, D. P. DiVicenzo, J. A. Smolin and W. K. Wotters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A* **54**, pp. 3824 (1996).

[14] C. H. Bennett, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wotters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.* **76**, pp. 722 (1996).

[15] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin and A. V. Thapliyal, "Exact and asymptotic measures of multipartite pure state entanglement," (1999). Disponível em *www.arXiv.org/quanth-ph/9908073.*

[16] 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 (1992).

[17] I. Bengtsson and J. Brännlund, "CP^n, or, entanglement illustrated," (2001). Disponível em *www.arXiv.org/quant-ph/0108064.*

[18] D. Bouwmeester, A. K. Ekert and A. Zeilinger (ed.), *The Physics of Quantum Information.* Berlin: Springer-Verlag, 2000.

[19] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger "Experimental quantum teleportation," *Nature* **390**, pp. 575 (1997).

[20] F. G. S. L. Brandão, "Quantifying entanglement with witness operators," *Phys. Rev. A* **72**, pp. 022310 (2005).

[21] S. Bravyi, "Entanglement entropy of multipartite pure states," *Phys. Rev. A* **67**, pp. 012313 (2003).

[22] G. K. Brennen, "An observable measure of entanglement for pure states of multi-qubit systems, " *Quantum Inf. Comput.* **3**, pp. 619 (2003).

[23] D. C. Brody and L. P. Hughstone, "Geometric quantum mechanics," *J. Geom. Phys.* **38**, pp. 19 (2001).

[24] D. Bruβ, "Entanglement splitting of pure bipartite quantum states," *Phys. Rev. A* **60**, pp. 4344 (1999).

[25] D. Bruβ, "Characterizing entanglement," *J. Math. Phys.* **43**, pp. 4237 (2002).

[26] T. Brun, I. Devetak and M.-H. Hsieh, "Correcting quantum errors with entanglement," (2006). Disponível em *www.arXiv.org/quant-ph/0610092.*

[27] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.* **78**, pp. 405 (1997).

[28] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. Sloane, "Quantum error correction via codes over $GF(4)$," *IEEE Trans. Inf. Theory* **44**, pp. 1369 (1998).

[29] H. A. Carteret and A. Sudbery, "Local symmetry properties of pure 3-qubit states," (1996). Disponível em *www.arXiv.org/quant-ph/0001091.*

[30] N. J. Cerf and C. Adami, "Quantum information theory of entanglement and measurement," (1996). Disponível em *www.arXiv.org/quant-ph/9605039.*

[31] I. L. Chuang, N. Gershenfeld and M. Kubinec, "Experimental implementation of fast quantum searching," *Phys. Rev. Lett* **18**, pp. 3408 (1998).

[32] I. L. Chuang, N. Gershenfeld, M. Kubinec and D. W. Leung, "Bulk quantum computation with nuclear-magnetic-resonance: theory and experiment," *Proc. R. Soc. Lond. A* **454**, pp. 447 (1998).

[33] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, "Bulk quantum computation with nuclear-magnetic-resonance: theory and experiment," *Phys. Rev. Lett.* **23**, pp. 880 (1969).

[34] V. Coffman, J. Kundu and W. K. Wooters, "Distributed entanglement," *Phys. Rev. A* **61**, pp. 052306 (1999).

[35] T. M. Cover and J. A. Thomas, *Elements of Informantion Theory.* Wiley-Interscience, NY, USA, 1991.

[36] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proc. R. Soc. Lond. A* **400**, pp. 97 (1985).

[37] D. Deutsch and R. Jozsa "Rapid solutions of problems by quantum computation," *Proc. R. Soc. Lond. A* **439**, pp. 553 (1992).

[38] D. P. DiVincenzo, "Quantum computation," *Science* **270**, pp.255 (1995).

[39] J. Du, X. Xu, H. Li, M. Shi, X. Zhou and R. Han, "Nash equilibirum in the quantum bottle of sexes game," (2000). Disponvível em *www.arXiv.org/quant-ph/0010050.*

[40] W. Dür, G. Vidal and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Phys. Rev. A* **62**, pp. 062314 (2000).

[41] J. Eisert, M. Wilkens and M. Lewenstein, "Quantum games and quantum strategies," *Phys. Rev. Lett.* **83**, pp. 3077 (1999).

[42] A. Einstein, B. Podolsky and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev. Lett.* **47**, pp.777 (1935).

[43] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, pp. 661 (1991).

[44] A. Ekert and P. L. Knight,"Entangled quantum systems and the Schmidt decomposition," *Am. J. Phys.* **63**, pp. 415 (1995).

[45] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.* **21**, pp.467 (1982).

[46] W. C. Gazzoni, C. Lavor e R. Palazzo Jr., "Uma proposta de critério de separabilidade para estados quânticos com 3 q-bits," *Anais do Primeiro Workshop e Escola de Computação e Informação Quântica (WECIQ), UcPel-Pelotas, RS*, 2006, pp.275.

[47] W. C. Gazzoni e R. Palazzo Jr., "Códigos *simplex* descrevem estados quânticos com máximo emaranhamento global," *Anais do XXVI Simpósio Brasileiro de Telecomunicações (SBrT'08), Rio Othon Palace-Rio de Janeiro, RJ*, 2008 (aceito para publicação).

[48] W. C. Gazzoni, R. Palazzo Jr. e C. Lavor, "Identificação de estados tripartite de q-bits puros com máximo valor de emaranhamento a partir de uma interpretação geométrica," *Anais do Segundo Workshop e Escola de Computação e Informação Quântica (WECIQ), Fiep-Campina Grande, PB*, 2007, pp. 70.

[49] W. C. Gazzoni, R. Palazzo Jr., C. Lavor e G. G. La Guardia, "Uma proposta de critério de completa separabilidade para estados quânticos puros com N q-bits," *Anais do Segundo Workshop e Escola de Computação e Informação Quântica (WECIQ), Fiep-Campina Grande, PB*, 2007, pp. 168.

[50] P. J. Giblin, *Graphs, Surfaces and Homology: An Introduction to Algebraic Topology.* Chapman and Hall, London, 1981.

[51] D. Gottesman, *Stabilizer Code and Quantum Error Correction*. PhD Thesis - California Institute of Technology, Pasadena, CA, 1997.

[52] J. Grabowski, M. Kus and G. Marmo, "Symmetries, group actions and entanglement," *Open Syst. Inf. Dyn.* **13**, pp.343 (2006).

[53] D. M. Greenberger, M. A. Horne, A. Shimony and A. Zeilinger, "Bell's theorem without inequalities," *Am. J. Phys.* **58**, pp.1131 (1990).

[54] L. K. Grover, "A fast quantum mechanical algorithm for database search," *28th Annual ACM Symposium on the Theory of Computing*, pp. 212, 1996. Disponível em *www.arXiv.org/quant-ph/9605043.*

[55] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.* **79**, pp. 325 (1997). Disponível em *www.arXiv.org/quant-ph/9706033.*

[56] P. Hall, and G. Higman, "On the lenght of p-soluble groups and reduction theorems for Burnide's problem," *Proc. London Math. Soc.* **3** (1956).

[57] J. Harris, *Algebraic Geometry - A First Course*. Springer-Verlag, New York, 1992.

[58] A. W. Harrow and M. A. Nielsen, "Robustness of quantum gates in the presence of noise," *Phys. Rev. A* **68**, pp. 012308 (2003).

[59] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland and W. K. Wootters, "Classical information capacity of a quantum channel," *Phys. Rev. A* **54**, pp. 1869 (1996).

[60] F. Hiai and D. Petz, "The proper formula for relative entropy and its assymptotics in quantum probability," *Comm. Math. Phys.* **143**, pp. 99 (1991).

[61] S. Hill and W. K. Wootters, "Entanglement of a pair of quantum bits," *Phys. Rev. Lett.* **78**, pp. 5022 (1997).

[62] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory* **44**, pp.269 (1998).

[63] P. Horodecki, "Separability criterion and inseparable mixed states with positive partial tranposition," *Phys. Lett. A* **232**, pp. 333 (1997).

[64] M. Horodecki, P. Horodecki and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," *Phys. Lett. A* **223**, pp. 1 (1996).

[65] M. Horodecki, P. Horodecki and R. Horodecki, "Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?," *Phys. Rev. Lett.* **80**, pp. 5239 (1998).

[66] M. Horodecki, P. Horodecki and R. Horodecki, "Limits for enatanglement measures," *Phys. Rev. Lett.* **84**, pp. 2014 (2000).

[67] L. H. Kauffman and S. J. Lomonaco Jr., "Entanglement criteria - quantum and topological," (2003). Disponível em *www.arXiv.org/quant-ph/0304091.*

[68] E. Knill and R. Laflamme, "A theory of quantum error-correcting codes," *Phys. Rev. A* **55**, pp. 900 (1997).

[69] M. Koashi, V. Buzeck and N. Imoto, "Entangled webs: Tight bound for symmetric sharing of entanglement," *Phys. Rev. A* **62**, pp. 050302 (2000).

[70] M. Koashi e A. Winter, "Monogamy of entanglement and other correlations," *Phys. Rev. A* **69**, pp. 022309 (2004).

[71] R. Landauer, "Irreversibility and heat generation in the computing process," *IBM J. Res. Dev.* **5**, pp. 183 (1961).

[72] S. Lin and D. J. Costello Jr. *Error Control Coding: Fundamentals and Applications*. Second Edition, Pearson Prentice Hall, NJ, 2004.

[73] N. Linden and S. Popescu, "On multi-particle entanglement," (1997). Disponível em *www.arXiv.org/quant-ph/9711016.*

[74] N. Linden, S. Popescu and W. K. Wootters, "Almost energy pure state of three qubits is completely determined by its two-particle reduced density matrices," *Phys. Rev. Lett.* **89**, pp. 207901 (2002).

[75] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, Netherlands: North-Holland Publishing Company, 1977.

[76] K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, "Dense coding in experimental quantum communication," *Phys. Rev. Lett.* **76**, pp. 4656 (1996).

[77] D. A. Meyer, "Quantum strategies," *Phys. Rev. Lett.* **82**, pp. 1052 (1999); **84**, pp. 789 (2000).

[78] D. A. Meyer and N. R. Wallach "Global entaglement in multiparticle systems," *J. Math. Phys.* **43**, n.09, pp. 4273 (2002).

[79] R. Mosseri and R. Dandoloff, "Geometry of entangled states, Bloch spheres and Hopf fibrations," (2001). Disponível em *www.arXiv.org/quant-ph/0108137.*

[80] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*. Princeton: United Press Princeton, 1955.

[81] M. A. Nilsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, MA: Cambridge University Press, 2000.

[82] M. A. Nielsen and J. Kempe, "Separable states are more disordered globally than locally," *Phys. Rev. Lett.* **86**, pp. 5184 (2001).

[83] T. R. de Oliveira, G. Rigolin and M. C. de Oliveira, "Genuine multipartite entanglement in quantum phase transition, " *Phys. Rev. A* **73**, pp. 010305 (2006).

[84] T. R. de Oliveira, G. Rigolin, M. C. de Oliveira and E. Miranda, "Multipartite entanglement signature of quantum phase transition," *Phys. Rev. Lett.* **97**, pp. 170401 (2006).

[85] T. J. Osborne and M. A. Nielsen, "Entanglement, quantum phase transitions, and density matrix renormalization," (2002). Disponível em *www.arXiv.org/quant-ph/0109024.*

[86] T. J. Osborne and M. A. Nielsen, "Entanglement in a simple quantum phase transition," *Phys. Rev. A* **66**, pp. 032110 (2002).

[87] T. J. Osborne and F. Verstraete, "General monogamy inequality for bipartite qubit entanglement," *Phys. Rev. Lett.* **96**, pp. 220503 (2006).

[88] A. Peres, *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, Dordrecht, 1995.

[89] A. Peres, "Separability criterion for density matrices," *Phys. Rev. Lett.* **76**, pp. 1413 (1996).

[90] D. T. Pope and G. J. Milburn, "Multipartite entanglement and qantum state exchange," *Phys. Rev. A* **67**, pp. 052107 (2003).

[91] G. Ribordy, J. Brendel, J. D. Gautier, N. Gisin and H. Zbinden, "Long distance entanglement based quantum key distribution," (2000). Disponível em *www.arXiv.org/quant-ph/0008039*.

[92] G. Rigolin, "Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement," *Phys. Rev. A* **71**, pp. 032303 (2005).

[93] G. Rigolin, *Estados Quânticos Emaranhados*. Tese de Doutorado, IFGW-UNICAMP, Campinas, SP, 2005.

[94] D. C. Santos, *Em Busca de um Entendimento Completo acerca do Emaranhamento*. Dissertação de Mestrado, IF-UFMG, Belo Horizonte, 2006.

[95] A. J. Scott, "Multipartite entanglement, quantum error-correcting codes, and entangling power of quantum evolution," *Phys. Rev. A* **69**, pp. 052330 (2004).

[96] E. Schrödinger, "Discussion o probability relations between separated systems," *Proc. Camb. Phil. Soc.* **31**, pp.555 (1935).

[97] B. Schumacher and M. A. Nielsen, "Quantum data processing and error-correction," *Phys. Rev. A* **54**, pp. 2629 (1996).

[98] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.* **27**, pp. 379 (1948).

[99] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings of the 35th Annual Symposium on Fundamentals of Computer Science*, 1997, pp. 124.

[100] T. Siegfried, *O Bit e o Pêndulo. A Nova Física da Informação*. Campus, Rio de Janeiro, 2000.

[101] R. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," *SIAM J. Comp.* **6**, pp. 84 (1976).

[102] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.* **77**, pp. 793 (1996).

[103] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. R. Soc. London A* **452**, pp. 2551 (1996).

[104] A. Sudbery, "On local invariants of pure three-qubit states," (2000). Disponível em *www.arXiv.org/quanth-ph/0001116*.

[105] A. V. Thapliyal, "On multipartite pure state entanglement," *Phys. Rev. A.* **59**, pp. 3336 (1999).

[106] B. M. Terhal, "Is entanglement monogamous?," (2003). Disponível em *www.arXiv.org/quant-ph/0307120.*

[107] M. O. Terra Cunha, *Emaranhamento: Caracterização, Manipulação e Conseqüências.* Tese de Doutorado, IF-UFMG, Belo Horizonte, MG, 2005.

[108] V. Vedral, "Quantum information theory from the relative entropy," *Rev. Mod. Phys.* **74**, pp. 197 (2002).

[109] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures," *Phys. Rev. A* **57**, pp. 1619 (1998).

[110] V. Vedral, M. B. Plenio, M. A. Rippin and P. L. Knight, "Quantifying entanglement," *Phys. Rev. Lett.* **78**, pp. 2275 (1997).

[111] F. Verstraete, K. Audenaert, J. Dehaene and B. De Moor, "A comparison between entanglement measures negativity and concurrence," *J. Phys. A: Math. Gen.* **34**, pp. 10327 (2001).

[112] F. Verstraete, J. Dehaene, B. De Moor and H. Verschelde, "Four qubits can be entangled in nine different ways," *Phys. Rev. A* **65**, pp. 052112 (2002).

[113] G. Vidal and R. F. Werner, "Computable measure of entanglement," *Phys. Rev. A* **65**, pp. 032314 (2002).

[114] T. C. Wei and P. M. Goldbart, "Geometric measure of entanglement and applications to bipartite and multipartite quantum states," *Phys. Rev. A* **68**, pp. 042307 (2003).

[115] T.-C. Wei, M. Ericsson, P. M. Golbart and W. J. Munro, "Connections between relative entropy of entanglement and geometric measure of entanglement," *Quant. Inf. Comp.* **4**, pp. 252 (2004).

[116] R. F. Werner, "Quantum states with EPR correlations admitting a hidden variable model," *Phys. Rev. A* **40**, pp.4277 (1989).

[117] R. F. Werner and M. M. Wolf, "Bell inequalities and entanglement," *Quant. Inf. Comp.* **1**, pp.1 (2001).

[118] R. F. Werner, "Quantum information - an invitation," (2001). Disponível em *www.arXiv.org/quant-ph/0101061.*

[119] H. Weyl, *The Theory of Groups and Quantum Mechanics*. Dover Publisher, Nova York, 1950.

[120] A. Wong and N. Christensen, "Potencial multiparticle entanglement measure," *Phys. Rev. A* **63**, pp. 044301 (2001).

[121] W. K. Wotters and W. H. Zurek, "A single quantum state cannot be cloned," *Nature* **299**, pp. 802 (1982).

[122] W. K. Wootters, "Quantum entanglement as a quantifiable resource," *Phil. Trans. R. Soc. London A* **356**, pp. 1717 (1998).

[123] W. K. Wootters, "Entanglement of formation of an arbitrary state of two qubits," *Phys. Rev. Lett.* **80**, pp. 2245 (1998).

[124] C.-S. Yu and H.-S. Song, "Multiparticle entanglement measure," *Phys. Rev. A* **71**, pp. 042331 (2005).

[125] C.-S. Yu and H.-S. Song, "Global entanglement of multipartite quantum states," *Phys. Rev. A* **73**, pp. 022325 (2005).

[126] K. Zyczkowski, P. Horodecki, A. Sanpera and M. Lewenstein, "Volume of the set of separable states," *Phys. Rev. A* **58**, pp. 883 (1998).