UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

FERNANDO VASCONCELOS MENDES

TELEPORTAÇÃO DE PORTAS QUÂNTICAS, ENTRELAÇADORES UNIVERSAIS E CONEXÕES COM A TEORIA DOS NÚMEROS

Fortaleza, 2015

FERNANDO VASCONCELOS MENDES

TELEPORTAÇÃO DE PORTAS QUÂNTICAS, ENTRELAÇADORES UNIVERSAIS E CONEXÕES COM A TEORIA DOS NÚMEROS

Tese apresentada ao Curso de Pós-Graduação em Engenharia de Teleinformática do Departamento de Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos para obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado. Linha de pesquisa: Sistemas e Dispositivos Quânticos.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA
2015

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca de Pós-Graduação em Engenharia - BPGE

M491t Mendes, Fernando Vasconcelos.
Teleportação de portas quânticas, entrelaçadores universais e conexões com a teoria dos números / Fernando Vasconcelos Mendes. – 2015.
238 f. : il. color. , enc. ; 30 cm.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2015.
Área de concentração: Eletromagnetismo Aplicado.
Orientação: Prof. Dr. Rubens Viana Ramos.

1. Teleinformática. 2. Teoria dos números. 3. Sequências. I. Título.

CDD 621.38

FERNANDO VASCONCELOS MENDES

TELEPORTAÇÃO DE PORTAS QUÂNTICAS, ENTRELAÇADORES UNIVERSAIS E CONEXÕES COM A TEORIA DE NÚMEROS

Tese submetida à Coordenação do Curso de Pós-Graduação em Engenharia de Teleinformática, da Universidade Federal do Ceará, como requisito parcial para a obtenção do grau de Doutor em Engenharia de Teleinformática, área de concentração Eletromagnetismo Aplicado.

Aprovada em 19/02/2015.

BANCA EXAMINADORA

Prof. Dr. Rubens Viana Ramos (Orientador)
Universidade Federal do Ceará - UFC

Prof. Dr. João Batista Rosa Silva
Universidade Federal do Ceará - UFC

Prof. Dr. José Cláudio do Nascimento (UFC)
Universidade Federal do Ceará - UFC

Prof. Dr. Renato Portugal
Laboratório Nacional de Computação Científica - LNCC

Prof. Dr. Carlile Campos Lavor
Universidade de Campinas - UNICAMP

À minha mãe, ao meu pai, aos meus irmãos e, especialmente, ao meu filho Fernando e à minha esposa Ana Carolina. Amo todos vocês!

Agradecimentos

Para todos aqueles que de alguma forma contribuíram para este trabalho, deixo meus mais sinceros agradecimentos. Dentre estes, especialmente agradeço:

Aos professores e funcionários do Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, pelo dedicado e louvável trabalho em prol da pesquisa acadêmica.

Aos amigos do Grupo de Informação Quântica (GIQ) pela serena acolhida e pelas muitas frutíferas discussões.

Ao professor Dr. Rubens Viana Ramos pela crença de que poderíamos desenvolver um bom trabalho, pelas sempre promissoras direções apontadas e pela segura orientação desta tese. Sou-lhe muito grato pelo apoio.

À minha esposa Ana Carolina e ao meu filho Fernando, pela compreensão e tolerância da minha presença ausente durante este período.

À insaciável comunidade acadêmica, em especial àqueles que lidam com a teoria da informação quântica.

"Não podemos permitir que a lógica seja nossa deusa: ela tem músculos poderosos, mas falta-lhe personalidade. A mente intuitiva é um presente sagrado, e a mente racional é uma serva fiel; infelizmente nós criamos uma sociedade que honra a serva fiel, e esquecemos o presente sagrado."

...

"Não é que eu seja mais inteligente ou esperto que os outros, minha qualidade é não abandonar rapidamente um problema. Quando examino minha maneira de pensar, chego à conclusão que o dom da imaginação sempre teve muito mais importância para mim que a capacidade de acumular informações; se eu não fosse físico, seria músico, porque penso como um compositor, olho minha vida como se fosse música. E no que diz respeito à minha vida pessoal, acho o vício silencioso muito mais interessante que a virtude ostensiva."

— Albert Einstein

Resumo

A presente tese está dividida em três partes: 1) Teleportação de portas quânticas; 2) Busca numérica por entrelaçadores universais; 3) Conexões entre a informação quântica e a teoria dos números. No que diz a teleportação de portas quânticas, um critério de separabilidade para matrizes normais é usada para encontrar as condições analíticas da preservação da separabilidade sob conjugação. Tais condições analíticas permitiram encontrar a forma geral de um elemento do grupo de Clifford em $\mathbb{C}^4$, assim como também entender o papel da base de medição no protocolo de teleportação de portas quânticas. Considerando a busca por entrelaçadores universais, o mesmo critério de separabilidade de matrizes normais foi utilizado como função de aptidão em uma heurística computacional aplicada para encontrar bons candidatos a entrelaçadores universais nos espaços de Hilbert de dimensões $\mathbb{C}^3 \otimes \mathbb{C}^4$ e $\mathbb{C}^4 \otimes \mathbb{C}^4$. Por fim, sobre as conexões da informação quântica com a teoria dos números, é apresentado um estudo da preparação e entrelaçamento de vários estados quânticos de múltiplos qubits baseados em sequências de números inteiros. Apresenta-se ainda o circuito quântico Riemanniano, um circuito quântico cujos autovalores são relacionados aos zeros da função Zeta de Riemann. A existência deste circuito prova que é sempre possível construir um sistema físico relacionado a uma quantidade finita de zeros.

Palavras-chave: Informação quântica. Teleportação de portas quânticas. Separabilidade do produto tensorial. Grupo de Clifford. Entrelaçadores universais. Função Zeta de Riemann.

Abstract

The present thesis can be divided in three parts: 1) Quantum gate teleportation; 2) Numerical search of universal entanglers; 3) Connections between quantum information and number theory. Regarding the quantum gate teleportation, a separability criterion of normal matrices is used to find the analytical conditions of the preservation of separability under conjugation. That analytical condition allowed to find the general formula of an element of $\mathbb{C}^4$ Clifford group, as well to understand the role of the basis of measurement in the quantum gate teleportation protocol. Considering the searching for universal entanglers, the same separability criterion of normal matrices was used as fitness function in a computational heuristics, in prder to find good candidates for universal entanglers in $\mathbb{C}^3 \otimes \mathbb{C}^4$ and $\mathbb{C}^4 \otimes \mathbb{C}^4$ Hilbert spaces. At last, in the connection of quantum information with the number theory, it is presented the study of the preparation and entanglement of several multi-qubit quantum states based in integer sequences, and the Riemannian quantum circuit, a quantum circuit whose eigenvalues are related to the zeros of the Riemann zeta function. The existence of such circuit proves that is always possible to construct a physical system related to a finite amount of zeros.

Keywords: Quantum information. Quantum gate teleportation. Separability of tensorial product. Clifford group. Universal entanglers. Riemann zeta function.

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

No século XX a humanidade experimentou seu maior ritmo de evolução científica, grandes avanços foram realizados em campos como a matemática, física, química, engenharia e medicina. Apenas para citar um exemplo, tem-se o Projeto Genoma Humano [3] iniciado em 1990 por iniciativa do Departamento de Energia dos Estados Unidos [4]. Com orçamento inicial de 50 bilhões de dólares e duração prevista de 15 anos, seu objetivo foi realizar um mapeamento genético do ser humano. Além disso, estava previsto a construção de um banco de dados estruturado para tais informações, a busca por ferramentas eficientes para a análise desses dados e, por fim, a disponibilização desses dados para potencializar novas pesquisas biológicas. Este, assim como muitos outros grandes projetos científicos desenvolvidos em nossa história recente, possui uma importante característica comum: o papel fundamental do poder computacional na catalisação das descobertas científicas. Essa é certamente uma das motivações da busca pela construção de um computador quântico.

A jornada pela obtenção de um computador quântico começou com Paul Benioff [5], que foi quem primeiro pensou na possibilidade de implementar máquinas de Turing baseadas na mecânica quântica, teve seu passo seguinte dado por Richard Feynman [6], que fez ponderações importantes sobre a natureza, indagando-se sobre a possibilidade de realizar simulações perfeitas das leis naturais usando computadores. Um pouco mais adiante, em 1985 [7], foi a vez de David Deutsch introduzir a ideia de que a mecânica quântica poderia ser utilizada não apenas para simular a natureza, mas também para realizar cálculos formais. É creditada a ele a atual ideia do que é um computador quântico, o modelo de circuitos quânticos e o enunciado do primeiro problema que um computador quântico resolveria de maneira mais eficiente que sua contrapartida clássica.

Embora a ideia de manipular a informação através de fenômenos quânticos fosse muito interessante seria necessário, como é de praxe na tecnologia, a formalização de um importante problema prático para o qual um computador quântico pudesse apresentar melhores resultados que os computadores clássicos. Nesse sentido, largos e definitivos passos foram dados

por Peter Shor e Lov Grover ao apresentarem, respectivamente, algoritmos para a fatoração [8] e busca em uma base de dados não estruturada [9]. Desde as descobertas de Shor e Gover uma grande quantidade de pesquisa tem sido devotada ao estudo da manipulação da informação através de fenômenos da mecânica quântica e muito progresso tem sido obtido.

A computação quântica surge como uma grande promessa para elevar o poder de processamento computacional a um novo patamar, onde os atuais computadores clássicos estão fisicamente impedidos de alcançar [10], permitindo-a executar eficientemente tarefas consideradas classicamente intratáveis [11], tais como a fatoração em números primos. Tal poder advém, basicamente, da exploração de fenômenos tais como superposição, interferência e entrelaçamento [12].

Por fim, faz-se mandatório ressaltar, Deutsch é muito enfático ao afirmar em [13] que a computação quântica não é apenas uma nova tecnologia para implementação da máquina de Turing tradicional. Conceitualmente um computador quântico é uma máquina capaz de efetuar tipos de computação completamente novos que são impossíveis, mesmo em princípio, para um computador clássico, como pode ser exemplificado através do algoritmo de Deutsch-Jozsa [10]. Portanto, a computação quântica é um meio inconfundivelmente novo de utilizar a natureza. Essencialmente disso decorre a necessidade do desenvolvimento de uma extensa e nova gama de ferramentas, protocolos e algoritmos que fundamentem esse corpo de conhecimento. Essa tese é uma pequena parte deste esforço global.

1.1 Teleportabilidade

Desde que foi proposta em [14] a teleportação tem sido alvo de intensa pesquisa, em parte por que ela talvez seja uma das mais intrigantes aplicações das correlações não clássicas apontadas por Einstein em seu famoso artigo [15] no qual contesta a completude da mecânica quântica no papel de descrever a realidade física da natureza.

Em linhas gerais a teleportação quântica é o processo através do qual se pode realizar a transferência de um estado quântico arbitrário de uma parte a outra sem que haja um canal quântico físico entre elas. Além da proposta original, muitos outros trabalhos buscaram fornecer explicações adicionais sobre o fenômeno, tais como [16] e [17].

Por mais interessante que algo pareça ser, na tecnologia se sabe que sua relevância reside essencialmente na sua aplicabilidade. Neste quesito a teleportação não deixa a desejar, justificando o motivo pelo qual ela assume um papel de destaque na teoria da informação quântica. Dentre essas aplicações destacam-se as seguintes áreas: criptografia, comunicação e construção de portas quânticas.

O presente trabalho é um passo adiante na generalização construída em [18] dos resultados apresentados por Gottesman e Chuang [1]. Aborda a teleportação de portas quânticas por várias perspectivas de modo a permitir um amplo entendimento sobre a questão. São estabelecidos critérios necessários e suficientes para definir a teleportabilidade de portas

quânticas, ou seja, a probabilidade de sucesso da teleportação de uma porta quântica de acordo com a base de medição e o estado entrelaçado recurso utilizados.

1.2 Entrelaçadores universais

Talvez não seja exagero afirmar que o entrelaçamento é o fenômeno mais estudado na teoria da informação quântica, nem tão pouco que ele é um dos mais contra-intuitivos fenômenos físicos conhecidos. Seja como for, fato é que o entrelaçamento quântico desempenha um papel central na teoria da informação quântica, considerado um recurso físico fundamental para muitas tarefas interessantes, tais como a teleportação [14] e alguns protocolos de criptografia [19].

Deste modo, uma relevante atenção tem sido dedicada ao estudo dos entrelaçadores [20–23], buscando entender suas propriedades, construção e aplicações. Uma classe particularmente interessante de entrelaçadores são os chamados entrelaçadores universais [24], portas quânticas capazes de transformar qualquer estado desentrelaçado (pertencentes a um espaço de Hilbert apropriado) em um estado entrelaçado. Neste trabalho são utilizadas algumas relações que verificam a separabilidade de estados quânticos para, com o apoio de heurísticas computacionais, buscar bons candidatos a entrelaçadores universais.

1.3 Informação quântica e teoria dos números

Há algum tempo surgiram trabalhos [25–27] estabelecendo importantes conexões entre a teoria da informação quântica e a teoria dos números. Mais recentemente, novos trabalhos [28–30] apontam fortes evidências de que a teoria da informação quântica pode ser um ambiente fértil para desenvolver e testar ideias relacionadas a teorias dos números. Estes trabalhos descrevem a manipulação de problemas importantes, tais como a Hipótese de Riemann e a Conjectura de Goldbach.

Neste trabalho são estudadas as propriedades de estados quânticos baseados em sequências de números inteiros, em especial o entrelaçamento e a preparação daqueles usando o algoritmo de Grover. Também, é mostrado como construir um circuito quântico cuja matriz unitária equivalente tem seus autovalores relacionados aos zeros da função zeta de Riemann. A quantidade de zeros considerados é igual à dimensão da matriz unitária correspondente ao circuito. De certa forma, tal circuito pode ser considerado um passo na realização da sugestão de Hilbert-Póyla em um espaço de dimensão finita.

1.4 Esta tese

1.4.1 Contribuições

As contribuições principais desta tese estão relacionadas à noção de separabilidade, à teleportação de portas quânticas e à algumas conexões com a teoria dos números. A lista a seguir aponta as contribuições alcançadas e algumas observações decorrentes dos objetivos centrais.

- ◇ Separabilidade
  - i. Proposição do teorema acerca da preservação da separabilidade sob conjugação (ver página 49).
  - ii. Proposição do teorema que define a forma geral de um elemento do grupo de Clifford (ver página 51).
  - iii. Apresentação da forma geral, em notação exponencial, de um elemento separável do grupo $U(4)$ (ver página 37).
  - iv. Formulação dos critérios para separabilidade de estados quânticos em partições e dimensões arbitrárias (ver página 91).
  - v. Aplicação da noção de separabilidade de estados quânticos na busca por entrelaçadores universais (ver página 95).
  - vi. Apontamento de incorretudes na literatura acerca de estados entrelaçados e entrelaçadores universais (ver páginas 92 e 94).
- ◇ Teleportabilidade
  - i. A formulação analítica que explicita o papel da base de medição na teleportação de um estado quântico arbitrário (ver página 57).
  - ii. Proposição do teorema da teleportabilidade que descreve as condições, necessárias e suficientes, sob as quais se obtém uma teleportação determinística de portas de dois qubits (ver página 66).
  - iii. A caracterização e parametrização de bases de medição úteis ao protocolo de teleportação de portas quânticas (ver página 64).
  - iv. A demonstração da teleportação de portas quânticas fora do grupo de Clifford (ver página 73).
  - v. A elucidação do papel do estado recurso no protocolo de teleportação de portas quânticas, incluindo a definição da classe de estados úteis ao processo (ver página 79).
- ◇ Teoria dos números

i. A definição do estado quântico sequência e análises acerca das propriedades de seu entrelaçamento e preparação usando o algoritmo de Grover (ver página 102).

ii. Apontadas algumas características dos estados sequências que sugerem contradições na literatura acerca da interpretação das propriedades do estado Primo (ver página 106).

iii. Proposição de novas sequências de números inteiros inspiradas em estados quânticos e entrelaçamento (ver página 118).

iv. A formulação do circuito quântico de Riemann, uma realidade física associada aos zeros da função Zeta de Riemann (ver página 132).

v. Discussão sobre o entrelaçamento do estado quântico de Riemann (ver página 129).

1.4.2 Conteúdo e estrutura

Esta tese está divida em 11 capítulos, iniciando por esta introdução. No Capítulo 2 a discussão é iniciada com uma revisão do seminal trabalho de Bennett e seus colaboradores [14] sobre a teleportação de estados quânticos arbitrários. São apresentados o circuito quântico e uma descrição analítica de sua execução. Prosseguindo, discute-se o trabalho de Gottesman-Chuang [1] no qual apresentam a teleportação como uma primitiva computacional e facilitadora da construção de portas quânticas tolerante a falhas. Ainda nesta seção são apresentados: o circuito quântico que descreve o processo, os resultados de uma simulação numérica deste circuito e também um procedimento que pode ser utilizado para a geração de estados chaves da teleportação.

O Capítulo 3, que fecha a parte de fundamentação conceitual desta tese iniciada no Capítulo 2, começa por expor uma descrição da representação de qudits arbitrários. Em seguida, é discutida a ação de portas quânticas sobre qudits, especialmente aquelas associadas ao processo de teleportação. Apresenta-se uma descrição analítica da teleportação de portas de dois qudits culminando em uma extensão do resultado para a teleportação de portas atuando sobre n qudits.

O Capítulo 4 desenvolve, com o apoio da noção de formas bilineares, uma das principais ferramentas usadas ao longo da tese, a definição das condições necessárias e suficientes para a separabilidade de uma da matriz. Apresenta ainda, como aplicações, os critérios para a preservação da separabilidade sob conjugação e a forma geral do grupo de Clifford.

O Capítulo 5 apresenta um desenvolvimento analítico da teleportação de estados quânticos através do qual é possível entender os papéis de cada elemento do protocolo e, por fim, perceber que o procedimento pode ser realizado a partir de uma base de medição arbitrária.

No Capítulo 6 tem-se o desenvolvimento da noção de teleportabilidade de portas quânticas e bases de medição através da qual se define quais os critérios uma porta quântica deve atender para ser considerada teleportável e quais critérios uma base de medição deve atender para poder ser utilizada no protocolo de teleportação de portas quânticas. Também é

discutida quando pode ser alcançada uma teleportação probabilística e a fidelidade do estado resultante em um cenário específico de ruído.

O Capítulo 7 completa o estudo acerca do protocolo de teleportação de portas quânticas abordando o problema sob a perspectiva do estado recurso usado. Define-se a classe de estados capazes de gerar uma teleportação determinística, assim como o resultado do protocolo quando usado estados fora desta classe.

No Capítulo 8 é aplicada a noção de separabilidade em matrizes densidades para encontrar critérios de separabilidade para estados puros. Posteriormente essa abordagem é aplicada na busca por portas quânticas que sejam boas candidatas a serem entrelaçadores universais, portas capazes de gerar entrelaçamento entre estados separáveis arbitrários.

O Capítulo 9 define os chamados estados quânticos sequências, estados construídos a partir de sequências de números inteiros, e analisa algumas propriedades do entrelaçamento presente em tais estados. São realizadas algumas comparações com o já conhecido estado Primo e uma discussão sobre a preparação destes estados usando o algoritmo de Grover é apresentada. Este entendimento pode ser útil ao desenvolvimento de protocolos em dimensões superiores e/ou testar ideias em teoria dos números.

O Capítulo 10 desenvolve a teoria do circuito quântico de Riemann, um circuito que representa uma realidade física associada aos zeros da função Zeta de Riemann. Ainda, é descrita uma aplicação do referido circuito e realizada uma análise do entrelaçamento presente no estado de Riemann.

Encerrando este trabalho, tem-se no Capítulo 11 a apresentação das conclusões e perspectivas de trabalhos futuros. Ainda, como complemento, esta tese traz no Apêndice A a descrição dos critérios de separabilidade de estados quânticos para vários casos particulares.

Parte I

Noções Introdutórias

Capítulo 2

Teleportação de estados e portas quânticas de dois qubits

Resumo

Neste capítulo serão revisados os conceitos fundamentais do processo de teleportação de estados quânticos arbitrários e apontado alguns dos pontos que fazem a teleportação assumir uma posição destacada na teoria da informação quântica. Esta discussão fornecerá parte da fundamentação necessária ao entendimento dos resultados apresentados nos próximos capítulos.

2.1 Introdução

Desde que foi proposta em [14], a teleportação tem sido alvo de intensa pesquisa, em parte por que ela talvez seja uma das mais intrigantes aplicações das correlações não clássicas apontadas por Einstein em seu famoso artigo [15] no qual contesta a completude da mecânica quântica no papel de descrever a realidade física da natureza.

Em linhas gerais, a teleportação quântica é o processo através do qual se pode realizar a transferência de um estado quântico arbitrário $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ de uma parte a outra sem que haja um portador do estado quântico. Além da proposta original, muitos outros trabalhos buscaram fornecer explicações adicionais sobre o fenômeno, tais como [16] e [17]. Várias realizações experimentais da teleportação já foram apresentadas à comunidade científica, incluindo o uso de fótons [31], ressonância magnética nuclear [32], e íons de cálcio presos em armadilhas [33].

Por mais interessante que algo pareça ser, na tecnologia sabe-se que sua relevância reside essencialmente na sua aplicabilidade. Neste quesito, a teleportação não deixa a desejar,

justificando o motivo pelo qual ela assume um papel de destaque na teoria da informação quântica. Dentre essa aplicações destacam-se as seguintes áreas:

- ◇ Criptografia quântica: [34–36]
- ◇ Comunicação e computação: [37–40]
- ◇ Construção de portas quânticas: [1, 41]

O restante deste capítulo está organizado da seguinte forma: A Seção 2.2 traz uma revisão do seminal trabalho de Bennett e seus colaboradores [14] sobre a teleportação de estados quânticos arbitrários. São apresentados o circuito quântico e uma descrição analítica de sua execução. Prosseguindo, a Seção 2.3 discute o trabalho de Gottesman e Chuang [1] no qual apresentam a teleportação como uma primitiva computacional e facilitadora da construção de portas quânticas tolerante a falhas. Ainda nesta seção, são apresentados o circuito quântico que descreve o processo, os resultados de uma simulação numérica deste circuito e também um procedimento que pode ser utilizado para a geração de estados chaves da teleportação. Por fim a Seção 2.4 apresenta as conclusões.

2.2 Teleportação de estados quânticos

O teleporte quântico é tradicionalmente explicado na literatura através de uma atividade a ser realizada entre duas partes cooperantes, normalmente intituladas Alice e Bob. O ponto central está na possibilidade de Alice enviar um estado quântico arbitrário, desconhecido mesmo para ela, a Bob sem que no entanto haja um portador físico entre eles. O estado recebido por Bob deve ser absolutamente idêntico ao enviado por Alice.

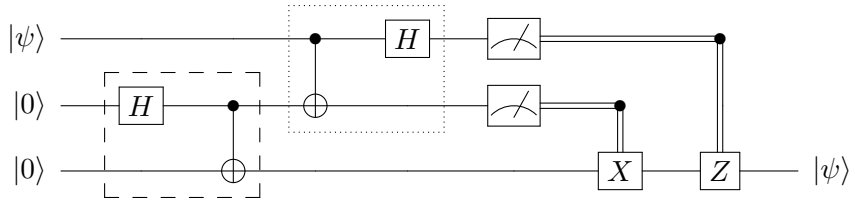
Sabendo que um estado quântico arbitrário de um sistema físico de dois níveis pode ser representado por $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, em que α e β são as amplitudes de probabilidade do estado, alguém pode pensar na possibilidade de transmissão clássica dos valores de α e β. Logo essa tentativa será abandonada por dois detalhes, primeiro a teleportação requer uma transferência perfeita, segundo os parâmetros α e β são números complexos que variam em um contínuo, apenas obedecendo a relação $|\alpha|^2 + |\beta|^2 = 1$. Desta maneira, transmitir os valores de α e β pode vir a requerer que uma quantidade infinita de informação seja enviada [42]. Para complicar ainda mais o cenário, quando não é Alice que gera $|\psi\rangle$ as leis da mecânica quântica impedem que ela consiga conhecer com exatidão os valores de α e β uma vez que ela dispõe de apenas uma cópia de $|\psi\rangle$.

Como pré-requisito fundamental para a realização da teleportação Alice e Bob devem compartilhar um par EPR e dispor de um canal clássico para troca de informação, pois, como será visto adiante, Alice necessitará enviar a Bob dois bits de informação. Na sequência será apresentada a descrição matemática do protocolo de teleportação.

2.2.1 Descrição matemática

A Figura 2.1 [42] mostra o circuito responsável por implementar o protocolo de teleportação. Os dois qubits superiores pertencem à Alice e o qubit inferior pertence a Bob. A caixa tracejada representa a geração do par EPR compartilhada por Alice e Bob, enquanto a caixa pontilhada representa a preparação para uma medição na base de Bell. Por fim o resultado da medição dos dois qubits superiores são tomados como controle das operações X e Z aplicadas ao qubit de Bob.

Figura 2.1: Circuito quântico que representa teleportação de um estado quântico arbitrário. Os dois primeiros qubits pertencem a Alice e o terceiro pertence a Bob.



O estado inicial do circuito é composto pelo estado quântico a ser teleportado $|\psi\rangle$ e o par EPR

$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.1}$$

compartilhado entre Alice e Bob, tal qual mostrado na equação Equação (2.4).

$$|\phi_0\rangle_{123} = |\psi\rangle\,|B_{00}\rangle \tag{2.2}$$

$$|\phi_0\rangle_{123} = (\alpha\,|0\rangle + \beta\,|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \tag{2.3}$$

$$|\phi_0\rangle_{123} = \frac{\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle}{\sqrt{2}}. \tag{2.4}$$

Dando sequência ao processamento do circuito tem-se o início da medição na base de Bell, representado pela porta $CNOT$ aplicada aos dois qubits de Alice, representado pelos índices 1 e 2. O alvo da $CNOT$ é a parte de Alice no par EPR enquanto o controle é o qubit a ser teleportado. O resultado dessa etapa é apresentado na Equação (2.5).

$$|\phi_1\rangle_{123} = \frac{\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle}{\sqrt{2}}. \tag{2.5}$$

A finalização do processo de medição na base de Bell é realizada pela aplicação da porta H no qubit alvo da teleportação, cujo resultado é expresso pela Equação (2.6).

$$|\phi_2\rangle_{123} = \frac{\alpha\,|000\rangle + \alpha\,|100\rangle + \alpha\,|011\rangle + \alpha\,|111\rangle + \beta\,|010\rangle - \beta\,|110\rangle + \beta\,|001\rangle - \beta\,|101\rangle}{2}. \tag{2.6}$$

Reagrupando os termos da Equação (2.6) de tal forma a colocar em evidência os possíveis valores clássicos resultantes da medição, obtém-se o formato apresentado na Equação (2.7).

$$|\phi_2\rangle_{123} = \frac{|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)}{2}. \tag{2.7}$$

Analisando os resultados até esse ponto, tem-se na Tabela 2.1[1], adaptada de [42], uma descrição do que ainda é necessário ser feito para completar o processo.

Tabela 2.1: Tabela de possíveis resultados da medição na base de Bell durante o processo de teleportação de um estado quântico arbitrário.

Medição	Estado resultante	Correção
00	$\alpha\|0\rangle + \beta\|1\rangle$	I
01	$\alpha\|1\rangle + \beta\|0\rangle$	X
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z
11	$\alpha\|1\rangle - \beta\|0\rangle$	ZX

Caso Alice resolvesse não mandar os bits clássicos oriundos da medição por ela realizada seria impossível completar a teleportação com sucesso uma vez que independentemente do estado a ser teleportado, a medição na base de Bell sempre apresentará resultados equiprováveis, portanto, mesmo que Alice dispusesse de várias cópias de $|\psi\rangle$ para repetir o processo Bob nunca conseguiria inferi-lo com certeza para o caso geral.

Essa característica garante que a teleportação não represente um paradoxo no que diz respeito à transmissão de informação acima da velocidade da luz. Como é requerida a transmissão de informação clássica, a velocidade com a qual a teleportação se realiza fica limitada à velocidade com a qual é transmitida a informação clássica participante do processo. Também se deve observar que o estado $|\psi\rangle$ originalmente utilizado por Alice é destruído[2] pelo processo de medição para posteriormente ser reconstruído por Bob usando sua partícula do par EPR, isso assegura que a teleportação não viole o teorema da não clonagem [42].

Seguindo então o protocolo, Alice envia para Bob os dois bits clássicos obtidos com a medição dos dois primeiros qubits (a forma como essa informação é representada e enviada é completamente irrelevante para o processo). Bob, de posse de tal informação, deve agora executar uma dentre quatro possíveis operações de correção, alcançando assim em to-

[1] Na notação de circuito vê-se a porta X sendo aplicada antes da porta Z, o que na representação usual da multiplicação de matrizes é descrita como ZX.

[2] Bennett e seus colaborados em seu trabalho original [14] apresentam a teleportação como um procedimento no qual um estado quântico pode ser dividido em duas partes, uma inteiramente clássica e outra inteiramente não clássica. Durante essa descrição eles utilizam os termos *disassemble* e *reconstruct*.

das as hipóteses a reconstrução do estado originalmente teleportado conforme mostrado pela Tabela 2.1.

Usando a discussão apresentada anteriormente tem-se que todas as propriedades associadas à partícula alvo da teleportação sobre o domínio de Alice são integralmente transmitidas à partícula integrante do par EPR que se encontra na posse de Bob. Nenhum mecanismo será capaz de identificar que a partícula de Bob foi alvo de uma teleportação, ela apresentará a mesma estatística de medidas e as mesmas correlações que a original, ou seja, caso a original se encontrasse entrelaçada com outros sistemas físicos a resultante da teleportação também estará de forma idêntica.

2.3 Teleportação de portas quânticas sobre qubits

No ano de 1999 Gottesman e Chuang apresentaram um importante trabalho [1] no qual apontavam duas interessantes aplicações para a teleportação: sua contribuição na construção de portas quânticas tolerantes a falhas e sua utilização como uma primitiva computacional. A implementação de computadores quânticos tem como uma das barreiras fundamentais as imperfeições das diversas propostas de realizações práticas [43], portanto técnicas e protocolos no sentido da implementação de operações tolerantes a falhas será fundamental, e muito tem sido feito nesse sentido [44–46]. Na outra direção, a de maior interesse para este trabalho, eles mostram que um computador quântico pode ser construído usando apenas operações quânticas sobre um qubit, medidas na base de Bell e estados GHZ [47]. No centro da proposição feita por eles está a medição sobre estados entrelaçados. Sabe-se que a medição pode ser considerada uma interface entre os mundos quântico e clássico, sendo considerada uma operação irreversível uma vez que destrói a informação quântica substituindo-a por informação clássica. Contudo eles argumentam que, encarando o processo sob o ponto de vista lógico, essa destruição não necessariamente ocorre em alguns casos, como principal exemplo disso citam a própria teleportação.

Nas seções seguintes será revisitado o procedimento utilizado por Gottesman e Chuang para fornecer uma espécie de generalização do processo de teleportação no qual o objetivo não é mais reconstruir no destino o estado inicial, mas sim o correspondente à ação de uma dada porta quântica atuando sobre este estado.

2.3.1 Teleportação da porta *CNOT*

O processo é exemplificado através da teleportação da porta $CNOT$, cujo circuito quântico correspondente é mostrado na Figura 2.2, sendo $|out\rangle = CNOT\,|\beta\rangle\,|\alpha\rangle$ e porta B representa uma medição na base de Bell cujo circuito pode ser visto na Figura 2.3. Uma análise cuidadosa do processo mostrará que se trata de uma idéia simples e similar à teleportação original, contudo traz consequências úteis e interessantes.

Figura 2.2: Circuito quântico para teleportar a porta $CNOT$ tal qual originalmente proposto em [1].

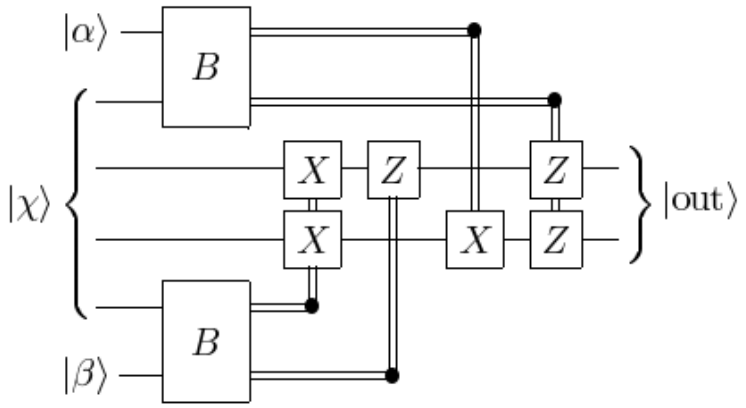
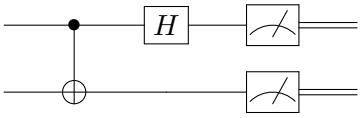


Figura 2.3: Circuito quântico que representa uma medição na base de Bell para dois qubits.



O estado $|\chi\rangle$ que aparece no circuito é considerado o recurso físico que habilita o processo de teleportação da porta $CNOT$, ele é representado pela Equação (2.8) e dois circuitos quânticos para gerá-lo são apresentados na Figura 2.4, em que $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ e $|\gamma\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$. O lado esquerdo da imagem apresenta a criação de $|\chi\rangle$ a partir de dois pares EPR, enquanto do lado direito tem-se a criação a partir de dois estados GHZ de três partículas.

$$|\chi\rangle = \frac{(|00\rangle + |11\rangle)\,|00\rangle + (|01\rangle + |10\rangle)\,|11\rangle}{2}. \tag{2.8}$$

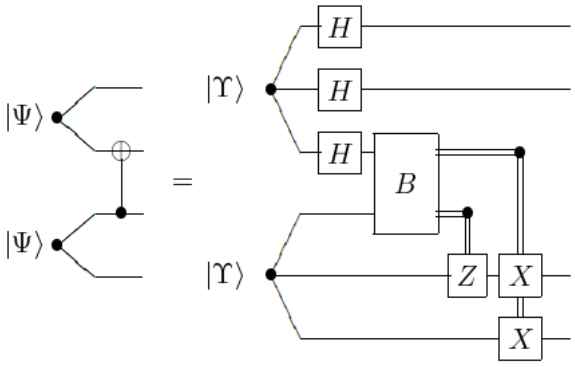
Um ponto essencial da proposta é perceber que uma conjugação por $CNOT$ preserva o grupo de Pauli, ou seja, algumas operações de Pauli sobre um qubit ocorridas antes de uma $CNOT$ será igual à outras operações de Pauli após uma $CNOT$. Ao conjunto de portas que apresentam essa propriedade dá-se o nome de grupo de Clifford [48], para qualquer uma dessas portas o procedimento aqui descrito será completado com sucesso. O grupo de Clifford C_2 operando sobre 2 qubits é dado por:

$$P_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY \pm Z, \pm iZ\}, \tag{2.9}$$

$$P_2 = P_1^{\otimes 2}, \tag{2.10}$$

$$C_2 = \left\{U \in U(4) \,|\, \sigma \in P_2 \Rightarrow U\sigma U^\dagger \in P_2\right\}. \tag{2.11}$$

Figura 2.4: Duas opções de circuitos quânticos para a criação do estado $|\chi\rangle$, Equação (2.8), tal qual originalmente proposto em [1].



Um exemplo da preservação do grupo de Pauli pela $CNOT$ é

$$CNOT(I \otimes Z)CNOT^{\dagger} = (Z \otimes Z). \tag{2.12}$$

Mesmo já mencionada a questão de que o procedimento será completado com sucesso para toda porta pertencente ao grupo de Clifford, Gottesman e Chuang indicam que a teleportação da $CNOT$ põe a teleportação como uma primitiva computacional, visto que a $CNOT$ mais portas de um qubit formam um conjunto universal [49]. A despeito de tudo já colocado até então neste capítulo a mais relevante contribuição do trabalho deles está na possibilidade de se realizar computação quântica usando apenas portas de um qubit, medidas na base de Bell e estados GHZ[3].

A fim de checar a proposta de Gottesman-Chuang foi realizada uma execução do circuito quântico apresentado na Figura 2.2. A Tabela 2.2 apresenta os resultados. Nela é possível ver o estado final do sistema associado a cada possibilidade de medição clássica e a correção associada. Para o estado geral de dois qubits $|\psi\rangle = v_0 |00\rangle + v_1 |01\rangle + v_2 |10\rangle + v_3 |11\rangle$ tem-se que $CNOT^{\perp} |\psi\rangle = v_0 |00\rangle + v_3 |01\rangle + v_2 |10\rangle + v_1 |11\rangle$[4], justo o estado final associado ao resultado 0000 da medição.

Tabela 2.2: Estado resultante da teleportação da porta $CNOT$ operando sobre um estado arbitrário de dois qubits em conjunto com a correção para cada medição clássica.

Medição	Resultado	Correção
0000	$v0 \|00\rangle + v3 \|01\rangle + v2 \|10\rangle + v1 \|11\rangle$	$(I \otimes I)$

Continua na próxima página...

[3]Uma importante questão apontada pelo trabalho é a possibilidade de realizar a $CNOT$ apenas com portas de um qubit, desde que se disponha de estados GHZ.

[4]Na notação utilizada $CNOT^{\perp}$ representa uma $CNOT$ tradicional mas agindo no primeiro qubit e sendo controlada pelo segundo.

Tabela 2.2 – continuação da página anterior.

Medição	Resultado	Correção
0001	$v0\,\|00\rangle - v3\,\|01\rangle + v2\,\|10\rangle - v1\,\|11\rangle$	$(I \otimes Z)$
0010	$v1\,\|00\rangle + v2\,\|01\rangle + v3\,\|10\rangle + v0\,\|11\rangle$	$(X \otimes X)$
0011	$-v1\,\|00\rangle + v2\,\|01\rangle - v3\,\|10\rangle + v0\,\|11\rangle$	$(I \otimes Z)(X \otimes X)$
0100	$v2\,\|00\rangle + v1\,\|01\rangle + v0\,\|10\rangle + v3\,\|11\rangle$	$(X \otimes I)$
0101	$v2\,\|00\rangle - v1\,\|01\rangle + v0\,\|10\rangle - v3\,\|11\rangle$	$(X \otimes Z)$
0110	$v3\,\|00\rangle + v0\,\|01\rangle + v1\,\|10\rangle + v2\,\|11\rangle$	$(I \otimes X)$
0111	$-v3\,\|00\rangle + v0\,\|01\rangle - v1\,\|10\rangle + v2\,\|11\rangle$	$(I \otimes ZX)$
1000	$v0\,\|00\rangle - v3\,\|01\rangle - v2\,\|10\rangle + v1\,\|11\rangle$	$(Z \otimes Z)$
1001	$v0\,\|00\rangle + v3\,\|01\rangle - v2\,\|10\rangle - v1\,\|11\rangle$	$(Z \otimes I)$
1010	$v1\,\|00\rangle - v2\,\|01\rangle - v3\,\|10\rangle + v0\,\|11\rangle$	$(Z \otimes Z)(X \otimes X)$
1011	$-v1\,\|00\rangle - v2\,\|01\rangle + v3\,\|10\rangle + v0\,\|11\rangle$	$(Z \otimes I)(X \otimes X)$
1100	$-v2\,\|00\rangle + v1\,\|01\rangle + v0\,\|10\rangle - v3\,\|11\rangle$	$(Z \otimes Z)(X \otimes I)$
1101	$-v2\,\|00\rangle - v1\,\|01\rangle + v0\,\|10\rangle + v3\,\|11\rangle$	$(ZX \otimes I)$
1110	$-v3\,\|00\rangle + v0\,\|01\rangle + v1\,\|10\rangle - v2\,\|11\rangle$	$(Z \otimes Z)(I \otimes X)$
1111	$v3\,\|00\rangle + v0\,\|01\rangle - v1\,\|10\rangle - v2\,\|11\rangle$	$(Z \otimes X)$

2.3.2 Geração do estado chave da teleportação para outras portas $\in C_2$

É possível estabelecer o procedimento básico para a geração de estados chaves que servem como recurso no processo de teleportação de outras portas quânticas $\in C_2$. Basta para tanto colocar a porta de dois qubits desejada para atuar nos qubits centrais de dois pares EPR, tal qual mostrado pela Figura 2.5. A Tabela 2.3 exibe alguns exemplos de estados chaves associados à porta cuja a ação eles são capazes de teleportar. É omitido na referida tabela o fator 1/2 na coluna que apresenta o estado chave, além disso as portas $CNOT$ e $SWAP$ serão representadas, respectivamente, pelos símbolos C_N e S_W. Ainda, $CNOT^{\perp}$ representará uma $CNOT$ controlada pelo segundo qubit.

Figura 2.5: Circuito quântico para a criação de estado chave utilizada no processo de teleportação de uma dada porta U.

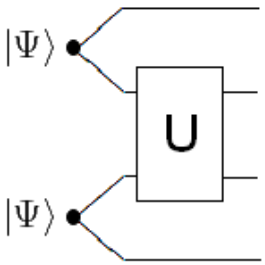


Tabela 2.3: Tabela exemplificando estados chaves de teleportação, bem como suas respectivas portas teleportadas.

Estado chave	Porta
$\|0000\rangle + \|0011\rangle + \|1101\rangle + \|1110\rangle$	C_N
$\|0000\rangle + \|0111\rangle + \|1010\rangle + \|1101\rangle$	$S_W C_N$
$\|0000\rangle + \|0111\rangle + \|1011\rangle + \|1100\rangle$	$C_N^{\perp}$
$\|0001\rangle + \|0010\rangle + \|1100\rangle + \|1111\rangle$	$(X \otimes I)C_N(X \otimes I)$
$\|0001\rangle + \|1010\rangle + \|0100\rangle + \|1111\rangle$	$S_W(I \otimes X)C_N^{\perp}(I \otimes X)$
$\|0001\rangle + \|0110\rangle + \|1010\rangle + \|1101\rangle$	$(X \otimes X)(I \otimes X)C_N^{\perp}(I \otimes X)$
$\|0001\rangle + \|0110\rangle + \|1011\rangle + \|1100\rangle$	$(X \otimes X)(I \otimes X)C_N^{\perp}(I \otimes X)$
$\|0001\rangle + \|1011\rangle + \|0110\rangle + \|1100\rangle$	$(X \otimes X)S_W(I \otimes X)C_N^{\perp}(I \otimes X)$
$\|0011\rangle + \|0100\rangle + \|1000\rangle + \|1111\rangle$	$(I \otimes X)C_N^{\perp}(I \otimes X)$
$\|0011\rangle + \|0100\rangle + \|1001\rangle + \|1110\rangle$	$(X \otimes X)S_W C_N$
$\|0011\rangle + \|0100\rangle + \|1110\rangle + \|1001\rangle$	$(X \otimes X)S_W C_N$
$\|0011\rangle + \|0110\rangle + \|1000\rangle + \|1101\rangle$	$(X \otimes X)S_W(I \otimes X)C_N^{\perp}(I \otimes X)$
$\|0011\rangle + \|1101\rangle + \|0110\rangle + \|1000\rangle$	$(X \otimes X)S_W(I \otimes X)C_N^{\perp}(I \otimes X)$
$\|0111\rangle + \|1001\rangle + \|0010\rangle + \|1100\rangle$	$(X \otimes X)S_W C_N^{\perp}$
$\|0111\rangle + \|1001\rangle + \|1010\rangle + \|0100\rangle$	$(X \otimes X)C_N$

2.4 Conclusão

Neste capítulo foi realizada uma revisão do protocolo de teleportação de estados arbitrários proposto por Bennett e seus colaboradores. Na sequência foi apresentada uma discussão sobre a proposta de Gottesman-Chuang na qual apresentam a teleportação como um facilitador na construção de portas tolerantes a falha e também como uma primitiva computacional. Foi apresentada uma execução do procedimento na qual se pode observar o estado resultante associado a cada possível valor clássico medido para o caso da teleportação da porta $CNOT$. Por fim descreveu-se a maneira de gerar estados chaves para a teleportação de portas quânticas dentro do grupo de Clifford.

Capítulo 3

Teleportação de portas quânticas atuando em n qudits

Resumo

Este capítulo apresenta uma descrição analítica que generaliza os resultados apresentados por Gottesman e Chuang para a obtenção da teleportação de portas quânticas de n qudits em dimensões arbitrárias. Com isso, fecha-se a parte de fundamentação deste trabalho.

3.1 Introdução

Conforme descrito no Capítulo 2, o trabalho proposto por Gottesman e Chuang [1] teve uma importância fundamental na teoria da informação quântica, tanto pela perspectiva de apresentar a teleportação como uma primitiva computacional quanto pela facilitação na construção de portas quânticas tolerantes a falhas. O trabalho original versa apenas sobre portas de dois qubits. A discussão a seguir faz uma generalização deste resultado para um espaço d-dimensional, ou seja operando sobre qudits de dimensão arbitrária. Após alcançado um resultado analítico descrevendo a teleportação de portas de dois qudits será feita uma consideração sobre quais portas quânticas podem ser utilizadas com sucesso no processo de teleportação. O objetivo é apresentar condições mais gerais que a proposta no trabalho original, onde a porta quântica deve pertencer ao grupo de Clifford [48].

O restante deste capítulo está organizado da seguinte forma: A discussão é iniciada na Seção 3.2 com uma revisão da representação de qudits. A Seção 3.3 discute a ação de portas quânticas sobre qudits, especialmente aquelas associadas ao processo de teleportação. A Seção 3.4 apresenta uma descrição analítica da generalização da teleportação de portas de 2

qudits. A Seção 3.5 mostra uma extensão do resultado para a teleportação de portas atuando sobre n qudits. Por fim, a Seção 3.6 apresenta as conclusões.

3.2 Representação de qudits

Como descrito anteriormente na Seção 2.2, um qubit é um estado quântico em um espaço de Hilbert de dimensão 2, portanto deve-se entendê-lo como uma combinação linear dos vetores da base canônica $B = \{|0\rangle, |1\rangle\}$ do referido espaço. Generalizando essa representação temos que um qudit é um estado quântico em um espaço de Hilbert d-dimensional. Neste caso a base[1] canônica é definida como

$$ {}_dB = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}. \tag{3.1} $$

Dessa forma, um estado quântico arbitrário em um espaço d-dimensional pode ser descrito como

$$ |{}_d\Psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \tag{3.2} $$

sendo $|\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{d-1}|^2 = 1$.

3.3 Portas quânticas sobre qudits

Uma vez descrita a representação de qudits, o próximo passo é mostrar a ação de portas quânticas sobre eles. Em essência serão estudadas apenas as portas integrantes do processo de teleportação, são elas:

- ◇ ${}_dX$, ${}_dZ$: As portas amplamente conhecidas que, aliada à porta ${}_dY$, compõem o grupo de *Pauli*[2].
- ◇ ${}_dF$: A porta que representa a transformada de *Fourier* quântica e desempenha para o caso geral o papel que a Hadamard desempenha no caso bidimensional.
- ◇ ${}_dG_{XOR}$: A porta que generaliza para o caso d-dimensional o papel da *CNOT* no caso bidimensional.

Existem algumas formas de chegar a esses resultados, como pode ser conferido em [50], mas ao longo deste trabalho, salvo quando mencionado o contrário, será utilizada a abordagem apresentada em [51].

[1] Na notação utilizada o sobrescrito a esquerda representa a dimensão de um estado ou porta quântica.
[2] Alguns autores também incluem a porta ${}_dI$.

3.3.1 A ação da porta ${}_dX$

A porta ${}_dX$ operando sobre qubits ($d = 2$) pode ser descrita como uma operação de soma módulo 2. Neste caso, pelo seu papel em inverter o bit de entrada ela é também conhecida como *bit-flip*. No entanto, para o caso d-dimensional esse papel não se mantém. A expressão

$$ {}_dX \left|k\right\rangle = \left|(k+1) \bmod d\right\rangle \tag{3.3}$$

mostra que a ação, na base computacional, é levar o estado de entrada ao estado da base imediatamente à sua direita ou retornar ao início, caso o estado de entrada seja o último da base. Esse comportamento mostra que o *bit-flip* observado na dimensão 2 é um caso específico de um comportamento mais geral denominado de *right shift bit*. Para a dimensão 4, por exemplo, a ação de ${}_4X$ nos estados da base computacional é dada por:

$$ {}_4X \left|0\right\rangle = \left|1\right\rangle , \tag{3.4}$$

$$ {}_4X \left|1\right\rangle = \left|2\right\rangle , \tag{3.5}$$

$$ {}_4X \left|2\right\rangle = \left|3\right\rangle , \tag{3.6}$$

$$ {}_4X \left|3\right\rangle = \left|0\right\rangle . \tag{3.7}$$

A representação matricial da porta ${}_dX$ é dada pela equação

$$ a_{mn} = \begin{cases} 1 & \text{se } m = (n+1) \bmod d \\ 0 & \text{caso contrário} \end{cases} . \tag{3.8}$$

Para as dimensões 2, 3 e 4 este procedimento dá origem às matrizes

$$ {}_2X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad {}_3X = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad {}_4X = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} . \tag{3.9}$$

3.3.2 A ação da porta ${}_dZ$

A ação da porta ${}_dZ$ para o caso bidimensional é também conhecida como *phase-flip* pelo seu papel em "inverter" a fase do qubit de entrada. A expressão que representa a ação da porta ${}_dZ$ em um estado da base canônica é

$$ {}_dZ \left|k\right\rangle = \left(e^{(2\pi i/d)}\right)^k \left|k\right\rangle . \tag{3.10}$$

Para o caso de $d = 4$ tem-se:

$$
\begin{aligned}
{}_4Z\,|0\rangle &= \left(e^{2\pi i/4}\right)^0 |0\rangle = |0\rangle\,, && (3.11)\\
{}_4Z\,|1\rangle &= \left(e^{2\pi i/4}\right)^1 |1\rangle = i\,|1\rangle\,, && (3.12)\\
{}_4Z\,|2\rangle &= \left(e^{2\pi i/4}\right)^2 |2\rangle = -\,|2\rangle\,, && (3.13)\\
{}_4Z\,|3\rangle &= \left(e^{2\pi i/4}\right)^3 |3\rangle = -i\,|3\rangle\,. && (3.14)
\end{aligned}
$$

A representação matricial da porta ${}_dZ$ é dada pela expressão

$$
a_{mn} = \begin{cases} e^{(2\pi i/d)^{m-1}} & \text{se } m = n \\ 0 & \text{se } m \neq n \end{cases}\,. \tag{3.15}
$$

Para as dimensões 2, 3 e 4 este procedimento origina as matrizes

$$
{}_2Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad {}_3Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & (\sqrt{3}i-1)/2 & 0 \\ 0 & 0 & -(\sqrt{3}i+1)/2 \end{bmatrix}, \quad {}_4Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{bmatrix}. \tag{3.16}
$$

3.3.3 A ação da porta Hadamard generalizada – ${}_dF$

Em $d = 2$ a porta Hadamard é um caso particular da transformada de Fourier discreta sobre um qubit. Para lidar com espaços de dimensão arbitrária ter-se-á que utilizar a versão genuína, daqui por diante denotada por ${}_dF$. A ação de ${}_dF$ na base computacional é

$$
{}_dF\,|k\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} e^{(2\pi i k l/d)}\,|l\rangle. \tag{3.17}
$$

Uma forma alternativa de expressar a Equação (3.17) e que será útil mais adiante faz uso da Equação (3.10) e é dada por

$$
{}_dF\,|k\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} ({}_dZ)^k\,|l\rangle. \tag{3.18}
$$

Para $d = 4$ tem-se:

$$
\begin{aligned}
{}_4F\,|0\rangle &= [|0\rangle + |1\rangle + |2\rangle + |3\rangle]\,/2, && (3.19)\\
{}_4F\,|1\rangle &= [|0\rangle + i\,|1\rangle - |2\rangle - i\,|3\rangle]\,/2, && (3.20)\\
{}_4F\,|2\rangle &= [|0\rangle - |1\rangle + |2\rangle - |3\rangle]\,/2, && (3.21)
\end{aligned}
$$

$$ {}_4F\,|3\rangle \;=\; [|0\rangle - i\,|1\rangle - |2\rangle + i\,|3\rangle]\,/2. \tag{3.22} $$

A representação matricial da porta ${}_dF$ é descrita pela expressão

$$ a_{mn} = e^{(2\pi i/d)^{mn}}/\sqrt{d}. \tag{3.23} $$

Ao seguir-se esse procedimento para as dimensões 2, 3 e 4 obtêm-se as matrizes

$$ {}_2F \;=\; \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad {}_3F = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & (\sqrt{3}i-1)/2 & -(\sqrt{3}i+1)/2 \\ 1 & -(\sqrt{3}i+1)/2 & (\sqrt{3}i-1)/2 \end{bmatrix}, \tag{3.24} $$

$$ {}_4F \;=\; \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}. \tag{3.25} $$

3.3.4 A ação da porta ${}_dG_{XOR}$

Por fim será descrita a porta ${}_dG_{XOR}$, cuja ação sobre qubits sabe-se ser equivalente à conhecida $CNOT$ e dada por $CNOT\,|k,l\rangle = |k,(k+l) \bmod 2\rangle$, portanto tem-se que ${}_2G_{XOR} = CNOT$. Intuitivamente, espera-se que a ação da porta ${}_dG_{XOR}$ esteja relacionada à ação da porta ${}_dX$ e, de fato, isso é observado em algumas generalizações presentes na literatura, como por exemplo a descrição apresentada em [51]. Contudo, pela constatação de maior aderência à abordagem analítica e resultados obtidos pelas simulações realizadas, optou-se nesse trabalho por utilizar a definição fornecida em [52], cuja ação é expressa pela equação

$$ {}_dG_{XOR}\,|k,l\rangle = |k,(k-l) \bmod d\rangle \equiv |k, k \ominus l\rangle\,. \tag{3.26} $$

Ao revisitar-se algumas das propriedades dessa definição tem-se[3,4]:

i. Ela é unitária, portanto reversível.

ii. Ela é Hermitiana.

iii. $k \ominus l \equiv 0\ (mod\ d)$ se, e somente se, $k = l$.

iv. Para o caso especial de qubits ela resume-se a ação padrão da $CNOT$, visto que $k \ominus l \equiv k \oplus l\ (mod\ 2)$.

[3] Em que $\ominus$ representa a subtração módulo d, portanto $a \ominus b$ equivale à $(a-b) \bmod d$.
[4] Em que $\oplus$ representa a adição módulo d, portanto $a \oplus b$ equivale à $(a+b) \bmod d$.

Além das propriedades apontadas em [52], nota-se que essa definição permite obter a porta ${}_dC_Z$[5] através de uma conhecida relação para o caso especial de qubits, mostrada na Equação (3.27)

$$ {}_2C_Z = ({}_2I \otimes {}_2H)\, {}_2CNOT\, ({}_2I \otimes {}_2H)\,. \tag{3.27} $$

A forma generalizada da Equação (3.27) é mostrada na Equação (3.28) e não pode ser obtida diretamente usando-se a definição dada em [51].

$$ {}_dC_Z = ({}_dI \otimes {}_dF)\, {}_dG_{XOR}\, ({}_dI \otimes {}_dF)\,. \tag{3.28} $$

Tem-se ainda que uma execução da teleportação de portas de dois qudits usando a definição em [51] não resulta em um estado que não requer correção para o valor clássico 0000 decorrente da medição. A ação da porta ${}_dG_{XOR}$ na base computacional para o caso $d = 4$ é dada por[6]:

$$ {}_4G_{XOR}\,|00\rangle = |00\rangle\,, \quad {}_4G_{XOR}\,|20\rangle = |22\rangle\,, \tag{3.29} $$

$$ {}_4G_{XOR}\,|01\rangle = |03\rangle\,, \quad {}_4G_{XOR}\,|21\rangle = |21\rangle\,, \tag{3.30} $$

$$ {}_4G_{XOR}\,|02\rangle = |02\rangle\,, \quad {}_4G_{XOR}\,|22\rangle = |20\rangle\,, \tag{3.31} $$

$$ {}_4G_{XOR}\,|03\rangle = |01\rangle\,, \quad {}_4G_{XOR}\,|23\rangle = |23\rangle\,, \tag{3.32} $$

$$ {}_4G_{XOR}\,|10\rangle = |11\rangle\,, \quad {}_4G_{XOR}\,|30\rangle = |33\rangle\,, \tag{3.33} $$

$$ {}_4G_{XOR}\,|11\rangle = |10\rangle\,, \quad {}_4G_{XOR}\,|31\rangle = |32\rangle\,, \tag{3.34} $$

$$ {}_4G_{XOR}\,|12\rangle = |13\rangle\,, \quad {}_4G_{XOR}\,|32\rangle = |31\rangle\,, \tag{3.35} $$

$$ {}_4G_{XOR}\,|13\rangle = |12\rangle\,, \quad {}_4G_{XOR}\,|33\rangle = |30\rangle\,. \tag{3.36} $$

A representação matricial da porta ${}_dG_{XOR}$ é obtida através da equação

$$ a_{mn} = \begin{cases} 1 & \text{se } m = [dx + (x-y) \bmod d] + 1 \;\forall\; n \in [1, d^2] \\ 0 & \text{caso contrário} \end{cases}\,, \tag{3.37} $$

em que

$$ x = (n-1) \text{ div } d; \quad y = (n-1) \bmod d. \tag{3.38} $$

[5] A porta Z controlada.

[6] Nota-se que para o caso d-dimensional perde-se a noção intuitiva de que uma porta controlada pelo qudit zero não altera o qudit alvo.

Para $d = 4$ este procedimento dá origem à matriz

$$ {}_4G_{XOR} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}. \tag{3.39} $$

3.3.5 Portas controladas

A ação de portas controladas sobre qubits é elementar. Como o controle apenas pode assumir os valores 0 e 1 tem-se que porta C_W corresponde a aplicação da porta W ao qubit alvo apenas quando o qubit de controle contém o valor 1. Para o caso de qudits a situação é menos trivial[7], a expressão que representa uma ação controlada sobre qudits é

$$ {}_dC_W \left|kl\right\rangle = \left|k\right\rangle \left({}_dW\right)^k \left|l\right\rangle . \tag{3.40} $$

Por fim, uma observação importante sobre todas as portas quânticas descritas até aqui é que com exceção da ${}_dG_{XOR}$ elas não são Hermitianas. Para o caso bidimensional sabe-se que as portas pertencentes ao grupo de Pauli – e muitas outras – são Hermitianas, portanto atendem a relação $\left({}_2U\right)^2 = {}_2I$. Contudo, para o caso d-dimensional a situação é diferente, tem-se agora uma relação mais ampla descrita pela equação

$$ \left({}_dU\right)^d = {}_dI \tag{3.41} $$

em que mesmo portas não Hermitianas podem atendê-la, tais como:

$$ \left({}_dX\right)^d = {}_dI \tag{3.42} $$

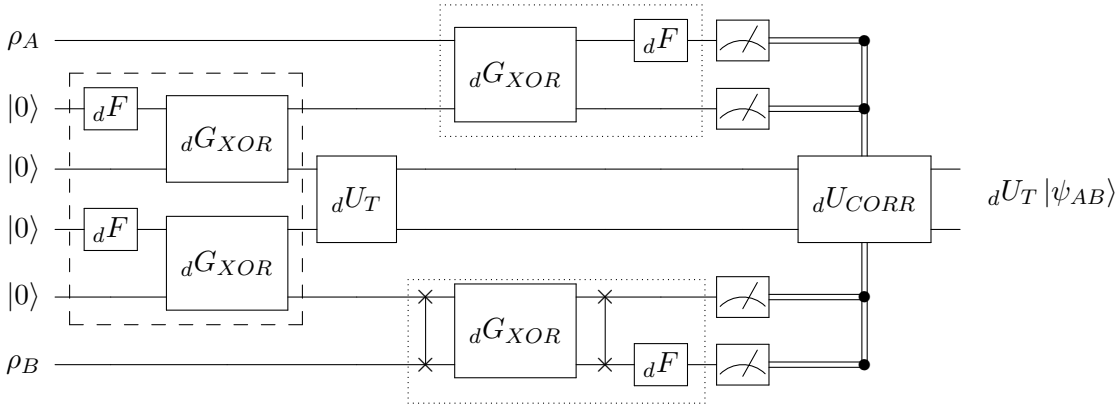
$$ \left({}_dZ\right)^d = {}_dI \tag{3.43} $$

[7] Diferente do caso particular de qubits uma operação controlada por um qudit com valor zero pode afetar o estado resultante.

3.4 Descrição analítica

Usando as definições apresentadas nas seções anteriores, pode-se generalizar o processo de teleportação para portas quânticas de dois qudits. O circuito representando tal processo pode ser visto na Figura 3.1, em que $\rho_A = Tr_B |\psi_{AB}\rangle \langle\psi_{AB}|$ e $\rho_B = Tr_A |\psi_{AB}\rangle \langle\psi_{AB}|$.

Figura 3.1: Circuito que representa teleportação de uma porta quântica operando sobre estados arbitrários de dois qudits.



Embora a descrição analítica iniciada a seguir assuma como entrada pares de Bell generalizados já formados, julgou-se interessante exibir a forma de gerá-los para uma dimensão arbitrária. O subcircuito responsável por isto está contido na área tracejada. A porta de dois qudits que será teleportada é representada por ${}_dU_T$.

As áreas pontilhadas, adiante denotadas por ${}_dU_M$, representam uma preparação para as medidas na base de Bell generalizada que serão realizadas conjuntamente sobre um qudit integrante de um par maximamente entrelaçado e um qudit alvo da teleportação. No final, ${}_dU_{CORR}$ representa o conjunto de portas de 1 qudit classicamente controláveis responsável por corrigir o estado final.

O processo de teleportação requer a utilização de pares de Bell generalizados, cuja representação d-dimensional é expressa por

$$ {}_dG_{XOR}({}_dF \otimes {}_dI) |0,0\rangle = \sum_{n=0}^{d-1} \frac{1}{\sqrt{d}} |n,n\rangle. \tag{3.44} $$

Desta maneira, o estado inicial do circuito é dado pelo produto tensorial entre um estado arbitrário de dois qudits e dois pares de Bell generalizados:

$$ |\psi_0\rangle = \sum_{k,l=0}^{d-1} \alpha_{kl} |k,l\rangle \otimes \sum_{n=0}^{d-1} \frac{1}{\sqrt{d}} |n,n\rangle \otimes \sum_{m=0}^{d-1} \frac{1}{\sqrt{d}} |m,m\rangle. \tag{3.45} $$

Deve ser observado que, por questões de clareza na manipulação das equações, $|\psi_0\rangle$ foi montado

com uma ordem diferente da exibida graficamente pelo circuito da Figura 3.1. Portanto, a disposição inicial $|\psi_0\rangle_{ABCDEF}$ é tal que os qudits AB são aqueles cuja porta a ser teleportada atuará e os qudits CD e EF representam os pares de Bell generalizados.

Com o objetivo de preparar o estado para uma medição na base de Bell generalizada é aplicada a porta ${}_dU_M = ({}_dF \otimes {}_dI)\,{}_dG_{XOR}$. O estado inicial é então posto na forma $|\psi_1\rangle_{ACBEDF}$ no qual cada qudit a ser teleportado está associado a um qudit integrante de um dos pares de Bell, conforme pode ser visto na Equação (3.46)

$$|\psi_1\rangle = \frac{1}{d}\sum_{k,l=0}^{d-1}\sum_{n,m=0}^{d-1}\alpha_{kl}\,|k,n\rangle \otimes |l,m\rangle \otimes |n,m\rangle. \tag{3.46}$$

Agora, seguindo a ordem descrita pelo circuito, tem-se a aplicação da porta ${}_dU_T$ aos dois qudits integrantes dos pares de Bell que não serão medidos. Isso levará o estado $|\psi_1\rangle$ ao estado exposto na Equação (3.47)

$$|\psi_2\rangle = \frac{1}{d}\sum_{k,l=0}^{d-1}\sum_{n,m=0}^{d-1}\alpha_{kl}\,|k,n\rangle \otimes |lm\rangle \otimes {}_dU_T\,|nm\rangle. \tag{3.47}$$

Na sequência tem-se a aplicação de ${}_dU_M$ aos dois pares de qudits que serão medidos, resultando em

$$|\psi_3\rangle = \frac{1}{d}\sum_{k,l=0}^{d-1}\sum_{n,m=0}^{d-1}\alpha_{kl}{}_dU_M\,|k,n\rangle\,{}_dU_M\,|l,m\rangle\,{}_dU_T\,|n,m\rangle. \tag{3.48}$$

Expandindo a aplicação de ${}_dU_M$ na Equação (3.48) resulta na aplicação da porta ${}_dG_{XOR}$ nos pares[8] AC e BE, seguida da aplicação da porta ${}_dF$ aos primeiros qudits dos pares – índices A e B – o que resultará em

$$|\psi_4\rangle = \frac{1}{d}\sum_{k,l=0}^{d-1}\sum_{n,m=0}^{d-1}\alpha_{kl}\,({}_dF \otimes {}_dI)\,{}_dG_{XOR}\,|k,n\rangle\,({}_dF \otimes {}_dI)\,{}_dG_{XOR}\,|l,m\rangle\,{}_dU_T\,|n,m\rangle. \tag{3.49}$$

Agora usando a Equação (3.26) na Equação (3.49) ter-se-á

$$|\psi_5\rangle = \frac{1}{d}\sum_{k,l=0}^{d-1}\sum_{n,m=0}^{d-1}\alpha_{kl}\,({}_dF \otimes {}_dI)\,|k,k\ominus n\rangle\,({}_dF \otimes {}_dI)\,|l,l\ominus m\rangle\,{}_dU_T\,|n,m\rangle. \tag{3.50}$$

[8] Nesse contexto não se trata de um par de Bell, mas um par formado por uma das partículas a ser teleportada mais uma partícula integrante de um par de Bell.

Desenvolvendo a operação da transformada de Fourier tem-se

$$|\psi_6\rangle = \frac{1}{d}\sum_{k,l=0}^{d-1}\sum_{n,m=0}^{d-1}\alpha_{kl}\sum_{x=0}^{d-1}\frac{1}{\sqrt{d}}e^{(2\pi ikx/d)}\,|x\rangle\,|k\ominus n\rangle\sum_{y=0}^{d-1}\frac{1}{\sqrt{d}}e^{(2\pi ily/d)}\,|y\rangle\,|l\ominus m\rangle\,{}_dU_T\,|n,m\rangle. \tag{3.51}$$

Agrupando os elementos da Equação (3.51) afins chega-se à

$$|\psi_6\rangle = \frac{1}{d^2}\sum_{k,l=0}^{d-1}\sum_{n,m=0}^{d-1}\sum_{x,y=0}^{d-1}\alpha_{kl}e^{(2\pi ikx/d)}e^{(2\pi ily/d)}\,|x\rangle\,|k\ominus n\rangle\,|y\rangle\,|l\ominus m\rangle\,{}_dU_T\,|n,m\rangle, \tag{3.52}$$

cuja matriz densidade [53, 54] $\rho = |\psi_6\rangle\langle\psi_6|$ é dada por

$$\begin{aligned}\rho = \frac{1}{d^4}\sum_{k,l,k',l'=0}^{d-1}\sum_{n,m,n',m'=0}^{d-1}\sum_{x,y,x',y'=0}^{d-1}&\alpha_{kl}\alpha^*_{k'l'}e^{(2\pi ikx/d)}e^{(2\pi ily/d)}\\ &|x\rangle\langle x'|\otimes|k\ominus n\rangle\langle k'\ominus n'|\otimes|y\rangle\langle y'|\otimes|l\ominus m\rangle\langle l'\ominus m'|\\ &e^{(-2\pi ik'x'/d)}e^{(-2\pi il'y'/d)}\otimes{}_dU_T\,|n,m\rangle\langle n',m'|\,{}_dU_T{}^\dagger.\end{aligned} \tag{3.53}$$

O estado final de dois qudits independente dos resultados das medições é dado por

$$\rho_{DF} = Tr_{ABCE}\left(|\psi\rangle\langle\psi|\right), \tag{3.54}$$

obtido através de um traço parcial [53, 54] para remover o sistema a ser medido, resultando em

$$\begin{aligned}\rho_{DF} = \frac{1}{d^4}\sum_{k,l,k',l'=0}^{d-1}\sum_{n,m,n',m'=0}^{d-1}\sum_{x,y,x',y'=0}^{d-1}&\langle x'|x\rangle\langle y'|y\rangle\langle k'\ominus n'|k\ominus n\rangle\\ &\langle l'\ominus m'|l\ominus m\rangle\,{}_dU_T\alpha_{kl}e^{(2\pi ikx/d)}e^{(2\pi ily/d)}\,|n,m\rangle\langle n',m'|\\ &\alpha^*_{k'l'}e^{(-2\pi ik'x'/d)}e^{(-2\pi il'y'/d)}{}_dU_T{}^\dagger.\end{aligned} \tag{3.55}$$

Agora, com base nas definições e propriedades da aritmética modular pode-se provar as expressões a seguir que serão utilizadas adiante na sequência da generalização:

$$k\oplus n = r \;\Rightarrow\; n\oplus k = r \;\Rightarrow\; n = r\ominus k, \tag{3.56}$$

$$k\ominus n = r \;\Rightarrow\; r\oplus n = k \;\Rightarrow\; n = k\ominus r. \tag{3.57}$$

Sendo os estados ortonormais tem-se $\langle x|x'\rangle = \delta_{x,x'}$ e $\langle y|y'\rangle = \delta_{y,y'}$, portanto, $\langle k'\ominus n'|k\ominus n\rangle = \delta_{(k'\ominus n')(k\ominus n)}$ e $\langle l'\ominus m'|l\ominus m\rangle = \delta_{(l'\ominus m')(l\ominus m)}$. Fazendo $k'\ominus n' = k\ominus n = r$ e $l'\ominus m' = l\ominus m = s$, e utilizando as Equações 3.56 e 3.57 chega-se a:

$$n = k\ominus r, \quad n' = k'\ominus r, \tag{3.58}$$

$$m = l \ominus s, \quad m' = l' \ominus s. \tag{3.59}$$

Aplicando os resultados obtidos nas Equações 3.58 e 3.59 na Equação (3.55), ou seja, efetuando os produtos internos, chega-se ao resultado

$$\rho_{DF} = \frac{1}{d^4} \sum_{k,l,k',l'=0}^{d-1} \sum_{r,s=0}^{d-1} \sum_{x,y=0}^{d-1} U_T \alpha_{kl} e^{[2\pi i(k\ominus r)x/d]} e^{[2\pi i(l\ominus s)y/d]} \left|k \ominus r, l \ominus s\right\rangle \left\langle k' \ominus r, l' \ominus s\right| \alpha^*_{k'l'} e^{[-2\pi i(k'\ominus r)x/d]} e^{[-2\pi i(l'\ominus s)y/d]} {}_dU_T{}^\dagger. \tag{3.60}$$

Observando-se que

$$e^{[2\pi i(k\ominus r)x/d]} \left|k \ominus r\right\rangle \equiv ({}_dZ)^x \left|k \ominus r\right\rangle \tag{3.61}$$

e usando este resultado na Equação (3.60) obtem-se

$$\rho_{DF} = \frac{1}{d^4} \sum_{k,l,k',l'=0}^{d-1} \sum_{r,s=0}^{d-1} \sum_{x,y=0}^{d-1} U_T \alpha_{kl} ({}_dZ^x \otimes {}_dZ^y) \left|k \ominus r, l \ominus s\right\rangle \left\langle k' \ominus r, l' \ominus s\right| \alpha^*_{k'l'} ({}_dZ^x \otimes {}_dZ^y)^\dagger {}_dU_T{}^\dagger. \tag{3.62}$$

Além disso

$$ {}_dX^q \left|p\right\rangle = \left|p \oplus q\right\rangle \tag{3.63}$$

$$ {}_dX^{-q} \left|p\right\rangle = \left|p \ominus q\right\rangle, \tag{3.64}$$

o que leva a Equação (3.62) à

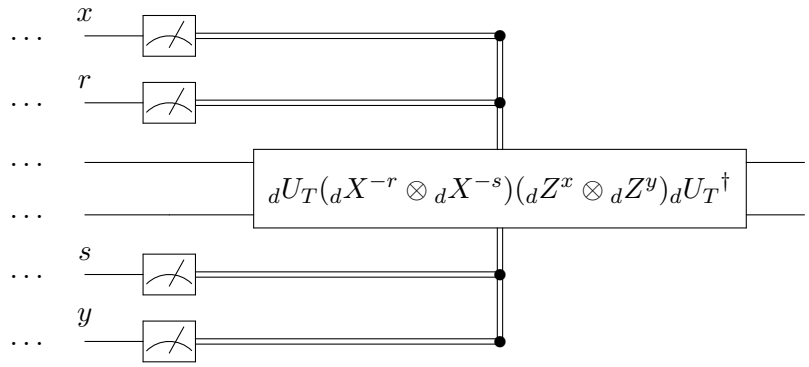
$$\rho_{DF} = \frac{1}{d^4} \sum_{k,l,k',l'=0}^{d-1} \sum_{r,s=0}^{d-1} \sum_{x,y=0}^{d-1} {}_dU_T \alpha_{kl} ({}_dX^{-r} \otimes {}_dX^{-s})({}_dZ^x \otimes {}_dZ^y) \left|k, l\right\rangle \left\langle k', l'\right| \alpha^*_{k'l'} ({}_dZ^x \otimes {}_dZ^y)^\dagger ({}_dX^{-r} \otimes {}_dX^{-s})^\dagger {}_dU_T{}^\dagger. \tag{3.65}$$

Concluindo, a Equação (3.65) pode ser reescrita como

$$\rho_{DF} = \frac{1}{d^4} \sum_{r,s=0}^{d-1} \sum_{x,y=0}^{d-1} {}_dU_T({}_dX^{-r} \otimes {}_dX^{-s})({}_dZ^x \otimes {}_dZ^y){}_dU_T{}^\dagger \left[{}_dU_T \sum_{k,l,k',l'=0}^{d-1} \alpha_{kl} \left|k, l\right\rangle \left\langle k', l'\right| \alpha^*_{k'l'} {}_dU_T{}^\dagger \right] {}_dU_T({}_dZ^x \otimes {}_dZ^y)^\dagger ({}_dX^{-r} \otimes {}_dX^{-s})^\dagger {}_dU_T{}^\dagger. \tag{3.66}$$

Desta forma, tem-se que o termo dentro dos colchetes na Equação (3.66) é justamente a ação da porta ${}_dU_T$ sobre um estado arbitrário de dois qudits. Deve-se notar que não apenas é apontada a generalização da teleportação de portas de dois qudits para uma dimensão arbitrária como também é provida a correção necessária associada aos possíveis valores clássicos da medição – endereçados por x, y, r e s. É possível vincular o resultado da medição dos qudits a cada uma das variáveis da correção, conforme mostrado na Figura 3.2.

Figura 3.2: Circuito que representa a correção da teleportação de uma porta de dois qudits.



Por outro lado os termos que envolvem lateralmente os colchetes indicam as circunstâncias sobre as quais a teleportação será executada com sucesso. A teleportação ocorrerá com sucesso sempre que

$$\begin{aligned} &{}_dU_T({}_dX^{-r} \otimes {}_dX^{-s})({}_dZ^{x} \otimes {}_dZ^{y}){}_dU_T{}^{\dagger} = \\ &V_1(x,y,r,s) \otimes V_2(x,y,r,s) \;\forall\; x,y,r,s \in [0,d-1], \end{aligned} \tag{3.67}$$

ou seja, sempre que a operação ${}_dU_T({}_dX^{-r} \otimes {}_dX^{-s})({}_dZ^{x} \otimes {}_dZ^{y}){}_dU_T{}^{\dagger}$ resultar em uma porta quântica decomponível no produto tensorial de duas outras portas de um qudit. Isto sempre ocorrerá se ${}_dU_T$ pertencer ao grupo de Clifford generalizado.

3.5 Teleportação de portas atuando sobre n-qudits

O procedimento descrito pode facilmente ser aplicado para obter-se uma generalização da teleportação de portas sobre n-qudits, de tal forma que chega-se à

$$\begin{aligned} \rho_{\lambda_1 \ldots \lambda n} = \frac{1}{(\sqrt{d})^{4n}} \sum_{r_1,\ldots,r_n,s_1,\ldots,s_n=0}^{d-1} &{}_dU_T({}_dX^{-r_1} \otimes \cdots \otimes {}_dX^{-r_n})({}_dZ^{s_1} \otimes \cdots \otimes {}_dZ^{s_n}){}_dU_T{}^{\dagger} \\ &\left[{}_dU_T \sum_{k_1,\ldots,k_n,k'_1,\ldots,k'_n=0}^{d-1} \alpha_{k_1,\ldots,k_n} \left|k_1,\ldots,k_n\right\rangle \left\langle k'_1,\ldots,k'_n\right| \alpha^{*}_{k'_1,\ldots,k'_n} {}_dU_T{}^{\dagger} \right] \\ &{}_dU_T({}_dZ^{s_1} \otimes \cdots \otimes {}_dZ^{s_n})^{\dagger}({}_dX^{-r_1} \otimes \cdots \otimes {}_dX^{-r_n})^{\dagger} {}_dU_T{}^{\dagger}. \end{aligned} \tag{3.68}$$

Naturalmente a teleportação será completada com sucesso quando

$$
\begin{aligned}
&{}_dU_T({}_dX^{-r_1} \otimes \cdots \otimes {}_dX^{-r_n})({}_dZ^{s_1} \otimes \cdots \otimes {}_dZ^{s_n})_dU_T{}^{\dagger} = \\
&\qquad V_1 \otimes \cdots \otimes V_n \ \forall\ r_1, \ldots, r_n, s_1, \ldots, s_n \in [0, d-1].
\end{aligned} \tag{3.69}
$$

A Equação (3.68) pode ser considerada uma generalização do processo de teleportação, uma vez que:

i. Para o caso de $d = 2$ e $n = 2$ tem-se o procedimento descrito por Gottesman-Chuang [1].

ii. Para o caso de $d = 2$, $n = 1$ e $U_T = I$ tem-se a teleportação original de Bennett [14].

3.6 Conclusão

Neste capítulo foi construída uma generalização da teleportação de portas de dois qubits originalmente proposta por Gottesman-Chuang de tal forma que ela opera sobre espaços de Hilbert de dimensão arbitrária. Por fim, a proposta apresenta como bônus o circuito de correção individual – associado ao resultado da medição clássica – a ser aplicado no estado resultante da teleportação a fim de restaurar o estado teleportado.

Parte II

Teleportabilidade

Capítulo 4

Sobre a separabilidade e algumas aplicações

Resumo

Neste capítulo serão encontradas as condições necessárias e suficientes para determinar se uma dada matriz U é separável, ou seja, se ela pode ser descrita na forma de um produto tensorial. Será dada uma ênfase destacada à discussão do caso particular de verificar se $U \in U(2)^{\otimes 2}$ ou $U \in U(4)/U(2)^{\otimes 2}$. Como exemplos de aplicações, serão discutidas a preservação da separabilidade sob conjugação e a forma geral de um elemento do grupo de Clifford, duas contribuições dessa tese.

4.1 Introdução

No contexto deste trabalho, separabilidade é a característica que uma dada matriz U de dimensão $m \times n$ eventualmente possui de poder ser escrita como um produto tensorial de j matrizes U_i de dimensões $m_i \times n_i$, tal como

$$U = U_1 \otimes U_2 \otimes \cdots \otimes U_j, \tag{4.1}$$

em que $m = m_1 \cdot m_2 \cdot ... \cdot m_j$ e $n = n_1 \cdot n_2 \cdot ... \cdot n_j$. Embora a técnica descrita ao longo deste capítulo possa ser facilmente aplicada ao caso geral, em virtude das aplicações objetivadas uma ênfase especial será dedicada ao caso em que U é uma matriz quadrada separável em duas partes, ou seja, $U = U_1 \otimes U_2$ com dimensão $n \times n$[1].

[1] Deste ponto em diante, não existindo o risco de ambiguidades, as matrizes quadradas terão suas dimensões descritas apenas como n.

Uma grande variedade de problemas são modelados matematicamente na forma de matrizes, portanto, há uma razoável expectativa de que o conteúdo aqui descrito possa encontrar aplicações em áreas variadas. Um exemplo interessante pode ser visto no trabalho [55] em que condições para separabilidade, especificamente para o caso em que $U \in M_{4\times4}(\mathbb{C})$, são estabelecidas em função do posto de uma representação matricial de um vetor e aplicadas para dar uma nova descrição da estrutura do espaço-tempo na teoria da relatividade restrita.

A técnica apresentada neste capítulo se baseia no fato de que o produto de Kronecker entre matrizes é uma forma bilinear [56, 57]. A motivação principal de lidar com este problema neste trabalho é aplicá-lo em tópicos da teoria da informação quântica, em particular, ao que se refere à teleportação da ação de portas quânticas e a busca/caracterização de entrelaçadores universais, ambos tópicos descritos em capítulos posteriores.

O restante deste capítulo está organizado da seguinte forma: A Seção 4.2 traz uma revisão de conceitos elementares empregados ao longo do capítulo. Na Seção 4.3, tem-se uma discussão de pontos chaves das formas bilineares. Seguindo, a Seção 4.4 demonstra formalmente uma técnica para verificação da separabilidade. Como exemplos de aplicação da técnica, tem-se na Seção 4.5 e Seção 4.6, respectivamente, a descrição da preservação da separabilidade sob conjugação e da forma geral de um elemento do grupo de Clifford. Por fim, a Seção 4.7 apresenta as conclusões.

4.2 Noções elementares

Algumas noções elementares, tais como relações de comutação e decomposição de matrizes, utilizadas no desenvolvimento dos resultados objetivados serão apresentadas ao longo dessa seção.

4.2.1 Relações de comutação

Toma-se σ_μ, em que $\mu \in \{I, X, Y, Z\}$, como representação das matrizes de Pauli de dimensão 2×2, portanto: $\sigma_I = I$, $\sigma_X = X$, $\sigma_Y = Y$ e $\sigma_Z = Z$. Então, o produto tensorial entre duas matrizes de Pauli será representado por $\sigma_{\mu\upsilon} = \sigma_\mu \otimes \sigma_\upsilon$ no qual, naturalmente, $\mu, \upsilon \in \{I, X, Y, Z\}$.

Algumas relações de comutação envolvendo as matrizes de Pauli, que podem ser verificadas facilmente utilizando a multiplicação usual de matrizes, serão importantes no desenvolvimento analítico apresentado no decorrer deste capítulo. Para $\mu, \upsilon \in \{X, Y, Z\}$, são elas:

$$[\sigma_{\mu\mu}, \sigma_{\upsilon\upsilon}] = 0 \quad \forall \quad \mu, \upsilon \tag{4.2a}$$

$$[\sigma_{\mu\mu}, \sigma_{I\mu}] = 0, \quad [\sigma_{\mu\mu}, \sigma_{\mu I}] = 0 \quad \forall \quad \mu \tag{4.2b}$$

$$[\sigma_{\mu I}, \sigma_{I\upsilon}] = 0, \quad [\sigma_{I\mu}, \sigma_{\upsilon I}] = 0 \quad \forall \quad \mu, \upsilon. \tag{4.2c}$$

Aliadas a estas, também serão importantes algumas relações de comutação envolvendo a forma exponencial das matrizes, são elas:

$$\left[e^{i\theta\sigma_{\mu\mu}}, \sigma_{\upsilon\upsilon}\right] = 0 \quad \forall \quad \mu, \upsilon \tag{4.3a}$$

$$\left[e^{i\theta\sigma_{\mu\mu}}, \sigma_{\eta\upsilon}\right] = 0 \quad \forall \quad \mu \neq \eta \neq \upsilon \tag{4.3b}$$

$$\left[e^{i\theta\sigma_{\mu\mu}}, \sigma_{I\mu}\right] = 0, \quad \left[e^{i\theta\sigma_{\mu\mu}}, \sigma_{\mu I}\right] = 0 \quad \forall \quad \mu. \tag{4.3c}$$

4.2.2 Forma separável de $SU(4)$

Um elemento U de $SU(4)$ é dito separável quando pode ser escrito como um produto tensorial de dois elementos de $SU(2)$, ou seja, $U = SU(2) \otimes SU(2)$. Sabe-se [42] ainda que qualquer elemento de $SU(2)$ pode ser expresso, usando a decomposição ZYZ, como o produto de exponenciais

$$U_\Lambda = e^{-i/2(\lambda_1 \cdot \sigma_Z)} \cdot e^{-i/2(\lambda_2 \cdot \sigma_Y)} \cdot e^{-i/2(\lambda_3 \cdot \sigma_Z)}, \tag{4.4}$$

em que $\lambda_1,\ \lambda_2, \lambda_3 \in \mathbb{R}$.

A Equação (4.4) pode ser usada para representar a forma geral de uma matriz separável em $SU(4)$ de uma maneira que posteriormente será conveniente, conforme é apresentado na Equação (4.5).

$$U_{\Lambda\Omega} = \begin{matrix} \left(e^{-i/2(\lambda_1 \cdot \sigma_Z)} \otimes e^{-i/2(\omega_1 \cdot \sigma_Z)}\right). \\ \left(e^{-i/2(\lambda_2 \cdot \sigma_Y)} \otimes e^{-i/2(\omega_2 \cdot \sigma_Y)}\right). \\ \left(e^{-i/2(\lambda_3 \cdot \sigma_Z)} \otimes e^{-i/2(\omega_3 \cdot \sigma_Z)}\right). \end{matrix} \tag{4.5}$$

Agora, observando as propriedades do produto tensorial descritas nas Equações (4.6) e (4.7), em que I é a matriz identidade, pode-se reescrever a Equação (4.5) em sua forma final, conforme mostrado na Equação (4.8).

$$e^A \otimes e^B = e^{A \oplus B}. \tag{4.6}$$

$$A \oplus B = A \otimes I + I \otimes B. \tag{4.7}$$

$$U_{\Lambda\Omega} = \begin{matrix} \left(e^{-i/2(\lambda_1 \cdot \sigma_{ZI} + \omega_1 \cdot \sigma_{IZ})}\right). \\ \left(e^{-i/2(\lambda_2 \cdot \sigma_{YI} + \omega_2 \cdot \sigma_{IY})}\right). \\ \left(e^{-i/2(\lambda_3 \cdot \sigma_{ZI} + \omega_3 \cdot \sigma_{IZ})}\right). \end{matrix} \tag{4.8}$$

4.2.3 Forma geral de $SU(4)$

A parametrização trivial de uma matriz $SU(4)$ requer dezesseis parâmetros complexos, no entanto, uma parametrização mais eficiente é conhecida a partir da decomposição Cartan's KAK [58], em que são requeridos apenas quinze parâmetros reais. Outra característica interessante da decomposição KAK, que será explorada mais adiante, é que a fatoração resultante possui uma parte separável, parametrizada por doze parâmetros reais, e uma parte não separável, parametrizada por três parâmetros reais. A Equação (4.9) apresenta a decomposição de um elemento U de $SU(4)$.

$$U = (U_A \otimes U_B) \cdot U_{NL} \cdot (U_C \otimes U_D). \tag{4.9}$$

As matrizes U_A, U_B, U_C e U_D compõem a parte local da matriz U e podem ser representadas pela Equação (4.8). Mais especificamente, o produto $(U_A \otimes U_B)$ será denotado como *parte local à esquerda* e o produto $(U_C \otimes U_D)$ como *parte local à direita*. A matriz U_{NL} representa a *parte não local* de U e pode ser expressa, a menos de uma fase global, por

$$U_{NL} = e^{i(\theta_1 \cdot \sigma_{XX} + \theta_2 \cdot \sigma_{YY} + \theta_3 \cdot \sigma_{ZZ})} \tag{4.10}$$

que representa a forma geral de um elemento estritamente não separável de $SU(4)$. Usando as relações de comutação descritas na Equação (4.2), pode-se reescrever a Equação (4.10) como

$$U_{NL} = e^{i(\theta_1 \cdot \sigma_{XX})} e^{i(\theta_2 \cdot \sigma_{YY})} e^{i(\theta_3 \cdot \sigma_{ZZ})}. \tag{4.11}$$

Por fim, usando as Equações (4.8) e (4.11) pode-se expandir a Equação (4.9) como mostrado na Equação (4.12), a forma geral explorada mais adiante neste capítulo.

$$U = \begin{bmatrix} \begin{pmatrix} e^{-i/2(a1 \cdot \sigma_{ZI} + b_1 \cdot \sigma_{IZ})}. \\ e^{-i/2(a2 \cdot \sigma_{YI} + b_2 \cdot \sigma_{IY})}. \\ e^{-i/2(a3 \cdot \sigma_{ZI} + b_3 \cdot \sigma_{IZ})} \end{pmatrix}. \\ e^{i(\theta_1 \cdot \sigma_{XX})} \cdot e^{i(\theta_2 \cdot \sigma_{YY})} \cdot e^{i(\theta_3 \cdot \sigma_{ZZ})}. \\ \begin{pmatrix} e^{-i/2(c1 \cdot \sigma_{ZI} + d_1 \cdot \sigma_{IZ})}. \\ e^{-i/2(c2 \cdot \sigma_{YI} + d_2 \cdot \sigma_{IY})}. \\ e^{-i/2(c3 \cdot \sigma_{ZI} + d_3 \cdot \sigma_{IZ})} \end{pmatrix}. \end{bmatrix} \tag{4.12}$$

4.3 Formas bilineares

Uma descrição profunda acerca de formas bilineares está fora do escopo deste trabalho, mas pode ser encontrada em bons livros de álgebra linear que abordam o tema, tais como [56, 57, 59, 60]. Serão apresentados apenas elementos chaves relacionados à abordagem descrita ao longo deste capítulo, a começar pela definição mais elementar[2].

Definição 4.1. *Sejam U e V espaços vetoriais sobre um corpo $\mathbb{K}$, um mapeamento $f : U \times V \to \mathbb{K}$ é uma forma bilinear se, e somente se,*

(i) $f(a\vec{u}_1 + b\vec{u}_2, \vec{v}) = af(\vec{u}_1, \vec{v}) + bf(\vec{u}_2, \vec{v})$

(ii) $f(\vec{u}, a\vec{v}_1 + b\vec{v}_2) = af(\vec{u}, \vec{v}_1) + bf(\vec{u}, \vec{v}_2)$

para todo $a, b \in \mathbb{K}$, todo $\vec{u}_i \in U$ e todo $\vec{v}_i \in V$.

A condição (i) expressa o fato de f ser linear no primeiro argumento enquanto a condição (ii) expressa o fato de f ser linear no segundo argumento. Tem-se ainda que a bilinearidade pode ser definida a partir de mapeamentos lineares [61], conforme definição adiante.

Definição 4.2. *Sejam g e h mapeamentos lineares arbitrários nos espaços vetoriais, respectivamente, U e V, então $f : U \times V \to \mathbb{K}$ definida por $f(\vec{u}, \vec{v}) = g(\vec{u})h(\vec{v})$, em que $\vec{u} \in U$ e $\vec{v} \in V$, é uma forma bilinear.*

4.3.1 Matriz de uma forma bilinear

De maneira análoga ao caso de transformações lineares, para toda forma bilinear há uma matriz que codifica todas as informações acerca da referida forma. Conforme apresentado formalmente na definição adiante, essa matriz depende de uma base em particular.

Definição 4.3. *Sejam U e V espaços vetoriais sobre o corpo $\mathbb{K}$ de dimensões, respectivamente, m e n, toma-se as bases $B_U = \{\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_m\}$ e $B_V = \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\}$ de modo que $\vec{u} = \sum_{i=1}^{m} a_i\vec{u}_i \in U$ e $\vec{v} = \sum_{j=1}^{n} b_j\vec{v}_j \in V$, em que $a_i, b_j \in \mathbb{K}$. Assim sendo, a forma bilinear $f : U \times V \to \mathbb{K}$ assume a forma*

$$f(\vec{u}, \vec{v}) = f\left(\sum_{i=1}^{m} a_i\vec{u}_i, \sum_{j=1}^{n} b_j\vec{v}_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i^* b_j f(\vec{u}_i, \vec{v}_j), \tag{4.13}$$

cuja representação matricial, em relação às bases B_U e B_V, é dada pela matriz $m \times n$

$$F = \begin{bmatrix} f(\vec{u}_1, \vec{v}_1) & \cdots & \cdots & f(\vec{u}_1, \vec{v}_n) \\ f(\vec{u}_2, \vec{v}_1) & \cdots & \cdots & f(\vec{u}_2, \vec{v}_n) \\ \vdots & \vdots & \vdots & \vdots \\ f(\vec{u}_m, \vec{v}_1) & \cdots & \cdots & f(\vec{u}_m, \vec{v}_n) \end{bmatrix}. \tag{4.14}$$

[2] Ao longo deste trabalho, o corpo $\mathbb{K}$ está representando os casos dos reais ($\mathbb{R}$) ou dos complexos ($\mathbb{C}$).

Portanto, para toda forma bilinear f há uma matriz $F = [f_{i,j}]_{m\times n} \in M_{m\times n}(\mathbb{K})$, de modo que a ação de f pode ser definida por

$$f(\vec{u},\vec{v}) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i^* b_j f_{i,j} = \vec{u}^\dagger F \vec{v} \tag{4.15}$$

que, inversamente, indica que toda matriz $M_{m\times n}(\mathbb{K})$ está associada à uma forma bilinear no espaço de formas bilineares. Uma vez fixadas as bases dos espaços essa relação é única e vê-se facilmente a partir da Definição 4.3 e da Equação (4.15) que

$$f(\vec{u}_i,\vec{v}_j) = f_{i,j}. \tag{4.16}$$

4.3.2 Produto de Kronecker entre matrizes

Sem perda de generalidade, o produto de Kronecker entre duas matrizes quadradas A e B de dimensões, respectivamente, m e n corresponde à uma matriz com m^2 blocos de dimensão n, resultando em uma matriz final de dimensão mn. A definição adiante formaliza esta operação matricial.

Definição 4.4. *Tomando-se as matrizes quadradas $A = [a_{i,j}]_{m\times m}$ e $B = [b_{p,q}]_{n\times n}$, com i, $j \in \{1,2,\cdots,m\}$ e $p,q \in \{1,2,\cdots,n\}$, tem-se que o produto de Kronecker $A\otimes B$ resulta em uma matriz de m^2 blocos em que o bloco (i,j) é a matriz quadrada $a_{i,j}B$. Portanto, a matriz $mn\times mn$ resultante é dada por*

$$A\otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix}, \tag{4.17}$$

de onde se pode concluir que $[A\otimes B]_{(i-1)n+p,(j-1)n+q} = a_{i,j}b_{p,q}$.

Esta definição pode facilmente ser usada para verificar a Proposição 4.1, apresentada adiante, que indica que o produto tensorial é uma forma bilinear [59].

Proposição 4.1. *Sejam A, B e C matrizes arbitrárias e r,s escalares arbitrários, observam-se as propriedades,*

(i) $A\otimes(B+C) = A\otimes B + A\otimes C$

(ii) $(A+B)\otimes C = A\otimes C + B\otimes C$

(iii) $rA\otimes B = A\otimes rB = r(A\otimes B)$,

de onde se pode concluir que

$$\left(\sum_i r_i A_i\right) \otimes \left(\sum_j s_j B_j\right) = \sum_{i,j} r_i s_j (A_i \otimes B_j), \tag{4.18}$$

portanto, o produto de Kronecker entre matrizes é uma forma bilinear.

4.3.3 Tensorial de formas bilineares

O primeiro passo para definir o produto tensorial de formas bilineares é entender como o produto tensorial é utilizado para expandir espaços vetoriais, conforme resumido na definição [57, 59] adiante.

Definição 4.5. *Se U e V são espaços vetoriais sobre o corpo $\mathbb{K}$ de dimensões, respectivamente, m e n, então $T = U \otimes V$ é um espaço vetorial sobre o corpo $\mathbb{K}$ de dimensão mn. Portanto, se $B_U = \{\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_m\}$ e $B_V = \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\}$ são bases, respectivamente, dos espaços vetoriais B e V, então $B_T = \{\vec{t}_1, \vec{t}_2, \cdots, \vec{t}_{m\cdot n}\}$, em que $\vec{t}_{n(i-1)+j} = \vec{u}_i \otimes \vec{v}_j$, é uma base do espaço vetorial T.*

A primeira parte da definição descreve a construção do espaço, enquanto a segunda descreve a base deste espaço construído. Por fim, juntas a Proposição 4.1 e a Definição 4.5 são suficientes [59] para concluir que

$$\mathbb{K}^{m\cdot n} = \mathbb{K}^m \otimes \mathbb{K}^n \tag{4.19}$$

e, portanto, pode-se afirmar que os vetores $\vec{t}_i \in B_T$ geram todo o espaço $\mathbb{K}^{m\cdot n}$. Agora, pode-se definir, sem perda de generalidade, o produto tensorial de formas bilineares conforme adiante.

Proposição 4.2. *Sejam U e V espaços vetoriais sobre o corpo $\mathbb{K}$ de dimensões, respectivamente, m e n, toma-se as bases $B_U = \{\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_m\}$ e $B_V = \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\}$ de, respectivamente, U e V, de modo que $\vec{u} = \sum_{i=1}^m a_i \vec{u}_i \in U$ e $\vec{v} = \sum_{k=1}^n c_k \vec{v}_k \in V$. Sejam ainda $f : U \times U \to \mathbb{K}$ e $g : V \times V \to \mathbb{K}$ formas bilineares cujas representações matriciais são, respectivamente, F e G, tem-se que*

$$\begin{aligned} f(\vec{u}, \vec{z}) \otimes g(\vec{v}, \vec{w}) &= f\left(\sum_{i=1}^m a_i \vec{u}_i, \sum_{j=1}^m b_j \vec{u}_j\right) \otimes g\left(\sum_{k=1}^n c_k \vec{v}_k, \sum_{l=1}^n d_l \vec{v}_l\right) && \text{(4.20a)} \\ &= \sum_{i=1}^m \sum_{j=1}^m a_i^* b_j f(\vec{u}_i, \vec{u}_j) \otimes \sum_{k=1}^n \sum_{l=1}^n c_k^* d_l g(\vec{v}_k, \vec{v}_l) && \text{(4.20b)} \\ &= \left(\vec{u}^\dagger F \vec{z}\right) \otimes \left(\vec{v}^\dagger G \vec{w}\right) = (\vec{u} \otimes \vec{v})^\dagger (F \otimes G)(\vec{z} \otimes \vec{w}) && \text{(4.20c)} \end{aligned}$$

é a forma bilinear $t : (U \times U) \times (V \times V) \to \mathbb{K}$ com base $T = [\vec{t}_{i,j}] = [\vec{u}_i \otimes \vec{v}_j]$.

De maneira análoga à Equação (4.15), tem-se que a aplicação da forma t sobre os vetores da base T resulta em

$$t(\vec{u}_i, \vec{u}_j, \vec{v}_k, \vec{v}_l) = f(\vec{u}_i, \vec{u}_j) \otimes g(\vec{v}_k, \vec{v}_l) = f_{i,j} \cdot g_{k,l}. \tag{4.21}$$

4.4 Análise de separabilidade

Nesta seção é explicada a abordagem algébrica utilizada para verificar a separabilidade de um elemento $U \in M_{n\times n}(\mathbb{K})$. A Seção 4.4.1 apresenta a abordagem que explora o fato do produto tensorial ser uma forma bilinear, enquanto a Seção 4.4.2 discute algumas alternativas que, por levarem à sistemas lineares mais simples, podem ser usadas para a análise de casos particulares.

4.4.1 Bilinearidade do produto tensorial

A técnica aqui descrita [56, 62] explora o fato do produto tensorial ser uma forma bilinear e permite não apenas verificar a separabilidade de uma matriz como também obter as matrizes que a compõem. Seu viés responsável pela verificação da separabilidade pode ser resumido no teorema adiante.

Teorema 4.1 (Separabilidade)**.** *Sejam U e V espaços vetoriais sobre o corpo $\mathbb{K}$ de dimensões m e n, respectivamente, tomam-se as bases $B_U = \{\vec{u}_1, \vec{u}_2, \cdots, \vec{u}_m\}$ e $B_V = \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\}$ de modo que $\vec{u} = \sum_{i=1}^{m} a_i\vec{u}_i \in U$ e $\vec{v} = \sum_{j=1}^{n} b_j\vec{v}_j \in V$, em que $a_i, b_j \in \mathbb{K}$. Sejam ainda os operadores lineares A, B e $C = A \otimes B$ que operam, respectivamente, sobre elementos dos espaços U, V e $T = U \otimes V$, pode-se definir o mapeamento bilinear $\Phi : (U \times U) \times (V \times V) \to \mathbb{K}$ expresso por*

$$\Phi(\vec{p}, \vec{q}, \vec{r}, \vec{s}) = (\vec{p} \otimes \vec{r})^{\dagger} \cdot C \cdot (\vec{q} \otimes \vec{s})\,. \tag{4.22}$$

Assim sendo, tem-se que é condição necessária e suficiente, para que C seja separável, que a relação

$$\Phi(\vec{p}_1, \vec{q}_1, \vec{r}_1, \vec{s}_1) \cdot \Phi(\vec{p}_2, \vec{q}_2, \vec{r}_2, \vec{s}_2) = \Phi(\vec{p}_1, \vec{q}_1, \vec{r}_2, \vec{s}_2) \cdot \Phi(\vec{p}_2, \vec{q}_2, \vec{r}_1, \vec{s}_1) \tag{4.23}$$

seja satisfeita para todos os vetores $\vec{p}_1, \vec{q}_1, \vec{p}_2, \vec{q}_2$ e $\vec{r}_1, \vec{s}_1, \vec{r}_2, \vec{s}_2$ pertencentes à, respectivamente, U e V.

Demonstração. Para verificar a primeira direção da implicação ($C = A \otimes B \to$ Equação (4.23))

basta aplicar a Equação (4.22) na Equação (4.23) substituindo C por $A \otimes B$

$$\begin{aligned}&(\vec{p}_1 \otimes \vec{r}_1)^\dagger \cdot (A \otimes B) \cdot (\vec{q}_1 \otimes \vec{s}_1) \cdot (\vec{p}_2 \otimes \vec{r}_2)^\dagger \cdot (A \otimes B) \cdot (\vec{q}_2 \otimes \vec{s}_2) = \\ &(\vec{p}_1 \otimes \vec{r}_2)^\dagger \cdot (A \otimes B) \cdot (\vec{q}_1 \otimes \vec{s}_2) \cdot (\vec{p}_2 \otimes \vec{r}_1)^\dagger \cdot (A \otimes B) \cdot (\vec{q}_2 \otimes \vec{s}_1)\end{aligned} \tag{4.24a}$$

$$\begin{aligned}&\left(\left(\vec{p}_1^\dagger \cdot A \cdot \vec{q}_1\right) \otimes \left(\vec{r}_1^\dagger \cdot B \cdot \vec{s}_1\right)\right) \cdot \left(\left(\vec{p}_2^\dagger \cdot A \cdot \vec{q}_2\right) \otimes \left(\vec{r}_2^\dagger \cdot B \cdot \vec{s}_2\right)\right) = \\ &\left(\left(\vec{p}_1^\dagger \cdot A \cdot \vec{q}_1\right) \otimes \left(\vec{r}_2^\dagger \cdot B \cdot \vec{s}_2\right)\right) \cdot \left(\left(\vec{p}_2^\dagger \cdot A \cdot \vec{q}_2\right) \otimes \left(\vec{r}_1^\dagger \cdot B \cdot \vec{s}_1\right)\right)\end{aligned}, \tag{4.24b}$$

de onde vê-se facilmente que a igualdade sempre será verdadeira para quaisquer vetores $\vec{p}_i$, $\vec{q}_j, \vec{r}_k, \vec{s}_l$, ou seja, trata-se de uma tautologia. Verificar a implicação inversa (Equação (4.23) $\rightarrow C = A \otimes B$) é menos direto, entretanto, em razão da linearidade é suficiente que a Equação (4.23) seja verificada para

$$\Phi(\vec{u}_i, \vec{u}_j, \vec{v}_p, \vec{v}_q) \cdot \Phi(\vec{u}_k, \vec{u}_l, \vec{v}_r, \vec{v}_s) = \Phi(\vec{u}_i, \vec{u}_j, \vec{v}_r, \vec{v}_s) \cdot \Phi(\vec{u}_k, \vec{u}_l, \vec{v}_p, \vec{v}_q), \tag{4.25}$$

em que $\vec{u}_i \in B_U$ e $\vec{v}_j \in B_V$. Seguindo, assume-se que C opera sobre um espaço com base $B_T = [t_{i,j}] = [u_i \otimes v_j]$, em que $t_{n(i-1)+j} = u_i \otimes v_j$, então, a partir das definições 4.5 e 4.3, pode-se definir a ação da Equação (4.22) nos vetores da base como

$$\begin{aligned}\Phi(\vec{u}_i, \vec{u}_j, \vec{v}_p, \vec{v}_q) &= (\vec{u}_i \otimes \vec{v}_p)^\dagger \cdot C \cdot (\vec{u}_j \otimes \vec{v}_q) && (4.26a)\\ &= \left(t_{(i-1)n+p}\right)^\dagger \cdot C \cdot \left(t_{(j-1)n+q}\right) && (4.26b)\\ &= C_{(i-1)n+p,(j-1)n+q}, && (4.26c)\end{aligned}$$

em que n diz respeito à dimensão do espaço V. Assim sendo, pode-se reescrever a Equação (4.25) como

$$C_{(i-1)n+p,(j-1)n+q} \cdot C_{(k-1)n+r,(l-1)n+s} = C_{(i-1)n+r,(j-1)n+s} \cdot C_{(k-1)n+p,(l-1)n+q} \tag{4.27}$$

de modo que, se a partir da Definição 4.4 se sabe que

$$(A \otimes B)_{(i-1)n+p,(j-1)n+q} = a_{i,j} b_{p,q}, \tag{4.28}$$

então se pode redefinir a Equação (4.27) como

$$a_{i,j} b_{p,q} \cdot a_{k,l} b_{r,s} = a_{i,j} b_{r,s} \cdot a_{k,l} b_{p,q} \ \ \forall \ \ i,j,k,l \in \{1,2,\cdots,m\} \text{ and } p,q,r,s \in \{1,2,\cdots,n\}, \tag{4.29}$$

justamente a forma geral de um produto de Kronecker entre matrizes, significando que se a Equação (4.23) é verdadeira, então $C = A \otimes B$ e, por fim, representa, de fato, condição

necessária e suficiente para a separabilidade do operador C. □

Agora, uma vez que a Equação (4.23) é satisfeita, pode-se então obter as matrizes A e B correspondentes definindo mais algumas formas bilineares. Antes, fixa-se $\vec{p}_0, \vec{q}_0, \vec{r}_0, \vec{s}_0$ de modo que $\Phi(\vec{p}_0, \vec{q}_0, \vec{r}_0, \vec{s}_0) = 1$, então se define as formas bilineares

$$\Psi_A(\vec{p}, \vec{q}) = \Phi(\vec{p}, \vec{q}, \vec{r}_0, \vec{s}_0) \tag{4.30}$$

$$\Psi_B(\vec{r}, \vec{s}) = \Phi(\vec{p}_0, \vec{q}_0, \vec{r}, \vec{s}), \tag{4.31}$$

de modo que existirão as matrizes A e B tal que

$$\Psi_A(\vec{p}, \vec{q}) = \vec{p}^{\dagger} \cdot A \cdot \vec{q} \tag{4.32}$$

$$\Psi_B(\vec{r}, \vec{s}) = \vec{r}^{\dagger} \cdot B \cdot \vec{s}. \tag{4.33}$$

Naturalmente, sabe-se a partir da Definição 4.3 que os elementos destas matrizes são dados, respectivamente, por $a_{ij} = \Psi_A(u_i, u_j)$ e $b_{ij} = \Psi_B(v_i, v_j)$, em que u_i pertence a uma base de U e v_i pertence a uma base de V. Na sequência, pode-se observar que

$$\Phi(\vec{p}, \vec{q}, \vec{r}, \vec{s}) = \Phi(\vec{p}, \vec{q}, \vec{r}_0, \vec{s}_0) \cdot \Phi(\vec{p}_0, \vec{q}_0, \vec{r}, \vec{s}), \tag{4.34}$$

então, observando as Equações (4.32) e (4.33), pode-se redefinir a Equação (4.34) como

$$\Phi(\vec{p}, \vec{q}, \vec{r}, \vec{s}) = (\vec{p}^{\dagger} \cdot A \cdot \vec{q}) \cdot (\vec{r}^{\dagger} \cdot B \cdot \vec{s}), \tag{4.35}$$

que, usando a Equação (4.22), leva imediatamente à

$$(\vec{p} \otimes \vec{r})^{\dagger} C (\vec{q} \otimes \vec{s}) = (\vec{p} \otimes \vec{r})^{\dagger} (A \otimes B)(\vec{q} \otimes \vec{s}). \tag{4.36}$$

Por fim, como o produto tensorial de vetores abrange $\mathbb{C}^{m \cdot n}$, tem-se que $C = A \otimes B$.

Convém ressaltar que o procedimento aqui apresentado é bastante geral no sentido que não impõe nenhuma estrutura especial aos operadores lineares A, B e C. Embora tenha sido descrito o caso para duas partições, o procedimento pode ser facilmente estendido para uma quantidade arbitrária de forma direta. Por fim, a Equação (4.25) leva à um sistema com $(m \cdot n)^4$ equações (não necessariamente únicas em virtude da comutatividade do produto interno e produto de escalares) que devem ser verificadas simultaneamente para indicar a separabilidade de uma dada matriz.

4.4.2 Abordagens alternativas

Embora não necessariamente aplicáveis a dimensões arbitrárias, duas outras técnicas podem ser utilizadas para testar a separabilidade, a saber: a decomposição KAK e a preservação de entrelaçamento. Para uma breve descrição de ambos os procedimentos, será tomado o caso particular de uma matriz $C \in SU(4)$.

Para verificar se C pode ser escrito como $C = A \otimes B$, em que $A, B \in SU(2)$, usando a decomposição KAK deve-se buscar as condições nas quais os ângulos θ_1, θ_2 e θ_3, que parametrizam a parte não local de C, assumem simultaneamente o valor zero. Embora se chegue a sistemas com números reduzidos de equações, surgem outros problemas envolvendo o cálculo da GSVD (*Generalized Singular Value Decomposition*) e a incidência de falsos positivos. Ainda, uma vez que a decomposição KAK não é única, essa formulação pode ser entendida como um problema de otimização.

O procedimento que usa a preservação do entrelaçamento, que resguarda alguma similaridade com o descrito em [55], utiliza-se de uma proposição da teoria da informação quântica que afirma que o entrelaçamento de um estado de dois qubits $|\psi\rangle$, portanto $|\psi\rangle \in \mathbb{C}^4$, é uma grandeza que não pode ser alterada por um operador linear na forma $A \otimes B$. Novamente, embora se chegue a um sistema com menor número de equações, há incidência de falsos positivos, normalmente associados à família das portas *Swap's* (casos em que $\theta_1 = \theta_2 = \theta_3 = n \cdot \pi/4$ para $n \in \mathbb{Z}$). Tem-se ainda que essa abordagem não é facilmente aplicada ao caso geral, uma vez que não há formulações algébricas simples para a análise de entrelaçamento em dimensões e partições arbitrárias.

4.5 Preservação da separabilidade sob conjugação

Como primeiro exemplo de aplicação da análise de separabilidade serão encontradas as condições sobre $U \in SU(4)$ para a preservação da separabilidade de um elemento $V \in SU(2) \otimes SU(2)$ sob conjugação por U. Para tanto, será utilizada especificamente a técnica descrita na Seção 4.4, cuja relação principal está expressa na Equação (4.25). Começa-se pela descrição, feita na seção seguinte, da ação de conjugação.

4.5.1 A ação de conjugação

Uma vez de posse das parametrizações de $SU(4)$ apresentadas na Seção 4.2, pode-se descrever a ação de conjugação cuja manutenção da separabilidade será estudada. Neste trabalho, o interesse recai sobre o cenário no qual uma matriz U não separável conjuga uma matriz V separável gerando uma nova matriz V', também separável. Essa operação é expressa por

$$V' = U \cdot V \cdot U^{\dagger}, \tag{4.37}$$

portanto, usando a Equação (4.8) e a Equação (4.12), pode-se expressar essa relação como apresentado na Equação (4.38).

$$V' = \begin{bmatrix} \begin{pmatrix} e^{-\frac{i}{2}(a_1\cdot\sigma_{ZI}+b_1\cdot\sigma_{IZ})}. \\ e^{-\frac{i}{2}(a_2\cdot\sigma_{YI}+b_2\cdot\sigma_{IY})}. \\ e^{-\frac{i}{2}(a_3\cdot\sigma_{ZI}+b_3\cdot\sigma_{IZ})} \end{pmatrix}. \\ \begin{pmatrix} e^{i(\theta_1\cdot\sigma_{XX})}. \\ e^{i(\theta_2\cdot\sigma_{YY})}. \\ e^{i(\theta_3\cdot\sigma_{ZZ})} \end{pmatrix}. \\ \begin{pmatrix} e^{-\frac{i}{2}(c_1\cdot\sigma_{ZI}+d_1\cdot\sigma_{IZ})}. \\ e^{-\frac{i}{2}(c_2\cdot\sigma_{YI}+d_2\cdot\sigma_{IY})}. \\ e^{-\frac{i}{2}(c_3\cdot\sigma_{ZI}+d_3\cdot\sigma_{IZ})} \end{pmatrix} \end{bmatrix} \cdot \begin{pmatrix} e^{-\frac{i}{2}(\lambda_1\cdot\sigma_{ZI}+\omega_1\cdot\sigma_{IZ})}. \\ e^{-\frac{i}{2}(\lambda_2\cdot\sigma_{YI}+\omega_2\cdot\sigma_{IY})}. \\ e^{-\frac{i}{2}(\lambda_3\cdot\sigma_{ZI}+\omega_3\cdot\sigma_{IZ})} \end{pmatrix} \cdot \begin{bmatrix} \begin{pmatrix} e^{\frac{i}{2}(c3\cdot\sigma_{ZI}+d_3\cdot\sigma_{IZ})}. \\ e^{\frac{i}{2}(c2\cdot\sigma_{YI}+d_2\cdot\sigma_{IY})}. \\ e^{\frac{i}{2}(c1\cdot\sigma_{ZI}+d_1\cdot\sigma_{IZ})} \end{pmatrix}. \\ \begin{pmatrix} e^{-i(\theta_3\cdot\sigma_{ZZ})}. \\ e^{-i(\theta_2\cdot\sigma_{YY})}. \\ e^{-i(\theta_1\cdot\sigma_{XX})} \end{pmatrix}. \\ \begin{pmatrix} e^{\frac{i}{2}(a3\cdot\sigma_{ZI}+b_3\cdot\sigma_{IZ})}. \\ e^{\frac{i}{2}(a2\cdot\sigma_{YI}+b_2\cdot\sigma_{IY})}. \\ e^{\frac{i}{2}(a1\cdot\sigma_{ZI}+b_1\cdot\sigma_{IZ})} \end{pmatrix} \end{bmatrix}. \tag{4.38}$$

Por outro lado, o caso particular mais útil ao objetivo deste capítulo pode ser obtido usando a Equação (4.11) no lugar da Equação (4.12), ou seja, o caso de uma matriz estritamente não local. Desse modo, V' assume a forma

$$V' = \begin{bmatrix} e^{i(\theta_1\cdot\sigma_{XX})}\cdot e^{i(\theta_2\cdot\sigma_{YY})}\cdot e^{i(\theta_3\cdot\sigma_{ZZ})}. \\ \left(e^{-i/2(\lambda_1\cdot\sigma_{ZI}+\omega_1\cdot\sigma_{IZ})}\right). \\ \left(e^{-i/2(\lambda_2\cdot\sigma_{YI}+\omega_2\cdot\sigma_{IY})}\right). \\ \left(e^{-i/2(\lambda_3\cdot\sigma_{ZI}+\omega_3\cdot\sigma_{IZ})}\right). \\ e^{-i(\theta_3\cdot\sigma_{ZZ})}\cdot e^{-i(\theta_2\cdot\sigma_{YY})}\cdot e^{-i(\theta_1\cdot\sigma_{XX})} \end{bmatrix}. \tag{4.39}$$

Neste ponto tem-se tudo o necessário para a parte central das considerações sobre a preservação da separabilidade sob conjugação. Agora, pegando o caso particular[3] de $U \in SU(4)$, ter-se-á um sistema com, após eliminações elementares, 72 equações e, da Equação (4.39) vê-se, 9 variáveis reais. Este sistema resultante mostra-se complexo mesmo para ferramentas de computação simbólica, portanto, faz-se necessário buscar alternativas de simplificação do problema, tais como as relações uniparamétricas descritas no tópico a seguir.

4.5.2 Relações uniparamétricas em Z e Y

As relações uniparamétricas são casos particulares da Equação (4.39) em que ambas as partes local e não local dependem de apenas um ângulo, ou seja, cada parte é inteiramente determinada por um parâmetro real. Tais relações serão denotadas $U_{\mu_{I\upsilon}\mu^\dagger}$ ou $U_{\mu_{\upsilon I}\mu^\dagger}$, em que $\mu \in \{X, Y, Z\}$ e $\upsilon \in \{Y, Z\}$. Os valores de μ decorrem da decomposição KAK enquanto os valores de υ decorrem da decomposição[4] ZYZ.

[3] Embora seja usada no decorrer desta seção a parametrização de $SU(4)$, tem-se que o aqui desenvolvido é igualmente válido para elementos de $U(4)$, basicamente em razão da diferença de ambos (um fator global) ser irrelevante para o processo de conjugação.

[4] Embora seja usada a decomposição ZYZ, os resultados se aplicam para quaisquer decomposições relacionadas do tipo $\sigma_\upsilon\sigma_\mu\sigma_\upsilon$, em que $\upsilon, \mu \in \{X, Y, Z\}$ e $\sigma_\mu \neq \sigma_\upsilon$.

O conjunto de todas as relações uniparamétricas em Z e Y pode ser resumido nas equações

$$U_{\mu_{I\upsilon}\mu^\dagger} = e^{i(\theta\cdot\sigma_{\mu\mu})}\cdot e^{-i/2(\lambda\cdot\sigma_{I\upsilon})}\cdot e^{-i(\theta\cdot\sigma_{\mu\mu})} \tag{4.40}$$

$$U_{\mu_{\upsilon I}\mu^\dagger} = e^{i(\theta\cdot\sigma_{\mu\mu})}\cdot e^{-i/2(\lambda\cdot\sigma_{\upsilon I})}\cdot e^{-i(\theta\cdot\sigma_{\mu\mu})}. \tag{4.41}$$

Então, usando a técnica descrita na Seção 4.4 pode-se encontrar, para todos os casos associados, os sistemas soluções das Equações (4.40) e (4.41) que, simplificando-se, recaem todos na Equação (4.42).

$$\sin\left(\frac{\lambda}{2}\right)\cdot\sin(2\theta)\cdot\left[e^{(i\cdot\frac{\lambda}{2})}\cdot\sin^2(\theta)+e^{(-i\cdot\frac{\lambda}{2})}\cdot\cos^2(\theta)\right]=0. \tag{4.42}$$

As soluções para a Equação (4.42) podem ser divididas em dois grupos, a saber, quando se tem $\mu=\upsilon$ e quando se tem $\mu\neq\upsilon$. Devido às relações de comutação descritas na Equação (4.2), quando $\mu=\upsilon$ tem-se que a separabilidade será preservada para todo $\theta,\lambda\in\mathbb{R}$. Quando se tem $\mu\neq\upsilon$ as soluções são dadas por

$$(\theta,\lambda)=\left\{\left((2\cdot k_1+1)\cdot\frac{\pi}{4},\ k_2\cdot\pi\right);\left(k_1\cdot\frac{\pi}{2},\ x\right);(x,\ 2\cdot k_2\cdot\pi)\right\}, \tag{4.43}$$

em que $x\in\mathbb{R}$ e $k_1,k_2\in\mathbb{Z}$.

Dentre as soluções encontradas, cabe observar que para $\theta=k_1(\pi/2)$ a matriz $e^{i(\theta\cdot\sigma_{\mu\mu})}$ é separável e para $\lambda=2\cdot k_2\cdot\pi$ as matrizes $e^{-i/2(\lambda\cdot\sigma_{\upsilon I})}$ e $e^{-i/2(\lambda\cdot\sigma_{I\upsilon})}$ são a identidade. Portanto, ambos os casos são considerados soluções triviais, qualquer conjugação será separável. Com base nas construções expostas até este ponto já é possível enunciar o Lema 4.1.

Lema 4.1 (Conjugação Uniparamétrica)**.** *Toda ação de conjugação uniparamétrica da forma $U_{\mu_{I\upsilon}\mu^\dagger}$ ou $U_{\mu_{\upsilon I}\mu^\dagger}$, em que $\mu,\upsilon\in\{X,Y,Z\}$, preserva a separabilidade de $e^{-i/2(\lambda\cdot\sigma_{I\upsilon})}$ ou $e^{-i/2(\lambda\cdot\sigma_{\upsilon I})}$ sempre que $\mu=\upsilon$, ou quando $\mu\neq\upsilon$ com $\theta=(2k_1+1)\frac{\pi}{4}$ e $\lambda=k_2\pi$, em que $k_1,k_2\in\mathbb{Z}$.*

Demonstração. Consequência direta das relações de comutação expressas na Equação (4.2) e das soluções da Equação (4.42). □

4.5.3 Relações de preservação de grupo

Na Seção 4.5.2 foram discutidas as relações de conjugação uniparamétricas e ficou demonstrado que, no caso mais restrito, a preservação da separabilidade ocorre apenas quando a matriz local pode ser expressa usando o ângulo $\lambda=k\pi$ e a matriz não local pode ser expressa usando o ângulo $\theta=(2k+1)\frac{\pi}{4}$, portanto, será útil entender o comportamento de operações sobre matrizes que assumem essas formas.

O objetivo principal é demonstrar a formação de grupos, isso permitirá utilizar algumas importantes operações mais adiante. Desse modo, são enunciados os Lemas (4.2) e (4.3).

Lema 4.2 (Preservação Grupo Local)**.** *Toma-se G como o conjunto das matrizes da forma $e^{-i/2(\lambda\cdot\sigma_{Iv})}$ ou $e^{-i/2(\lambda\cdot\sigma_{vI})}$ com $\lambda = k\cdot\pi$, em que $v \in \{X,Y,Z\}$ e $k \in \mathbb{Z}$, então $(G,*)$, em que a operação $*$ é a multiplicação usual de matrizes, forma um grupo.*

Demonstração. Das Equações (4.4)-(4.8) se sabe que $e^{-i/2(\lambda\cdot\sigma_{Iv})} = \left(I \otimes e^{-i/2(\lambda\cdot\sigma_v)}\right)$ e, de modo análogo, que $e^{-i/2(\lambda\cdot\sigma_{vI})} = \left(e^{-i/2(\lambda\cdot\sigma_v)} \otimes I\right)$. Os casos particulares em Y e Z são

$$U_x = e^{-i/2(\lambda\cdot\sigma_X)} = \begin{bmatrix} \cos(\lambda\cdot\frac{\pi}{2}) & -\sin(\lambda\cdot\frac{\pi}{2})i \\ -\sin(\lambda\cdot\frac{\pi}{2})i & \cos(\lambda\cdot\frac{\pi}{2}) \end{bmatrix} \tag{4.44a}$$

$$U_y = e^{-i/2(\lambda\cdot\sigma_Y)} = \begin{bmatrix} \cos(\lambda\cdot\frac{\pi}{2}) & -\sin(\lambda\cdot\frac{\pi}{2}) \\ \sin(\lambda\cdot\frac{\pi}{2}) & \cos(\lambda\cdot\frac{\pi}{2}) \end{bmatrix} \tag{4.44b}$$

$$U_z = e^{-i/2(\lambda\cdot\sigma_Z)} = \begin{bmatrix} (-1)^{-\frac{\lambda}{2}} & 0 \\ 0 & (-1)^{\frac{\lambda}{2}} \end{bmatrix} \tag{4.44c}$$

e com álgebra elementar percebe-se que U_x, U_y e U_z se tornam $\pm I$ quando k é par. Por outro lado, quando k é ímpar, U_x, U_y e U_z assumem os valores

$$U_x = \pm ZY = \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \tag{4.45a}$$

$$U_y = \pm XZ = \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tag{4.45b}$$

$$U_z = \pm XY = \pm \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}. \tag{4.45c}$$

Portanto, como U_x, U_y e U_z pertencem ao grupo de Pauli, qualquer produto matriciais envolvendo-os permanecerá no grupo de Pauli, consequentemente, em função de $k\cdot\pi$. □

Lema 4.3 (Preservação Grupo Não Local)**.** *Toma-se G como o conjunto das matrizes da forma $e^{-i/2(\lambda\cdot\sigma_{Iv})}$ ou $e^{-i/2(\lambda\cdot\sigma_{vI})}$ com $\lambda = k\cdot\pi$, em que $v \in \{X,Y,Z\}$ e $k \in \mathbb{Z}$, e H como o conjunto de matrizes da forma $e^{i\left(k\cdot\frac{\pi}{4}\cdot\sigma_{\mu\mu}\right)}$, em que $\mu \in \{X,Y,Z\}$ e $k \in \mathbb{Z}$, então $(G,\dagger)$, na qual a operação $\dagger$ é a conjugação de G por H $(h\cdot g\cdot h^\dagger)$, forma um grupo.*

Demonstração. De modo similar ao descrito na demonstração do Lema 4.2, a preservação do grupo é verificada de forma trivial. □

4.5.4 Teorema da separabilidade sob conjugação

Uma vez que foram apresentadas todas as ferramentas necessárias, pode-se agora chegar a um dos resultados principais deste capítulo, o teorema da preservação da separabilidade sob conjugação enunciado a seguir.

Teorema 4.2 (Separabilidade Sob Conjugação)**.** *Dada uma matriz U não local em $U(4)$ com decomposição KAK $U = e^{i\theta_0} \cdot (U_A \otimes U_B) \cdot U_{NL} \cdot (U_C \otimes U_D)$, com $U_{NL} = e^{i(\theta_{XX} \cdot \sigma_{XX})} . e^{i(\theta_{YY} \cdot \sigma_{YY})} . e^{i(\theta_{ZZ} \cdot \sigma_{ZZ})}$ em que $\theta_{\mu\mu}$ são ditos serem os ângulos não locais, e uma matriz local $L = (L_1 \otimes L_2)$, L terá sua separabilidade preservada na conjugação por U, ou seja, $L' = ULU^\dagger = (L'_1 \otimes L'_2)$, quando os ângulos não locais $\theta_{\mu\mu}$ não nulos forem $(2k_\mu + 1)\pi/4$ e os ângulos locais λ_υ oriundos de $(U_C \otimes U_D) \cdot L \cdot (U_C^\dagger \otimes U_D^\dagger)$ forem $n \cdot \pi$, em que $k, n \in \mathbb{Z}$, $\mu, \upsilon \in \{X, Y, Z\}$. Essas condições podem ser relaxadas em casos decorrentes de relações de comutação, tais como: I) se existir apenas um ângulo não local $\theta_{\mu\mu}$ diferente de zero, então o ângulo local correspondente λ_μ pode assumir qualquer valor real; II) quando todos os ângulos não locais $\theta_{\mu\mu}$ forem iguais a $(2k_\mu + 1)\pi/4$, então todos os ângulos locais λ_υ podem assumir quaisquer valores reais.*

Demonstração. Partindo de um caso específico, tem-se na Equação (4.11) a forma geral de uma matriz estritamente não local e na Equação (4.39) sua ação de conjugação que, usando as relações de comutação da Equação (4.2), pode ser escrita como

$$\begin{gathered} e^{i\left(k_1 \cdot \frac{\pi}{4} \cdot \sigma_{XX}\right)} . e^{i\left(k_3 \cdot \frac{\pi}{4} \cdot \sigma_{ZZ}\right)} . e^{i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . \\ \left(e^{-i/2(\lambda_1 \cdot \sigma_{ZI} + \omega_1 \cdot \sigma_{IZ})}\right) . \\ \left(e^{-i/2(\lambda_2 \cdot \sigma_{YI} + \omega_2 \cdot \sigma_{IY})}\right) . \\ \left(e^{-i/2(\lambda_3 \cdot \sigma_{ZI} + \omega_3 \cdot \sigma_{IZ})}\right) . \\ e^{-i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . e^{-i\left(k_3 \cdot \frac{\pi}{4} \cdot \sigma_{ZZ}\right)} . e^{-i\left(k_1 \cdot \frac{\pi}{4} \cdot \sigma_{XX}\right)} . \end{gathered} \tag{4.46}$$

Então, reagrupando e inserindo $I = e^{-i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . e^{i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)}$ entre alguns dos termos tem-se

$$\begin{gathered} e^{i\left(k_1 \cdot \frac{\pi}{4} \cdot \sigma_{XX}\right)} . e^{i\left(k_3 \cdot \frac{\pi}{4} \cdot \sigma_{ZZ}\right)} . \\ e^{i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} \left(e^{-i/2(\lambda_1 \cdot \sigma_{ZI} + \omega_1 \cdot \sigma_{IZ})}\right) . e^{-i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . \\ e^{i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . \left(e^{-i/2(\lambda_2 \cdot \sigma_{YI} + \omega_2 \cdot \sigma_{IY})}\right) . e^{-i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . \\ e^{i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . \left(e^{-i/2(\lambda_3 \cdot \sigma_{ZI} + \omega_3 \cdot \sigma_{IZ})}\right) . e^{-i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . \\ e^{-i\left(k_3 \cdot \frac{\pi}{4} \cdot \sigma_{ZZ}\right)} . e^{-i\left(k_1 \cdot \frac{\pi}{4} \cdot \sigma_{XX}\right)} \end{gathered} \tag{4.47}$$

em que cada uma das conjugações por $e^{i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)}$ podem ser escritas como

$$e^{i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} . e^{-i/2(\lambda_1 \cdot \sigma_{\upsilon I} + \omega_1 \cdot \sigma_{I\upsilon})} . e^{-i\left(k_2 \cdot \frac{\pi}{4} \cdot \sigma_{YY}\right)} \tag{4.48}$$

que, novamente usando as relações de comutação e inserindo I, resulta em

$$e^{i\left(k_2\cdot\frac{\pi}{4}\cdot\sigma_{YY}\right)}\cdot e^{-i/2(\lambda_1\cdot\sigma_{\upsilon I})}\cdot e^{-i\left(k_2\cdot\frac{\pi}{4}\cdot\sigma_{YY}\right)}\cdot e^{i\left(k_2\cdot\frac{\pi}{4}\cdot\sigma_{YY}\right)}\cdot e^{-i/2(\omega_1\cdot\sigma_{I\upsilon})}\cdot e^{-i\left(k_2\cdot\frac{\pi}{4}\cdot\sigma_{YY}\right)}. \quad (4.49)$$

Agora, deve-se observar na Equação (4.49) que em decorrência do Lema 4.1 cada uma das duas conjugações será separável. Além disso, pelo Lema 4.3 se tem que cada um dos resultados será uma matriz cuja fatoração na decomposição ZYZ se dará com os ângulos locais em função de $n\cdot\pi$, em que $n\in\mathbb{Z}$. Por fim, de acordo com o Lema 4.2 o produto destes resultados também preservará a forma em função de $n\cdot\pi$. Deste modo, o mesmo procedimento pode ser repetido para as demais partes não locais ($e^{i\left(k_1\cdot\frac{\pi}{4}\cdot\sigma_{XX}\right)}$ e $e^{i\left(k_3\cdot\frac{\pi}{4}\cdot\sigma_{ZZ}\right)}$) na Equação (4.46) para demonstrar que, nas condições previstas pelo teorema, o resultado será sempre uma matriz separável.

Para finalizar, faz-se necessário considerar o caso de uma matriz $U(4)$ não local arbitrária, ou seja, uma matriz $U=e^{i\theta_0}\cdot(U_A\otimes U_B)\cdot U_{NL}\cdot(U_C\otimes U_D)$. Para tanto, convém inicialmente observar que a parte local à esquerda de U não influencia no processo por ficar fora da conjugação, apenas a parte local à direita será considerada. Facilmente se nota que, mesmo neste caso, todos os lemas utilizados permanecem válidos. Apenas não será utilizada somente a matriz sendo conjugada mas também a parte local à direita da matriz não local, ou seja, $(U_C\otimes U_D)\cdot L\cdot(U_C^\dagger\otimes U_D^\dagger)$ deverá resultar em uma matriz decomposta em função de $n\cdot\pi$, ou em uma das condições de relaxamento do Teorema 4.2. □

4.6 Forma geral do grupo de Clifford

Como segundo exemplo de aplicação da análise de separabilidade será demonstrada a forma geral de um elemento do grupo de Clifford. Um resultado bastante conhecido na literatura é que $C=\langle C_{NOT},H,S\rangle$, o grupo de Clifford, preserva $P=\langle X,Y,Z\rangle$, o grupo de Pauli, sob conjugação, portanto, para todo $c\in C$ e $p\in P$, $c\cdot p\cdot c^\dagger\in P$. Entretanto, ainda que largamente difundido na literatura não é conhecida uma fórmula algébrica que defina a forma geral de uma matriz pertencente ao grupo de Clifford, resolver esta questão é o objetivo desta seção.

4.6.1 Preservação de P_1

Denota-se P_n e C_n, respectivamente, os grupos de Pauli e Clifford cujos elementos pertençam ao grupo $U(2^n)$. Deste modo, inicia-se enunciando o Lema 4.4 acerca da preservação do grupo de Pauli sob conjugação por matrizes em $U(2)$.

Lema 4.4 (Preservação P_1)**.** *Seja L uma matriz arbitrária pertencente ao grupo $U(2)$ na forma $e^{-i/2\cdot\gamma}\cdot e^{-i/2(\lambda_1\cdot\sigma_\mu)}\cdot e^{-i/2(\lambda_2\cdot\sigma_\upsilon)}\cdot e^{-i/2(\lambda_3\cdot\sigma_\mu)}$, em que $\mu,\upsilon\in\{X,Y,Z\}$ e $\mu\neq\upsilon$, e P um elemento do grupo de Pauli, tem-se que $L\cdot P\cdot L^\dagger=P'$, em que P' é também um elemento do grupo de Pauli, sempre que os ângulos locais (λ_i) de L forem $k\cdot\frac{\pi}{2}$ com $k\in\mathbb{Z}$.*

Demonstração. O caso particular uniparamétrico da estrutura de preservação do grupo de Pauli pela conjugação por elementos de $U(2)$ é descrita pelo sistema de equações gerado por

$$\left(e^{-i/2(\lambda\cdot\sigma_\mu)}\right)\cdot\sigma_\upsilon\cdot\left(e^{i/2(\lambda\cdot\sigma_\mu)}\right)=\sigma_\eta\quad\forall\quad\mu,\upsilon,\eta\in\{X,Y,Z\},\tag{4.50}$$

cujas soluções triviais ocorrem para $\lambda=0$ ou $\mu=\upsilon$ e as não triviais ocorrem para $\mu\neq\upsilon\neq\eta$, $\lambda=k\cdot\frac{\pi}{2}$ e $k\in\mathbb{Z}$. Assim sendo, fica fácil perceber que para o caso geral representado por

$$\left(e^{-i/2(\lambda_1\cdot\sigma_\mu)}\cdot e^{-i/2(\lambda_2\cdot\sigma_\upsilon)}\cdot e^{-i/2(\lambda_3\cdot\sigma_\mu)}\right)\cdot\sigma_\upsilon\cdot\left(e^{i/2(\lambda_3\cdot\sigma_\mu)}\cdot e^{i/2(\lambda_2\cdot\sigma_\upsilon)}\cdot e^{i/2(\lambda_1\cdot\sigma_\mu)}\right)=\sigma_\eta\tag{4.51}$$

tem-se o mesmo conjunto de soluções da Equação (4.50). Isso implica dizer que qualquer matriz fatorável conforme proposto pelo Lema 4.4 preserva o grupo P_1 sob conjugação. □

4.6.2 Preservação de P_n

Sabe-se [63] que o grupo C_n pode ser construído, usando o produto tensorial e o produto usual de matrizes, a partir de C_1 e C_2. Portanto, uma vez que a forma de C_1 está, à um fator de fase global, descrita no Lema 4.4, o passo seguinte é descrever a forma de C_2. Assim sendo, usando os lemas e teoremas apresentados no decorrer do capítulo já é possível enunciar a forma geral de um elemento do grupo de Clifford, conforme pode ser visto no Teorema 4.3.

Teorema 4.3 (Forma Geral de Clifford)**.** *Toda matriz $U=(L_1\otimes L_2)\cdot U_{NL}\cdot(R_1\otimes R_2)$, elemento de $U(4)$, pertence ao grupo de Clifford se, e somente se, puder ser decomposta na forma*

$$\begin{pmatrix} e^{-\frac{i}{2}(\alpha_1\cdot\sigma_{\mu I}+\beta_1\cdot\sigma_{I\mu})}. \\ e^{-\frac{i}{2}(\alpha_2\cdot\sigma_{\upsilon I}+\beta_2\cdot\sigma_{I\upsilon})}. \\ e^{-\frac{i}{2}(\alpha_3\cdot\sigma_{\mu I}+\beta_3\cdot\sigma_{I\mu})} \end{pmatrix}\cdot e^{i\frac{\pi}{4}(k_\eta\cdot\sigma_{\eta\eta})}\cdot e^{i\frac{\pi}{4}(k_\upsilon\cdot\sigma_{\upsilon\upsilon})}\cdot e^{i\frac{\pi}{4}(k_\mu\cdot\sigma_{\mu\mu})}\cdot\begin{pmatrix} e^{-\frac{i}{2}(\lambda_1\cdot\sigma_{\mu I}+\omega_1\cdot\sigma_{I\mu})}. \\ e^{-\frac{i}{2}(\lambda_2\cdot\sigma_{\upsilon I}+\omega_2\cdot\sigma_{I\upsilon})}. \\ e^{-\frac{i}{2}(\lambda_3\cdot\sigma_{\mu I}+\omega_3\cdot\sigma_{I\mu})} \end{pmatrix},\tag{4.52}$$

em que os ângulos locais $\alpha_i,\beta_i,\lambda_i,\omega_i$ são $n\cdot\pi/2$ com $n\in\mathbb{Z}$ e os fatores dos ângulos não locais $k_i\in\mathbb{Z}$, com $\mu,\upsilon,\eta\in\{X,Y,Z\}$ e $\eta\neq\upsilon\neq\mu$.

Demonstração. O primeiro passo é provar que se U estiver fatorada conforme proposto no teorema ela estará em Clifford. Pois bem, está na definição do grupo de Clifford que este preserva o grupo de Pauli sob conjugação, portanto, tem-se que

$$U\cdot(\sigma_\mu\otimes\sigma_\upsilon)\cdot U^\dagger=(\sigma_\eta\otimes\sigma_\nu)\tag{4.53}$$

para todo $\mu,\upsilon,\eta,\nu\in\{I,X,Y,Z\}$. Disto, percebe-se como consequência que U deve preservar a separabilidade de $(\sigma_\mu\otimes\sigma_\upsilon)$, então U deve atender aos critérios do Teorema 4.2 segundo o qual para

$$(L_1\otimes L_2)\cdot U_{NL}\cdot(R_1\otimes R_2)\cdot(\sigma_\mu\otimes\sigma_\upsilon)\cdot(R_1\otimes R_2)^\dagger\cdot U_{NL}^\dagger\cdot(L_1\otimes L_2)^\dagger\tag{4.54}$$

resultar em uma matriz separável tem-se que U_{NL} deve ter seus ângulos não locais como múltiplos ímpares de $\pi/4$ e $(R_1 \otimes R_2) \cdot (\sigma_\mu \otimes \sigma_\upsilon) \cdot (R_1 \otimes R_2)^\dagger$ deve possuir uma fatoração na qual seus ângulos locais sejam múltiplos inteiros de π. Toda matriz de Pauli, à um fator de fase global, possui fatoração com ângulos locais múltiplos inteiros de π, portanto, usando o Lema 4.4 vê-se que $(R_1 \otimes R_2) \cdot (\sigma_\mu \otimes \sigma_\upsilon) \cdot (R_1 \otimes R_2)^\dagger$ atenderá ao critério de separabilidade requerido pelo Teorema 4.2 e, assim sendo,

$$U_{NL} \cdot (R_1 \otimes R_2) \cdot (\sigma_\mu \otimes \sigma_\upsilon) \cdot (R_1 \otimes R_2)^\dagger \cdot U_{NL}^\dagger \tag{4.55}$$

será uma matriz separável fatorável com ângulos locais múltiplos de π. Para o caso particular, aqui permitido, de k_i assumir valores pares (incluindo o zero), U_{NL} assume uma forma separável fatorável com ângulos locais múltiplos de π (ou a própria identidade). Entretanto, usando novamente o Lema 4.4 vê-se, de maneira análoga ao caso anterior, que a Equação (4.55) resulta em uma matriz de Pauli, assim como sua subsequente conjugação por $(L_1 \otimes L_2)$, mostrada na Equação (4.54), também resultará. Convém ressaltar dois casos triviais: I) Quando todos os fatores k_i forem zeros então U_{NL} assume a forma da identidade e a preservação de Pauli decorre do Lema 4.4 em torno de $(L_1 \otimes R_1)$ e $(L_2 \otimes R_2)$; II) Quando da condição de relaxamento II do Teorema 4.2 e U_{NL} assume a forma de uma SWAP, então novamente a preservação de Pauli decorre do Lema 4.4 em torno de $(L_1 \otimes R_2)$ e $(L_2 \otimes R_1)$.

Isso é plenamente suficiente para afirmar que, uma vez que existe uma fatoração de U na forma proposta ela estará em Clifford. O segundo, e último, passo é provar a relação de volta, ou seja, que se U está em Clifford então existe uma fatoração da forma proposta. Da teoria de grupos se sabe que qualquer elemento do grupo pode ser obtido pelo produto (nesse caso específico o produto se refere ao produto usual de matrizes) de seus geradores. Sabe-se ainda que o grupo de Clifford tem como geradores $\{C_{NOT}, H, S\}$, cujas fatorações são

$$C_{NOT} = \begin{pmatrix} e^{-\frac{i}{2}\left(-\frac{3\pi}{2}\cdot\sigma_{ZI}+\frac{\pi}{2}\cdot\sigma_{IZ}\right)}. \\ e^{-\frac{i}{2}\left(\frac{3\pi}{2}\cdot\sigma_{YI}+\frac{3\pi}{2}\cdot\sigma_{IY}\right)}. \\ e^{-\frac{i}{2}\left(-\frac{\pi}{2}\cdot\sigma_{IZ}\right)} \end{pmatrix} \cdot \left(e^{i\pi/4} \cdot e^{i(\pi/4\cdot\sigma_{XX})}\right) \cdot \begin{pmatrix} e^{-\frac{i}{2}(\pi\cdot\sigma_{IZ})}. \\ e^{-\frac{i}{2}\left(\frac{\pi}{2}\cdot\sigma_{YI}\right)}. \\ e^{-\frac{i}{2}(-2\pi\cdot\sigma_{ZI}-\pi\cdot\sigma_{IZ})} \end{pmatrix} \tag{4.56a}$$

$$H = e^{i\frac{\pi}{2}} \cdot e^{-\frac{i}{2}\left(\frac{\pi}{2}\cdot\sigma_Y\right)} \cdot e^{-\frac{i}{2}(\pi\cdot\sigma_Z)} \tag{4.56b}$$

$$S = e^{i\frac{\pi}{4}} \cdot e^{-\frac{i}{2}(\pi\cdot\sigma_Z)} \cdot e^{-\frac{i}{2}\left(-\frac{\pi}{2}\cdot\sigma_Y\right)} \cdot e^{-\frac{i}{2}(-\pi\cdot\sigma_Z)}, \tag{4.56c}$$

portanto, como os geradores estão na forma proposta no teorema e todo elemento do grupo é um produto destes geradores que manterão, quando em $U(2)$, a forma prevista pelo Lema 4.4, tem-se que a forma descrita na Equação (4.52) gera todo o grupo de Clifford, como se queria demonstrar. □

4.6.3 Análise de um caso particular

Para fins meramente didáticos, tomar-se-á o caso particular de $U = \left(I \otimes e^{\frac{-i}{2}(\frac{\pi}{6}\sigma_Z)}\right) \cdot e^{i\frac{\pi}{4}\sigma_{ZZ}} \cdot \left(I \otimes e^{\frac{-i}{2}(\frac{\pi}{3}\sigma_Z)}\right)$ para se tecer algumas explicações. Para tanto, faz-se a pergunta: estaria U no grupo de Clifford? Uma análise apressada pode levar à falsa conclusão de que ela não

estaria em Clifford por não estar fatorada na forma prevista pelo Teorema 4.3. O ponto central da questão é que, embora U não esteja fatorada na forma prevista existe uma fatoração de U compatível com a forma geral de Clifford apresentada pelo teorema, portanto U está de fato em Clifford. Como $e^{i\frac{\pi}{4}\sigma_{ZZ}}$ comuta com $\left(I \otimes e^{\frac{-i}{2}\theta\sigma_Z}\right)$ então existirão infinitas decomposições para U, entretanto, como $\pi/6 + \pi/3 = \pi/2$ há uma fatoração na forma descrita pelo teorema.

4.7 Conclusão

Neste capítulo, após a introdução de alguns tópicos elementares tais como relações de comutações e fatorações de matrizes em $U(2)$ e $U(4)$, foi revisada a teoria acerca das formas bilineares. Usando essas ferramentas foi descrita uma abordagem capaz de verificar a separabilidade de uma matriz arbitrária e, como aplicações, foram apontadas as condições para a preservação da separabilidade sob conjugação e a forma geral do grupo de Clifford. Outras aplicações serão apresentadas em capítulos posteriores desta tese.

Capítulo 5

O papel da base de medição na teleportação de estados quânticos

Resumo

Neste capítulo é discutido o procedimento pelo qual a teleportação de estados quânticos pode ser obtida através de circuitos compostos de bases de medição arbitrárias e, ao final, serão analisados alguns casos particulares.

5.1 Introdução

Conforme tradicionalmente descrita, a teleportação de um estado quântico arbitrário entre duas partes que compartilham um par EPR é realizada através de uma medição na base de Bell do qubit a ser teleportado juntamente com um dos qubits integrantes do par EPR. O resultado da medição é então enviado classicamente à outra parte que, com base neste, realiza a correção adequada utilizando portas de Pauli de um qubit.

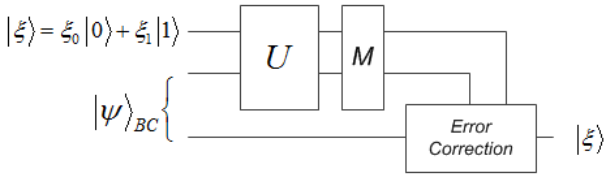
Este procedimento foi detalhadamente descrito no Capítulo 2, no entanto, conforme foi apresentado em [64] e [65], é possível utilizar bases arbitrárias para executar o protocolo de teleportação para um estado quântico arbitrário de um qubit. Na sequância será revisitado esse resultado usando um procedimento algébrico, ligeiramente diferente dos trabalhos citados, que será útil na construção da extensão do protocolo de teleportação de portas quânticas apresentado no Capítulo 6.

O restante deste capítulo está organizado da seguinte forma: A Seção 5.2 mostra a construção analítica que proporcionará o entendimento do papel da base de medição na teleportação de estados quânticos. Na Seção 5.3 tem-se a análise de alguns casos particulares e, por fim, a Seção 5.4 apresenta as conclusões.

5.2 Teleportação parametrizável

Para proceder com a investigação pretendida, no lugar do circuito comumente descrito na literatura será utilizado uma versão parametrizável em vários aspectos, a saber: o estado recurso da teleportação ($|\Psi\rangle_{AB}$), a porta utilizada como preparação para medição (U), a base de medição (M) e as portas de correção. Este circuito parametrizável pode ser visto na Figura 5.1.

Figura 5.1: Circuito parametrizável para teleportação de estados quânticos.



Uma vez descrito o circuito, pode-se analisar a evolução do estado quântico através dele, conforme iniciado na Equação (5.1), em que V_i é uma operação de um qubit associada à correção de erro.

$$(U \otimes I)\,|\xi\rangle_A\,|\psi\rangle_{BC} = \sum_{i=1}^{4} \sqrt{p_i}\,|\beta_i\rangle_{AB}\,V_i\,|\xi\rangle_C\,. \tag{5.1}$$

Convém ressaltar que, para uma teleportação com sucesso deve ser observada a condição $\langle\beta_i|\beta_j\rangle = \delta_{ij}$, pois $\{|\beta_1\rangle, |\beta_2\rangle, |\beta_3\rangle, |\beta_4\rangle\}$ formam a base de medição. Assim, fazendo o produto interno de $\langle\beta_j|$ com a Equação (5.1) tem-se

$$\langle\beta_j|\,(U \otimes I)\,|\xi\rangle\,|\psi\rangle = \sum_{i=1}^{4} \sqrt{p_i}\,\langle\beta_j|\beta_i\rangle\,V_i\,|\xi\rangle \tag{5.2}$$

que, removendo-se os casos ortogonais chega-se à

$$\langle\beta_j|\,(U \otimes I)\,|\xi\rangle\,|\psi\rangle = \sqrt{p_j}V_j\,|\xi\rangle\,. \tag{5.3}$$

Na sequância, usa-se a forma geral de um estado quântico de dois qubits, portanto, substitui-se $|\Psi\rangle$ por $\sigma_{00}\,|00\rangle + \sigma_{01}\,|01\rangle + \sigma_{10}\,|10\rangle + \sigma_{11}\,|11\rangle$ na Equação (5.3) e se obtém

$$\langle\beta_j|\,(U \otimes I)\,(\sigma_{00}\,|\xi\rangle\,|00\rangle + \sigma_{01}\,|\xi\rangle\,|01\rangle + \sigma_{10}\,|\xi\rangle\,|10\rangle + \sigma_{11}\,|\xi\rangle\,|11\rangle) = \sqrt{p_j}V_j\,|\xi\rangle\,. \tag{5.4}$$

Fazendo a distribuição e reorganizando os termos semelhantes chega-se à

$$\begin{bmatrix} (\sigma_{00}\,\langle\beta_j\,|U|\,\xi 0\rangle + \sigma_{10}\,\langle\beta_j\,|U|\,\xi 1\rangle)\,|0\rangle + \\ (\sigma_{01}\,\langle\beta_j\,|U|\,\xi 0\rangle + \sigma_{11}\,\langle\beta_j\,|U|\,\xi 1\rangle)\,|1\rangle \end{bmatrix} = \sqrt{p_j}V_j\,|\xi\rangle\,. \tag{5.5}$$

Agora, substituindo

$$|\xi\rangle = \xi_0 |0\rangle + \xi_1 |1\rangle , \tag{5.6}$$

$$U |\xi 0\rangle = \xi_0 U |00\rangle + \xi_1 U |10\rangle , \tag{5.7}$$

$$U |\xi 1\rangle = \xi_0 U |01\rangle + \xi_1 U |11\rangle , \tag{5.8}$$

$$V_j = \begin{bmatrix} v_{11}^j & v_{12}^j \\ v_{21}^j & v_{22}^j \end{bmatrix} , \tag{5.9}$$

na Equação (5.5), obtém-se

$$\begin{aligned} &\left[\begin{array}{l} \xi_0 \left(\sigma_{00} \langle\beta_j |U| 00\rangle + \sigma_{10} \langle\beta_j |U| 01\rangle\right) + \\ \xi_1 \left(\sigma_{00} \langle\beta_j |U| 10\rangle + \sigma_{10} \langle\beta_j |U| 11\rangle\right) \end{array} \right] |0\rangle + \\ &\left[\begin{array}{l} \xi_0 \left(\sigma_{01} \langle\beta_j |U| 00\rangle + \sigma_{11} \langle\beta_j |U| 01\rangle\right) + \\ \xi_1 \left(\sigma_{01} \langle\beta_j |U| 10\rangle + \sigma_{11} \langle\beta_j |U| 11\rangle\right) \end{array} \right] |1\rangle \end{aligned} = \sqrt{p_j} \left[\begin{array}{l} \left(\xi_0 v_{11}^j + \xi_1 v_{12}^j\right) |0\rangle + \\ \left(\xi_0 v_{21}^j + \xi_1 v_{22}^j\right) |1\rangle \end{array} \right] . \tag{5.10}$$

Com isso, a matriz V_j pode ser obtida diretamente a partir da Equação (5.10). Fazendo $U_{xy} = U |xy\rangle \ \forall \ x, y \in \{0, 1\}$ tem-se que

$$V_j = \frac{1}{\sqrt{p_j}} \begin{bmatrix} \sigma_{00} \langle\beta_j|U_{00}\rangle + \sigma_{10} \langle\beta_j|U_{01}\rangle & \sigma_{00} \langle\beta_j|U_{10}\rangle + \sigma_{10} \langle\beta_j|U_{11}\rangle \\ \sigma_{01} \langle\beta_j|U_{00}\rangle + \sigma_{11} \langle\beta_j|U_{01}\rangle & \sigma_{01} \langle\beta_j|U_{10}\rangle + \sigma_{11} \langle\beta_j|U_{11}\rangle \end{bmatrix} . \tag{5.11}$$

A Equação (5.11) mostra a relação entre a porta U de dois qubits usada como preparação para medição, as portas de correção dadas por $V_j^\dagger$ e a base de medição utilizada no processo de teleportação. A Equação (5.11) pode convenientemente ser reescrita como

$$V_j = \frac{1}{\sqrt{p_j}} \sigma \beta_j = \frac{1}{\sqrt{p_j}} \begin{bmatrix} \sigma_{00} & \sigma_{10} \\ \sigma_{01} & \sigma_{11} \end{bmatrix} \begin{bmatrix} \langle\beta_j|U_{00}\rangle & \langle\beta_j|U_{10}\rangle \\ \langle\beta_j|U_{01}\rangle & \langle\beta_j|U_{11}\rangle \end{bmatrix} . \tag{5.12}$$

É largamente sabido que uma teleportação só é possível com a existência de entrelaçamento, isso fica evidenciado na Equação (5.12). Uma vez que V_j deve pertencer a $SU(2)$ tem-se que $|det(V_j)| = 1$, portanto, o determinante da matriz σ tem de ser diferente de zero. Faz-se interessante observar que $|det(\sigma)|^2$ é numericamente igual à uma medida de entrelaçamento (concorrência) para estados puros de dois qubits, assim sendo, o estado de dois qubits

usado como recurso na teleportação não pode ser desentrelaçado.

Agora, considerando o caso no qual os resultados obtidos pela medição são equiprováveis, $p_j = 1/4$, e o estado usado como recurso é maximamente entrelaçado, $\sigma_{00} = \sigma_{11} = 1/\sqrt{2}$ e $\sigma_{01} = \sigma_{10} = 0$, a Equação (5.12) pode ser simplificada para

$$V_j = \sqrt{2} \begin{bmatrix} \langle \beta_j | U_{00} \rangle & \langle \beta_j | U_{10} \rangle \\ \langle \beta_j | U_{01} \rangle & \langle \beta_j | U_{11} \rangle \end{bmatrix}. \tag{5.13}$$

A Equação (5.13) fornece uma visão clara e objetiva do relacionamento entre os parâmetros enunciados no circuito e será tomada como base para a análise de alguns casos particulares.

5.3 Análise de casos particulares

Pode ser facilmente verificado que dada uma porta U e a base de medição $M = \{(|U_{00}\rangle \pm |U_{11}\rangle)/\sqrt{2}, (|U_{01}\rangle \pm |U_{10}\rangle)/\sqrt{2}\}$, as matrizes de correção $V_j^\dagger$ são as matrizes de Pauli. Convém ressaltar que isso é válido para qualquer que seja U e não apenas para o cenário tradicionalmente descrito na literatura que utiliza $U = (H \otimes I) \cdot C_{NOT}$ e M sendo a base canônica. Por exemplo, se para este mesmo U a base M for a base de Bell, as matrizes $V_j^\dagger$ de correção são as descritas na Equação (5.14).

$$V_1^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, V_2^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, V_3^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, V_4^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}. \tag{5.14}$$

De maneira análoga, usando a base de Bell mas com $U = (H \otimes I) \cdot C_{\pi/8}$, tem-se como matrizes $V_j^\dagger$ de correção as apresentadas na Equação (5.15).

$$V_1^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -\frac{(1-i)}{\sqrt{2}} \end{bmatrix}, V_2^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & \frac{(1-i)}{\sqrt{2}} \end{bmatrix}, V_3^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & \frac{(1-i)}{\sqrt{2}} \end{bmatrix}, V_4^\dagger = \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ 1 & \frac{(1-i)}{\sqrt{2}} \end{bmatrix}. \tag{5.15}$$

Agora, para um exemplo sem a utilização da base de Bell pode-se fazer $M = \{(|U_{00}\rangle \mp e^{i \cdot \frac{\pi}{4}} |U_{11}\rangle)/\sqrt{2}, (|U_{01}\rangle \mp e^{i \cdot \frac{\pi}{4}} |U_{10}\rangle)/\sqrt{2}\}$, em que a ação da porta U na base canônica é expressa por:

$$U_{x0} = U|x0\rangle = [|00\rangle + (-1)^x |10\rangle]/\sqrt{2}, \tag{5.16}$$

$$U_{x1} = U|x1\rangle = \left[\frac{(1+i)}{\sqrt{2}}\right]^x [|01\rangle + (-1)^x |11\rangle]/\sqrt{2}. \tag{5.17}$$

Com esta combinação, as matrizes $V_j^\dagger$ de correção serão $V_1^\dagger = [\pi/8]$, $V_2^\dagger = [\pi/8] \cdot Z$, $V_3^\dagger = X \cdot S$

e $V_4^\dagger = X \cdot S \cdot Z$, em que

$$\pi/8 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i.\frac{\pi}{4}} \end{bmatrix}, S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{5.18}$$

5.4 Conclusão

Neste capítulo foi revisitado o procedimento através do qual a teleportação de estados quânticos pode ser obtida através de circuitos diversos e não apenas através do bem conhecido circuito proposto por Bennet. Foi apresentada a equação que descreve o relacionamento entre os parâmetros envolvidos no processo de teleportação com bases arbitrárias. Por fim, foram analisados alguns casos particulares, incluindo um não utilizando a base de Bell.

Capítulo 6

Teleportabilidade de portas quânticas e bases de medição

Resumo

Este capítulo apresenta uma das contribuições desta tese ao desenvolver a teoria que descreve a noção de teleportabilidade de portas quânticas de acordo com a base de medição, conceito associado à habilidade de uma porta quântica ser teleportável através de uma base de medição ou, de modo inverso, a habilidade de uma base de medição ser usada para a teleportar uma dada porta quântica.

6.1 Introdução

Nos capítulos anteriores foram descritas as ferramentas necessárias ao desenvolvimento da teoria que será construída neste capítulo e permitirá um entendimento preciso dos fatores envolvidos na teleportação com sucesso da ação de uma porta quântica, ou mesmo quando esta poderá ser alcançada apenas de forma probabilística.

Após o trabalho de Gottesman e Chuang [1], e mesmo após a expansão em [18], ainda restaram lacunas no completo entendimento da teleportação de portas quânticas, lacunas estas que são pretensões deste trabalho elucidar. Tais questionamentos permeiam por várias etapas do protocolo de teleportação, tais como:

- Seria possível realizar teleportações de portas quânticas utilizando outra base de medição além da base de Bell?
- Como se caracterizar uma base de medição capaz de realizar teleportações de portas quânticas?

- As correções podem ser realizadas com portas fora do grupo de Pauli?
- Seria possível realizar a teleportação de uma porta fora do grupo de Clifford?
- Mais abstratamente, toda porta cuja separabilidade é preservada quando conjugada por um elemento do grupo de Clifford pertence ao grupo de Pauli?

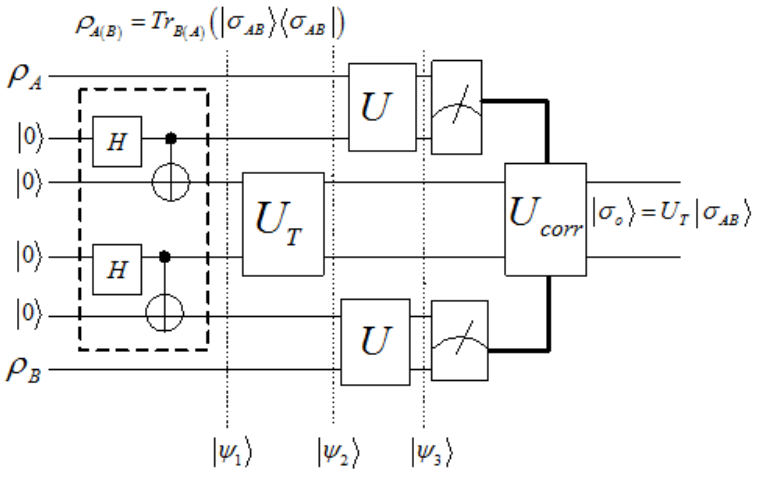
Para trabalhar a resposta de cada uma dessas questões será enunciado um teorema que descreve de forma clara as condições necessárias envolvendo a porta quântica e a base de medição para que o protocolo de teleportação seja determinístico.

O restante deste capítulo está organizado da seguinte forma: A Seção 6.2 mostra a construção analítica que proporcionará um entendimento mais profundo da teleportação portas quânticas. Na Seção 6.3 é feita a caracterização de bases de medições úteis à teleportações, são fornecidas algumas parametrizações para gerá-las. Seguindo, tem-se na Seção 6.4 a formulação do teorema acerca da teleportabilidade. Na Seção 6.5 é feita uma análise da teleportabilidade de algumas bases de medição. A Seção 6.6 demonstra alguns exemplos de teleportações de portas fora do grupo de Clifford.Por fim a Seção 6.7 apresenta as conclusões.

6.2 Teleportação parametrizável

Neste trabalho, assim como foi realizado com a teleportação de estados quânticos, são buscadas expansões que permitam a teleportação de portas através de bases de medição diversas. Para tanto, será utilizada a versão parametrizável do circuito para teleportação de portas quânticas exibida na Figura 6.1.

Figura 6.1: Circuito parametrizável para a teleportação de portas quânticas.



Seguindo um procedimento análogo ao utilizado nos Capítulos 3 e 5 pode-se analisar o circuito apresentado na Figura 6.1 e concluir que para uma teleportação com sucesso o estado imediatamente antes das medições deve ser o descrito na Equação (6.1), com

$|\sigma_{AB}\rangle = \sigma_{00}|00\rangle + \sigma_{01}|01\rangle + \sigma_{10}|10\rangle + \sigma_{11}|11\rangle$.

$$
\begin{aligned}
|\psi_3\rangle = \frac{1}{2} & \left[\begin{array}{l}
\sigma_{00}\left(\begin{array}{l} U|00\rangle U_T|00\rangle U|00\rangle + U|00\rangle U_T|01\rangle U|01\rangle + \\ U|01\rangle U_T|10\rangle U|00\rangle + U|01\rangle U_T|11\rangle U|01\rangle \end{array} \right) + \\
\sigma_{01}\left(\begin{array}{l} U|00\rangle U_T|00\rangle U|10\rangle + U|00\rangle U_T|01\rangle U|11\rangle + \\ U|01\rangle U_T|10\rangle U|10\rangle + U|01\rangle U_T|11\rangle U|11\rangle \end{array} \right) + \\
\sigma_{10}\left(\begin{array}{l} U|10\rangle U_T|00\rangle U|00\rangle + U|10\rangle U_T|01\rangle U|01\rangle + \\ U|11\rangle U_T|10\rangle U|00\rangle + U|11\rangle U_T|11\rangle U|01\rangle \end{array} \right) + \\
\sigma_{11}\left(\begin{array}{l} U|10\rangle U_T|00\rangle U|10\rangle + U|10\rangle U_T|01\rangle U|11\rangle + \\ U|11\rangle U_T|10\rangle U|10\rangle + U|11\rangle U_T|11\rangle U|11\rangle \end{array} \right)
\end{array} \right] \\
& = \tfrac{1}{4}\sum_{n,m=0}^{4} V_{nm} U_T |\sigma_{AB}\rangle |\beta_n\rangle |\beta_m\rangle .
\end{aligned}
\tag{6.1}
$$

Agora, usando $U_{xy} = U|xy\rangle \;\; \forall \; x, y \in \{0,1\}$ e fazendo o produto interno de $\langle\beta_j|\langle\beta_k|$ com a Equação (6.1) obtém-se

$$
\begin{aligned}
\frac{1}{2} & \left[\begin{array}{l}
\left(\begin{array}{l} \langle\beta_j|U_{00}\rangle \langle\beta_k|U_{00}\rangle U_T\sigma_{00}|00\rangle + \langle\beta_j|U_{00}\rangle \langle\beta_k|U_{01}\rangle U_T\sigma_{00}|01\rangle \\ \langle\beta_j|U_{01}\rangle \langle\beta_k|U_{00}\rangle U_T\sigma_{00}|10\rangle + \langle\beta_j|U_{01}\rangle \langle\beta_k|U_{01}\rangle U_T\sigma_{00}|11\rangle \end{array} \right) + \\
\left(\begin{array}{l} \langle\beta_j|U_{00}\rangle \langle\beta_k|U_{10}\rangle U_T\sigma_{01}|00\rangle + \langle\beta_j|U_{00}\rangle \langle\beta_k|U_{11}\rangle U_T\sigma_{01}|01\rangle \\ \langle\beta_j|U_{01}\rangle \langle\beta_k|U_{10}\rangle U_T\sigma_{01}|10\rangle + \langle\beta_j|U_{01}\rangle \langle\beta_k|U_{11}\rangle U_T\sigma_{01}|11\rangle \end{array} \right) + \\
\left(\begin{array}{l} \langle\beta_j|U_{10}\rangle \langle\beta_k|U_{00}\rangle U_T\sigma_{10}|00\rangle + \langle\beta_j|U_{10}\rangle \langle\beta_k|U_{01}\rangle U_T\sigma_{10}|01\rangle \\ \langle\beta_j|U_{11}\rangle \langle\beta_k|U_{00}\rangle U_T\sigma_{10}|10\rangle + \langle\beta_j|U_{11}\rangle \langle\beta_k|U_{01}\rangle U_T\sigma_{10}|11\rangle \end{array} \right) + \\
\left(\begin{array}{l} \langle\beta_j|U_{10}\rangle \langle\beta_k|U_{10}\rangle U_T\sigma_{11}|00\rangle + \langle\beta_j|U_{10}\rangle \langle\beta_k|U_{11}\rangle U_T\sigma_{11}|01\rangle \\ \langle\beta_j|U_{11}\rangle \langle\beta_k|U_{10}\rangle U_T\sigma_{11}|10\rangle + \langle\beta_j|U_{11}\rangle \langle\beta_k|U_{11}\rangle U_T\sigma_{11}|11\rangle \end{array} \right)
\end{array} \right] \\
& = \tfrac{1}{4} V_{jk} U_T \left[\sigma_{00}|00\rangle + \sigma_{01}|01\rangle + \sigma_{10}|10\rangle + \sigma_{11}|11\rangle\right]
\end{aligned}
\tag{6.2}
$$

que, substituindo

$$
\beta_{jk} = \sqrt{2}\begin{bmatrix} \langle\beta_j|U_{00}\rangle & \langle\beta_j|U_{10}\rangle \\ \langle\beta_j|U_{01}\rangle & \langle\beta_j|U_{11}\rangle \end{bmatrix} \otimes \sqrt{2}\begin{bmatrix} \langle\beta_k|U_{00}\rangle & \langle\beta_k|U_{10}\rangle \\ \langle\beta_k|U_{01}\rangle & \langle\beta_k|U_{11}\rangle \end{bmatrix} \tag{6.3}
$$

na Equação (6.2) chega-se à

$$
U_T \beta_{jk} |\sigma_{AB}\rangle = V_{jk} U_T |\sigma_{AB}\rangle . \tag{6.4}
$$

A Equação (6.4) indica que para a porta U_T ser teleportada com correções locais a porta U (preparação para medição) e a base de medição devem ver escolhidas de tal forma que

$$
V_{jk} = (V_j \otimes V_k) = U_T \cdot (\beta_j \otimes \beta_k) \cdot U_T^{\dagger} \quad \forall \; j,k \in \{1,2,3,4\}. \tag{6.5}
$$

Por sua vez, as correções serão dadas pelas transpostas conjugadas de V_{jk}.

Em outras palavras, uma correção composta de portas de um qubit será possível se, e somente se, a conjungação das matrizes β_{jk} (oriundas da relação entre a porta U e a base de medição) por U_T preservar a separabilidade de $\beta_j \otimes \beta_k$. Por exemplo, para o caso de $U = I_4$ e uma medição na base de Bell, U_T pode ser qualquer porta pertencente ao grupo de Clifford e as portas de correção $V_{jk}^{\dagger}$ pertencerão ao grupo de Pauli, um caso clássico na literatura.

6.3 Caracterização de uma base de medição

No Capítulo 5 ficou demonstrado que a teleportação de um estado quântico pode ser alcançada usando uma base arbitrária, o procedimento descreve inclusive qual será a correção requerida. No entanto, quando se discute a teleportação de portas quânticas a Equação (6.5) indica que o cenário é diferente. Disso emerge a questão: quais bases podem ser utilizadas para teleportação de portas quânticas?

A busca por essa resposta inicia revisitando a Equação (6.6) que indica como obter as matrizes oriundas da base de medição usada no processo de teleportação.

$$\beta_j = \sqrt{2} \begin{bmatrix} \langle \beta_j | U_{00} \rangle & \langle \beta_j | U_{10} \rangle \\ \langle \beta_j | U_{01} \rangle & \langle \beta_j | U_{11} \rangle \end{bmatrix}. \tag{6.6}$$

Basicamente, a restrição associada as parametrizações obtidas é que elas resultem em matrizes β_j unitárias, $\beta_j \cdot \beta_j^{\dagger} = \beta_j^{\dagger} \cdot \beta_j = I$, o que leva ao sistema descrito na Equação (6.7).

$$\begin{cases} |\langle \beta_j | U_{00} \rangle|^2 + |\langle \beta_j | U_{10} \rangle|^2 = 1/2 \\ |\langle \beta_j | U_{01} \rangle|^2 + |\langle \beta_j | U_{11} \rangle|^2 = 1/2 \\ |\langle \beta_j | U_{00} \rangle|^2 + |\langle \beta_j | U_{01} \rangle|^2 = 1/2 \\ |\langle \beta_j | U_{10} \rangle|^2 + |\langle \beta_j | U_{11} \rangle|^2 = 1/2 \\ \langle \beta_j | U_{00} \rangle \langle \beta_j | U_{01} \rangle^* = -\langle \beta_j | U_{10} \rangle \langle \beta_j | U_{11} \rangle^* \\ \langle \beta_j | U_{00} \rangle \langle \beta_j | U_{10} \rangle^* = -\langle \beta_j | U_{01} \rangle \langle \beta_j | U_{11} \rangle^* \end{cases}. \tag{6.7}$$

Para o caso particular de U igual a identidade e uma dada base $\beta = \{|\beta_j\rangle\}$, em que $|\beta_j\rangle = [b_{j1}, b_{j2}, b_{j3}, b_{j4}]^T$ com $j \in \{1, 2, 3, 4\}$, leva o sistema descrito na Equação (6.7) ao sistema apresentado na Equação (6.8).

$$\begin{cases} |b_{j1}|^2 + |b_{j3}|^2 = 1/2 \\ |b_{j2}|^2 + |b_{j4}|^2 = 1/2 \\ |b_{j1}|^2 + |b_{j2}|^2 = 1/2 \\ |b_{j3}|^2 + |b_{j4}|^2 = 1/2 \\ b_{j1} b_{j2}^* = -b_{j3} b_{j4}^* \\ b_{j1} b_{j3}^* = -b_{j2} b_{j4}^* \end{cases}. \tag{6.8}$$

Afim de investigar a teleportabilidade de uma dada base foram buscada algumas parametrizações que atendam aos critérios descritos nas Equações (6.7)–(6.8).

6.3.1 Parametrização com uma variável complexa

Para quaisquer valores tais que $|a|^2 + |b|^2 = 1/2$ uma base dotada de teleportabilidade pode ser obtida através da Equação (6.9), portanto, variando um único parâmetro complexo é possível obter infinitas bases capazes de realizar teleportação. Convém apontar que pequenas variações de sinais e conjugação na Equação (6.9) podem facilmente gerar outras parametrizações válidas.

$$\beta_{ab} = \left\{ \begin{pmatrix} a^* \\ b \\ -a^* \\ -b \end{pmatrix}, \begin{pmatrix} b^* \\ -a \\ -b^* \\ a \end{pmatrix}, \begin{pmatrix} -b \\ a^* \\ -b \\ a^* \end{pmatrix}, \begin{pmatrix} a \\ b^* \\ a \\ b^* \end{pmatrix} \right\}. \tag{6.9}$$

Essa parametrização leva às matrizes β_j descritas na Equação (6.10).

$$\beta_1 = \sqrt{2}\begin{bmatrix} a & -b^* \\ b & a^* \end{bmatrix}, \beta_2 = \sqrt{2}\begin{bmatrix} b^* & a \\ -a^* & b \end{bmatrix}, \beta_3 = \sqrt{2}\begin{bmatrix} -a & -b^* \\ -b & a^* \end{bmatrix}, \beta_4 = \sqrt{2}\begin{bmatrix} -b^* & a \\ a^* & b \end{bmatrix}. \tag{6.10}$$

6.3.2 Parametrização com três variáveis reais

Tomam-se as colunas de U_{NL}, parte não local resultante de uma decomposição KAK, como vetores da base, conforme descrito por

$$\beta_{NL} = \left\{ \begin{pmatrix} \cos(\theta^-)e^{i\theta_3} \\ 0 \\ 0 \\ \sin(\theta^-)ie^{i\theta_3} \end{pmatrix}, \begin{pmatrix} 0 \\ \cos(\theta^+)e^{-i\theta_3} \\ \sin(\theta^+)ie^{-i\theta_3} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \sin(\theta^+)ie^{-i\theta_3} \\ \cos(\theta^+)e^{-i\theta_3} \\ 0 \end{pmatrix}, \begin{pmatrix} \sin(\theta^-)ie^{i\theta_3} \\ 0 \\ 0 \\ \cos(\theta^-)e^{i\theta_3} \end{pmatrix} \right\}, \tag{6.11}$$

em que $\theta^+ = \theta_1 + \theta_2$ e $\theta^- = \theta_1 - \theta_2$. Conforme apontado anteriormente, uma base dotada de teleportabilidade precisa atender as restrições definidas nas Equações (6.7)-(6.8), isso leva às seguintes restrições:

$$\begin{cases} 2\cos^2(\theta_1 - \theta_2) = 1 \\ 2\sin^2(\theta_1 - \theta_2) = 1 \\ 2\sin^2(\theta_1 + \theta_2) = 1 \\ 2\cos^2(\theta_1 + \theta_2) = 1 \end{cases}. \tag{6.12}$$

Resolvendo este sistema de equações chega-se às possíveis 26 soluções mostradas

aos pares na Equação (6.13).

$$(\theta_1,\theta_2)=\begin{cases}(\pi,\frac{\pi}{4})\,;(\frac{\pi}{4},\pi)\,;\\ (0,\pm\frac{\pi}{4})\,;(\pm\frac{\pi}{4},0)\,;\left(0,\pm\frac{3\pi}{4}\right)\,;\left(\pm\frac{3\pi}{4},0\right)\,;\\ (\pm\frac{\pi}{2},\pm\frac{\pi}{4})\,;(\pm\frac{\pi}{4},\pm\frac{\pi}{2})\,;\left(\pm\frac{\pi}{2},\pm\frac{3\pi}{4}\right)\,;\left(\pm\frac{3\pi}{4},\pm\frac{\pi}{2}\right)\end{cases}. \tag{6.13}$$

Essa parametrização leva às matrizes β_j descritas na Equação (6.14).

$$\beta_1=\sqrt{2}\begin{bmatrix}\cos(\theta_1-\theta_2)\cdot e^{-i\theta_3} & 0\\ 0 & -\sin(\theta_1-\theta_2)\cdot ie^{-i\theta_3}\end{bmatrix}. \tag{6.14a}$$

$$\beta_2=\sqrt{2}\begin{bmatrix}0 & -\sin(\theta_1+\theta_2)\cdot ie^{i\theta_3}\\ \cos(\theta_1+\theta_2)\cdot e^{i\theta_3} & 0\end{bmatrix}. \tag{6.14b}$$

$$\beta_3=\sqrt{2}\begin{bmatrix}0 & \cos(\theta_1+\theta_2)\cdot e^{i\theta_3}\\ -\sin(\theta_1+\theta_2)\cdot ie^{i\theta_3} & 0\end{bmatrix}. \tag{6.14c}$$

$$\beta_4=\sqrt{2}\begin{bmatrix}-\sin(\theta_1-\theta_2)\cdot ie^{-i\theta_3} & 0\\ 0 & \cos(\theta_1-\theta_2)\cdot e^{-i\theta_3}\end{bmatrix}. \tag{6.14d}$$

Destes resultados apresentados, faz-se as seguintes observações:

1. A teleportabilidade de uma base desta classe depende apenas dos parâmetros θ_1 e θ_2.
2. Observando a forma descrita na Equação (6.11) e os resultados apresentados na Equação (6.13), tem-se uma parametrização para geração de infinitas bases com teleportabilidade. Para tanto, basta variar o parâmetro θ_3 e/ou uma fase global (θ_0).

6.4 Teorema da teleportabilidade

Com o arcabouço desenvolvido no Capítulo 4 e nas seções anteriores deste capítulo, torna-se possível enunciar o Teorema 6.1 que descreve precisamente as condições nas quais a ação de uma porta quântica de dois qubits pode ser teleportada de forma determinística.

Teorema 6.1 (Teleportabilidade)**.** *Dada uma porta quântica de dois qubits U com decomposição KAK $(U_A\otimes U_B)\cdot U_{NL}\cdot(U_C\otimes U_D)$ e uma base de medição $M=\{|\beta_1\rangle,|\beta_2\rangle,|\beta_3\rangle,|\beta_4\rangle\}$, a porta quântica U será teleportada deterministicamente se U_{NL} e $(U_C\otimes U_D)\cdot(\beta_j\otimes\beta_k)\cdot(U_C^\dagger\otimes U_D^\dagger)$, em que $\beta_{j,k}$ são as matrizes oriundas da base M, estão de acordo com o Teorema 4.2.*

Demonstração. A partir da Equação (6.5), pode-se notar que para uma teleportação determinística com correções locais a separabilidade das matrizes oriundas da base de medição, cuja

forma de β_j está descrita na Equação (6.6), deve ser preservada sob conjugação de U. De outro modo, substituindo U na Equação (6.5), tem-se que a expressão

$$U_{NL} \cdot (U_C \otimes U_D) \cdot (\beta_j \otimes \beta_k) \cdot (U_C^\dagger \otimes U_D^\dagger) \cdot U_{NL}^\dagger \tag{6.15}$$

deve resultar em uma matriz separável, portanto, faz-se necessário que U_{NL} e $(U_C \otimes U_D) \cdot (\beta_j \otimes \beta_k) \cdot (U_C^\dagger \otimes U_D^\dagger)$ estejam em conformidade com o Teorema 4.2 que descreve os critérios para a preservação da separabilidade sob conjugação. □

A partir do Teorema 6.1 diversas questões interessantes podem ser observadas, tais como:

- A parte não local U_{NL} da porta U a ser teleportada deve ter uma decomposição KAK cujos ângulos θ_i estejam em função de $2(k_i + 1) \cdot \pi/4$, com $k_i \in \mathbb{Z}$.
- A componente $(U_A \otimes U_B)$, parte local à esquerda de U, não é relevante para o processo de teleportação.
- A conjugação de β_{jk}, as matrizes oriundas da base, por $(U_C \otimes U_D)$, a parte local à direta da porta U_T, deve possuir uma decomposição ZYZ com ângulos λ_μ em função de $k_\mu \pi$, em que $k_\mu \in \mathbb{Z}$.
- Toda porta quântica cujos ângulos não locais sejam todos não nulos e múltiplos inteiros de $\pi/4$ podem ser teleportadas usando qualquer base dotada de teleportabilidade.

6.5 Análise de teleportabilidade de algumas bases

Uma vez definidos meios de caracterizar bases de medição úteis à teleportação, serão tomados alguns exemplos para aprofundamento da questão. Para tanto, serão utilizadas as bases M_{Bell}, M_C e M_D descritas adiante. Para iniciar, a base

$$M_{Bell} = \left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \right\} \tag{6.16}$$

leva, usando a Equação (6.6), às matrizes

$$\beta_{bell_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \beta_{bell_2} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \beta_{bell_3} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \beta_{bell_4} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{6.17}$$

Lembrando que usando a decomposição ZYZ uma matriz em $U(2)$ pode ser decomposta na forma

$$U_\Lambda = e^{-i/2(\lambda_0)} \cdot e^{-i/2(\lambda_1 \cdot \sigma_Z)} \cdot e^{-i/2(\lambda_2 \cdot \sigma_Y)} \cdot e^{-i/2(\lambda_3 \cdot \sigma_Z)}, \tag{6.18}$$

com $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$, pode-se verificar que os ângulos oriundos da decomposição das matrizes β_{bell_i} são

$$\beta_{bell_1} = [0,0,0,0]\,, \quad \beta_{bell_2} = \left[\frac{\pi}{2}, \pi, -\pi, 0\right], \quad \beta_{bell_3} = \left[\frac{\pi}{2}, 0, \pi, 0\right], \quad \beta_{bell_4} = \left[\frac{\pi}{2}, \pi, 0, 0\right]. \tag{6.19}$$

Na sequência, a base

$$M_C = \left\{ \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{pmatrix} \right\} \tag{6.20}$$

leva às matrizes

$$\beta_{c_1} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \beta_{c_2} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix}, \quad \beta_{c_3} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}, \quad \beta_{c_4} = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{6.21}$$

cujos ângulos oriundos da decomposição ZYZ são

$$\beta_{c_1} = \left[\tfrac{\pi}{2}, \pi, -\tfrac{3\pi}{2}, 0\right], \quad \beta_{c_2} = \left[0, 0, \tfrac{3\pi}{2}, 0\right], \quad \beta_{c_3} = \left[0, 0, -\tfrac{3\pi}{2}, 0\right], \quad \beta_{c_4} = \left[\tfrac{\pi}{2}, 0, \tfrac{\pi}{2}, 0\right]. \tag{6.22}$$

Por fim, a base

$$M_D = \left\{ \begin{pmatrix} \frac{i}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{-i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{i}{\sqrt{2}} \end{pmatrix} \right\}. \tag{6.23}$$

leva às matrizes

$$\beta_{d_1} = \begin{bmatrix} -i & 0 \\ 0 & 1 \end{bmatrix}, \quad \beta_{d_2} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \beta_{d_3} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \beta_{d_4} = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}, \tag{6.24}$$

cujos ângulos oriundos da decomposição ZYZ são

$$\beta_{d_1} = \left[\frac{3\pi}{4}, -\frac{3\pi}{2}, 0, 0\right], \quad \beta_{d_2} = \left[\frac{\pi}{2}, 0, \pi, 0\right], \quad \beta_{d_3} = \left[\frac{\pi}{2}, \pi, -\pi, 0\right], \quad \beta_{d_4} = \left[\frac{3\pi}{4}, \frac{3\pi}{2}, 0, 0\right]. \tag{6.25}$$

A partir dos Teoremas (4.2) e (6.1) é possível determinar a probabilidade de uma

dada porta ser teleportada com sucesso usando uma determinada base, alguns exemplos podem ser vistos na Tabela 6.1. Basicamente, essa probabilidade é dada pela quantidade de resultados de medição que atendem à preservação da separabilidade, dividido pelo total.

Tabela 6.1: Probabilidade de sucesso da teleportação de algumas portas quânticas usando as bases M_{Bell}, M_C e M_D.

Porta	M_{Bell}	M_C	M_D
C_{NOT}	1	0	0.5
$C_{\pi/8}$	0.5	0	0.5
${C_{NOT}}^{1/2}$	0.5	0	0.25
$SWAP^{1/2}$	0.25	0.25	0.25
$\exp(i\frac{\pi}{4}\sigma_{YY})$	1	1	0.25

Faz-se interessante ressaltar que a relação entre o resultado da medição e a preservação da separabilidade é determinística e conhecida a priori, portanto, é possível identificar quando a teleportação falhou para repeti-la até que se obtenha um sucesso. Como exemplos, a Tabela 6.2 apresenta essa relação para a teleportação das portas ${C_{NOT}}^{1/2}$ e $SWAP^{1/2}$ usando a base de Bell. Tomando a decomposição KAK da porta a ser teleportada, sempre que a expressão

$$U_{NL} \cdot (U_C \otimes U_D) \cdot (\beta_j \otimes \beta_k) \cdot (U_C^\dagger \otimes U_D^\dagger) \cdot U_{NL}^\dagger \tag{6.26}$$

resultar em uma matriz separável a teleportação será considerada um sucesso e o estado original poderá ser recuperado com correções locais, caso contrário a teleportação será considerada falha. Os dois primeiros bits obtidos com a medição estão associados ao índice j das matrizes oriundas da base, enquanto os dois últimos bits estão associados ao índice k. Outros exemplos são apresentados nas seções seguintes.

Tabela 6.2: Resultado da teleportação de algumas portas quânticas usando a base M_{Bell} em função dos resultados das medições.

Medição	${C_{NOT}}^{1/2}$	$SWAP^{1/2}$	Medição	${C_{NOT}}^{1/2}$	$SWAP^{1/2}$
0000	Sucesso	Sucesso	1000	Sucesso	Falha
0001	Sucesso	Falha	1001	Sucesso	Falha
0010	Falha	Falha	1010	Falha	Sucesso
0011	Falha	Falha	1011	Falha	Falha
0100	Falha	Falha	1100	Falha	Falha

Continua na próxima página...

Tabela 6.2 – continuação da página anterior.

Medição	${C_{NOT}}^{1/2}$	$SWAP^{1/2}$	Medição	${C_{NOT}}^{1/2}$	$SWAP^{1/2}$
0101	Falha	Sucesso	1101	Falha	Falha
0110	Sucesso	Falha	1110	Sucesso	Falha
0111	Sucesso	Falha	1111	Sucesso	Sucesso

6.5.1 Análise de um caso particular I: $\exp(i\frac{\pi}{4}\sigma_{YY})$

Tomando o caso da teleportação da porta $\exp(i\frac{\pi}{4}\sigma_{YY})$ usando a base M_D como exemplo, vê-se que o processo apenas logrará êxito quando a medição resultar em 0101, 0110, 1001 ou 1010, que corresponderá, respectivamente, às combinações (β_{d_2}, β_{d_2}), (β_{d_2}, β_{d_3}), (β_{d_3}, β_{d_2}) e (β_{d_3}, β_{d_3}). Isso decorre do fato de que apenas as matrizes β_{d_2} e β_{d_3} possuem uma decomposição compatível com o requerido pelo teorema da teleportabilidade. Considerando a porta $\exp(i\frac{\pi}{4}\sigma_{YY})$ na base M_{bell}, vê-se que a teleportação pode ser realizada de forma determinística, o mesmo acontece para a base M_C.

6.5.2 Análise de um caso particular II: $SWAP^{1/2}$

No que diz respeito à porta $SWAP^{1/2}$, sua teleportabilidade probabilística tem uma explicação que decorre da estrutura das portas da família das $Swap's$. A $SWAP^{1/2}$ tem sua parte não-local na forma $\exp[i\cdot\pi/8\cdot(\sigma_{XX}+\sigma_{YY}+\sigma_{ZZ})]$ e pode ser verificado simbolicamente que toda porta na forma $\exp[i\cdot\theta\cdot(\sigma_{XX}+\sigma_{YY}+\sigma_{ZZ})]$ preserva a separabilidade quando conjuga $(A\otimes A)$ para todo $A\in U(2)$ e $\theta\in\mathbb{R}$. Deste modo, percebe-se facilmente que a teleportação resultará em sucesso sempre que as matrizes oriundas da base forem $\beta_{jj}=(\beta_j\otimes\beta_j)$, ou seja, para os resultados de medição 0000, 0101, 1010 e 1111.

6.5.3 Análise de um caso particular III: ${C_{NOT}}^{1/2}$

Por outro lado, o caso da ${C_{NOT}}^{1/2}$ se mostra mais elaborado. A menos de um fator de fase global, a parte não-local da ${C_{NOT}}^{1/2}$ é dada por $\exp(i\frac{\pi}{8}\sigma_{YY})$ e suas portas locais à direita são:

$$B_1=\frac{1}{2}\begin{bmatrix}1-i & -1+i\\ 1+i & 1+i\end{bmatrix},\quad B_0=\frac{1}{\sqrt{2}}\begin{bmatrix}0 & 1-i\\ -1-i & 0\end{bmatrix}. \tag{6.27}$$

Tomando a base M_D como exemplo, pode-se verificar algebricamente que teleportações com sucesso ocorrem quando são medidos os valores 0010, 0101, 1001 e 1110. As conjugações das portas locais associadas a estes valores são:

$$B_1\cdot\beta_{d_1}\cdot B_1^{\dagger} \;=\; \left[\frac{3\pi}{4},0,-\frac{3\pi}{2},0\right], \tag{6.28a}$$

$$B_1 \cdot \beta_{d_2} \cdot B_1^\dagger = \left[\frac{\pi}{2}, \pi, \pi, 0\right], \tag{6.28b}$$

$$B_1 \cdot \beta_{d_3} \cdot B_1^\dagger = \left[\frac{\pi}{2}, -\pi, 0, 0\right], \tag{6.28c}$$

$$B_1 \cdot \beta_{d_4} \cdot B_1^\dagger = \left[-\frac{\pi}{4}, 0, -\frac{\pi}{2}, 0\right], \tag{6.28d}$$

$$B_0 \cdot \beta_{d_2} \cdot B_0^\dagger = \left[\frac{\pi}{2}, \pi, \pi, 0\right], \tag{6.28e}$$

$$B_0 \cdot \beta_{d_3} \cdot B_0^\dagger = \left[\frac{\pi}{2}, 0, -\pi, 0\right]. \tag{6.28f}$$

Deste modo, os quatro casos de sucesso são dados pelas conjugações adiante na Equação (6.29).

$$\exp\left(i\frac{\pi}{8}\sigma_{YY}\right) \cdot \left(B_1 \cdot \beta_{d_1} \cdot B_1^\dagger \otimes B_0 \cdot \beta_{d_3} \cdot B_0^\dagger\right) \cdot \exp\left(i\frac{\pi}{8}\sigma_{YY}\right)^\dagger. \tag{6.29a}$$

$$\exp\left(i\frac{\pi}{8}\sigma_{YY}\right) \cdot \left(B_1 \cdot \beta_{d_2} \cdot B_1^\dagger \otimes B_0 \cdot \beta_{d_2} \cdot B_0^\dagger\right) \cdot \exp\left(i\frac{\pi}{8}\sigma_{YY}\right)^\dagger. \tag{6.29b}$$

$$\exp\left(i\frac{\pi}{8}\sigma_{YY}\right) \cdot \left(B_1 \cdot \beta_{d_3} \cdot B_1^\dagger \otimes B_0 \cdot \beta_{d_2} \cdot B_0^\dagger\right) \cdot \exp\left(i\frac{\pi}{8}\sigma_{YY}\right)^\dagger. \tag{6.29c}$$

$$\exp\left(i\frac{\pi}{8}\sigma_{YY}\right) \cdot \left(B_1 \cdot \beta_{d_4} \cdot B_1^\dagger \otimes B_0 \cdot \beta_{d_3} \cdot B_0^\dagger\right) \cdot \exp\left(i\frac{\pi}{8}\sigma_{YY}\right)^\dagger. \tag{6.29d}$$

Olhando atentamente, pode-se constatar que os casos representados pelas Equações (6.29a)-(6.29d) estão aderentes, basicamente em decorrência de relações de comutação, ao previsto pelo Teorema 6.1.

6.6 Teleportação além da base de Bell

Esta seção apresenta novos resultados a respeito da teleportação de portas quânticas, incia-se com a teleportação de portas fora do grupo de Clifford usando a base de Bell e em seguida é apresentado um procedimento para a construção de bases para a teleportação de portas que não podem ser teleportadas de forma determinística usando a base de Bell.

6.6.1 Cenário baseado no *maximal torus*

Utilizando como inspiração o *maximal torus* [66] do grupo $SU(4)$, chegou-se ao conjunto de portas $T(\theta_1, \theta_2, \theta_3)$ mostradas na Equação (6.30) com algumas propriedades inte-

ressantes a serem discutidas na sequência.

$$T_1 = \begin{bmatrix} e^{i\theta_1} & 0 & 0 & 0 \\ 0 & e^{i\theta_2} & 0 & 0 \\ 0 & 0 & e^{i\theta_3} & 0 \\ 0 & 0 & 0 & e^{i(\theta_1+\theta_2+\theta_3)} \end{bmatrix}, \quad T_2 = \begin{bmatrix} e^{i\theta_1} & 0 & 0 & 0 \\ 0 & e^{i\theta_2} & 0 & 0 \\ 0 & 0 & e^{i\theta_3} & 0 \\ 0 & 0 & 0 & e^{-i(\theta_1+\theta_2+\theta_3)} \end{bmatrix},$$
$$T_3 = \begin{bmatrix} 0 & 0 & 0 & e^{i\theta_1} \\ 0 & 0 & e^{i\theta_2} & 0 \\ 0 & e^{i\theta_3} & 0 & 0 \\ e^{i(\theta_1+\theta_2+\theta_3)} & 0 & 0 & 0 \end{bmatrix}, \quad T_4 = \begin{bmatrix} 0 & 0 & 0 & e^{i\theta_1} \\ 0 & 0 & e^{i\theta_2} & 0 \\ 0 & e^{i\theta_3} & 0 & 0 \\ e^{-i(\theta_1+\theta_2+\theta_3)} & 0 & 0 & 0 \end{bmatrix}. \tag{6.30}$$

Como as portas T_j, $j \in \{1,2,3,4\}$, possuem propriedades similares, será tomada como exemplo a porta T_1 para uma análise mais aprofundada. Para $\theta_1 = 0$ a porta T_1 torna-se separável, portanto, fora do interesse dessa análise. Por outro lado, para $\theta_1 = \pi/2$ e quaisquer valores de θ_2 e θ_3, T_1 é teleportável através das bases M_{Bell} e M_D, mas não é teleportável através da base M_C.

Na Tabela 6.3 pode-se ver o resultado da conjugação das matrizes β da base M_D, descritas na Equação (6.24), pela porta T_1, com $\theta_1 = \pi/2$, em função dos ângulos θ_2 e θ_3.

Tabela 6.3: Correções requeridas pela teleportação da ação da porta T_1 em função do resultado da medição (j e k) e dos ângulos (θ_2 e θ_3) escolhidos.

j	k	$V_{jk} = T_1 \cdot (\beta_j \otimes \beta_k) \cdot T_1^\dagger$	j	k	$V_{jk} = T_1 \cdot (\beta_j \otimes \beta_k) \cdot T_1^\dagger$
1	1	$P \otimes -P$	3	1	$V_3 \otimes iPZ$
1	2	$PZ \otimes -V_2Z$	3	2	$-V_3Z \otimes iV_2$
1	3	$PZ \otimes iV_2$	3	3	$V_3Z \otimes -V_2Z$
1	4	$P \otimes PYX$	3	4	$-V_3 \otimes P$
2	1	$-V_3Z \otimes PZ$	4	1	$PYX \otimes P$
2	2	$V_3 \otimes V_2$	4	2	$-V_2Z \otimes iP$
2	3	$V_3 \otimes -V_2Z$	4	3	$P \otimes -V_2$
2	4	$-V_3Z \otimes iP$	4	4	$PZ \otimes PZ$

sendo

$$V_2 = \begin{bmatrix} 0 & -ie^{-i\theta_2} \\ ie^{i\theta_2} & 0 \end{bmatrix} \quad \text{e} \quad V_3 = \begin{bmatrix} 0 & -ie^{-i\theta_3} \\ ie^{i\theta_3} & 0 \end{bmatrix}. \tag{6.31}$$

Pode ser notado que na teleportação da porta $T_1(\pi/2, \theta_2, \theta_3)$ as correções para $(j,k) \in \{(1,1);(1,4);(4,1);(4,4)\}$ independem dos valores de θ_2 e θ_3, portanto, são conhecidas

previamente. Isso pode facilmente ser observado a partir da Tabela 6.3. Contudo, a propriedade realmente interessante da porta $T_1(\pi/2, \theta_2, \theta_3)$ é que ela pode ser parametrizada para ficar fora do grupo de Clifford e ainda sim ser teleportável, um resultado desconhecido na literatura.

Por exemplo, para $T_1(\pi/2, \pi/8, \pi/8)$ a Equação (6.32) mostra um exemplo em que não se observa a preservação do grupo de Pauli sob conjugação.

$$T_1\left(\frac{\pi}{2}, \frac{\pi}{8}, \frac{\pi}{8}\right) \cdot (X \otimes Z) \cdot T_1\left(\frac{\pi}{2}, \frac{\pi}{8}, \frac{\pi}{8}\right)^\dagger = \left(\begin{bmatrix} 0 & 1 \\ -\frac{1+i}{\sqrt{2}} & 0 \end{bmatrix} \otimes \begin{bmatrix} ie^{-i\pi/8} & 0 \\ 0 & ie^{-i\pi/8} \end{bmatrix} \right). \tag{6.32}$$

Da mesma forma, para $\theta_1 = \pi/2$, $\theta_2 = \pi/7$ e $\theta_3 = \pi/13$ não se observa a preservação do grupo de Pauli sob conjugação, conforme pode ser visto em

$$T_1\left(\frac{\pi}{2}, \frac{\pi}{7}, \frac{\pi}{13}\right) \cdot (X \otimes Z) \cdot T_1\left(\frac{\pi}{2}, \frac{\pi}{7}, \frac{\pi}{13}\right)^\dagger = \left(\begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix} \otimes \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \right), \tag{6.33}$$

em que $a = -0.8855 - 0.4647i$ e $b = 0.2393 + 0.9709i$. Analisando as decomposições KAK destes exemplos, dadas por

$$T_1\left(\tfrac{\pi}{2},\tfrac{\pi}{8},\tfrac{\pi}{8}\right) = \begin{pmatrix} e^{-\frac{i}{2}\left(\frac{5\pi}{8}\cdot\sigma_{ZI} + \frac{\pi}{8}\cdot\sigma_{IZ}\right).} \\ e^{-\frac{i}{2}\left(\frac{\pi}{2}\cdot\sigma_{YI} + \frac{\pi}{2}\cdot\sigma_{IY}\right).} \\ e^{-\frac{i}{2}(-\pi\cdot\sigma_{IZ})} \end{pmatrix} \cdot \left(e^{-i\frac{\pi}{8}} \cdot e^{-i\frac{\pi}{4}\sigma_{XX}}\right) \cdot \begin{pmatrix} e^{-\frac{i}{2}(-\pi\cdot\sigma_{ZI}).} \\ e^{-\frac{i}{2}\left(-\frac{3\pi}{2}\cdot\sigma_{YI} + -\frac{3\pi}{2}\cdot\sigma_{IY}\right).} \\ e^{-\frac{i}{2}\left(-\frac{\pi}{2}\cdot\sigma_{ZI}\right)} \end{pmatrix} \tag{6.34a}$$

$$T_1\left(\tfrac{\pi}{2},\tfrac{\pi}{7},\tfrac{\pi}{13}\right) = \begin{pmatrix} e^{-\frac{i}{2}(\alpha_1\cdot\sigma_{ZI} + \beta_1\cdot\sigma_{IZ}).} \\ e^{-\frac{i}{2}(-\pi\cdot\sigma_{IY}).} \\ e^{-\frac{i}{2}(\alpha_3\cdot\sigma_{ZI} + \beta_3\cdot\sigma_{IZ})} \end{pmatrix} \cdot \left(e^{-i\frac{51}{364}} \cdot e^{-i\frac{\pi}{4}\sigma_{ZZ}}\right) \cdot \begin{pmatrix} e^{-\frac{i}{2}(2\pi\cdot\sigma_{ZI} + -\pi\cdot\sigma_{IZ}).} \\ e^{-\frac{i}{2}(-\pi\cdot\sigma_{IY}).} \\ e^{-\frac{i}{2}\left(-\pi\cdot\sigma_{ZI} + \frac{3\pi}{2}\cdot\sigma_{IZ}\right)} \end{pmatrix}, \tag{6.34b}$$

em que $\alpha_1 \approx -2.2730$, $\alpha_3 \approx 0.9439$, $\beta_1 \approx -0.3479$ e $\beta_3 \approx -1.7674$, pode-se melhor entender a razão deste comportamento. Primeiro, claramente se percebe que ambas as portas não são aderentes ao Teorema 4.3, o que é esperado uma vez que elas não pertencem ao grupo de Clifford. Depois, pode-se observar que, em relação à ambas as portas, tanto a parte não local quanto a parte local a direita atendem ao Teorema 4.2, tornando-as aderentes ao Teorema 6.1.

Deste modo, tem-se uma parametrização para gerar infinitas portas fora de Clifford que, por serem teleportáveis através da base de Bell corroboram a tese descrita em [18] ao expandir [1], e por serem teleportáveis através da base M_D corrobora o desenvolvido neste trabalho que aponta para a possibilidade de uso de outras bases além da base de Bell.

6.6.2 Cenário baseado em transformação de similaridades

Esta seção mostra como podem ser usadas transformações de similaridade para encontrar portas quânticas que darão uma resposta positiva a pergunta: existe uma porta quântica U que pode ser teleportada por uma dada base M mas que não pode ser teleportada pela base de Bell? A relevância da questão reside principalmente no fato de que a proposta ori-

ginal de Gottesman e Chuang para a teleportação de portas quânticas prevê apenas a utilização da base de Bell.

A partir do conhecimento desenvolvido acerca de teleportabilidade se sabe que isso implica em existir uma base M tal que β_j^M, as matrizes oriundas da base, e $U_{RA} \otimes U_{RB}$, a parte local a direita da porta U, isoladamente não satisfaçam os critérios de separabilidade, no entanto, $(U_{RA} \otimes U_{RB}) \cdot \beta_{jk}^M \cdot (U_{RA}^\dagger \otimes U_{RB}^\dagger)$ satisfaça.

Para construir um caso mais abrangente, é tomada uma porta quântica U cuja parte local a direita é composta por

$$U_{RA} = e^{\left(-\frac{i\pi}{16}\right)} \cdot e^{\left(-\frac{i\pi}{8} \cdot \sigma_Z\right)} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+1}{\sqrt{2}} \end{bmatrix} \tag{6.35a}$$

$$U_{RB} = e^{\left(\frac{i\pi}{14}\right)} \cdot e^{\left(-\frac{i\pi}{14} \cdot \sigma_Z\right)} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{-i\pi}{7}} \end{bmatrix}. \tag{6.35b}$$

Agora, as bases M_A e M_B serão montadas usando transformações de similaridade conforme as Equações (6.36) e (6.37) mostradas adiante.

$$\beta_{MA_1} = \sigma_I. \tag{6.36a}$$
$$\beta_{MA_2} = U_{RA}^\dagger \cdot \sigma_X \cdot U_{RA}. \tag{6.36b}$$
$$\beta_{MA_3} = U_{RA}^\dagger \cdot \sigma_Y \cdot U_{RA}. \tag{6.36c}$$
$$\beta_{MA_4} = U_{RA}^\dagger \cdot \sigma_X\sigma_Y \cdot U_{RA}. \tag{6.36d}$$

$$\beta_{MB_1} = \sigma_I. \tag{6.37a}$$
$$\beta_{MB_2} = U_{RB}^\dagger \cdot \sigma_X \cdot U_{RB}. \tag{6.37b}$$
$$\beta_{MB_3} = U_{RB}^\dagger \cdot \sigma_Y \cdot U_{RB}. \tag{6.37c}$$
$$\beta_{MB_4} = U_{RB}^\dagger \cdot \sigma_X\sigma_Y \cdot U_{RB}. \tag{6.37d}$$

Neste ponto, basta utilizar a Equação (6.6) para, a partir das matrizes β, encontrar cada um dos vetores da base correspondente. O resultado pode ser visto nas Equações (6.38) e (6.39) com, quando cabível, aproximação de quatro dígitos.

$$M_A = \left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1+i}{2} \\ \frac{1-i}{2} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1-i}{2} \\ \frac{1+i}{2} \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{-i}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{i}{\sqrt{2}} \end{pmatrix} \right\}. \tag{6.38}$$

$$M_B = \left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} 0 \\ 0.6371 + 0.3068i \\ 0.6371 - 0.3068i \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0.6371 - 0.3068i \\ 0.6371 + 0.3068i \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{-i}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{i}{\sqrt{2}} \end{pmatrix} \right\}. \tag{6.39}$$

Deste modo, as bases M_A e M_B podem ser utilizadas para teleportar qualquer porta quântica na forma $U = (U_{LA} \otimes U_{LB}) \cdot \left\{ e^{i\left[(2k_1+1)\frac{pi}{4} \cdot \sigma_{XX}\right]} \cdot e^{i\left[(2k_1+1)\frac{pi}{4} \cdot \sigma_{YY}\right]} \cdot e^{i\left[(2k_3+1)\frac{pi}{4} \cdot \sigma_{ZZ}\right]} \right\} \cdot (U_{RA} \otimes U_{RB})$ de forma determinística para quaisquer $k_1, k_2, k_3 \in \mathbb{Z}$ e $U_{LA}, U_{LB} \in U(2)$. Convém ainda ressaltar que as matrizes β_{MA_j} e β_{MB_k} formam grupos sob a multiplicação usual de matrizes.

6.7 Conclusão

Neste capítulo foi enunciado o teorema da teleportabilidade que descreve as condições necessárias e suficientes para que uma dada porta quântica possa ser teleportada de modo determinístico usando uma dada base de medição. Foi realizada a caracterização de bases de medições úteis à teleportações e fornecidas algumas parametrizações para gerá-las. As condições explicitadas pelo teorema foram utilizadas para apontar a possibilidade, mostrando exemplos, da teleportação de portas fora do grupo de Clifford.

Capítulo 7

O papel do estado recurso na teleportação

Resumo

A contribuição descrita neste capítulo completa o estudo acerca do protocolo de teleportação de portas quânticas de dois qubits na medida que descreve o papel do estado quântico de quatro qubits usado como recurso. Foram definidas três classes nas quais se pode classificar estados recursos e como se dá o resultado do processo para cada um dos dois casos.

7.1 Introdução

Até o presente momento o estado usado como recurso da teleportação é composto por dois pares de Bell. Por outro lado, este capítulo descreve uma análise do protocolo de teleportação de portas quânticas de dois qubits usando como recurso um estado geral de quatro qubits. Três diferentes situações são encontradas. Descreve-se como a porta quântica de dois qubits, cuja ação será teleportada, e o resultado do protocolo da teleportação dependem do estado quântico de quatro qubits usado como recurso no processo. Em particular, mostra-se o caso em que uma teleportação probabilística pode ser realizada usando a base canônica $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ na medição. Adicionalmente, mostra-se alguns resultados do processo de teleportação quando usado como recurso estados maximamente entrelaçados de quatro qubits presentes na literatura.

O restante deste capítulo está organizado da seguinte forma: A Seção 7.2 descreve a formulação da matriz Υ, oriunda do protocolo de teleportação, e mostra sua relação com algumas classes de estados já definidas na literatura. Na sequência, tem-se na Seção 7.3 a

descrição de como a forma da matriz ϒ, gerada a partir do estado recurso, afeta o resultado da teleportação. Por fim a Seção 7.4 apresenta as conclusões.

7.2 A matriz ϒ

Tomando-se $|\sigma\rangle$ como um estado geral de quatro qubits na forma

$$|\sigma\rangle = \sum_{k,l,m,n=0}^{1} \sigma_{klmn} |klmn\rangle = \sum_{i=0}^{15} \sigma_i |i\rangle , \tag{7.1}$$

pode-se definir a matriz

$$\Upsilon = \begin{bmatrix} \sigma_0 & \sigma_1 & \sigma_8 & \sigma_9 \\ \sigma_2 & \sigma_3 & \sigma_{10} & \sigma_{11} \\ \sigma_4 & \sigma_5 & \sigma_{12} & \sigma_{13} \\ \sigma_6 & \sigma_7 & \sigma_{14} & \sigma_{15} \end{bmatrix} \tag{7.2}$$

composta exclusivamente pelos coeficientes de $|\sigma\rangle$ seguindo um padrão que emerge naturalmente, de modo análogo ao mostrado na Equação (5.12) obtida a partir da Equação (5.11), a partir do desenvolvimento analítico do processo de teleportação usando como recurso um estado geral de quatro qubits. Neste caso, tem-se particular interesse em duas circunstâncias: 1) quando $\Upsilon = \frac{1}{2}U_\sigma$, em que U_σ é uma matriz unitária; 2) quando ϒ é normal ($[\Upsilon, \Upsilon^\dagger] = 0$) mas 2Υ não é unitária, ou quando ϒ não é normal.

Mais adiante será mostrado como o tipo da matriz ϒ está associado ao resultado do processo de teleportação, mas por hora o foco será em analisar como algumas relações entre ϒ e o entrelaçamento presente no estado correspondente. Para tanto, convém lembrar que o determinante de ϒ é um invariante [67] que pode ser usado (junto com outros invariantes) para classificar estados de quatro qubits segundo algumas classes pré-estabelecidas. Por exemplo, de acordo com a classificação dada em [2] existem dezesseis classes distintas, a saber: 1, $2a$, $2b$, $2c$, $2d$, $3a$, $3b$, $3c$, $3d$, $3e$, $3f$, $4a$, $4b$, $4c$, $4d$ e 5. Na Tabela 7.1, para cada uma das classes citadas, tem-se: o estado canônico, o valor do entrelaçamento de quatro vias calculado pela medida π_4 [68], o tipo da matriz ϒ correspondente e, por fim, o valor do determinante de ϒ.

Tabela 7.1: Tipo da matriz ϒ correspondente aos estados canônicos das classes definidas em [2]. U → 2Υ é unitária; N → ϒ é normal mas 2Υ não é unitária; Ñ → ϒ não é normal.

Classe	Estado canônico	π_4	Tipo	det(ϒ)
1	$\|\psi_1\rangle = 1/\sqrt{2}(\|0000\rangle + \|0111\rangle)$	0	Ñ	0
$2a$	$\|\psi_{2a}\rangle = 1/\sqrt{2}(\|0000\rangle + \|1111\rangle)$	1	N	0
$2b$	$\|\psi_{2b}\rangle = 1/2(\|0000\rangle + \|0101\rangle + \|1010\rangle - \|1111\rangle)$	1	U	1/16
$2c$	$\|\psi_{2c}\rangle = 1/2(\|0000\rangle + \|0110\rangle + \|1001\rangle - \|1111\rangle)$	1	N	1/16

Continua na próxima página...

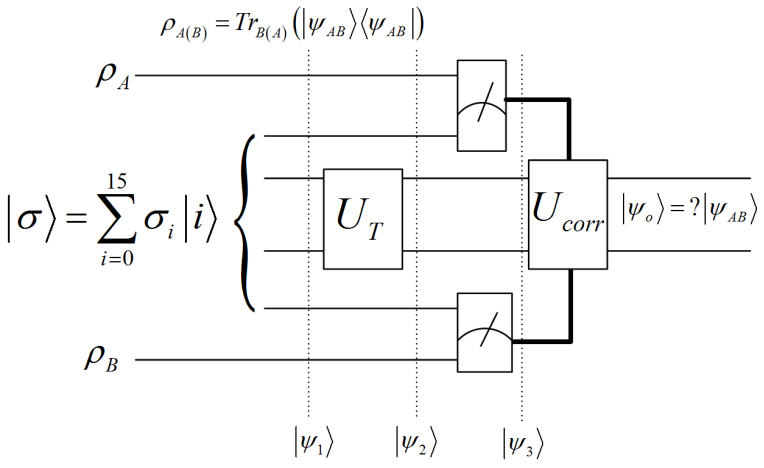
Tabela 7.1 – continuação da página anterior.

Classe	Estado canônico	π_4	Tipo	$\det(\Upsilon)$
$2d$	$\|\psi_{2d}\rangle = 1/\sqrt{6}(\|0001\rangle + \|0010\rangle + \|0100\rangle + \|1000\rangle + \sqrt{2}\,\|1111\rangle)$	1	N	0
$3a$	$\|\psi_{3a}\rangle = 1/2(\|0000\rangle + \|0101\rangle + \|1010\rangle + \|1111\rangle)$	0	U	$-1/16$
$3b$	$\|\psi_{3b}\rangle = 1/2(\|0000\rangle + \|0011\rangle + \|1100\rangle + \|1111\rangle)$	0	U	$1/16$
$3c$	$\|\psi_{3c}\rangle = 1/\sqrt{6}(\|0000\rangle + \|0000\rangle + \|0000\rangle + \|0000\rangle + \|0000\rangle + \|1111\rangle)$	0,1975	N	0
$3d$	$\|\psi_{3d}\rangle = 1/\sqrt{8}\left(\begin{array}{c}\|0000\rangle - \|0011\rangle + \|0101\rangle + \|0110\rangle + \\ \|1001\rangle - \|1010\rangle + \|1100\rangle + \|1111\rangle\end{array}\right)$	1	Ñ	0
$3e$	$\|\psi_{3e}\rangle = 1/3(\|0000\rangle + \|0101\rangle - 2\,\|0110\rangle + \|1001\rangle + \|1010\rangle + \|1111\rangle)$	0,6243	Ñ	$-1/27$
$3f$	$\|\psi_{3f}\rangle = 1/3(\|0000\rangle + \|0011\rangle - 2\,\|0101\rangle + \|1010\rangle + \|1100\rangle + \|1111\rangle)$	0,6243	Ñ	$-1/27$
$4a$	$\|\psi_{4a}\rangle = 1/\sqrt{17}(\|0000\rangle + \|0011\rangle + 3\,\|0101\rangle + \|1010\rangle - 2\,\|1100\rangle + \|1111\rangle)$	0,1217	Ñ	$-5/289$
$4b$	$\|\psi_{4b}\rangle = 1/\sqrt{12}(\|0000\rangle + 2\,\|0011\rangle + \|0101\rangle + \|1010\rangle + 2\,\|1100\rangle + \|1111\rangle)$	0,0625	N	$1/48$
$4c$	$\|\psi_{4c}\rangle = 1/\sqrt{12}(\|0000\rangle + \|0011\rangle + 2\,\|0101\rangle + 2\,\|1010\rangle + \|1100\rangle + \|1111\rangle)$	0,0625	N	$-1/48$
$4d$	$\|\psi_{4d}\rangle = 1/3(2\,\|0000\rangle - \|0011\rangle - \|0101\rangle + \|1010\rangle + \|1100\rangle + \|1111\rangle)$	0,6243	Ñ	0
5	$\|\psi_5\rangle = 1/\sqrt{12}(\|0000\rangle + \|0011\rangle + \|0101\rangle + 2\,\|1010\rangle + 2\,\|1100\rangle + \|1111\rangle)$	0,0560	Ñ	0

7.3 Teleportação de portas de dois qubits

O esquema para teleportação de portas quânticas de dois qubits considerando um estado geral de quatro qubits pode ser visto na Figura 7.1. O estado de quatro qubits $|\sigma\rangle$ contém

Figura 7.1: Circuito para teleportação de portas de dois qubits usando um estado geral de quatro qubits.



o entrelaçamento requerido para o protocolo de teleportação. Seguindo o procedimento usado em [69], tem-se depois de alguma álgebra que o estado resultante será

$$|\psi_o\rangle = \sum_{j,k=0}^{3} \frac{1}{2} U_T \Upsilon \beta_{jk} |\psi_{AB}\rangle \tag{7.3}$$

em que

$$\beta_{jk} = \beta_j \otimes \beta_k = \sqrt{2}\begin{bmatrix} \langle\beta_j|U_{00}\rangle & \langle\beta_j|U_{10}\rangle \\ \langle\beta_j|U_{01}\rangle & \langle\beta_j|U_{11}\rangle \end{bmatrix} \otimes \sqrt{2}\begin{bmatrix} \langle\beta_k|U_{00}\rangle & \langle\beta_k|U_{10}\rangle \\ \langle\beta_k|U_{01}\rangle & \langle\beta_k|U_{11}\rangle \end{bmatrix}, \tag{7.4}$$

A base de medição usada nas Equações (7.3) e (7.4) é $\{\beta_1, \beta_2, \beta_3, \beta_4\}$. A novidade nesta formulação do problema é a presença da matriz Υ, discutida na Seção 7.2, que depende basicamente do estado de quatro qubits usado como recurso no protocolo de teleportação.

7.3.1 O caso em que $\Upsilon = 1/2U_\sigma$

Consideram-se agora os diferentes resultados decorrentes dos tipos da matriz Υ, a começar pelo caso em que $\Upsilon = 1/2U_\sigma$, quando então o estado de saída será

$$|\psi_o\rangle = \sum_{j,k=0}^{3} \frac{1}{4} U_T U_\sigma \beta_{jk} |\psi_{AB}\rangle \tag{7.5}$$

e a teleportação se dará com sucesso se

$$\begin{aligned} |\psi_o\rangle &= \sum_{j,k=0}^{3} \frac{1}{4} U_T U_\sigma \beta_{jk} |\psi_{AB}\rangle \\ &= \sum_{j,k=0}^{3} \frac{1}{4} (U_T U_\sigma \beta_{jk} U_\sigma^\dagger U_T^\dagger) U_T U_\sigma |\psi_{AB}\rangle \\ &= \sum_{j,k=0}^{3} \frac{1}{4} (V_j \otimes V_k) U_T U_\sigma |\psi_{AB}\rangle , \end{aligned} \tag{7.6}$$

em que V_j e V_k são portas de um qubit. Aplicando-se a correção $U_{corr} = \left(V_j^\dagger \otimes V_k^\dagger\right)$ se obtém como resultado o estado $U_T U_\sigma |\psi_{AB}\rangle$. O resultado apresentado na Equação (7.6) deixa claro o papel do estado recurso de quatro qubits frente ao resultado final do protocolo de teleportação: a porta cuja ação efetivamente é teleportada é $U_T U_\sigma$, em que U_σ decorre diretamente do estado recurso. A Equação (7.6) proporciona ainda um outro ponto de vista acerca do protocolo de teleportação, vê-se que se pode fazer $U_T = I$ de modo que a porta teleportada decorra exclusivamente de uma escolha apropriada do estado recurso $|\sigma\rangle$.

A probabilidade de sucesso da teleportação dependerá ainda da base de medição utilizada, conforme explicado pelo Teorema 1 proposto em [69]. Tomando-se o caso particular em que $U_T = I$, pode-se mostrar facilmente que o estado recurso requerido para a teleportação de U_σ é

$$|\sigma\rangle = (I \otimes U_\sigma \otimes I) \cdot \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right). \tag{7.7}$$

Agora, lembrando que U_σ pode ser decomposta usando KAK [58] de modo que sua parte estritamente não local seja dada por $U_{NL} = e^{i\cdot(\theta_x\cdot\sigma_{XX}+\theta_y\cdot\sigma_{YY}+\theta_z\cdot\sigma_{ZZ})}$, em que $\sigma_{jj} = \sigma_j \otimes \sigma_j$ para $j \in \{X, Y, Z\}$, pode-se concluir:

1. O entrelaçamento de quatro vias, medido usando π_4, depende exclusivamente da parte não local de U_σ. Em particular, quando o estado $|\sigma\rangle$ tem entrelaçamento de quatro vias zero a porta U_σ tem ângulos não locais $\theta_x = \theta_y = \theta_z = 0$, portanto, é separável no produto de duas portas de um qubit.

2. De acordo com o Teorema 1 proposto em [69], a porta U_σ pode ser teleportada se, e somente se, seus ângulos não locais θ_i forem 0 ou $(2k_i + 1)\pi/4$, em que $k_i \in \mathbb{Z}$. Entretanto, nesta situação (excetuando-se o caso trivial de $\theta_x = \theta_y = \theta_z = 0$) o estado $|\sigma\rangle$ é maximamente entrelaçado, ou seja, $\pi_4(|\sigma\rangle) = 1$, portanto, é condição necessária (mas não suficiente) para uma teleportação determinística de U_σ que ela surja a partir de um estado $|\sigma\rangle$ maximamente entrelaçado. Por outro lado, como será visto posteriormente, nem sempre um estado maximamente entrelaçado $|\sigma\rangle$ tem sua correspondente porta quântica U_σ teleportável.

Por fim, vê-se que o caso considerado nesta seção corresponde ao caso tradicional tratado em [1] onde o estado de quatro qubits recurso da teleportação é o produto tensorial entre dois pares de Bell $((|00\rangle + |11\rangle)/2^{1/2})$. Deste modo, U_σ se torna a identidade e, como consequência, a porta teleportada, como mostrado na Figura 7.1, é U_T através do estado recurso $(I \otimes U_T \otimes I) \cdot ((|00\rangle + |11\rangle)/2^{1/2} \otimes (|00\rangle + |11\rangle)/2^{1/2})$.

7.3.2 O caso em que 2Υ não é unitária mas Υ é normal

Não sendo 2Υ unitária, mas Υ normal, tem-se que $\Upsilon = UDU^\dagger$ e gera como estado resultante

$$\rho_o = \frac{1}{4}\sum_{j,k=0}^{3} \left|\psi_o^{jk}\right\rangle \left\langle\psi_o^{jk}\right| = \frac{1}{4}\sum_{j,k=0}^{3} \frac{\Upsilon\beta_{jk}\left|\psi_{ab}\right\rangle \left\langle\psi_{ab}\right| \beta_{jk}^\dagger \Upsilon^\dagger}{\left\langle\psi_{ab}\left|\beta_{jk}^\dagger \Upsilon^\dagger \Upsilon \beta_{jk}\right|\psi_{ab}\right\rangle}, \tag{7.8}$$

em que

$$\left|\psi_o^{jk}\right\rangle = \frac{1}{\sqrt{\langle\psi_{ab}|\beta_{jk}^\dagger U \begin{bmatrix} |\lambda_0|^2 & 0 & 0 & 0 \\ 0 & |\lambda_1|^2 & 0 & 0 \\ 0 & 0 & |\lambda_2|^2 & 0 \\ 0 & 0 & 0 & |\lambda_3|^2 \end{bmatrix} U^\dagger \beta_{jk}|\psi_{ab}\rangle}} U \begin{bmatrix} \lambda_0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 \\ 0 & 0 & 0 & \lambda_3 \end{bmatrix} U^\dagger \beta_{jk}|\psi_{ab}\rangle \tag{7.9}$$

$$\left|\psi_0^{jk}\right\rangle = U\left(\frac{\lambda_0\langle 00|U^\dagger\beta_{jk}|\psi_{ab}\rangle|00\rangle+\lambda_1\langle 01|U^\dagger\beta_{jk}|\psi_{ab}\rangle|01\rangle+\lambda_2\langle 10|U^\dagger\beta_{jk}|\psi_{ab}\rangle|10\rangle+\lambda_3\langle 11|U^\dagger\beta_{jk}|\psi_{ab}\rangle|11\rangle}{\sqrt{\left|\lambda_0\langle 00|U^\dagger\beta_{jk}|\psi_{ab}\rangle\right|^2+\left|\lambda_1\langle 01|U^\dagger\beta_{jk}|\psi_{ab}\rangle\right|^2+\left|\lambda_2\langle 10|U^\dagger\beta_{jk}|\psi_{ab}\rangle\right|^2+\left|\lambda_3\langle 11|U^\dagger\beta_{jk}|\psi_{ab}\rangle\right|^2}}\right). \tag{7.10}$$

Nas Equações (7.9) e (7.10), λ_i representa um autovalor de Υ, em que $i \in \{0,1,2,3\}$. Ainda, a Equação (7.10) pode ser reescrita como

$$\left|\psi_0^{jk}\right\rangle = U\left(\frac{\lambda_0\langle 00|V_{jk}U^\dagger|\psi_{ab}\rangle|00\rangle+\lambda_1\langle 01|V_{jk}U^\dagger|\psi_{ab}\rangle|01\rangle+\lambda_2\langle 10|V_{jk}U^\dagger|\psi_{ab}\rangle|10\rangle+\lambda_3\langle 11|V_{jk}U^\dagger|\psi_{ab}\rangle|11\rangle}{\sqrt{\left|\lambda_0\langle 00|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2+\left|\lambda_1\langle 01|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2+\left|\lambda_2\langle 10|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2+\left|\lambda_3\langle 11|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2}}\right), \tag{7.11}$$

em que $V_{jk} = U^\dagger\beta_{jk}U$. Agora, considera-se o caso particular em que se observam as seguintes características: 1) é escolhida a base de Bell para medições, portanto, as correções são feitas usando portas do grupo de Pauli; 2) U faz parte do grupo de Clifford; 3) O estado de entrada é tal que $U^\dagger|\psi_{ab}\rangle = |00\rangle$. Neste caso, a Equação (7.11) se torna

$$\left|\psi_0^{jk}\right\rangle = U\left(\frac{\lambda_0\langle 00|\sigma_{jk}|00\rangle|00\rangle+\lambda_1\langle 01|\sigma_{jk}|00\rangle|01\rangle+\lambda_2\langle 10|\sigma_{jk}|00\rangle|10\rangle+\lambda_3\langle 11|\sigma_{jk}|00\rangle|11\rangle}{\sqrt{\left|\lambda_0\langle 00|\sigma_{jk}|00\rangle\right|^2+\left|\lambda_1\langle 01|\sigma_{jk}|00\rangle\right|^2+\left|\lambda_2\langle 10|\sigma_{jk}|00\rangle\right|^2+\left|\lambda_3\langle 11|\sigma_{jk}|00\rangle\right|^2}}\right). \tag{7.12}$$

A Tabela 7.2 mostra os possíveis estados na saída, de acordo com o resultado da medição, quando $\lambda_i \neq 0$.

Tabela 7.2: Estados na saída na Equação (7.12) de acordo com os resultados da medição usando a base de Bell.

σ_{jk}	$\left\|\psi_o^{jk}\right\rangle$	σ_{jk}	$\left\|\psi_o^{jk}\right\rangle$
$I\otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\|00\rangle$	$\sigma_Y\otimes I$	$\left\|\psi_o^{jk}\right\rangle = iU\|10\rangle$
$I\otimes\sigma_X$	$\left\|\psi_o^{jk}\right\rangle = U\|01\rangle$	$\sigma_Y\otimes\sigma_X$	$\left\|\psi_o^{jk}\right\rangle = iU\|11\rangle$
$I\otimes\sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\|01\rangle$	$\sigma_Y\otimes\sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = -U\|11\rangle$
$I\otimes\sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\|00\rangle$	$\sigma_Y\otimes\sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = iU\|10\rangle$
$\sigma_X\otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\|10\rangle$	$\sigma_Z\otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\|00\rangle$
$\sigma_X\otimes\sigma_X$	$\left\|\psi_o^{jk}\right\rangle = U\|11\rangle$	$\sigma_Z\otimes\sigma_X$	$\left\|\psi_o^{jk}\right\rangle = U\|01\rangle$
$\sigma_X\otimes\sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\|11\rangle$	$\sigma_Z\otimes\sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\|01\rangle$
$\sigma_X\otimes\sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\|10\rangle$	$\sigma_Z\otimes\sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\|00\rangle$

Como pode ser notado na Tabela 7.2, o estado resultante não é a aplicação de uma operação unitária aplicada ao estado de entrada $|\psi_{ab}\rangle$. O estado resultado é, a menos de um fator de fase global, probabilisticamente, um dos possíveis estados: $U|00\rangle$, $U|01\rangle$, $U|10\rangle$, $U|11\rangle$, em que U decorre da decomposição de Υ e, portanto, depende do estado $|\sigma\rangle$ recurso da teleportação. Deste modo, na verdade é teleportada a ação de U sobre a base canônica. Pode-se notar que não é requerida correção, isso ocorre porque não se pode escolher o estado a ser teleportado, o resultado é intrinsecamente probabilístico.

Como outro exemplo, considera-se o estado maximamente entrelaçado de quatro qubits

$$|\xi\rangle = (|0000\rangle + |0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)/\sqrt{8}, \tag{7.13}$$

para o qual se tem

$$\Upsilon = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = U \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 0 \\ 0 & 0 & 0 & 1/\sqrt{2} \end{bmatrix} U^\dagger \tag{7.14}$$

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{bmatrix}. \tag{7.15}$$

Portanto, neste caso a Equação (7.10) se reduz a

$$\left|\psi_0^{jk}\right\rangle = U \left(\frac{(\langle 00| \beta_{jk} |\psi_{ab}\rangle + \langle 11| \beta_{jk} |\psi_{ab}\rangle) |10\rangle + (\langle 01| \beta_{jk} |\psi_{ab}\rangle + \langle 10| \beta_{jk} |\psi_{ab}\rangle) |11\rangle}{\sqrt{|(\langle 00| \beta_{jk} |\psi_{ab}\rangle + \langle 11| \beta_{jk} |\psi_{ab}\rangle)|^2 + |\langle 01| \beta_{jk} |\psi_{ab}\rangle + \langle 10| \beta_{jk} |\psi_{ab}\rangle|^2}} \right). \tag{7.16}$$

Tomando novamente a base de Bell para medições e $|\psi_{ab}\rangle = |00\rangle$, tem-se na Tabela 7.3 os possíveis estados na saída.

Tabela 7.3: Estados na saída da Equação (7.16) de acordo com os resultados da medição usando a base de Bell.

σ_{jk}	$\left\|\psi_o^{jk}\right\rangle$	σ_{jk}	$\left\|\psi_o^{jk}\right\rangle$
$I \otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\|10\rangle$	$\sigma_Y \otimes I$	$\left\|\psi_o^{jk}\right\rangle = iU\|11\rangle$
$I \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = U\|11\rangle$	$\sigma_Y \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = iU\|10\rangle$
$I \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\|11\rangle$	$\sigma_Y \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = -U\|10\rangle$
$I \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\|10\rangle$	$\sigma_Y \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = iU\|11\rangle$
$\sigma_X \otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\|11\rangle$	$\sigma_Z \otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\|10\rangle$
$\sigma_X \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = U\|10\rangle$	$\sigma_Z \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = U\|11\rangle$
$\sigma_X \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\|10\rangle$	$\sigma_Z \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\|11\rangle$
$\sigma_X \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\|11\rangle$	$\sigma_Z \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\|10\rangle$

Como mostrado na Tabela 7.3, apenas a ação de U sobre dois estados da base canônica são teleportados, isso acontece porque Υ na Equação (7.14) tem apenas dois auto-

valores não nulos. Em geral, um estado na forma $a\left|0000\right\rangle + b\left|0011\right\rangle + c\left|0101\right\rangle + d\left|0110\right\rangle + d\left|1001\right\rangle + c\left|1010\right\rangle + b\left|1100\right\rangle + a\left|1111\right\rangle$ [70] produz uma matriz Υ normal.

7.3.3 O caso em que Υ não é normal

Por fim, considera-se o último caso, quando Υ não é normal. Mesmo não sendo uma matriz normal, ainda é possível definir uma diagonalização para a matriz Υ envolvendo matrizes unitárias. Aplicando primeiramente a decomposição polar, tem-se $\Upsilon = UH$, em que U é unitária e H é hermitiana. Agora, a matriz hermitiana, sendo normal, é decomposta como $H = VDV^\dagger$, de modo que $\Upsilon = UVDV^\dagger = WDV^\dagger$, em que D é uma matriz diagonal cujos elementos são os autovalores de H. Com isso, o estado resultante se torna

$$\rho_o = \sum_{j,k=0}^{3} \frac{1}{4} \left|\psi_0^{jk}\right\rangle \left\langle\psi_0^{jk}\right| = \sum_{j,k=0}^{3} \frac{1}{4} \frac{\Upsilon\beta_{jk}\left|\psi_{ab}\right\rangle \left\langle\psi_{ab}\right| \beta_{jk}^\dagger \Upsilon^\dagger}{\left\langle\psi_{ab}\right| \beta_{jk}^\dagger \Upsilon^\dagger \Upsilon \beta_{jk} \left|\psi_{ab}\right\rangle} \tag{7.17}$$

$$\left|\psi_0^{jk}\right\rangle = \frac{1}{\sqrt{\left\langle\psi_{ab}\right|\beta_{jk}^\dagger V \begin{bmatrix} |\lambda_0|^2 & 0 & 0 & 0 \\ 0 & |\lambda_1|^2 & 0 & 0 \\ 0 & 0 & |\lambda_2|^2 & 0 \\ 0 & 0 & 0 & |\lambda_3|^2 \end{bmatrix} V^\dagger \beta_{jk} \left|\psi_{ab}\right\rangle}} W \begin{bmatrix} \lambda_0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 \\ 0 & 0 & 0 & \lambda_3 \end{bmatrix} V^\dagger \beta_{jk} \left|\psi_{ab}\right\rangle \Rightarrow \tag{7.18}$$

$$\left|\psi_0^{jk}\right\rangle = W \left(\frac{\lambda_0 \langle 00|V^\dagger \beta_{jk}|\psi_{ab}\rangle |00\rangle + \lambda_1 \langle 01|V^\dagger \beta_{jk}|\psi_{ab}\rangle |01\rangle + \lambda_2 \langle 10|V^\dagger \beta_{jk}|\psi_{ab}\rangle |10\rangle + \lambda_3 \langle 11|V^\dagger \beta_{jk}|\psi_{ab}\rangle |11\rangle}{\sqrt{\left|\lambda_0 \langle 00|V^\dagger \beta_{jk}|\psi_{ab}\rangle\right|^2 + \left|\lambda_1 \langle 01|V^\dagger \beta_{jk}|\psi_{ab}\rangle\right|^2 + \left|\lambda_2 \langle 10|V^\dagger \beta_{jk}|\psi_{ab}\rangle\right|^2 + \left|\lambda_3 \langle 11|V^\dagger \beta_{jk}|\psi_{ab}\rangle\right|^2}} \right). \tag{7.19}$$

Este resultado é similar ao da Equação (7.10), mas agora λ_i's representam os autovalores da matriz H e não os da matriz Υ. Além disso, tem-se que $Tr(\Upsilon\Upsilon^\dagger) = Tr(HH^\dagger) = 1$ e, portanto, $\sum_i |\lambda_i|^2 = 1$. Agora, considera-se o caso em que a base de Bell é usada para medição, V pertence ao grupo de Clifford e o estado de entrada é tal que $V^\dagger \left|\psi_{ab}\right\rangle = \left|00\right\rangle$, então a Equação (7.19) é reduzida para

$$\left|\psi_0^{jk}\right\rangle = W \left(\frac{\lambda_0 \langle 00|\sigma_{jk}|00\rangle |00\rangle + \lambda_1 \langle 01|\sigma_{jk}|00\rangle |01\rangle + \lambda_2 \langle 10|\sigma_{jk}|00\rangle |10\rangle + \lambda_3 \langle 11|\sigma_{jk}|00\rangle |11\rangle}{\sqrt{\left|\lambda_0 \langle 00|\sigma_{jk}|00\rangle\right|^2 + \left|\lambda_1 \langle 01|\sigma_{jk}|00\rangle\right|^2 + \left|\lambda_2 \langle 10|\sigma_{jk}|00\rangle\right|^2 + \left|\lambda_3 \langle 11|\sigma_{jk}|00\rangle\right|^2}} \right). \tag{7.20}$$

Observando-se a Equação (7.20), pode-se ver como resultado a teleportação da ação de W sobre um conjunto de estados, entretanto, neste caso W não pertence a Clifford. Outra possibilidade para uma matriz não normal é usar a decomposição de Schur $\Upsilon = UTU^\dagger$,

em que T é uma matriz triangular superior. Como exemplo, toma-se o estado [71]

$$|\xi\rangle = (|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle)/\sqrt{8}, \tag{7.21}$$

para o qual se tem a seguinte matriz Υ e correspondente decomposição:

$$\Upsilon = \frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = UTU^\dagger = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1/\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/\sqrt{2} \\ 0 & 0 & 0 & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \end{bmatrix}^\dagger. \tag{7.22}$$

Deste modo, o estado na saída do protocolo de teleportação será

$$\rho_o = \sum_{j,k=0}^{3} \frac{1}{4} \left|\psi_0^{jk}\right\rangle \left\langle\psi_0^{jk}\right| = \sum_{j,k=0}^{3} \frac{1}{4} \frac{\Upsilon\beta_{jk}\,|\psi_{ab}\rangle\,\langle\psi_{ab}|\,\beta_{jk}^\dagger\Upsilon^\dagger}{\langle\psi_{ab}|\,\beta_{jk}^\dagger\Upsilon^\dagger\Upsilon\beta_{jk}\,|\psi_{ab}\rangle} \tag{7.23}$$

$$\left|\psi_0^{jk}\right\rangle = \frac{U\left(|00\rangle\langle 00| + |10\rangle\langle 11|\right)U^\dagger\beta_{jk}\,|\psi_{ab}\rangle}{\sqrt{2}} = \tag{7.24}$$

$$\left|\psi_0^{jk}\right\rangle = U\frac{\left(\langle 00|\,\beta_{jk}\,|\psi_{ab}\rangle + \langle 11|\,\beta_{jk}\,|\psi_{ab}\rangle\right)|00\rangle + \left(\langle 10|\,\beta_{jk}\,|\psi_{ab}\rangle - \langle 01|\,\beta_{jk}\,|\psi_{ab}\rangle\right)|10\rangle}{\sqrt{\left|\left(\langle 00|\,\beta_{jk}\,|\psi_{ab}\rangle + \langle 11|\,\beta_{jk}\,|\psi_{ab}\rangle\right)\right|^2 + \left|\langle 10|\,\beta_{jk}\,|\psi_{ab}\rangle - \langle 01|\,\beta_{jk}\,|\psi_{ab}\rangle\right|^2}}. \tag{7.25}$$

Mais uma vez, tomando a base de Bell para medições e $|\psi_{ab}\rangle = |00\rangle$, tem-se na Tabela 7.4 os possíveis estados na saída.

Tabela 7.4: Estados na saída da Equação (7.25) de acordo com os resultados da medição usando a base de Bell.

σ_{jk}	$\left\|\psi_o^{jk}\right\rangle$	σ_{jk}	$\left\|\psi_o^{jk}\right\rangle$
$I \otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\,\|00\rangle$	$\sigma_Y \otimes I$	$\left\|\psi_o^{jk}\right\rangle = iU\,\|10\rangle$
$I \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = -U\,\|10\rangle$	$\sigma_Y \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = iU\,\|00\rangle$
$I \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = -iU\,\|10\rangle$	$\sigma_Y \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = -U\,\|00\rangle$
$I \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\,\|00\rangle$	$\sigma_Y \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\,\|10\rangle$
$\sigma_X \otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\,\|10\rangle$	$\sigma_Z \otimes I$	$\left\|\psi_o^{jk}\right\rangle = U\,\|00\rangle$
$\sigma_X \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = U\,\|00\rangle$	$\sigma_Z \otimes \sigma_X$	$\left\|\psi_o^{jk}\right\rangle = -U\,\|10\rangle$
$\sigma_X \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\,\|00\rangle$	$\sigma_Z \otimes \sigma_Y$	$\left\|\psi_o^{jk}\right\rangle = iU\,\|10\rangle$
$\sigma_X \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\,\|10\rangle$	$\sigma_Z \otimes \sigma_Z$	$\left\|\psi_o^{jk}\right\rangle = U\,\|00\rangle$

Como pode ser visto na Tabela 7.4, apenas a ação de U sobre dois estados da base computacional é teleportada.

7.4 Conclusão

Neste capítulo é completado o estudo acerca do protocolo de teleportação da ação de portas de dois qubits na medida que estuda o papel desempenhado pelo estado recurso no protocolo. A partir dessa nova perspectiva, pode-se definir duas classes para tais estados recurso: 1) o conjunto de estados que emerge quando $\Upsilon = 1/2U_\sigma$, para U_σ unitária; 2) o conjunto de estados que emerge quando Υ é normal mas 2Υ não é unitária ou quando Υ não é normal. As principais diferenças no protocolo quando estados de ambas as classes são utilizados são:

- Classe 1
    1. A base de medição é importante para definir a probabilidade de sucesso, bem como as correções associadas.
    2. Uma teleportação determinística é alcançada apenas se o estado recurso for, segundo π_4, maximamente entrelaçado.
    3. O estado teleportado é a ação de U sobre o estado de entrada do protocolo, como normalmente se almeja.
- Classe 2
    1. Ocorre probabilisticamente a teleportação da ação de U sobre um conjunto de estados.
    2. A base de medição e o estado de entrada são usados para definir o possível conjunto de estados resultantes.
    3. Não é utilizada correção no processo.

Adicionalmente, mostrou-se a teleportação probabilística dos estados da base canônica através de uma porta de dois qubits dentro do grupo de Clifford, para o caso de Υ ser normal, ou através de uma porta fora do grupo de Clifford quando Υ não é normal. Nos casos particulares em que os estados descritos na Equação (7.13) e na Equação (7.21) são utilizados, tem-se que o resultado é, probabilisticamente, um par de Bell.

Parte III

Entrelaçadores Universais

Capítulo 8

Busca por entrelaçadores universais

Resumo

Este capítulo apresenta uma contribuição desta tese na medida que aplica a noção de separabilidade matricial para encontrar condições nas quais um dado estado quântico pode ser considerado separável, ou seja, não entrelaçado em dadas partições. Na sequência, tais condições são aplicadas para conjecturar algumas portas quânticas como sendo entrelaçadores universais. As ferramentas desenvolvidas foram capazes de apontar contraexemplos na literatura, tanto sobre estados entrelaçados quanto sobre entrelaçadores universais.

8.1 Introdução

Uma crescente atenção tem sido dedicada ao estudo dos entrelaçadores [20–23], buscando entender suas propriedades, construção e aplicações. Uma classe particularmente interessante de entrelaçadores são os chamados entrelaçadores universais [24], portas quânticas capazes de transformar qualquer estado desentrelaçado (pertencentes a um espaço de Hilbert apropriado) em um estado entrelaçado.

Embora seja apontado na literatura que, na medida que se lida com dimensões maiores, os entrelaçadores universais se tornam abundantes, não é uma tarefa fácil afirmar que uma dada porta quântica é um entrelaçador universal. Neste trabalho são utilizadas algumas relações que verificam a separabilidade de estados quânticos para, com o apoio de heurísticas computacionais, buscar bons candidatos a entrelaçadores universais [72]. Com isso, algumas portas quânticas que operam nos espaços $\mathbb{C}^3 \otimes \mathbb{C}^4$ e $\mathbb{C}^4 \otimes \mathbb{C}^4$ são conjecturadas como sendo entrelaçadores universais. Adicionalmente, a eficácia da abordagem proposta pode ser verificada ao ser capaz de invalidar conhecidos resultados da literatura, tanto a respeito de estados entrelaçados quanto de entrelaçadores universais.

O restante deste capítulo está organizado da seguinte forma: A Seção 8.2 cobre algumas definições elementares usadas ao longo do capítulo. Uma descrição da aplicação da noção de separabilidade para verificar estados entrelaçados é dada na Seção 8.3, o mesmo é feito no contexto da análise de entrelaçadores universais na Seção 8.4. Na Seção 8.5 é descrita a abordagem utilizada para conjecturar algumas portas como entrelaçadores universais. Por fim, as conclusões são apresentadas na Seção 8.6.

8.2 Noções elementares

Esta seção traz uma rápida revisão acerca de estados quânticos d-dimensionais, medidas de entrelaçamento e entrelaçadores universais.

8.2.1 Medidas de entrelaçamento

Conforme já apresentado no Capítulo 3, um qudit é um estado quântico d-dimensional cuja forma geral, usando a base canônica, é dado por

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \tag{8.1}$$

em que α_i obedece à condição de normalização $|\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{d-1}|^2 = 1$. Um medição em $|\psi\rangle$ na base canônica implica que se obterá o resultado i com probabilidade $|\alpha_i|^2$. Diz-se que um dado estado $|\psi\rangle_{AB}$ é separável se ele pode ser descrito como o produto tensorial de dois outros estados, formalmente, se $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$. Por outro lado, se $|\psi\rangle_{AB}$ é um estado entrelaçado suas partes não podem ser descritas isoladamente, apenas o sistema como um todo, deste modo, não existem $|\psi\rangle_A$ e $|\psi\rangle_B$ tal que $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$.

Por sua vez, o entrelaçamento é um recurso físico e há medidas consolidadas para avaliar o grau de correlação de um sistema quântico biparte, tais como a entropia de Von Neumann [73], a concorrência [74], a PPT [75] e a negatividade [76]. Cada uma dessas medidas de entrelaçamento possuem particularidades, mas neste capítulo será usada apenas a entropia de Von Neumann. Dado um estado entrelaçado biparte puro $|\psi\rangle_{AB}$, o entrelaçamento calculado pela entropia de Von Neumann é dado por

$$E_{VN}(\rho_A) = -Tr(\rho_A \cdot \log(\rho_A)), \tag{8.2}$$

em que $\rho_A = Tr_B\left(|\psi\rangle_{AB} \langle\psi|\right)$.

8.2.2 Entrelaçadores universais

Uma porta quântica U que opera em dois qudits é um entrelaçador se existe um dado estado separável $|\psi\rangle_{AB}$ tal que $E_{VN}(U|\psi\rangle_{AB}) \neq 0$. Em outras palavras, qualquer porta

capaz de gerar entrelaçamento entre dois estados separáveis é considerada um entrelaçador.

A noção de poder de entrelaçamento foi desenvolvida em [77] para ajudar na caracterização do entrelaçamento gerado por uma porta quântica, enquanto em [22] se estabeleceu uma conexão com alguns invariantes, ambos os conceitos relacionam portas quânticas com a mesma capacidade de gerar entrelaçamento. Em [78] foi introduzido o conceito de entrelaçadores perfeitos, portas capazes de gerar um estado maximamente entrelaçado a partir de estados desentrelaçados. Uma classe mais específica de entrelaçadores foi definida em [79] como resposta à questão: existe entrelaçador perfeito capaz de gerar estados maximamente entrelaçados a partir de todos os estados de uma base desentrelaçada? Essa classe particular de entrelaçadores recebeu o nome de entrelaçadores perfeitos especiais. Então, dados quatro estados separáveis ortogonais um entrelaçador perfeito especial é capaz de gerar estados maximamente entrelaçados a partir dos quatro estados.

Por fim, uma classe de entrelaçadores ainda mais geral foi introduzida em [24], chamada entrelaçadores universais, em resposta à questão: existem entrelaçadores capazes de entrelaçar qualquer par de estados separáveis? Formalmente, um entrelaçador universal é uma porta U tal que $E_{VN}(U(|\phi\rangle_m \otimes |\psi\rangle_n)) \neq 0 \ \forall \ |\phi\rangle_m, |\psi\rangle_n$, em que $|\phi\rangle_m$ e $|\psi\rangle_n$ são estados arbitrários de um qudit de dimensões, respectivamente, m e n. Foi apontado em [24] que entrelaçadores universais existem se, e somente se, $\min(m,n) \geq 3$ e $(m,n) \neq (3,3)$. Entretanto, construir explicitamente um entrelaçador universal para operar em um sistema biparte arbitrário $m \otimes n$ é uma questão que permanece em aberto. Um exemplo explícito para o espaço $\mathbb{C}^3 \otimes \mathbb{C}^4$ foi dado em [80], o qual será discutido em detalhes posteriormente, e em [81] foram apresentados dois entrelaçadores universais aplicáveis à sistemas bosônicos e fermiônicos.

8.3 Separabilidade de estados quânticos

Nesta seção são descritas algumas condições para verificação da separabilidade de estados quânticos, para tanto, são usadas as condições necessárias e suficientes, estabelecidas no Capítulo 4, para verificar a separabilidade de uma matriz arbitrária. Começa-se por observar que se $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ é um estado separável, então sua matriz densidade correspondente também o será, formalmente, $\rho = (|\psi_1\rangle\langle\psi_1|) \otimes (|\psi_2\rangle\langle\psi_2|)$. Deste modo, a abordagem consiste em simplesmente checar a separabilidade da matriz ρ, conforme veremos para alguns casos adiante.

Relembrando a partir do Capítulo 4, para verificar a hipótese de que $\rho = |\psi\rangle\langle\psi|$ é um estado separável na forma $|\psi_1\rangle\langle\psi_1| \otimes |\psi_2\rangle\langle\psi_2|$, em que $|\psi\rangle \in \mathbb{C}^{m\cdot n}$, $|\psi_1\rangle \in \mathbb{C}^m$ e $|\psi_2\rangle \in \mathbb{C}^n$, tem-se que, a partir do mapeamento $\gamma(\vec{p},\vec{q},\vec{r},\vec{s}) = (\vec{p}\otimes\vec{r})^\dagger \cdot \rho \cdot (\vec{q}\otimes\vec{s})$, deve-se observar

$$\gamma(\vec{p}_1,\vec{q}_1,\vec{r}_1,\vec{s}_1)\cdot\gamma(\vec{p}_2,\vec{q}_2,\vec{r}_2,\vec{s}_2) = \gamma(\vec{p}_1,\vec{q}_1,\vec{r}_2,\vec{s}_2)\cdot\gamma(\vec{p}_2,\vec{q}_2,\vec{r}_1,\vec{s}_1) \tag{8.3}$$

para todos os vetores $\{\vec{p}_i,\vec{q}_i\}$ em uma base de $\mathbb{C}^m$ e $\{\vec{r}_j,\vec{s}_j\}$ em uma base de $\mathbb{C}^n$. Tomando o

caso específico da forma da Equação (8.1) para $d = 2$ e aplicando o procedimento, tem-se que um dado estado será separável se

$$\alpha_0\alpha_3 - \alpha_1\alpha_2 = 0 \tag{8.4}$$

que, como já era esperado, coincide com um resultado largamente conhecido na literatura: a medida de entrelaçamento concorrência [74]. No geral, a checagem de biseparabilidade de um dado estado quântico recai em um sistema de equações polinomiais envolvendo os coeficientes do estado. A separabilidade é verificada se todas as equações resultarem em zero, caso contrário o estado não é separável. Por exemplo, em [82] foi apontado que o estado de três qutrits

$$|\kappa\rangle = \frac{1}{\sqrt{6}}\left(|000\rangle - |011\rangle - |112\rangle + |120\rangle - |202\rangle + |221\rangle\right) \tag{8.5}$$

é biseparável, mas se pode ver que este não é o caso. Tomando-se as bipartições $\rho_A = Tr_{BC}(|\kappa\rangle\langle\kappa|)$, $\rho_B = Tr_{AC}(|\kappa\rangle\langle\kappa|)$ e $\rho_C = Tr_{AB}(|\kappa\rangle\langle\kappa|)$ vê-se que elas falham ao se verificar algumas das condições que atestam a separabilidade de um qutrit. Por exemplo,

$$\alpha_1 \cdot \alpha_{15} - \alpha_6 \cdot \alpha_{10} = -\frac{1}{6} \quad \text{para} \quad \rho_{A\_BC} \tag{8.6a}$$

$$\alpha_1 \cdot \alpha_{11} - \alpha_2 \cdot \alpha_{10} = -\frac{1}{6} \quad \text{para} \quad \rho_{B\_AC} \tag{8.6b}$$

$$\alpha_1 \cdot \alpha_{13} - \alpha_4 \cdot \alpha_{10} = -\frac{1}{6} \quad \text{para} \quad \rho_{AB\_C}. \tag{8.6c}$$

Sobre o estado $|\kappa\rangle$ foi perguntado em [82]: "Como é possível que dois diferentes estados (um separável e outro não separável) tenham a mesma correlação baseada no entrelaçamento?" Não se acredita que isso seja possível, mas esta não é a questão, a realidade é que o estado $|\kappa\rangle$ não é separável.

Aplicando este procedimento aos estados pertencentes ao espaço $\mathbb{C}^3 \otimes \mathbb{C}^4$, ver-se-á que a separabilidade de um estado arbitrário $|\alpha_{34}\rangle = \alpha_1|01\rangle + \alpha_2|02\rangle + \alpha_3|03\rangle + \cdots + \alpha_{12}|23\rangle$ será verificada quando $\sum_{i=1}^{18}|\xi_i| = 0$, na qual

$$\begin{aligned}
&\xi_1 = \alpha_0\alpha_5 - \alpha_1\alpha_4, \quad \xi_2 = \alpha_0\alpha_6 - \alpha_2\alpha_4, \quad \xi_3 = \alpha_0\alpha_7 - \alpha_3\alpha_4,\\
&\xi_4 = \alpha_0\alpha_9 - \alpha_1\alpha_8, \quad \xi_5 = \alpha_0\alpha_{10} - \alpha_2\alpha_8, \quad \xi_6 = \alpha_0\alpha_{11} - \alpha_3\alpha_8,\\
&\xi_7 = \alpha_1\alpha_6 - \alpha_2\alpha_5, \quad \xi_8 = \alpha_1\alpha_7 - \alpha_3\alpha_5, \quad \xi_9 = \alpha_1\alpha_{10} - \alpha_2\alpha_9,\\
&\xi_{10} = \alpha_1\alpha_{11} - \alpha_3\alpha_9, \quad \xi_{11} = \alpha_2\alpha_7 - \alpha_3\alpha_6, \quad \xi_{12} = \alpha_2\alpha_{11} - \alpha_3\alpha_{10},\\
&\xi_{13} = \alpha_4\alpha_9 - \alpha_5\alpha_8, \quad \xi_{14} = \alpha_4\alpha_{10} - \alpha_6\alpha_8, \quad \xi_{15} = \alpha_4\alpha_{11} - \alpha_7\alpha_8,\\
&\xi_{16} = \alpha_5\alpha_{10} - \alpha_6\alpha_9, \quad \xi_{17} = \alpha_5\alpha_{11} - \alpha_7\alpha_9, \quad \xi_{18} = \alpha_6\alpha_{11} - \alpha_7\alpha_{10}.
\end{aligned} \tag{8.7}$$

De modo análogo, o procedimento quando aplicado aos estados pertencentes ao espaço $\mathbb{C}^4 \otimes \mathbb{C}^4$ revela que a separabilidade de um estado arbitrário $|\alpha_{44}\rangle = \alpha_1|01\rangle + \alpha_2|02\rangle + \alpha_3|03\rangle + \cdots +$

$\alpha_{16}|33\rangle$ será verificada quando $\sum_{i=1}^{36}|\zeta_i| = 0$, em que

$$\begin{aligned}
&\zeta_1 = \alpha_0\alpha_5 - \alpha_1\alpha_4, \quad \zeta_2 = \alpha_0\alpha_6 - \alpha_2\alpha_4, \quad \zeta_3 = \alpha_0\alpha_7 - \alpha_3\alpha_4,\\
&\zeta_4 = \alpha_0\alpha_9 - \alpha_1\alpha_8, \quad \zeta_5 = \alpha_0\alpha_{10} - \alpha_2\alpha_8, \quad \zeta_6 = \alpha_0\alpha_{11} - \alpha_3\alpha_8,\\
&\zeta_7 = \alpha_0\alpha_{13} - \alpha_1\alpha_{12}, \quad \zeta_8 = \alpha_0\alpha_{14} - \alpha_2\alpha_{12}, \quad \zeta_9 = \alpha_0\alpha_{15} - \alpha_3\alpha_{12},\\
&\zeta_{10} = \alpha_1\alpha_6 - \alpha_2\alpha_5, \quad \zeta_{11} = \alpha_1\alpha_7 - \alpha_3\alpha_5, \quad \zeta_{12} = \alpha_1\alpha_{10} - \alpha_2\alpha_9,\\
&\zeta_{13} = \alpha_1\alpha_{11} - \alpha_3\alpha_9, \quad \zeta_{14} = \alpha_1\alpha_{14} - \alpha_2\alpha_{13}, \quad \zeta_{15} = \alpha_1\alpha_{15} - \alpha_3\alpha_{13},\\
&\zeta_{16} = \alpha_2\alpha_7 - \alpha_3\alpha_6, \quad \zeta_{17} = \alpha_2\alpha_{11} - \alpha_3\alpha_{10}, \quad \zeta_{18} = \alpha_2\alpha_{15} - \alpha_3\alpha_{14},\\
&\zeta_{19} = \alpha_4\alpha_9 - \alpha_5\alpha_8, \quad \zeta_{20} = \alpha_4\alpha_{10} - \alpha_6\alpha_8, \quad \zeta_{21} = \alpha_4\alpha_{11} - \alpha_7\alpha_8,\\
&\zeta_{22} = \alpha_4\alpha_{13} - \alpha_5\alpha_{12}, \quad \zeta_{23} = \alpha_4\alpha_{14} - \alpha_6\alpha_{12}, \quad \zeta_{24} = \alpha_4\alpha_{15} - \alpha_7\alpha_{12},\\
&\zeta_{25} = \alpha_5\alpha_{10} - \alpha_6\alpha_9, \quad \zeta_{26} = \alpha_5\alpha_{11} - \alpha_7\alpha_9, \quad \zeta_{27} = \alpha_5\alpha_{14} - \alpha_6\alpha_{13},\\
&\zeta_{28} = \alpha_5\alpha_{15} - \alpha_7\alpha_{13}, \quad \zeta_{29} = \alpha_6\alpha_{11} - \alpha_7\alpha_{10}, \quad \zeta_{30} = \alpha_6\alpha_{15} - \alpha_7\alpha_{14},\\
&\zeta_{31} = \alpha_8\alpha_{13} - \alpha_9\alpha_{12}, \quad \zeta_{32} = \alpha_8\alpha_{14} - \alpha_{10}\alpha_{12}, \quad \zeta_{33} = \alpha_8\alpha_{15} - \alpha_{11}\alpha_{12},\\
&\zeta_{34} = \alpha_9\alpha_{14} - \alpha_{10}\alpha_{13}, \quad \zeta_{35} = \alpha_9\alpha_{15} - \alpha_{11}\alpha_{13}, \quad \zeta_{36} = \alpha_{10}\alpha_{15} - \alpha_{11}\alpha_{14}.
\end{aligned} \tag{8.8}$$

Este mesmo procedimento pode ser aplicado para se obter as condições de separabilidade de estados quânticos para partições e dimensões arbitrárias. Por exemplo, assumindo um estado no espaço $2 \otimes n$ com coeficientes $\alpha_1, \alpha_2, \cdots, \alpha_{2n}$ em que $\sum_{i=1}^{2n}|\alpha_i|^2 = 1$, ele será separável se, e somente se,

$$\sum_{i=1}^{n-1}\sum_{j=0}^{n-i}|\alpha_i \cdot \alpha_{j+n+2} - \alpha_{j+2} \cdot \alpha_{i+n}| = 0. \tag{8.9}$$

Algumas equações de separabilidade são mostradas no Apêndice A. Analisando-se numericamente o teste de biseparabilidade na dimensão $m \otimes n$, pode-se perceber que o número de equações ($\#eq$) associadas é dado por

$$\#eq = \left(\frac{m(m-1)}{2}\right) \cdot \left(\frac{n(n-1)}{2}\right) \tag{8.10a}$$

$$= (mn) \cdot \left(\frac{(m-1)\cdot(n-1)}{4}\right) \tag{8.10b}$$

$$= \frac{m^2n^2 - m^2n - mn^2 - mn}{4}, \tag{8.10c}$$

de onde é possível concluir que se trata de um polinômio de grau 2. Entretanto, ainda mais interessante é o fato que a proporção entre o número de equações e a dimensão do estado testado (mn) é dada por

$$\left(\frac{(m-1)\cdot(n-1)}{4}\right), \tag{8.11}$$

uma grandeza linear, portanto, pode-se afirmar que o teste de separabilidade proposto é efici-

ente.

8.4 Análise da universalidade de entrelaçadores

Ainda que não seja conhecido um teste simples para verificar se uma dada porta quântica é um entrelaçador universal, acredita-se que a abordagem aqui descrita pode contribuir com novas ideias acerca do tema uma vez que propõe uma abordagem algébrica ligeiramente diferente. Isso parte do fato de que, se U é um entrelaçador universal, então a matriz densidade

$$\rho = U(|\psi\rangle \langle\psi|)U^{\dagger} \tag{8.12}$$

não será separável para todo todo $|\psi\rangle$. Isto é equivalente a aplicar a Equação (8.3) na Equação (8.12) e verificar se o sistema de equações correspondente não possui solução (além da trivial em que todas as variáveis são zero). Pode-se também verificar se $E_{VN}(U|\psi\rangle) \neq 0$ para todo estado $|\psi\rangle$, mas além das limitações de particionamento e dimensionalidade impostos pelas medidas de entrelaçamento, manipular tais medidas simbolicamente costuma ser uma tarefa complicada. Ainda segundo [80], pode-se usar a expressão $U(|\alpha_A\rangle \otimes |\beta_A\rangle) = |\alpha_B\rangle \otimes |\beta_B\rangle$ para verificar se U é um entrelaçador universal, mas isso envolve o dobro de variáveis que o requerido para a abordagem descrita aqui.

Neste trabalho não foi possível resolver o problema inteiramente a ponto de fornecer uma parametrização explícita capaz de gerar entrelaçadores universais, mas a discussão de casos particulares pode contribuir gerando novas ideias sobre o tema. Por exemplo, analisando algumas manipulações algébricas simples, pode-se facilmente verificar o lema enunciado adiante.

Lema 8.1. *Se uma dada matriz U é um entrelaçador universal que opera no espaço $\mathbb{C}^n$, então todas suas n colunas são vetores que representam estados não separáveis.*

Demonstração. Toma-se $|u_i\rangle$ como a i-ésima coluna da matriz U e $|v_i\rangle$ como o i-ésimo estado da base canônica do espaço $\mathbb{C}^n$, então $U \cdot |v_i\rangle = |u_i\rangle$, portanto, se $|u_i\rangle$ é um estado separável então U não é um entrelaçador universal. □

Uma consequência direta do Lema 8.1 é que portas controladas não podem ser entrelaçadores universais. Mas existe um caso ainda mais interessante. Até onde se sabe, o único exemplo de entrelaçador universal que opera no espaço $(3 \otimes 4)$, enunciado em [80] e corroborado em [81,83],

é a porta quântica

$$U_H = \begin{bmatrix} + & - & - & - & - & - & - & - & - & - & - & - \\ + & + & - & + & - & - & - & + & + & + & - & + \\ + & + & + & - & + & - & - & - & + & + & + & - \\ + & - & + & + & - & + & - & - & - & + & + & + \\ + & + & - & + & + & - & + & - & - & - & + & + \\ + & + & + & - & + & + & - & + & - & - & - & + \\ + & + & + & + & - & + & + & - & + & - & - & - \\ + & - & + & + & + & - & + & + & - & + & - & - \\ + & - & - & + & + & + & - & + & + & - & + & - \\ + & - & - & - & + & + & + & - & + & + & - & + \\ + & + & - & - & - & + & + & + & - & + & + & - \\ + & - & + & - & - & - & + & + & + & - & + & + \end{bmatrix}, \tag{8.13}$$

em que os símbolos + e − significam, respectivamente, $1/\sqrt{12}$ e $-1/\sqrt{12}$. Entretanto, a partir do Lema 8.1 se pode ver que U_H não é um entrelaçador universal uma vez que a primeira coluna representa um estado separável. De fato, tem-se que

$$U_H \left(|0\rangle_3 \otimes |0\rangle_4\right) = F_3|0\rangle_3 \otimes F_4|0\rangle_4, \tag{8.14}$$

portanto $E_{VN}\left[U_H \left(|0\rangle_3 \otimes |0\rangle_4\right)\right] = 0$. Neste caso, $|0\rangle_d$ representa o estado zero d-dimensional, enquanto F_d representa a transformada de Fourier operando no espaço $\mathbb{C}^d$, cuja descrição será dada adiante.

8.5 Busca por entrelaçadores universais

Ainda que não seja conhecida uma decomposição KAK similar a usada para o caso de $SU(4)$, mas aplicável para uma dimensão arbitrária, é razoável supor que se pode decompor uma porta U qualquer de modo a extrair sua parte estritamente não local. Seguramente esta parte não local é ingrediente fundamental para compor o entendimento acerca da estrutura dos entrelaçadores universais. Enquanto não é conhecida uma abordagem para construir explicitamente entrelaçadores universais arbitrários, conhecer alguns exemplos pode ser útil na busca pelo entendimento de suas propriedades gerais. Embora para altas dimensões, conforme apontado em [80], uma matriz unitária escolhida aleatoriamente tende a ser um entrelaçador universal, construi-los a partir de portas quânticas mais familiares pode fornecer pistas interessantes acerca dessa estrutura.

Segundo as estratégicas algébricas conhecidas para lidar com o problema, verificar se uma porta é ou não um entrelaçador universal é um problema intratável, isso emerge do fato que resolver um sistema de equações polinomiais é, em geral, um problema NP-Completo.

Entretanto, na prática, encontrar um contraexemplo que prova que uma dada porta não é um entrelaçador universal é uma tarefa mais factível. Deste modo, neste trabalho foi utilizada uma quantidade expressiva de estratégias em um algoritmo de Evolução Diferencial [84, 85] para incrementar sua capacidade de encontrar contraexemplos que invalidem candidatos a entrelaçadores universais, incluindo: o uso da Equação (8.3) aplicada na Equação (8.12) e $E_{VN}\left(U\left|\psi\right\rangle\right)$ como funções de aptidão, variação no tamanho da população, na taxa de crossover, no fator de escala, detecção de estagnação de convergência e detecção de perda de diversidade da população. A aplicação da abordagem a casos sabidamente falsos indicam a corretude do procedimento, por exemplo, a porta U_H é invalidada em poucos segundos ao encontrar o estado $\left|0\right\rangle_3 \otimes \left|0\right\rangle_4$ como contraexemplo.

O objetivo principal é encontrar bons candidatos à entrelaçadores universais a partir de portas largamente conhecidas na literatura, portanto, foram testadas as portas F_{12}, X_{12}, Y_{12} e Z_{12} operando sobre o produto tensorial $\left|\psi_A\right\rangle_3 \otimes \left|\psi_B\right\rangle_4$ e, de modo análogo, as portas F_{16}, X_{16}, Y_{16} e Z_{16} operando sobre o produto tensorial $\left|\psi_A\right\rangle_4 \otimes \left|\psi_B\right\rangle_4$. Tais portas são a generalização [1, 18] d-dimensional das portas X, Z e F (transformada de Fourier em um qudit) [86], definidas como

$$X_d\left|k\right\rangle = \left|(k+1) \bmod d\right\rangle \tag{8.15a}$$

$$Z_d\left|k\right\rangle = \left(e^{(2\pi i/d)}\right)^k \left|k\right\rangle \tag{8.15b}$$

$$F_d\left|k\right\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} e^{(2\pi i k l/d)} \left|l\right\rangle, \tag{8.15c}$$

cujos elementos da representação matricial de cada uma delas é dado por

$$\left(X_d\right)_{mn} = \begin{cases} 1 & \text{if } m = (n+1) \bmod d \\ 0 & \text{otherwise} \end{cases}, \tag{8.16a}$$

$$\left(Z_d\right)_{mn} = \begin{cases} e^{(2\pi i/d)^{m-1}} & \text{se } m = n \\ 0 & \text{se } m \neq n \end{cases}, \tag{8.16b}$$

$$\left(F_d\right)_{mn} = e^{(2\pi i/d)^{mn}}/\sqrt{d}. \tag{8.16c}$$

Adicionalmente, faz-se $Y_d = i \cdot X_d Z_d$. Embora todas essas portas não sejam separáveis em (3⊗4) ou $(4 \otimes 4)$, todas elas falham quando submetidas ao algoritmo de avaliação de candidatos a entrelaçadores universais. Poucos segundos são suficientes para encontrar um contraexemplo. Depois da falha com essas portas optou-se por definir novos candidatos a partir de funções e/ou produtos dessas portas listadas, mas também falharam $\sqrt{X_{12}}$, $\sqrt{Z_{12}}$, $\sqrt{X_{16}}$, e $\sqrt{Z_{16}}$. Entretanto, foi possível encontrar alguns bons candidatos, são eles:

$$U_{E1} \quad = \quad \sqrt{Y_{12}}, \tag{8.17a}$$

$$U_{E2} = \sqrt{Y_{16}}, \tag{8.17b}$$
$$U_{E3} = \sqrt{X_{12}}^{\dagger} \cdot F_{12} \cdot \sqrt{X_{12}}, \tag{8.17c}$$
$$U_{E4} = \sqrt{X_{16}}^{\dagger} \cdot F_{16} \cdot \sqrt{X_{16}}. \tag{8.17d}$$

Todas as exaustivas tentativas de encontrar contraexemplos para as portas descritas na Equação (8.17) falharam. Nenhum ganho foi observado após vários dias de execução do algoritmo. Este comportamento embasa a Conjectura 8.1. Os valores mínimos de entrelaçamento encontrados, para cada porta, pelo algoritmo de avaliação quando usada a entropia de Von Neumann na busca por contraexemplos são mostrados na Tabela 8.1.

Conjectura 8.1. *As portas* $\sqrt{Y_d}$ *e* $\sqrt{X_d}^{\dagger} \cdot F_d \cdot \sqrt{X_d}$ *operando sobre o espaço* $(m \otimes n)$ *são entrelaçadores universais para* $d = 12$ $(3 \otimes 4)$ *e* $d = 16$ $(4 \otimes 4)$.

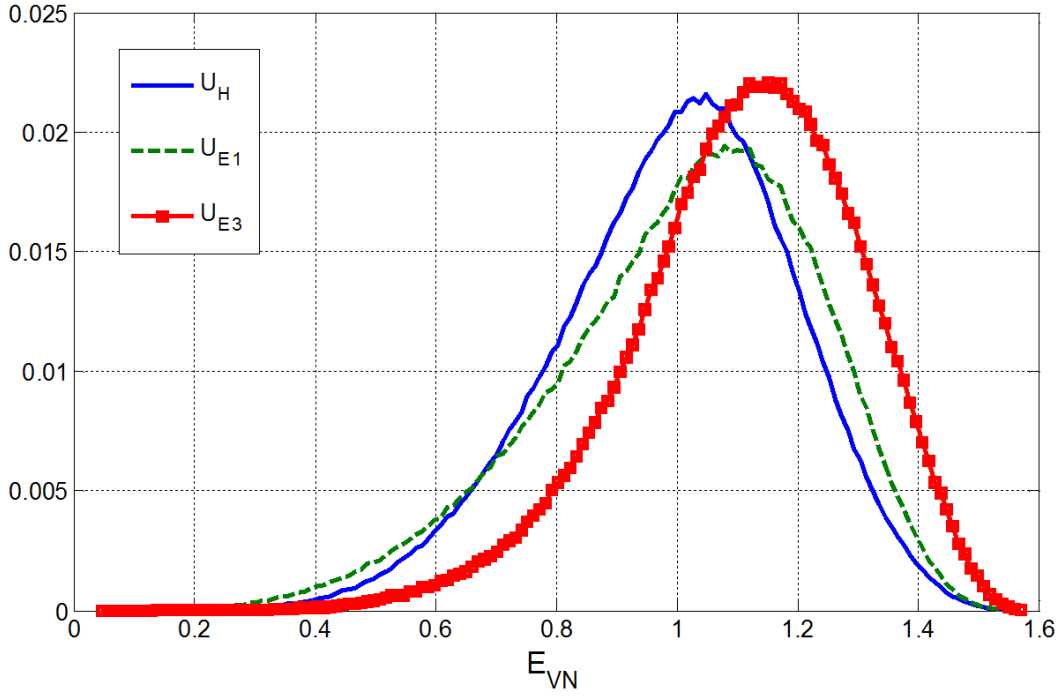
Tabela 8.1: Entrelaçamento mínimo gerado pelas portas U_{E1}, U_{E2}, U_{E3} e U_{E4} encontrados pelo algoritmo de avaliação.

Porta	Mínimo
U_{E1}	0 0.00001619968719695217664934251689 97
U_{E2}	0 0.00005732525053554026861057230091 13
U_{E3}	0 0.00502355595369780201508991268610 77
U_{E4}	0 0.00013082551874226520265999396119 83

Mostra-se curioso o fato de $\sqrt{Y_d}$ ser potencialmente um entrelaçador universal enquanto para $\sqrt{X_d}$ e $\sqrt{Z_d}$, conforme apontado anteriormente, rapidamente são encontrados contra exemplos e, portanto, são descartados como candidatos.

Por fim, foi analisado o entrelaçamento gerado pelas portas U_H, U_{E1} e U_{E3} sobre um milhão de estados separáveis montados a partir do produto tensorial de colunas de matrizes geradas aleatoriamente [87,88], esta distribuição é mostrada na Figura 8.1. Pode-se ver que as portas U_{E1} e U_{E3} geram, na média, mais entrelaçamento que U_H, mas naturalmente o espaço amostral é muito pequeno para permitir concluir que este comportamento é uma propriedade correlacionada com o provável fato de U_{E1} e U_{E3} serem entrelaçadores universais.

Figura 8.1: Distribuição do entrelaçamento gerado pelas portas U_H, U_{E1} e U_{E3} sobre um milhão de estados separáveis gerados aleatoriamente.



8.6 Conclusão

Neste capítulo foi descrita uma abordagem que pode ser usada para verificar a separabilidade de um estado quântico em partições e dimensões arbitrárias. Esta abordagem permitiu verificar, usando sua correspondente matriz densidade, que um estado de três qutrits apontado em [82] como separável era, de fato, não separável. Permitiu também mostrar que um exemplo de entrelaçador universal dado em [80] era falso. Com o apoio de uma heurística baseada na diferenciação evolutiva foi possível conjecturar algumas portas, construídas a partir de outras largamente conhecidas na literatura, como sendo entrelaçadores universais. É possível que isso venha a dar pistas na investigação das propriedades de tais portas. Por fim, acredita-se que, ainda que similarmente difícil, o melhor caminho para chegar ao completo entendimento acerca da estrutura dos entrelaçadores universais, incluindo encontrar uma parametrização para gerá-los, é usar a abordagem aqui descrita com uma parametrização de matrizes unitárias [88, 89] e estratégias para solução de sistemas de equações polinomiais [90–92].

Parte IV

Informação Quântica e a Teoria dos Números

Capítulo 9

Estados quânticos sequências

Resumo

Este capítulo apresenta a definição dos chamados estados quânticos sequências*, estados construídos a partir de sequências de números inteiros, bem como uma análise sobre algumas propriedades do entrelaçamento e a preparação destes estados através do algoritmo de Grover. Este entendimento pode ser útil ao desenvolvimento de protocolos em dimensões superiores e/ou testar ideias em teoria dos números.*

9.1 Introdução

Há algum tempo surgiram trabalhos [25–27] estabelecendo conexões entre a teoria da informação quântica e a teoria dos números. Mais recentemente, novos trabalhos [28–30] apontam fortes evidências de que a teoria da informação quântica pode ser um ambiente fértil para desenvolver e testar ideias relacionadas à teorias dos números. Estes trabalhos descrevem a manipulação de problemas importantes, tais como a Hipótese de Riemann e a Conjectura de Goldbach.

Neste capítulo são estudadas as propriedades de alguns estados quânticos sequências [93], em especial o entrelaçamento e a preparação usando o algoritmo de Grover. Este entendimento pode ser útil ao desenvolvimento de protocolos em dimensões superiores e/ou testar ideias em teoria dos números. Por exemplo, algum esforço [94–96] tem sido dedicado à busca por estados maximamente entrelaçados, mas isto é uma tarefa difícil, no melhor de nosso conhecimento não há exemplos descritos na literatura para estados com mais de sete qubits. Portanto, se um dado protocolo requer apenas que as bipartições formadas pela separação de um dos qubits dos demais sejam maximamente entrelaçadas, pode-se usar o estado PA aqui descrito para n-qubits, cuja preparação pode ser feita de modo eficiente. Por outro lado, no

que diz respeito à teoria dos números, tem-se como exemplo o estudo [29,30] acerca do estado Primo, um caso particular de estado sequência.

O restante deste capítulo é organizado como se segue. Uma discussão sobre a definição dos estados sequências e uma breve descrição de algumas sequências de inteiros são apresentadas na Seção 9.2. A Seção 9.3 mostra uma análise detalhada das propriedades do entrelaçamento de um conjunto de estados sequências. Na Seção 9.4, são descritas considerações sobre como preparar os estados sequências. Algumas novas sequências são introduzidas e analisadas na Seção 9.5. Por fim, as conclusões do capítulo são apresentadas na Seção 9.6.

9.2 Estados Quânticos Sequências

A partir de uma sequência finita de números inteiros pode-se definir o estado quântico sequência como se segue. Fazendo $S = (s_1, s_2, s_3, \cdots, s_k)$ ser um conjunto contendo os primeiros k elementos de uma sequência de inteiros menores que d^n, um estado quântico sequência de n-qudits é definido como

$$\left|S_n^d\right\rangle = \frac{1}{\sqrt{\tau(d^n)}} \sum_{i=1}^{k} |s_i\rangle \,, \tag{9.1}$$

em que τ é a função de contagem da sequência S que retorna a soma dos quadrados das quantidades de cada elemento dentro da sequência. No caso particular da sequência não ter elementos repetidos, τ retornará simplesmente o número de elementos dentro do conjunto e, como consequência, o estado quântico resultante será uma superposição equiprovável dos elementos da sequência. Então, usando a Equação (9.1), pode-se definir o mapeamento $\xi_n^d : \mathbb{Z}^k \to \mathbb{C}^{d^n}$, no qual $S(k) < d^n \; \forall \; k$, que toma uma sequência finita de números inteiros e retorna o estado quântico de n-qudits correspondente[1], por exemplo:

$$\xi_3^2(\{0,7\}) = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right), \tag{9.2a}$$

$$\xi_3^2(\{0,1,1,2,3,3,3,7\}) = \frac{1}{4} \left(|000\rangle + 2\,|001\rangle + |010\rangle + 3\,|011\rangle + |111\rangle\right), \tag{9.2b}$$

$$\xi_2^3(\{0,1,1,2,3,3,3,7\}) = \frac{1}{4} \left(|00\rangle + 2\,|01\rangle + |02\rangle + 3\,|10\rangle + |21\rangle\right). \tag{9.2c}$$

Usando esta definição serão construídos diversos estados quânticos, cujas propriedades serão estudadas, associados à várias sequências de números inteiros descritas na literatura [97]. Uma breve descrição de algumas dessas sequências usadas ao longo do trabalho pode ser conferida adiante.

- Primo (A000040): Seguramente uma das mais famosas sequência de números inteiros,

[1] No restante do capítulo será tratado apenas o caso particular de qubits ($d = 2$) em que o índice superior d é omitido. Além disso, sempre que não gerar ambiguidades será também omitido o índice inferior n.

está relacionada aos mais importantes problemas da teoria dos números, tais como a Conjectura de Goldbach e a Hipótese de Riemann. Seus primeiros elementos são $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$.

- Fibonacci (A000045): Esta famosa sequência é gerada a partir de uma fórmula recursiva em que um dado elemento é a soma dos dois elementos anteriores. Cresce rapidamente, existem apenas 43 elementos no intervalo $[0, 2^{28})$. A razão entre dois elementos consecutivos tende para a razão áurea ($\frac{1+\sqrt{5}}{2}$). Seus primeiros elementos são $\{0, 1, 1, 2, 3, 5, 8, 13, 21, 34\}$.

- Happy (A007770): Composta pelos números cuja sucessiva soma dos quadrados dos dígitos do número alcança o valor 1, por exemplo: $7 \to 7^2 = 49 \to 4^2 + 9^2 = 97 \to 9^2 + 7^2 = 130 \to 1^2 + 3^2 + 0^2 = 10 \to 1^2 + 0^2 = 1$. Seus primeiros elementos são $\{1, 7, 10, 13, 19, 23, 28, 31, 32, 44\}$.

- Lucky (A000959): De modo análogo aos números primos, trata-se de uma sequência gerada a partir do conjunto dos números inteiros por uma peneira onde para cada elemento $S(k)$ são removidos todos os elementos na posição $S(k) \cdot j$ para todo $j \in \mathbb{Z}$ e $k > 1$. Seus primeiros elementos são $\{1, 3, 7, 9, 13, 15, 21, 25, 31, 33\}$.

- Abundant (A005101): Sequência composta pelos números cuja soma dos divisores de $S(k)$ excede $2 \cdot S(k)$. Seus primeiros elementos são $\{12, 18, 20, 24, 30, 36, 40, 42, 48, 54\}$.

- Triangular (A000217): Consiste das quantidades de objetos que podem ser empilhados para formar triângulos equiláteros, possui a fórmula fechada $S(k) = \frac{k(k+1)}{2}$. Seus primeiros elementos são $\{0, 1, 3, 6, 10, 15, 21, 28, 36, 45\}$.

- Lazy (A000124): Composta pelos números máximos de pedaços de um círculo formados por um dado número de cortes retos, possui a fórmula fechada $S(k) = \frac{k(k+1)}{2} + 1$, bastante similar à geradora da sequência Triangular. Seus primeiros elementos são $\{1, 2, 4, 7, 11, 16, 22, 29, 37, 46\}$.

- Padovan (A000931): Composta por um padrão similar à sequência de Fibonacci, mas com $S(0) = 1$, $S(1) = S(2) = 0$ e $S(k) = S(k-2) + S(k-3)$ para $k > 2$. De maneira análoga àquela, cresce rapidamente, existem apenas 76 elementos no intervalo $[0, 2^{28})$. Seus primeiros elementos são $\{1, 0, 0, 1, 0, 1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16\}$.

- SPrime (A005097): Formada pelos números primos submetidos à uma operação de rotação de bits à direita, a motivação para isso é remover a característica constante dos números primos maiores que 2 serem todos ímpares e estudar a consequência disso sobre o entrelaçamento do referido estado. Seus primeiros elementos são $\{1, 1, 2, 3, 5, 6, 8, 9, 11, 14\}$.

- $\text{PA}^{[r]}$ (A008587): Trata-se de uma família de sequências geradas por progressões aritméticas de razão r. Seus primeiros elementos, para $r = 5$, são $\{0, 5, 10, 15, 20, 25, 30, 35, 40, 45\}$.

Seguindo, pode-se usar a Equação (9.1) para construir exemplos de estados de 4 qubits relacionados a algumas dessas sequências apresentadas, tais como

$$|Fib_4\rangle = \frac{1}{\sqrt{10}}\Big(|0000\rangle + 2\,|0001\rangle + |0010\rangle + |0011\rangle + |0101\rangle + |1000\rangle + |1101\rangle \Big), \tag{9.3a}$$

$$|Hpy_4\rangle = \frac{1}{2}\left(|0001\rangle + |0111\rangle + |1010\rangle + |1101\rangle\right), \tag{9.3b}$$

$$|Lck_4\rangle = \frac{1}{\sqrt{6}}\Big(|0001\rangle + |0011\rangle + |0111\rangle + |1001\rangle + |1101\rangle + |1111\rangle \Big), \tag{9.3c}$$

relacionados, respectivamente, às sequências Fibonacci, Happy e Lucky. Por fim, o estado Primo, construído a partir da sequência de números primos e estudado em [29], que será usado ao longo deste capítulo para fins de comparações, para $n = 4$ assume a forma

$$|Pri_4\rangle = \frac{1}{\sqrt{6}}\Big(|0010\rangle + |0011\rangle + |0101\rangle + |0111\rangle + |1011\rangle + |1101\rangle \Big). \tag{9.4}$$

9.3 Análise de Entrelaçamento

Como não há disponível uma medida de entrelaçamento multiparte genuíno para estados de dimensão arbitrária, será usada uma estratégia já adotada em outros trabalhos [29, 94–96], faz-se a soma de todas as bipartições relevantes, a média de todas as bipartições relevantes e também a média de apenas algumas bipartições específicas. Uma definição mais formal será apresentada adiante.

Dado um estado quântico de n qubits existem 2^n diferentes traços parciais, mas é fácil observar que apenas $2^{n-1} - 1$ são relevantes para cálculo do entrelaçamento. Isto decorre do fato que o entrelaçamento presente em um dado traço parcial de ρ com relação ao índice i é sempre igual ao presente naquele em relação ao índice complementar de i. Por exemplo, dada a matriz densidade de um estado de 4 qubits ρ_{ABCD}, o entrelaçamento em $T_{R_{AB}}(\rho_{ABCD})$ é sempre igual ao em $T_{R_{CD}}(\rho_{ABCD})$. Então, o entrelaçamento da i-ésima bipartição será dado por

$$E_i(|\phi\rangle) = E_{VN}(T_{R_{i^c}}(\rho)), \tag{9.5}$$

sendo E_{VN} é a entropia de Von Neumann (a medida de entrelaçamento escolhida para as análises neste capítulo) e i^c é o índice complementar de i. No geral, a despeito da restrição adotada para o cálculo baseada na simetria, pode-se considerar i um valor arbitrário no intervalo $[1, 2^n - 1)$ e sua representação binária é tomada para indicar no traço parcial a posição dos subsistemas que ficam (representados pelas posições com 1) e os que são traçados fora

(representados pelas posições com zero), isto é útil para indicar livremente qualquer bipartição do estado em algumas circunstâncias. Por exemplo, tomando o estado $|\phi\rangle$ de 4 qubits descrito anteriormente como referência, tem-se que $E_5(|\phi\rangle)$, o entrelaçamento da bipartição $i = 5$ (0101 em binário), será obtido através do traço parcial que mantém os subsistemas BD e traça fora os subsistemas AC. Ainda, em alguns casos será útil analisar especificamente as partições que dividem o estado entre o k-ésimo qubit e os demais, de modo a entender o quão entrelaçado é cada qubit do estado com os $n-1$ qubits restantes, essa caso será descrito por

$$E_k^{th}(|\phi\rangle) = E_{2^{k-1}}(|\phi\rangle), \tag{9.6}$$

em que k varia de 1 a n.

Ao longo deste capítulo será usada a noção de que um estado maximamente entrelaçado é aquele que apresenta entrelaçamento igual ao limite superior teórico predito para uma dada medida de entrelaçamento. Este limite superior pode ser obtido através da consideração de um estado puro hipotético de n-qubits em que todas suas matrizes densidades marginais sejam completamente mistas [95]. Portanto, o entrelaçamento total é dado por

$$E_{sum}^{all}(|\phi\rangle) = \sum_{i=1}^{2^{n-1}-1} E_i(|\phi\rangle), \tag{9.7}$$

mas, em geral, é mais apropriado usar, no lugar do total, a média de todas as bipartições relevantes para buscar entender o comportamento da evolução do entrelaçamento em função de n, então se faz

$$E_{avg}^{all}(|\phi\rangle) = \frac{E_{sum}^{all}(|\phi\rangle)}{2^{n-1}-1}. \tag{9.8}$$

Entretanto, calcular esta métrica rapidamente se torna inviável em virtude do esforço computacional requerido, então em alguns casos será útil calcular apenas a média do entrelaçamento de cada um dos qubits para com os demais que compõem o estado, tal como

$$E_{avg}^{th}(|\phi\rangle) = \frac{1}{n}\sum_{k=1}^{n} E_k^{th}(|\phi\rangle). \tag{9.9}$$

Uma vez que envolve apenas as bipartições da forma $(1, n-1)$, portanto um total de n bipartições, permitirá seu uso para estados em dimensões maiores que as alcançadas por E_{avg}^{all}. Uma vez dada as definições de E_k^{th}, E_{avg}^{all} e E_{avg}^{th}, pode-se iniciar as análises.

9.3.1 Sequências no espaço de 4 qubits

A maior parte das sequências estudadas neste trabalho não contém repetição de elementos, portanto, recaem no caso particular de sequências que geram estados quânticos que

são superposições equiprováveis. Deste modo, faz-se importante entender como este fato afeta a capacidade dessa classe de estados portar entrelaçamento em relação aos demais estados do espaço. Para tanto, será buscado responder a questão: Qual a sequência finita de inteiros que resulta em estados de 4 qubits[2] com maior entrelaçamento?

Dentre todas os possíveis conjuntos finitos de inteiros sem repetição entre 0 e 15 que resultam em diferentes estados sequências (basicamente são ignorados conjuntos que resultam em estados sequências que se equivalem pela ação da porta X), apenas seis ($\approx 0.13\%$) compartilham o mesmo valor máximo encontrado, são elas $Q^1 = \{0, 3, 13, 14\}$, $Q^2 = \{0, 5, 11, 14\}$, $Q^3 = \{0, 6, 11, 13\}$, $Q^4 = \{0, 7, 9, 14\}$, $Q^5 = \{0, 7, 10, 13\}$ e $Q^6 = \{0, 7, 11, 12\}$, com

$$E_{sum}^{all}\left(\xi_4(Q^i)\right) = 9, \tag{9.10}$$

para $i \in \{1, 2, 3, 4, 5, 6\}$. Contudo, deve-se lembrar que o limite superior de E_{sum}^{all} para 4 qubits é 10 e, mesmo sabendo [98] que não existe estado que alcance este limite no espaço de Hilbert de dimensão 4, existem outros estados que ultrapassam o valor 9, como o estado

$$|\phi_{HS}\rangle = \frac{1}{\sqrt{6}}\left[|0011\rangle + |1100\rangle + \omega(|0110\rangle + |1001\rangle) + \omega^2(|0101\rangle + |1010\rangle)\right], \tag{9.11}$$

no qual $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ e $E_{sum}^{all}(|\phi_{HS}\rangle) \approx 9.3774$, conjecturado ser o maior entrelaçamento existente nesta dimensão. Por outro lado, todos os estados que decorrem da Equação (9.10) e o definido na Equação (9.11) possuem $E_{avg}^{th} = 1$, o limite superior desta abordagem. Este fato precisa ser considerado no estudo dos estados sequências, principalmente porque sugere que usar apenas E_{avg}^{th} não é uma opção adequada. Outros importantes exemplos que explicitam essa divergência são os estados gerados pelas sequências $\{0, 15\}$ (estado EPR) e $\{0, 3, 5, 6, 9, 10, 12, 15\}$, ambos possuem $E_{sum}^{all} = 7$ e $E_{avg}^{th} = 1$, isso mostra que tais estados possuem menos entrelaçamento que $|\phi_{HS}\rangle$.

Por fim, tomando-se $S^{HS} = \{3, 5, 6, 9, 10, 12\}$, a sequência subjacente de $|\phi_{HS}\rangle$, o entrelaçamento observado no estado sequência correspondente é $E_{sum}^{all}(\xi_4(S^{HS})) \approx 5.9145$ e $E_{avg}^{th}(\xi_4(S^{HS})) \approx 0.7129$. Isso denota um comportamento predominante, apenas ocasionalmente se encontram sequências cujos estados resultantes não podem ter seu entrelaçamento incrementado se admitido ajustes arbitrários dos coeficientes (sem que, no entanto, se mude a sequência de inteiros associada ao estado).

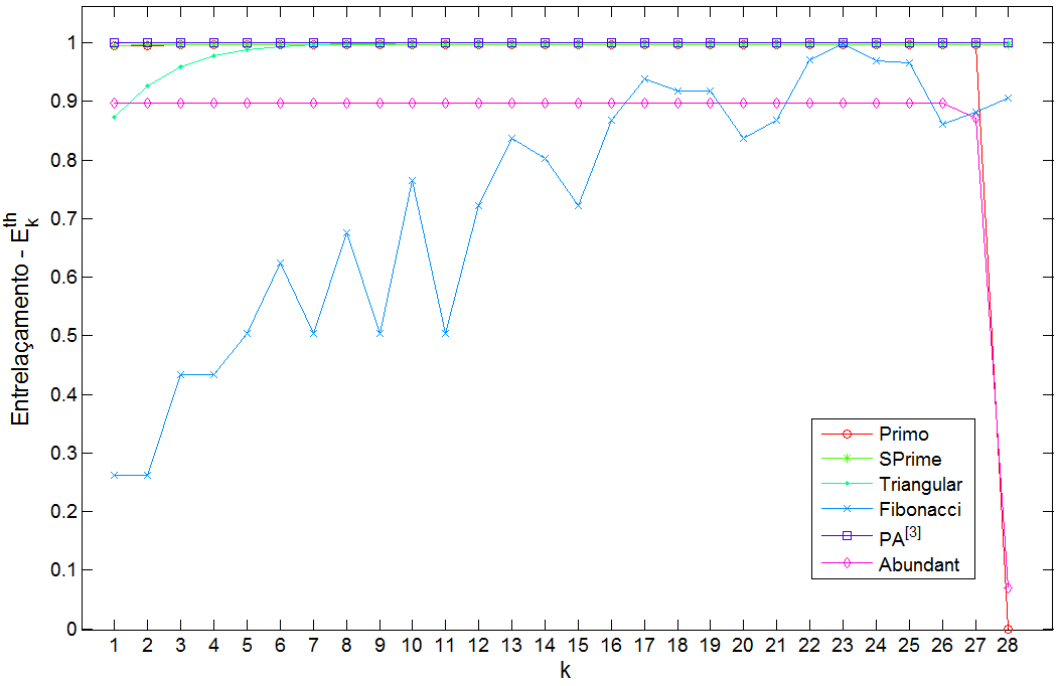
9.3.2 Análise do k-ésimo qubit do estado – E_k^{th}

Muitas conexões interessante entre o estado Primo e alguns importantes problemas na teoria dos números foram estudadas em [29, 30], assim como também muitas características

[2] A quantidade de estados sequências de n qubits é dada por $\sum_{k=2}^{2^k-1} \frac{2^n!}{k!\cdot(2^n-k)!}$, então $n = 4$ é a maior dimensão do espaço de Hilbert na qual podemos fazer uma busca completa usando um computador pessoal em uma quantidade razoável de tempo.

de seu entrelaçamento, como o fato de que o entrelaçamento do último qubit para com os demais decresce exponencialmente com n. Então emerge a questão: existem outros estados

Figura 9.1: O entrelaçamento do k-ésimo qubit para com os demais (E_k^{th}) em alguns estados sequências de 28 qubits.



sequências que contornam essa suposta desvantagem? Tem-se na Figura 9.1 um ponto de partida para a discussão desta questão, ela mostra o entrelaçamento do k-ésimo qubit para com os demais em alguns estados sequências de 28 qubits. Primeiramente, deve-se notar que o estado Abundant segue um comportamento similar ao do estado Primo, todos os qubits são altamente entrelaçados entre si, com exceção do último que, em ambos os casos, é desentrelaçado dos demais $n-1$ qubits. Um coerente argumento dado em [29] associa este comportamento com o fato de que os números primos são formados quase que exclusivamente por números ímpares, mas este não é o caso dos números Abundant, cujo estado correspondente apresenta comportamento similar. O estado SPrime foi construído para contornar essa característica dos números primos, faz-se um deslocamento de bits para direita em cada número primo de modo a se obter um balanceamento entre número ímpares e pares.

Por outro lado, o estado Fibonacci mostra um comportamento bem diferente, não se observa um alto entrelaçamento entre os qubits individualmente. Além disso, os estados SPrime, Triangular (mesmo tendo menos entrelaçamento entre os qubits iniciais) e PA$^{[3]}$ superam o entrelaçamento presente no estado Primo sob esta perspectiva, todos eles sem a desvantagem de ter o último qubit desentrelaçado em relação aos demais.

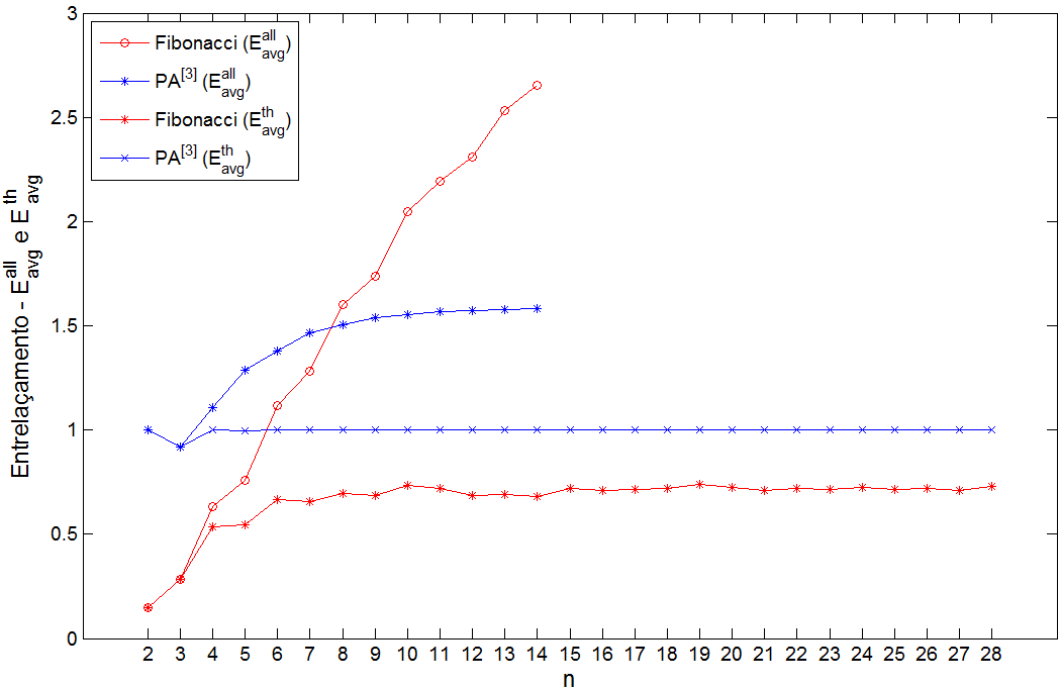
9.3.3 Entrelaçamento médio dos k-ésimos qubits do estado – E^{th}_{avg}

Analisando apressadamente a Figura 9.1, pode-se concluir que o estado PA$^{[3]}$ possui mais entrelaçamento que o estado Fibonacci, mas um olhar mais atento revelará que isso não é verdade. Um resumo do entrelaçamento médio presente nestes estados é mostrado na Tabela 9.1 e, mais adiante, a Figura 9.2 mostra que embora $E^{th}_{avg}\left(\left|PA^{[3]}_n\right\rangle\right) > E^{th}_{avg}(|Fib_n\rangle)$, tem-se que $E^{all}_{avg}\left(\left|PA^{[3]}_n\right\rangle\right) < E^{all}_{avg}(|Fib_n\rangle)$.

Tabela 9.1: O entrelaçamento médio dos k-ésimos qubits, E^{th}_{avg}, dos estados sequências de 28 qubits apresentados na Figura 9.1.

Estado	$\approx E^{th}_{avg}$	Estado	$\approx E^{th}_{avg}$
Prime	0.9606	Triangular	0.9897
SPrime	0.9964	Abundant	0.8660
Fibonacci	0.7302	PA$^{[3]}$	1.0000

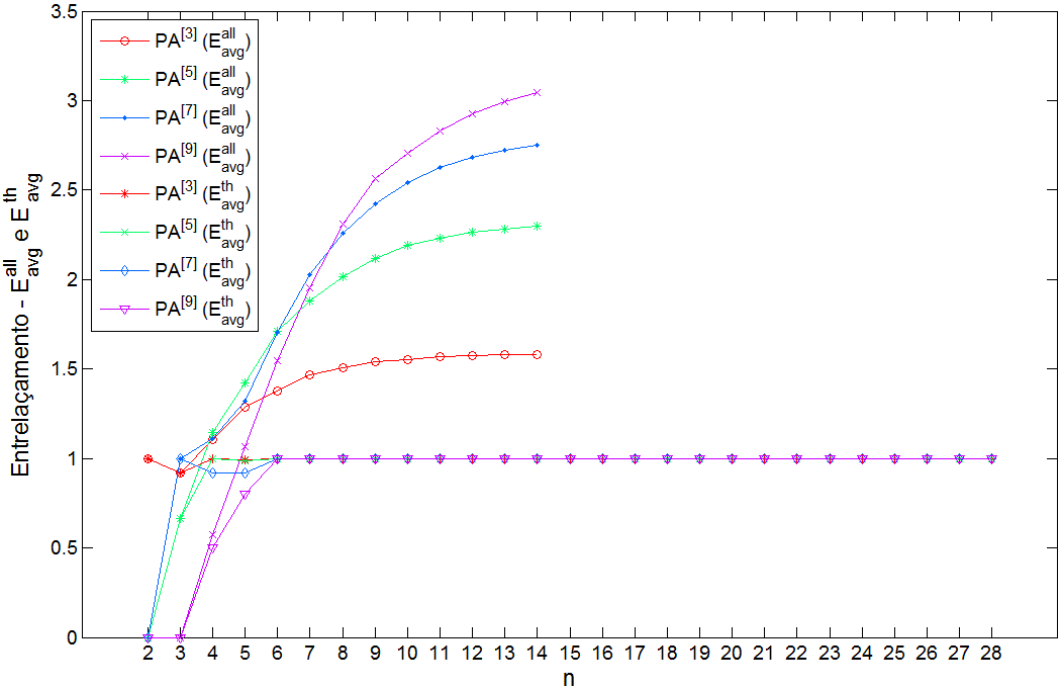
Figura 9.2: Entrelaçamento médio dos k-ésimos qubits (E^{th}_{avg}) e o entrelaçamento médio de todas as bipartições (E^{all}_{avg}) para os estados Fibonacci e PA$^{[3]}$ de n qubits.



9.3.4 Uma breve análise do estado PA$^{[r]}$

No contexto do vínculo da informação quântica com a teoria dos números seria interessante entender de onde emerge o entrelaçamento do estado Primo. Não surpreende o fato de que toda tentativa de entender o entrelaçamento é complicada e cheia de armadilhas. Uma possível suposição de [29] é que o entrelaçamento do estado Primo emerge da aleatoriedade intrínseca dos números primos. Mas, como se nota na Figura 9.1 e na Tabela 9.1, tomando E^{th}_{avg} como referência, existem estados sequências originários de sequências triviais que superam o entrelaçamento presente no estado Primo. Talvez o mais elementar destes seja o estado PA$^{[r]}$, para o qual há na Figura 9.3 uma análise do entrelaçamento em função de $r \in \{3, 5, 7, 9\}$.

Figura 9.3: Entrelaçamento médio dos k-ésimos qubits (E^{th}_{avg}) e o entrelaçamento médio de todas as bipartições (E^{all}_{avg}) para estados PA$^{[r]}$ de n qubits e $r \in \{3, 5, 7, 9\}$.

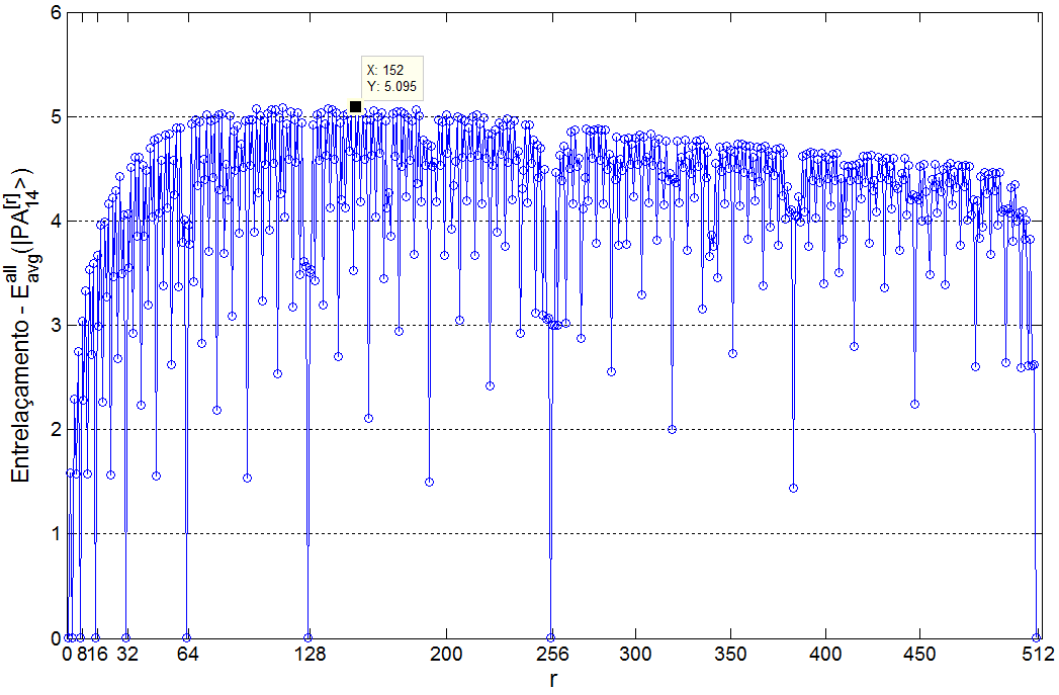


Pode-se ver que o estado PA$^{[r]}$ tende a gerar estados com todos os k-ésimos qubits maximamente entrelaçados entre si, ou seja, $E^{th}_k(\text{PA}^{[r]}) = 1$ para todo k. Além disso, não é difícil ver que estados PA$^{[r]}$ não possuem entrelaçamento quando r é uma potência de dois, isso ocorre basicamente porque nestes casos o estado assume a forma

$$\left|PA_n^{[r=2^k]}\right\rangle = \left(H\left|0\right\rangle\right)^{\otimes(n-k)} \otimes \left(\left|0\right\rangle\right)^{\otimes k}, \tag{9.12}$$

em que H é a porta Hadamard e n é o número de qubits do estado, ou seja, um estado completamente desentrelaçado. Porém, uma visão mais detalhada de como a razão r afeta o entrelaçamento médio do estado PA$^{[r]}$ pode ser vista na Figura 9.4.

Figura 9.4: Entrelaçamento médio de todas as bipartições (E_{avg}^{all}) do estado $\mathrm{PA}^{[r]}$ de 14 qubits em função de r.



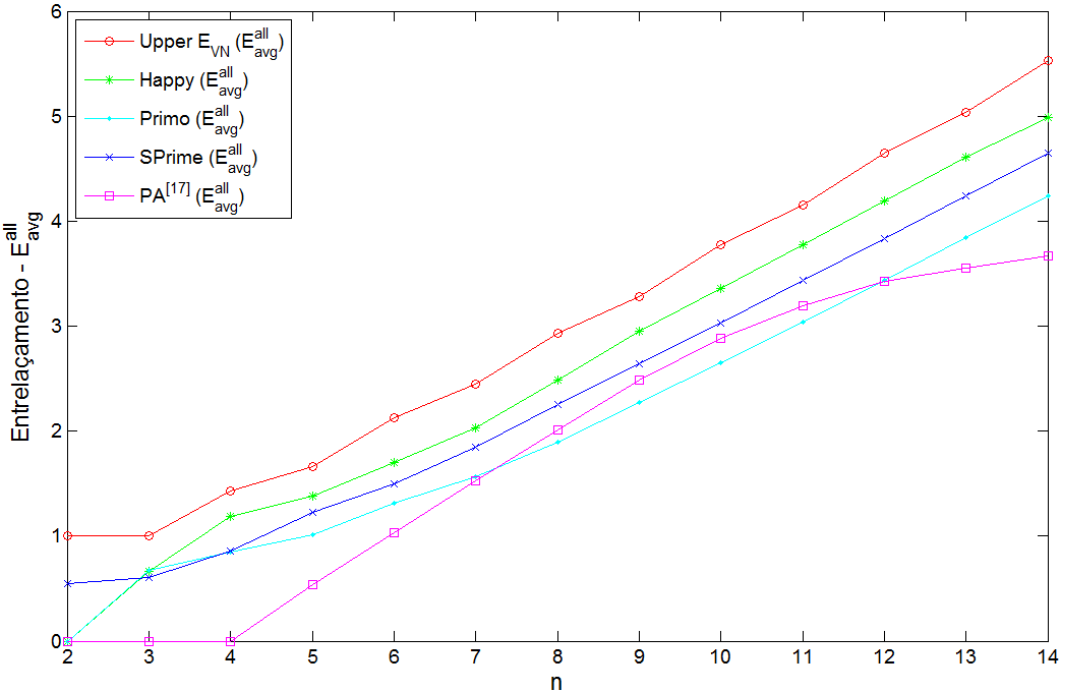
9.3.5 Padrão de formação e entrelaçamento

Uma das questões mais interessantes e intrigantes acerca do estado Primo (também extensível para outros estados sequências) é sobre o quão entrelaçado ele é. Em [29, 30] é apontado que o estado Primo carrega consigo uma grande quantidade de entrelaçamento mas, de fato, quão próximo está o estado Primo de um estado de n qubits maximamente entrelaçado?

Analisando a Figura 9.5, pode-se ver que, dentro do curto espaço observado, o entrelaçamento do estado Primo parece crescer linearmente com o limite superior da entropia de Von Neumann. Entretanto, pode-se ver que ambos os estados SPrime e Happy superam o entrelaçamento presente no estado Primo. Enquanto o estado Primo alcança aproximadamente 68% do limite superior teórico, os estados SPrime e Happy alcançam 74% e 78%, respectivamente. Por outro lado, embora o estado $\mathrm{PA}^{[17]}$ supere o estado Primo em um estágio inicial ele logo começa a se distanciar do limite superior.

Tomando uma perspectiva mais geral, vê-se que o padrão de recorrência da sequência subjacente ao estado sequência é determinante para as propriedades do entrelaçamento, mas talvez não de maneira tão óbvia. No estado PA se percebe que, mesmo selecionando variados valores de r, observa-se o mesmo padrão no qual $E_{avg}^{th}(\left|PA^{[r]}\right\rangle)$ converge para o limite superior enquanto $E_{sum}^{all}(\left|PA^{[r]}\right\rangle)$ se distancia do limite superior teórico. Este comportamento foi mostrado na Figura 9.3 e, como deve ser enfatizado, a interseção entre as sequências subjacentes varia apenas entre 11% e 20%. Na Figura 9.6 se notam outros casos, os estados Fibonacci

Figura 9.5: Entrelaçamento médio do estado Primo (E^{all}_{avg}) comparado com outros estados sequências e com o limite superior da entropia de Von Neumann (Upper E_{VN}).



e Padovan seguem um comportamento similar e possuem apenas cinco elementos em comum ($\approx 7\% - 10\%$) em suas sequências subjacentes.

Os números Lucky [99] não são tão famosos quanto os números primos, mas ambos podem ser gerados usando a mesma abordagem geral: peneiras [100]. Diante disso, torna-se inevitável questionar: assim como os número primos, teriam os números Lucky algum tipo de padrão de formação aleatório inacessível? Infelizmente, este trabalho não responde esta pergunta, mas se percebe claramente que as propriedades do entrelaçamento dos estados Lucky e Primo seguem um comportamento semelhante e suas sequências subjacentes possuem apenas $\approx 7\%$ de elementos comuns. Pode-se notar também o comportamento similar dos estados Happy, Polygonal e Triangular. De um certo modo, embora a interseção entre as sequências subjacentes dos estados Polygonal e Triangular tenha apenas um elemento, a similaridade não é inesperada porque ambas possuem uma fórmula fechada muito semelhante. Entretanto, a similaridade com o estado Happy é curiosa, aparentemente eles não seguem um procedimento similar de geração e a interseção entre as sequências subjacentes é relativamente baixa. A Tabela 9.2 mostra a interseção entre algumas sequências, a célula (i, j) indica o percentual de elementos presentes na interseção entre i e j em relação a sequência i.

Figura 9.6: Comparação de similaridades no comportamento do entrelaçamento médio (E^{all}_{avg}) de alguns estados sequências.

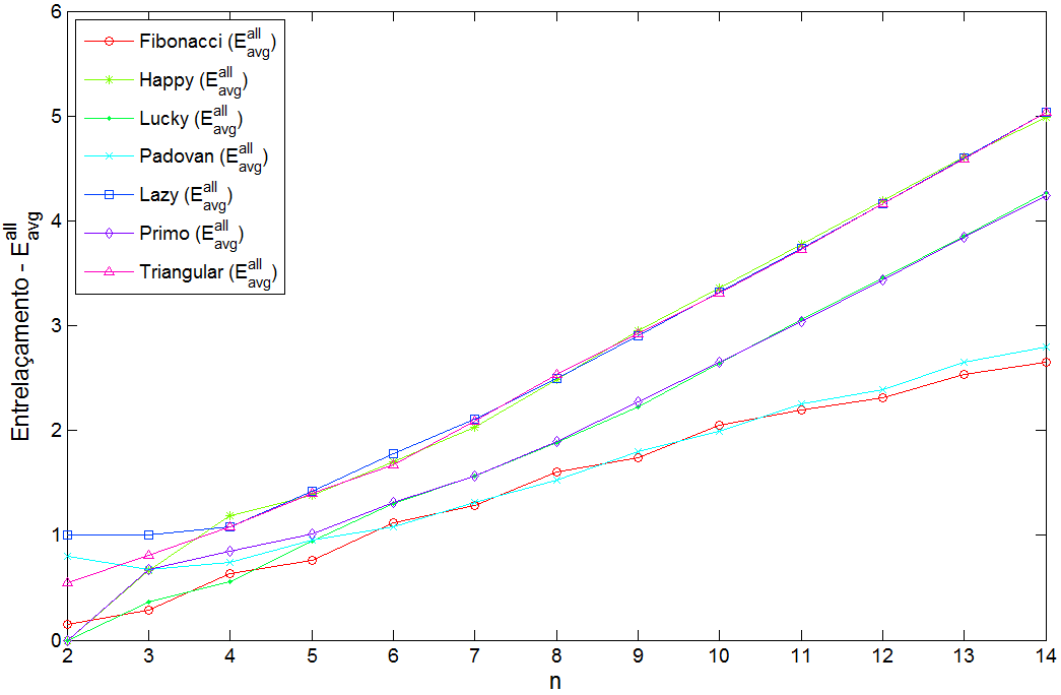


Tabela 9.2: Interseção relativa entre as sequências subjacentes aos estados Happy, Polygonal e Triangular.

	Happy	Polygonal	Triangular
Happy	-	0.0086%	0.0079%
Polygonal	13.9663%	-	0.0043%
Triangular	12.9176%	0.0043%	-

9.4 Preparação de estados sequências

Esta seção revisita a preparação do estado Primo apresentada em [29] dando ênfase aos testes de primalidade e suas correspondentes abordagens quânticas para, posteriormente, apresentar uma análise de eficiência da preparação de um estado sequência arbitrário.

9.4.1 Preparação do estado Primo

São descritas em [29] essencialmente duas abordagens para a preparação do estado Primo, a primeira segue o caminho de prover um circuito quântico que implementa um algoritmo clássico de teste de primalidade (U_{tp}) de tal modo que

$$U_{tp}\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle = \frac{1}{\sqrt{2^n}}\left(\sqrt{\pi(2^n)}\,|P_n\rangle|0\rangle + \sqrt{2^n-\pi(2^n)}\,|C_n\rangle|1\rangle\right), \tag{9.13}$$

em que $|C_n\rangle$ é estado quântico normalizado representando uma superposição de todos os nú-

meros compostos menores ou iguais a $2^n - 1$. Uma vez que

$$U_{tp} |x\rangle |0\rangle = \begin{cases} |x\rangle |0\rangle & \text{se } x \text{ é primo} \\ |x\rangle |1\rangle & \text{se } x \text{ não é primo} \end{cases}, \tag{9.14}$$

tem-se que o estado Primo é obtido se a medição da ancila representada pelo último qubit resultar em 0. Usando o teorema dos números primos (TNP) é possível observar que a probabilidade de se obter o estado primo com esta abordagem é dada por

$$\text{Prob}(|P_n\rangle) = \frac{\pi(2^n)}{2^n} = \frac{1}{n \log 2} \tag{9.15}$$

que se trata de uma expressão polinomial, portanto, tem-se que este procedimento probabilístico pode ser considerado eficiente.

Por outro lado, em oposição à primeira, a segunda abordagem é determinística. Neste caso, o teste de primalidade é aplicado como um oráculo (U_o) para o algoritmo de Grover de tal modo que

$$U_o |x\rangle = (-1)^{\chi_\pi(x)} |x\rangle , \tag{9.16}$$

em que χ_π é uma função característica (ou identificadora) dos números primos, ou seja, $\chi_\pi(x) = 1$ se x é primo e 0 caso contrário. Deste modo, o oráculo U_o irá atuar em toda uma superposição de estados invertendo o sinal apenas daqueles que representarem números primos. Esta abordagem também é considerada eficiente (mais detalhes serão apresentados na Seção 9.4.2), apenas 7 chamadas ao oráculo são suficientes para gerar o estado Primo de 100 *qubits*, ou seja, uma superposição de todos os números primos menores que 2^{100}.

Talvez o mais interessante, em um sentido geral, teste de primalidade conhecido seja o AKS apresentado em [101], o primeiro a ser simultaneamente polinomial, determinístico e incondicional. Trata-se de uma prova de que verificar a primalidade de um número é um problema cuja ordem de complexidade reside na classe **P**. Entretanto, em virtude da natureza relativamente mais simples do teste de Miller-Rabin [102], ele foi o escolhido em [29] para a construção da versão quântica de um teste de primalidade. Segundo o algoritmo proposto por Miller-Rabin, para determinar se um dado número x é primo primeiro se faz

$$x - 1 = d2^s, \tag{9.17}$$

em que d é um número ímpar. Então, escolhe-se uma testemunha (*witness*) a, em que $1 \leq a \leq x$, e se calcula

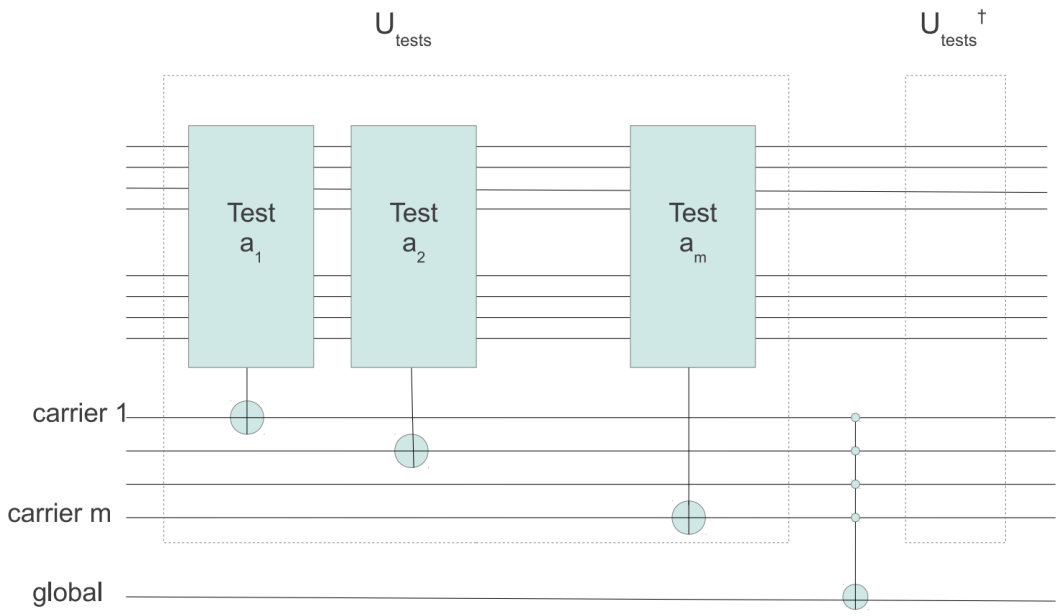
$$\begin{aligned} a^d &\not\equiv 1 \pmod{x} \\ a^{2^r d} &\not\equiv -1 \pmod{x} \quad 0 \leq r \leq s-1, \end{aligned} \tag{9.18}$$

caso ambos os testes sejam verificados x é considerado um número composto.

Por outro lado, se um dos testes falhar nenhuma decisão pode ser tomada acerca de x e a passa a ser considerado um forte mentiroso (*strong liar*). Nota-se que o teste de Miller-Rabin é essencialmente probabilístico, a maneira usual de mitigar essa questão é repetir o teste usando diferentes testemunhas para aumentar a probabilidade de uma verificação acertada. Usando k testemunhas é capaz de se obter uma taxa de erro menor que 2^{-2k}, fazer $k = n$, em que n é o número de qubits do estado Primo, é suficiente para a maioria dos fins práticos. Sabe-se ainda que, assumindo que seja verdadeira a hipótese generalizada de Riemann, o uso de $\log^2 x$ testemunhas é suficiente para considerar o teste determinístico, por exemplo, executando o teste para todo $a \in \{2, 3, 5, 7, 11, 13, 17\}$ é possível verificar corretamente todos os números primos menores que $3 \cdot 10^{14}$.

As principais partes do circuito quântico que implementa o teste de primalidade clássico de Miller-Rabin são mostradas nas Figuras 9.7 e 9.8.

Figura 9.7: Oráculo do circuito quântico que implementa o teste de primalidade clássico de Miller-Rabin.



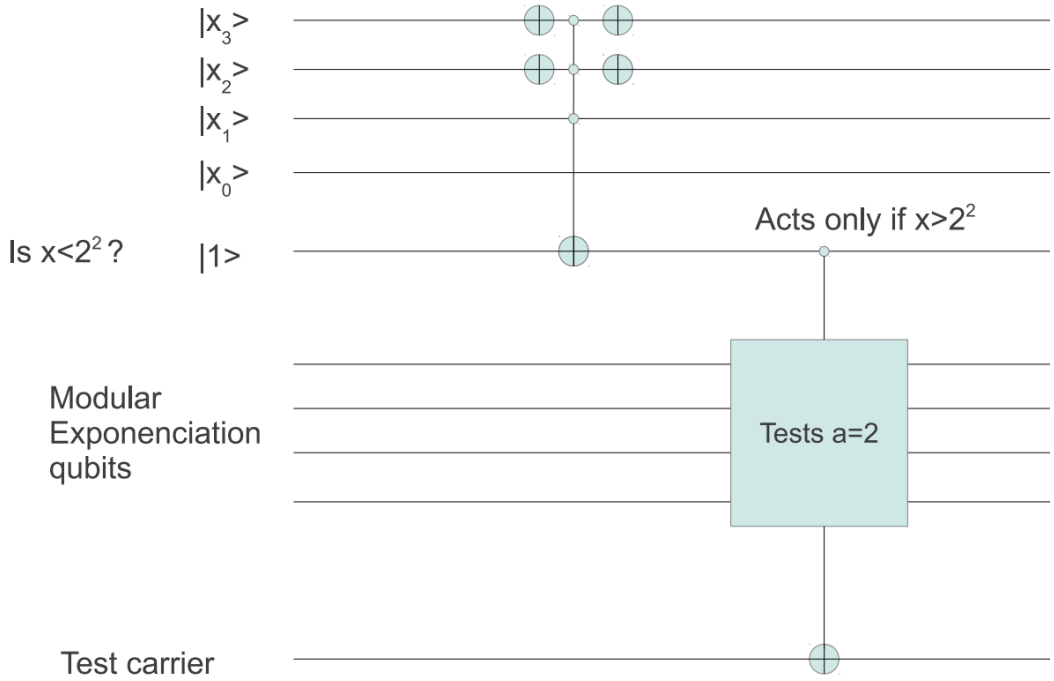
Fonte: Imagem apresentada originalmente como FIG. 2 no trabalho [29].

Basicamente são seguidos os passos previstos no algoritmo clássico, na Figura 9.7 se nota uma série de módulos que implementam a exponenciação modular presente no teste de Miller-Rabin como

$$U_{a,r} \sum_x |x\rangle |0\rangle = \sum_x |x\rangle \left| a^{2^r d} \pmod{x} \right\rangle . \tag{9.19}$$

Por outro lado, a Figura 9.8 o procedimento que garante que cada exponenciação modular

Figura 9.8: Parte do circuito quântico que implementa o teste de primalidade clássico de Miller-Rabin responsável por garantir que apenas testemunhas menores que x serão testadas.



Fonte: Imagem apresentada originalmente como FIG. 3 no trabalho [29].

apenas é executada para testemunhas a menores que x, isso é feito através do controle pelos qubits mais significativos.

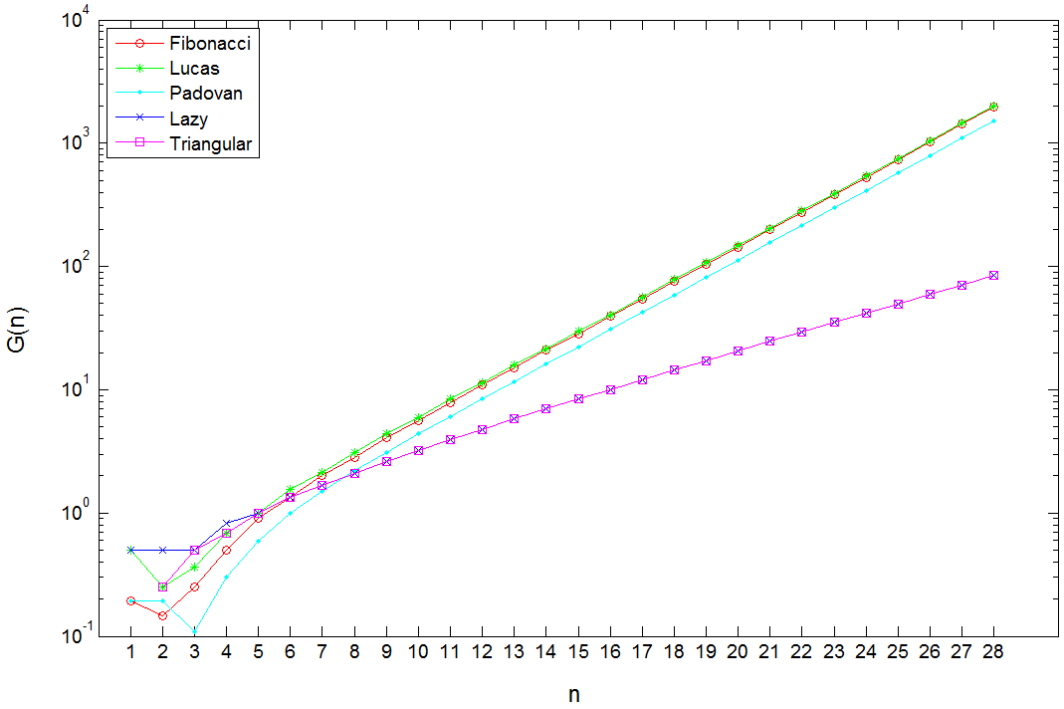
9.4.2 Análise de eficiência

A abordagem usada para preparar o estado Primo em [29] através do algoritmo de Grover [9] pode ser usada para preparar outros estados sequências, desde que esteja disponível um oráculo capaz de verificar se um dado elemento pertence à referida sequência. Basicamente, isso implica em buscar por $\tau(2^n)$ elementos dentro de um conjunto de 2^n no total. O algoritmo de Grover pode realizar essa tarefa em $O\left(\sqrt{\frac{2^n}{\tau(2^n)}}\right)$. Portanto, o número de iterações é dado por

$$G(n) = \frac{\pi}{4 \arcsin\left(\sqrt{\frac{\tau(2^n)}{2^n}}\right)} - \frac{1}{2}. \tag{9.20}$$

Agora, pode-se analisar as iterações necessárias para gerar os estados quânticos sequências descritos anteriormente, para começar, pode-se ver na Figura 9.9 que os estados Fibonacci, Lucas, Padovan, Polygonal e Triangular, usando uma escala logarítmica, crescem aparentemente de forma linear com n. Além disso, os três primeiros, assim como os dois últimos, compartilham um comportamento similar.

Figura 9.9: Número de iterações do Grover, em função do número de qubits, para a preparação dos estados Fibonacci, Lucas, Padovan, Lazy e Triangular.



Por outro lado, a Figura 9.10 mostra que o mesmo não acontece para os estados Abundant, Happy, Hashard, Lucky, Prime e SPrime, ainda que tomada como referência uma escala logarítmica. Entretanto, os estados Abundant e Happy parecem tender a um comportamento constante. Cabe ressaltar que o estado SPrime também supera o estado Primo no que diz respeito a eficiência de sua preparação através do algoritmo de Grover. Por fim, como de certo modo é esperado, a Figura 9.11 mostra que o estado PA apresenta um comportamento que converge rapidamente para um valor constante.

Figura 9.10: Número de iterações do Grover, em função do número de qubits, para a preparação dos estados Abundant, Happy, Harshad, Lucky, Primo e SPrime.

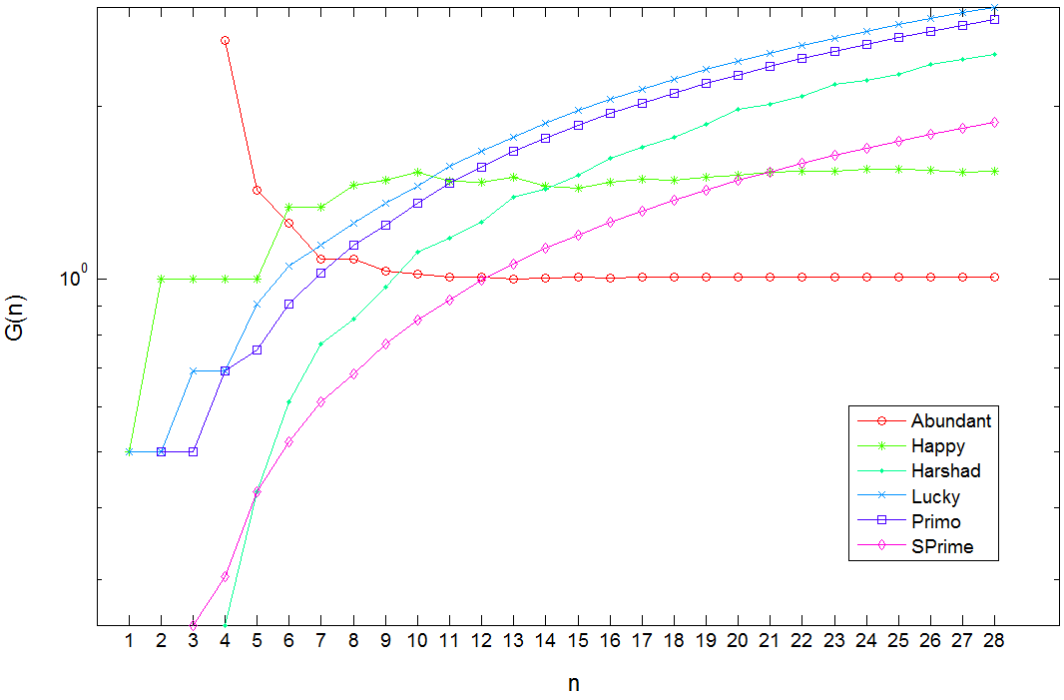
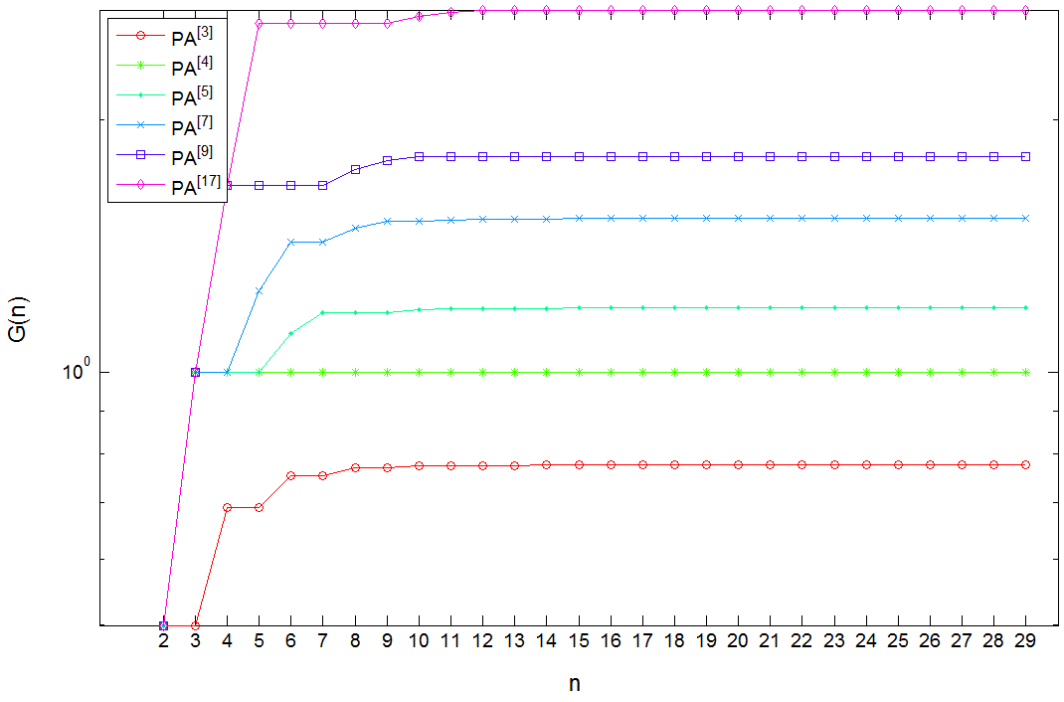


Figura 9.11: Número de iterações do Grover, em função do número de qubits, para a preparação do estado $\mathrm{PA}^{[r]}$ para $r \in \{3, 4, 5, 7, 9, 17\}$.



9.5 Novas sequências

Nesta seção serão construídas algumas novas sequências para comparação com algumas daquelas apresentadas anteriormente. Algumas vezes será tomado o caminho inverso, gerando uma sequência de números inteiros a partir de estados quânticos.

9.5.1 S1 – Comportamento oscilatório do entrelaçamento

Define-se uma sequência de números inteiros associada a um estado quântico de n qubits que apresenta um comportamento oscilatório no entrelaçamento como se segue. Inicia-se com $S1 = \{0, 3\}$, portanto, $|S1_2\rangle = \xi_2(S1) = (|00\rangle + |11\rangle)/\sqrt{2}$. Agora, a partir deste estado de 2 qubits, pode-se expandir a sequência iterativamente para obter a subjacente ao estado $|S1_n\rangle$ (de n qubits) seguindo os seguintes passos ($k = 2, 3, ..., n-1$):

- Se k é par, faz-se $S1 = S1 \cup \max(\{1, 2, \cdots, 2^n - 1\} - S1)$ e $k = k + 1$. Este passo acrescenta apenas um elemento à sequência.
- Se k é ímpar, faz-se $S1 = S1 \cup \text{bitxor}(S1, 2^{n+1} - 1)$ e $k = k + 1$, em que *bitxor* é a operação de bitwise *xor* em cada um dos elementos de $S1$. Este passo pode até dobrar o tamanho da sequência, mas elementos repetidos são desconsiderados.

Este procedimento leva aos elementos mostrados na Equação (9.21) para $n = 14$.

$$S1 = \left\{ \begin{array}{c} 0, 2, 3, 12, 13, 14, 15, 48, 49, 50, 51, 60, 61, 62, 63, 192, 193, 194, \\ 195, 204, 205, 206, 207, 240, 241, 242, 243, 252, 253, 254, 255, 768, \\ 769, 770, 771, 780, 781, 782, 783, 816, 817, 818, 819, 828, 829, 830, \\ 831, 960, 961, 962, 963, 972, 973, 974, 975, 1008, 1009, 1010, 1011, \\ 1020, 1021, 1022, 1023, 3072, 3073, 3074, 3075, 3084, 3085, 3086, \\ 3087, 3120, 3121, 3122, 3123, 3132, 3133, 3134, 3135, 3264, \cdots \end{array} \right\} \tag{9.21}$$

9.5.2 S2 – Generalização do estado Higuchi & Sudbery

A sequência aqui apresentada decorre, em certo sentido, de uma generalização do estado HS [98] para n qubits construída seguindo o padrão de simetria encontrado no estado original de 4 qubits. A sequência $S2$ é gerada algoritmicamente em blocos para preencher um estado de n qubits, em que n é sempre um número par. Para tanto, inicia-se com $S2 = \{\}$, $k = 4$ e se geram mais elementos fazendo:

1: $S2 \leftarrow [\,]$;
2: **while** $(k \leq n)$ **do**
3: $\quad s \leftarrow \text{bin2dec}([\text{zeros}(k/2)\ \text{ones}(k/2)])$;
4: $\quad sk \leftarrow [s]$;
5: $\quad$ **for** $p := k/2$ **to** 1 **do**
6: $\quad\quad s \leftarrow s + 2^{p-1}$;

7: $sk \leftarrow sk \cup s$;
8: **end for**
9: $sk \leftarrow sk \cup \text{bitxor}(sk, 2^k - 1)$;
10: $S2 \leftarrow S2 \cup sk$;
11: $k \leftarrow k + 2$;
12: **end while**
13: **return** $S2$;

Este procedimento leva aos elementos mostrados na Equação (9.22) para $n = 14$.

$$S2 = \left\{ \begin{array}{l} 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 23, 27, 29, 30, 31, 47, 49, 50, \\ 52, 55, 56, 59, 61, 62, 63, 95, 111, 119, 123, 125, 126, 127, 191, \\ 223, 225, 226, 228, 232, 239, 240, 247, 251, 253, 254, 255, 383, \\ 447, 479, 495, 503, 507, 509, 510, 511, 767, 895, 959, 961, 962, \\ 964, 968, 976, 991, 992, 1007, 1015, 1019, 1021, 1022, 1023, \cdots \end{array} \right\} \tag{9.22}$$

9.5.3 S3 – Progressão aritmética com razão periódica

Uma interessante sequência, $S3$, pode ser montada usando uma progressão aritmética cuja razão r apresenta, no lugar do tradicional comportamento constante, um comportamento periódico em torno de uma sequência secundária. Para gerar a sequência de razões será usada a função

$$f_r(a, b, c) = \text{abs}(\text{round}(10^a \cdot \tan(\pi \cdot [0 : b, b : -1 : 0]) + c)) + 1, \tag{9.23}$$

que para os valores $a = 16$, $b = 127$ e $c = 5$ resulta em

$$S_r = \{6, 5, 4, 2, 1, 2, 3, 5, 6, 7, 8, 45, 11, 26, \cdots\} \tag{9.24}$$

com 256 elementos em que, conforme pode ser visto a partir da definição de f_r, a segunda metade é exatamente igual a primeira metade mas em ordem inversa. Agora, usando S_r pode-se gerar a sequência $S3$ para números menores que 2^n usando o algoritmo a seguir.

1: $S3 \leftarrow [0]$;
2: $r_i \leftarrow b; k \leftarrow 2$;
3: **while** (true) **do**
4: $e \leftarrow S3(k - 1) + S_r((r_i \mod b) + 1)$;
5: $r_i \leftarrow r_i + 1$;
6: **if** $(e < 2^n)$ **then**
7: $S3(k) \leftarrow e$;
8: $k \leftarrow k + 1$;

```
    else
        break;
    end if
end while
return S3;
```

Este procedimento leva aos elementos mostrados na Equação (9.25) para $n = 14$. Uma variedade de novas sequências podem ser geradas dentro dessa família simplesmente escolhendo diferentes valores para os parâmetros a, b e c, ou ainda, famílias inteiramente novas podem ser geradas usando outras funções geradoras para a sequência secundária de razões.

$$S3 = \left\{ \begin{array}{c} 0, 6, 11, 15, 17, 18, 20, 23, 28, 34, 41, 49, 94, 105, 131, 144, 194, \\ 210, 231, 249, 304, 324, 340, 434, 494, 519, 530, 575, 640, 670, \\ 676, 780, 849, 884, 885, 920, 994, 1034, 1040, 1154, 1233, 1278, \\ 1431, 1457, 1541, 1733, 1749, 1872, 1927, 1982, 2145, 2161, 2255, \\ 2339, 2364, 2497, 2542, 2607, 2779, 2785, 2889, 3101, 3136, 3279, \\ 3314, 3388, 3570, 3576, 3690, 3755, 3800, 3953, 3979, 4063, \cdots \end{array} \right\} \tag{9.25}$$

9.5.4 Análise das novas sequências

Na Figura 9.12 vê-se que o maior entrelaçamento médio de todas as bipartições é alcançado pelo estado $|S3_n\rangle$, sendo ele o que mais se aproxima do limite teórico previsto pela medida, superando ambos os estados Primo e Happy. Vê-se que os estados gerados pelas sequências $S1$ e $S2$ possuem ambos o entrelaçamento com comportamento oscilatório e cuja superioridade de intensidades se alternam entre si. Esse comportamento oscilatório e alternância de intensidades se repetem quando analisado o entrelaçamento médio dos k-ésimos (E^{th}_{avg}) qubits, conforme mostrado na Figura 9.13. Neste quesito, também se observa a superioridade da sequência $S3$ frente às demais analisadas. O mesmo ocorre quando analisado o entrelaçamento do k-ésimo qubit, visto na Figura 9.14, em um estado de 28 qubits. Neste aspecto ocorrem diferenças entre os estados $|S1_n\rangle$ e $|S2_n\rangle$, o primeiro tem seus qubits individuais maximamente entrelaçados, com exceção dos dois últimos. Por outro lado, o segundo apresenta um crescimento gradual (com viés oscilatório) do entrelaçamento do k-ésimo qubit. Por fim, a eficiência na preparação, mostrado na Figura 9.15, usando o algoritmo de Grover também mostra algumas diferenças entre $|S1_n\rangle$ e $|S2_n\rangle$. Agora, enquanto o primeiro é que apresenta um comportamento oscilatório, o segundo parece implicar em um crescimento linear. Por outro lado, neste aspecto o estado $|S3_n\rangle$ se mostra ligeiramente menos eficiente que o estado Primo. Por fim, fica claramente caracterizado que a sequência $S3$ apresenta o conjunto mais interessante de propriedades dentre todas as sequências analisadas.

Figura 9.12: Comparação das novas sequências enunciadas com os estados Primo e Happy no que se refere ao entrelaçamento médio de todas as bipartições E_{avg}^{all}.

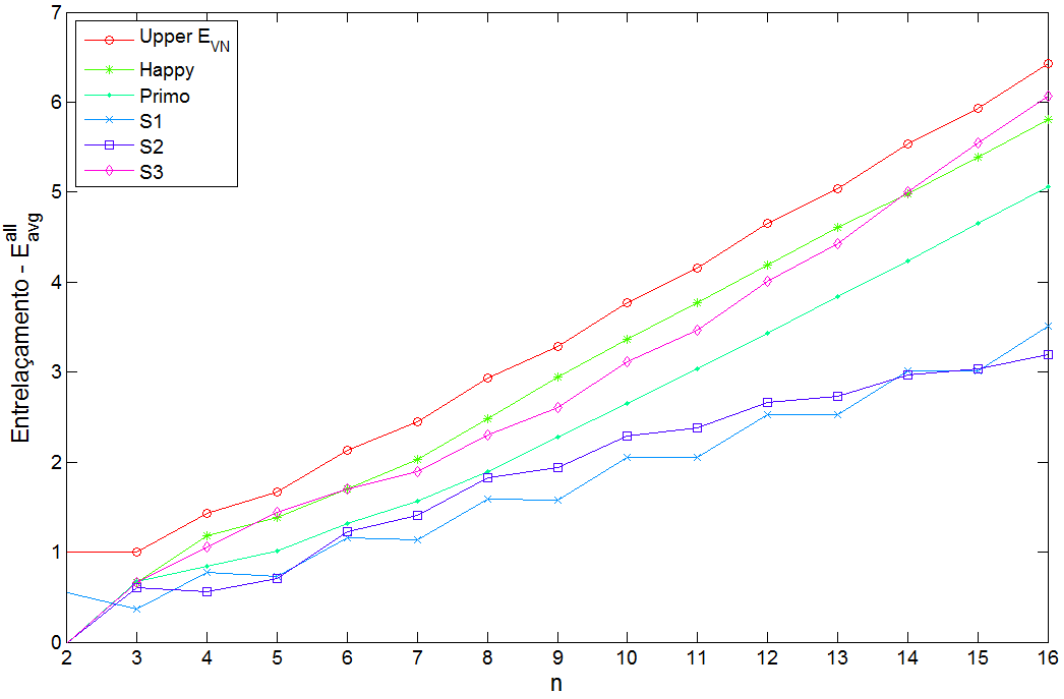


Figura 9.13: Comparação das novas sequências enunciadas com os estados Primo e Happy no que se refere ao entrelaçamento médio dos k-ésimos qubits E_{avg}^{th}.

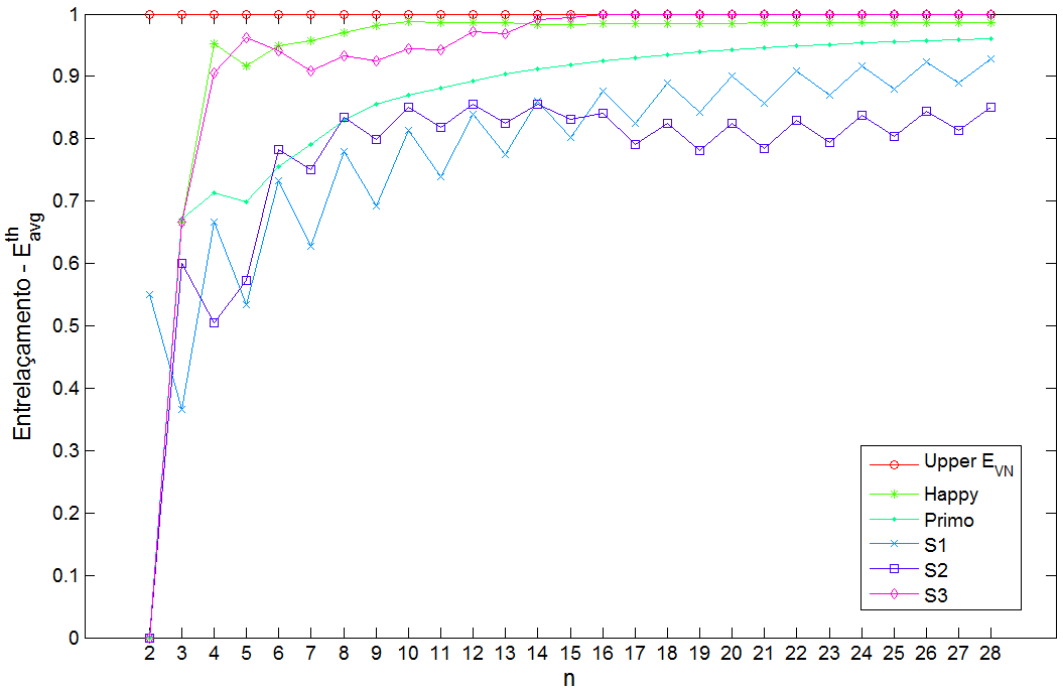


Figura 9.14: Comparação das novas sequências enunciadas com os estados Primo e Happy no que se refere ao entrelaçamento do k-ésimo qubit E_k^{th}.

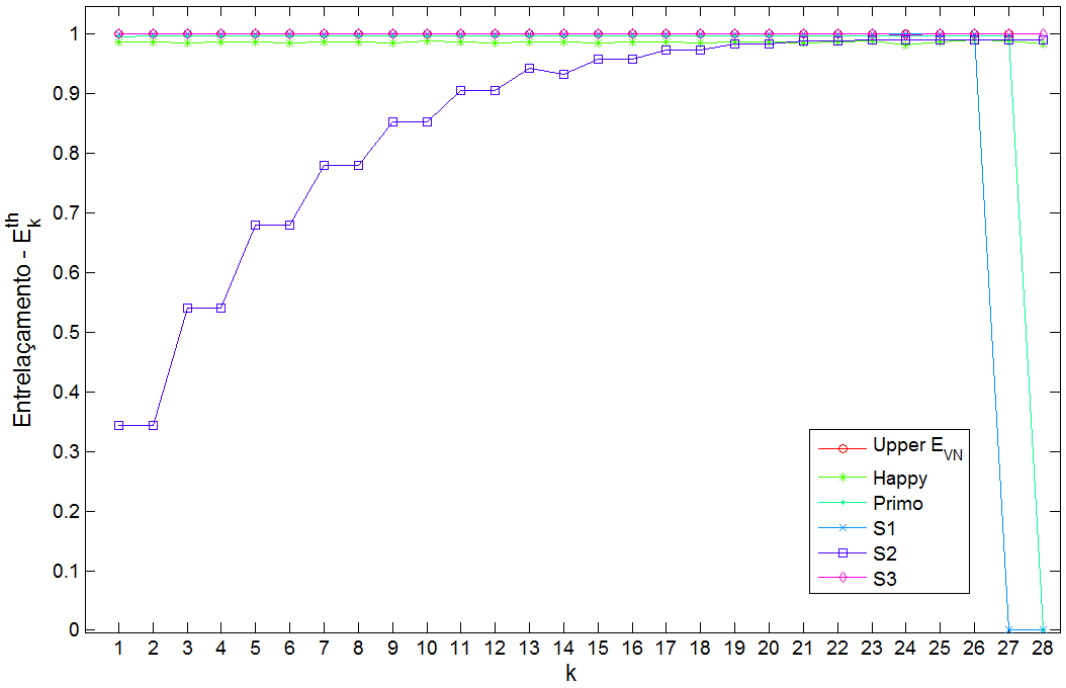
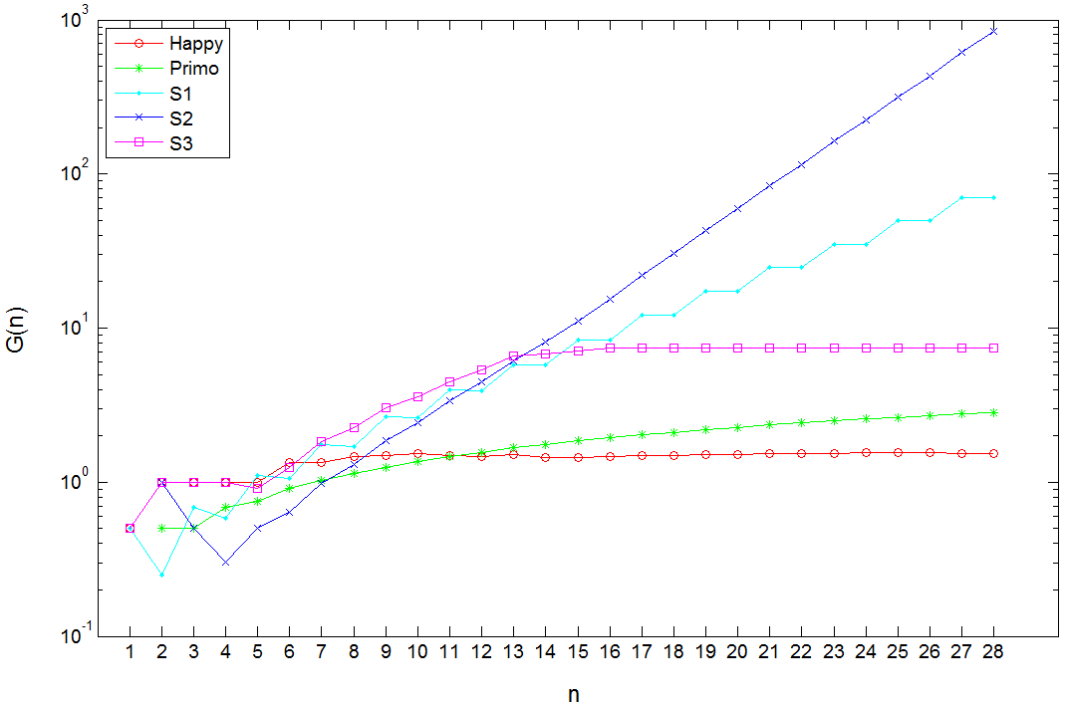


Figura 9.15: Comparação das novas sequências enunciadas com os estados Primo e Happy no que se refere ao número de iterações para preparação via Grover $G(n)$.



9.6 Conclusão

Neste capítulo foi enunciado o estado quântico sequência, construído a partir de sequências de números inteiros, estudadas as propriedades de seu entrelaçamento e também sua preparação usando o algoritmo de Grover. Foram mostrados exemplos para mostrar o quão complexo pode ser discutir o grau de entrelaçamento de um dado estado. Apresentou-se algumas comparações sobre propriedades do entrelaçamento que sugerem maiores similaridades entre estados oriundos de sequências que emergem de padrões/abordagem similares que entre estados oriundos de sequências com maior interseção entre si. Os estados Primo e Lucky são bons exemplos, também o são os estados Fibonacci e Padovan.

Foram apresentados diversos estados sequências que superam o estado Primo em alguns aspectos, mas se mostrou evidente que qualquer tipo de associação de propriedades clássicas com o entrelaçamento são muito difíceis. Pôde-se ver que mesmo o estado $\mathrm{PA}^{[r]}$, que emerge de um padrão trivial de incremento, contém mais entrelaçamento entre seus k-ésimos qubits que o estado Primo. A comparação entre os estados Fibonacci e $\mathrm{PA}^{[3]}$, mostrada na Figura 9.2, mostra uma armadilha que pode levar a conclusões inadequadas, permitindo concluir que E^{th}_{avg} não é suficiente para entender o cenário geral acerca do entrelaçamento de um dado estado.

Os estados propostos Happy e SPrime também superam as propriedades gerais de entrelaçamento do estado Primo, E^{all}_{avg} e E^{th}_{avg}, ambos sem a desvantagem de ter o último qubit desentrelaçado dos demais. Na Figura 9.5 foi possível ver que, entre todos os estados baseados em sequências conhecidas analisados, o estado Happy é aquele que carrega mais entrelaçamento, entretanto, ele é superado pelo estado associado à nova sequência $S3$, conforme pôde ser visto na Figura 9.12. Também foi apresentado uma análise do comportamento do entrelaçamento presente no estado $\mathrm{PA}^{[r]}$ em função de r. Mostrou-se ainda que também é possível seguir o caminho inverso, gerando novas sequências de inteiros a partir de estados quânticos, tais como $S1$, $S2$ e $S3$.

Por fim, foi analisada a eficiência de preparação de alguns estados sequências usando o algoritmo de Grover, incluindo a análise do comportamento de k interações em função de τ, a função de contagem da sequência subjacente.

Capítulo 10

Circuito Quântico de Riemann

Resumo

A teoria dos números é um campo da matemática abstrata que tem encontrado um ambiente fértil na física teórica. Em particular, vários sistemas físicos estão relacionados aos zeros da função zeta de Riemann. Neste capítulo, será apresentada como contribuição a teoria de um circuito quântico relacionado a um número finito de zeros da função zeta de Riemann.

10.1 Introdução

Tem-se percebido um crescente interesse em sistemas quânticos relacionados a problemas na teoria dos números [29, 103, 104]. Este interesse advém desde o estágio inicial da mecânica quântica, quando Hilbert e Pólya discutiram a possibilidade de uma solução física para a hipótese de Riemann: os zeros da função zeta de Riemann poderiam ser o espectro de um operador $R = I/2 + iH$, em que iH é autoadjunto e interpretado como um Hamiltoniano.

Atualmente, tem-se discutido [105–107] vários sistemas físicos relacionados aos zeros da função zeta de Riemann. Em [108] os autores, tendo um número finito de zeros da função zeta de Riemann, usaram um método numérico para encontrar um potencial quântico para reproduzir tais zeros como autovalores de energia. No contexto da mecânica clássica, foi demonstrado em [109] que a transformada de Mellin da probabilidade de um corpo escapar de um sistema de bilhar circular aberto, quando as aberturas estão separadas por 0°, 60°, 90°, 120° ou 180°, é unicamente determinada pela função Zeta de Riemann. No contexto da física quântica, [110] estabeleceu um mapeamento entre a função Zeta de Riemann e um sistema mecânico quântico caótico ainda desconhecido. De modo mais específico, modelos foram propostos [105] tanto em associação com o espectro de energia positiva quanto com

espectro de energia negativa. Também são conhecidas conexões com a física nuclear [111, 112], física da matéria condensada [113, 114] e física estatística [115, 116].

Neste capítulo, será mostrado como construir um circuito quântico, daqui em diante referenciado como circuito quântico de Riemann, cuja matriz unitária equivalente tem seus autovalores relacionados aos zeros da função zeta de Riemann. A quantidade de zeros considerados será igual à dimensão da matriz unitária correspondente ao circuito. De algum modo, tal circuito pode ser considerado um passo na realização da sugestão de Hilbert-Póyla em um espaço de dimensão finita. Além disso, a existência de tal circuito implica, ao menos em princípio, que é sempre possível construir um sistema físico relacionado a qualquer número finito de zeros da função usando um computador quântico. Adicionalmente, também será mostrado um algoritmo quântico baseado no circuito quântico de Riemann e discutido brevemente o entrelaçamento biparte gerado pelo circuito quando aplicado a uma dada classe de estados quânticos de até dezesseis qubits.

O restante deste capítulo está organizado da seguinte forma: Na Seção 10.2 é apresentado o procedimento para a construção da matriz unitária cujos autovalores estão relacionados aos zeros da função zeta de Riemann. A Seção 10.3 discute algumas aplicações para o circuito de Riemann. Na sequência, a Seção 10.5 expõe o circuito quântico relacionado a matriz desenvolvida na Seção 10.2. Por fim a Seção 10.6 apresenta as conclusões.

10.2 Construção da matriz unitária Riemanniana

Toma-se $s_1, s_2, s_3, ..., s_k$, como o conjunto dos k primeiros zeros não triviais da função zeta de Riemann, $\zeta(s) = \sum_n (1/n^s)$. É sempre possível construir uma matriz unitária $k \times k$ cujos autovalores são s_j^*/s_j para $j = 1, 2, ..., k$. Inicialmente, introduz-se a matriz $k \times k$

$$G = \begin{bmatrix} s_k & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & s_{k-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & s_{k-2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & s_3 & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \cdots & (s_1+s_2)/2 & (s_1-s_2)/2 \\ 0 & 0 & 0 & 0 & \cdots & (s_1-s_2)/2 & (s_1+s_2)/2 \end{bmatrix}. \tag{10.1}$$

Os k autovalores de G são os zeros $s_1, s_2, s_3, ..., s_k$. Escrevendo os zeros na forma $s_j = a + ib_j$, em que ambos a (como será explicado posteriormente, o método proposto trabalha apenas para zeros com a mesma parte real) e b_j são números reais, a matriz G pode ser reescrita

como a soma de duas matrizes $G = aI + iB$

$$G = aI + iB = a\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} + i\begin{bmatrix} b_k & 0 & 0 & 0 & 0 \\ 0 & b_{k-1} & 0 & 0 & 0 \\ 0 & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \cdots & (b_1+b_2)/2 & (b_1-b_2)/2 \\ 0 & 0 & \cdots & (b_1-b_2)/2 & (b_1+b_2)/2 \end{bmatrix}. \quad (10.2)$$

Agora, a matriz $G' = (1/a)G = I + i(1/a)B$ tem autovalores $s_1/a, s_2/a, s_3/a, ...,$ s_k/a, enquanto a matriz $G'^{\dagger} = (1/a)G^{\dagger} = I - i(1/a)B$ tem autovalores $s_1^*/a, s_2^*/a, s_3^*/a, ..., s_k^*/a$. Então, uma vez que B é Hermitiana, a matriz unitária Riemanniana pode ser obtida pela razão $G'^{\dagger}/G'$, conforme mostrado na Equação (10.3).

$$U_R = \frac{G'^{\dagger}}{G'} = \frac{I - i(1/a)B}{I + i(1/a)B}. \quad (10.3)$$

Os autovalores de U_R são exatamente $e^{i\theta_j} = s_j^*/s_j$, para $j = 1, 2, ..., k$. Como pode ser notado, o procedimento descrito funciona apenas para zeros que tenham a mesma parte real, então considerando $a = 1/2$, tem-se

$$\theta_j = -\pi + \tan^{-1}\left[-b_j/\left(\frac{1}{4} - b_j^2\right)\right]. \quad (10.4)$$

Pode-se notar que, se no lugar de G tal qual definida na Equação (10.1) fosse definida G como uma matriz diagonal cujos elementos seriam $s_1, s_2, s_3, ..., s_k$, poderiam ser usados zeros com diferentes partes rais (caso eles existam). Entretanto, neste caso, não poderia ser obtida G' como uma soma envolvendo a identidade, deste modo não seria possível construir a matriz unitária U_R.

Algumas informações sobre os ângulos θ_j na Equação (10.4) podem ser obtidas a partir da fórmula de Riemann-von Mangoldt: o número de zeros da função Zeta de Riemann $a + ib_j$ com $0 < b \leq T$ é assintoticamente dado por $N(T) = (T/2\pi)\log(T/2\pi e) + O(\log(T))$. Agora, considera-se a seguinte aproximação:

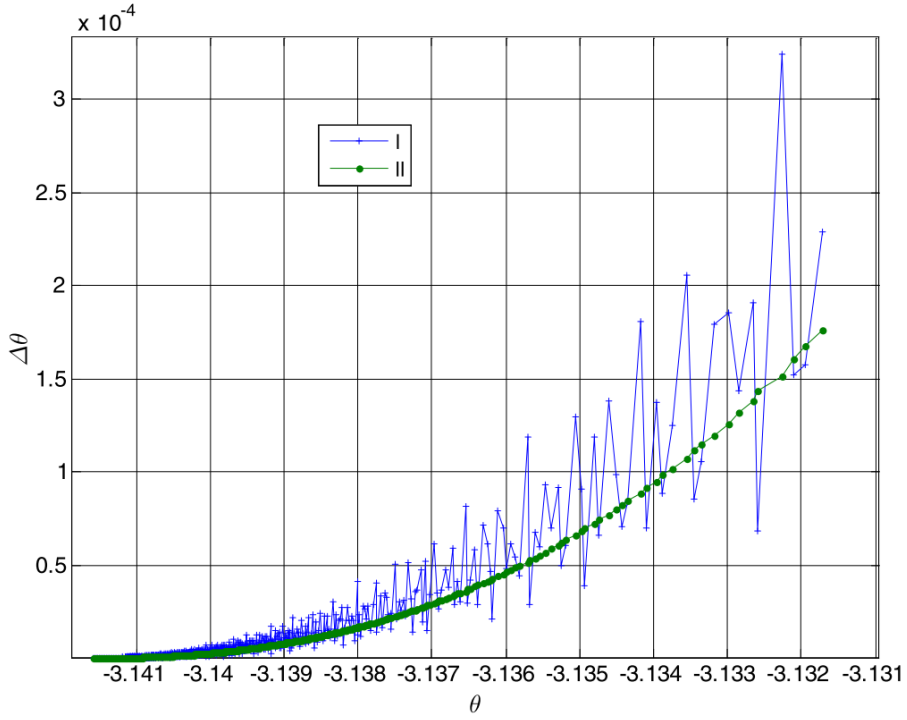
$$\begin{aligned} \theta_j &= -\pi + \tan^{-1}\left[-b_j/\left(\frac{1}{4} - b_j^2\right)\right] \\ &\approx -\pi + \tan^{-1}(1/b_j) \\ &\approx -\pi + 1/b_j. \end{aligned} \quad (10.5)$$

Por exemplo, para o menor zero (positivo) na linha crítica ($b_1 \sim 14,134725142000001$) tem-se $|\theta_1 - (-\pi + 1/b_1)| \sim 3 \times 10^{-5}$. A quantidade de θ's no intervalo $[\theta_1, \theta_1 - \epsilon]$ (em que $\epsilon \ll \theta_1$ é um ângulo bastante pequeno) é assintoticamente dado pela fórmula Riemann-von

Mangoldt com $T = 1/\epsilon$. A distância entre dois ângulos consecutivos θ_j e θ_{j+1} é $\Delta\theta_j \sim (1/b_j) - (1/b_{j+1}) = (b_{j+1} - b_j)/(b_{j+1} \cdot b_j) \sim (\Delta b_j)(\pi + \theta_{j+1})(\pi + \theta_j)$. Entretanto, a distância entre a parte imaginária de dois zeros consecutivos, Δb_j, é assintoticamente dado por $2\pi/\log(j)$, por isso, $\Delta\theta_j \sim (2\pi/\log(j))(\pi + \theta_{j+1})(\pi + \theta_j)$. Um gráfico de $\Delta\theta$ versus θ pode ser visto na Figura 10.1. A curva (I) é obtida usando zeros com $b \in [101,3178510060000; 120000, 3764067760]$ enquanto a curva (II) é a fórmula analítica $(2\pi/\log(j))(\pi + \theta_{j+1})(\pi + \theta_j)$ para $j \in [30, 169165]$ (o trigésimo zero é $1/2 + i101,3178510060000$ e o zero de número 169165 é $1/2 + i120000,3764067760$).

Por fim, uma vez que b_j cresce quando j cresce, θ_j se aproxima de $-\pi$ quando j cresce. Contudo, o valor de $\sum_1^\infty (\pi + \theta_j)$ não parece convergir (uma verificação numérica usando os primeiros 2.001.052 zeros providos por Odlyzko [117] pode ser realizada facilmente). Isto pode ser entendido levando-se em consideração que, para valores elevados de j, $b_j \sim 2\pi j/\log(j)$ e, por isso, $\sum_j 1/b_j$ não converge por ser maior que a série harmônica.

Figura 10.1: Distância entre dois θ's consecutivos versus θ: (I) Obtidos usando zeros com $b \in [101.3178510060000, 120000.3764067760]$. (II) $(2\pi/\log(j))(\pi + \theta_{j+1})(\pi + \theta_j)$ para $j \in [30, 169165]$.



10.3 Aplicações do circuito quântico Riemanniano

Uma vez que o termo $-\pi$ na Equação (10.4) aparecerá como uma fase global nos estados quânticos, deste ponto em diante ele não será mais levado em consideração, assume-

se então que $\theta_j \sim 1/b_j$. Agora, considera-se $|\psi_0\rangle, |\psi_1\rangle, ..., |\psi_{k-1}\rangle$ o conjunto dos autovetores de U_R $(k \times k)$, em que $|\psi_j\rangle$ é o autovetor associado ao autovalor $\exp(i\theta_j)$. Agora, pode-se descrever um algoritmo quântico para calcular o valor de $\sum_{j=0}^{k-1} \theta_j$, em que k é o número de zeros da função zeta de Riemann considerados. Primeiramente, defini-se o operador quântico T que desloca o autoestado por uma unidade, isto é,

$$T|\psi_j\rangle = \left|\psi_{(j+1) \bmod k}\right\rangle. \tag{10.6}$$

Na sequência, defini-se o estado quântico de Riemann como

$$|\psi_R\rangle = U_R \sum_{j=1}^{k} \frac{1}{\sqrt{k}} |\psi_j\rangle = \sum_{j=1}^{k} \frac{1}{\sqrt{k}} e^{i\theta_j} |\psi_j\rangle. \tag{10.7}$$

Agora, aplicando a Equação (10.6) na Equação (10.7) chega-se a

$$(TU_R)^k \sum_{j=1}^{k} \frac{1}{\sqrt{k}} |\psi_j\rangle = e^{i\left(\sum_{m=1}^{k} \theta_m\right)} \sum_{j=1}^{k} \frac{1}{\sqrt{k}} |\psi_j\rangle. \tag{10.8}$$

Assim, o estado quântico $(1/\sqrt{k}) \sum_{j=0}^{k-1} |\psi_j\rangle$ é um autovetor do operador $(TU_R)^k$ com autovalor correspondente $e^{i\left(\sum_{m=0}^{k-1} \theta_m\right)}$, portanto, o algoritmo quântico de estimação de autovalores [118] pode ser usado para obter uma estimativa do valor de $\sum_{m=0}^{k-1} \theta_m$. De modo similar, pode-se definir um algoritmo quântico para estimar o valor de $\sum_{m=1}^{k-1} \Delta_{m+1,m}$, em que $\Delta_{m+1,m}$ é a diferença dos ângulos de dois autovalores consecutivos: $\theta_{m+1} - \theta_m$ (portanto, $\sum_{m=1}^{k-1} \Delta_{m+1,m} = \theta_k - \theta_1$). Neste caso, pode-se notar que $R|\psi_j\rangle = \exp(\theta_{j+1} - \theta_j)|\psi_j\rangle$ se $R = (TU_R)^\dagger (U_R T)$. Portanto, $T(TR)^{k-1}|\psi_1\rangle = \exp(i \sum_{m=1}^{k} \Delta_{m+1,m})|\psi_1\rangle$ e, novamente, $\sum_{m=1}^{k-1} \Delta_{m+1,m}$ pode ser estimado usando o algoritmo quântico de estimação de autovalores.

10.4 Entrelaçamento do estado de Riemann

O estado Riemanniano $|\psi_R\rangle$ de n qubits carrega informação acerca dos primeiros k zeros da função zeta de Riemann, $k = 2^n$. Portanto, faz-se interessante, conforme apresentada na sequência, uma análise do entrelaçamento multiparte gerado pela aplicação da matriz unitária Riemanniana ao estado $|\psi_R\rangle$ descrito na Equação (10.7) que, na base canônica, possui a forma

$$|\psi_R\rangle = \begin{bmatrix} e^{i\theta_k}|00...00\rangle + e^{i\theta_{k-1}}|00...01\rangle + \cdots + \\ \sqrt{2}e^{i\left(\frac{\theta_0+\theta_1+\pi/4}{2}\right)} \sin(\frac{\theta_0-\theta_1-\pi/4}{2})|11..10\rangle + \\ \sqrt{2}e^{i\left(\frac{\theta_0+\theta_1-\pi/4}{2}\right)} \cos(\frac{\theta_0-\theta_1-\pi/4}{2})|11..11\rangle \end{bmatrix}. \tag{10.9}$$

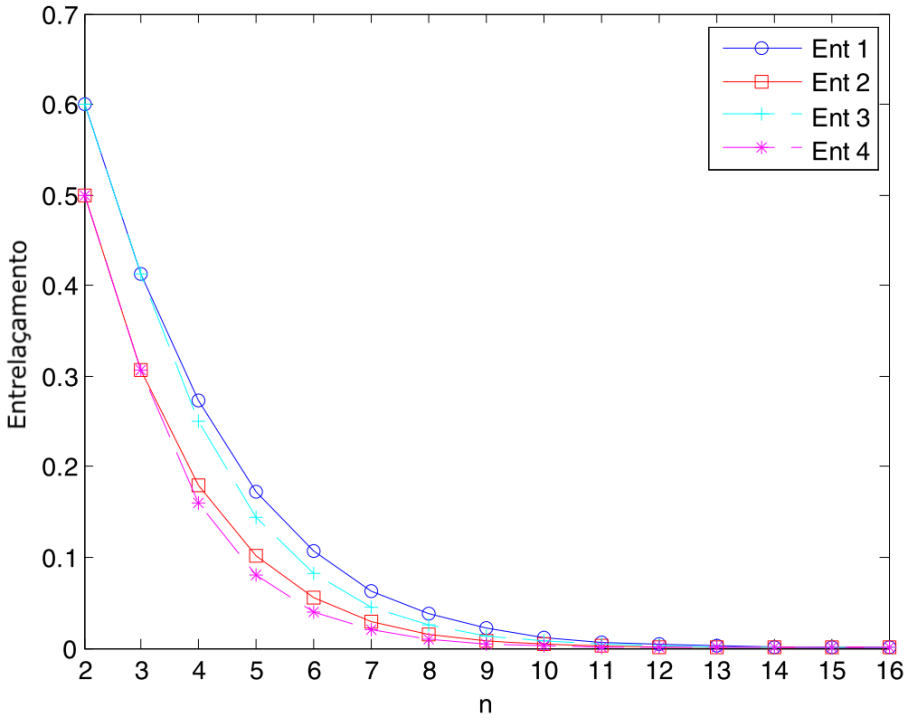
Para o cálculo do entrelaçamento multiparte, são utilizadas medidas de entrelaçamento baseadas na entropia de von-Neumann e na entropia linear, definidas como

$$S_{VN} = -tr\left[\rho \log_2(\rho)\right], \tag{10.10}$$

$$S_L = 2\left[1 - tr(\rho^2)\right]. \tag{10.11}$$

Os entrelaçamentos em função do número de qubits de $|\psi_R\rangle$ são mostrados na Figura 10.2. Os valores Ent_1 e Ent_2 são as médias dos entrelaçamentos bipartes de todas as partições do

Figura 10.2: Entrelaçamento médio biparte em função do número de qubits do estado de Riemannian dado na Equação (10.9).



estado de Riemann, enquanto Ent_3 e Ent_4 são as médias dos entrelaçamentos considerando apenas as bipartições em que uma das partes tem apenas um qubit:

$$Ent_1 = \frac{1}{2^{n-1}-1} \sum_{k=1}^{2^{n-1}-1} S_{VN}(\rho_{\Omega_k \_ \Omega - \Omega_k}), \tag{10.12}$$

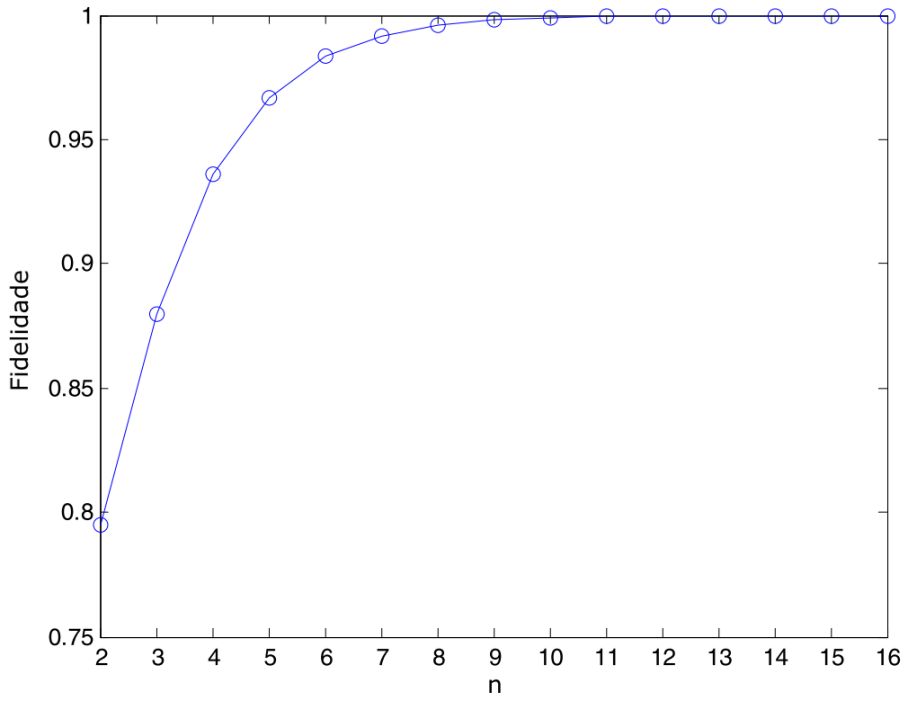
$$Ent_2 = \frac{1}{2^{n-1}-1} \sum_{k=1}^{2^{n-1}-1} S_L(\rho_{\Omega_k \_ \Omega - \Omega_k}), \tag{10.13}$$

$$Ent_3 = \frac{1}{n}\sum_{k=1}^{n} S_{VN}(\rho_{1_k\_\Omega-1_k}), \tag{10.14}$$

$$Ent_4 = \frac{1}{n}\sum_{k=1}^{n} S_{L}(\rho_{1_k\_\Omega-1_k}). \tag{10.15}$$

Nas equações (10.12)–(10.15), o termo Ω representa o conjunto completo dos n qubits, Ω_k representa um subconjunto em particular, 1_k representa uma partição contendo um único qubit e $\Omega - \Omega_k$ é o subconjunto dos elementos de Ω que não pertencem a Ω_k. Como pode ser notado na figura, quanto maior o número de qubits (n) menor é o entrelaçamento médio. Isto acontece em razão de maiores valores de j implicarem em $\theta_j \sim \arctan^{-1}(1/b_j) \sim 0$. Deste modo, o estado Riemanniano se aproxima de $H^{\otimes n}\left|0\right\rangle^{\otimes n}$, como pode ser visto na Figura 10.3. Isto pode

Figura 10.3: Fidelidade, dada por $\langle\psi_R\left|H^{\otimes n}\right|0\rangle^{\otimes n}$, em função do número de qubits.



ser melhor analisado lembrando que, uma vez que ambos são estados puros, a distância entre eles pode ser simplesmente dada pela fidelidade: $F = \left|\langle\psi_R\left|H^{\otimes n}\right|0\rangle^{\otimes n}\right|^2$. Portanto, pode-se mostrar que $\lim_k^{\infty} F = 1$, em que $k = 2^n$, iniciando por notar que

$$\left|\sum_{j=0}^{k} e^{i\theta_j}\right|^2 = \sum_{j,l=1}^{k} e^{i(\theta_j-\theta_l)} \tag{10.16a}$$

$$= \sum_{j=1}^{k} 1 + 2 \sum_{\substack{j,l=1 \\ (j>l)}}^{k} \cos(\theta_j - \theta_l) \tag{10.16b}$$

$$\approx k + 2 \sum_{\substack{j,l=0 \\ (j>l)}}^{k} \cos\left(\frac{1}{b_j} - \frac{1}{b_l}\right) \tag{10.16c}$$

$$\approx k + 2 \sum_{\substack{j,l=0 \\ (j>l)}}^{k} \left(1 - \frac{(b_j^{-1} - b_l^{-1})^2}{2}\right) \tag{10.16d}$$

$$\approx k + 2 \sum_{\substack{j,l=0 \\ (j>l)}}^{k} 1 = k + 2\frac{k(k-1)}{2} = k^2. \tag{10.16e}$$

Observa-se que foi utilizado $\cos(\phi) \sim 1 - \phi^2 \sim 1$, uma vez que $(b_j^{-1} - b_l^{-1})$ é muito pequeno. Retomando a fidelidade, após alguma álgebra se conclui que

$$F = \frac{1}{k^2} \left| \sum_{j=1}^{k} e^{i\theta_j} - e^{i\theta_2} + (\sqrt{2} - 1)e^{i\theta_1} \right|^2, \tag{10.17}$$

de onde se pode notar que quando k cresce, o termo fora do somatório permanece constante enquanto o somatório cresce, tornando-se dominante. Deste modo, usando Equação (10.16) se percebe que $F \sim 1$ quando k cresce.

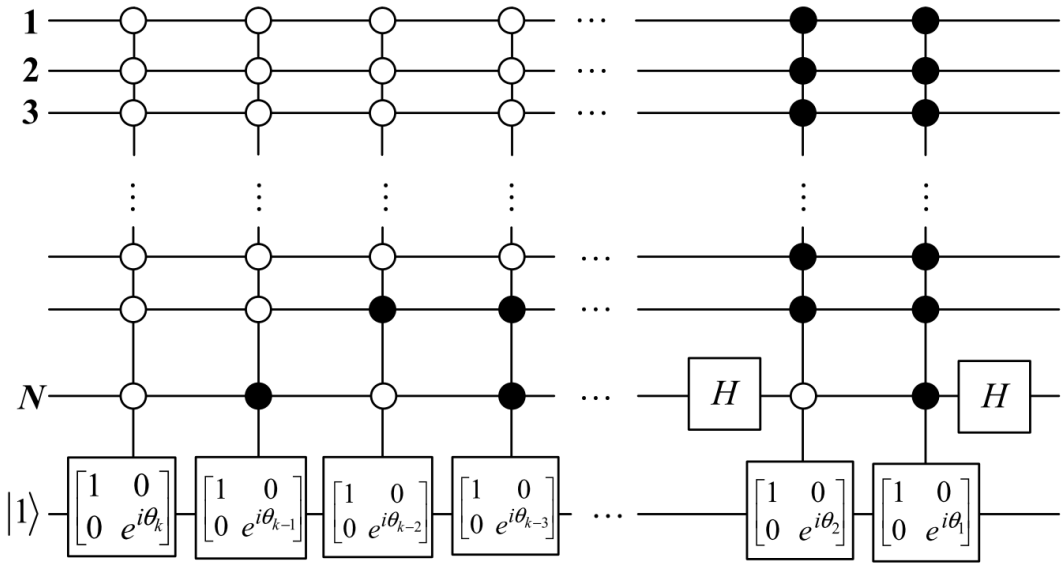
Comparando o entrelaçamento do estado de Riemann com o entrelaçamento calculado para o estado Primo dado em [29], pode-se ver que o estado Primo tem uma maior quantidade de entrelaçamento médio. Esta diferença é, de algum modo, esperada, embora ambos os estados estejam relacionados aos números primos essa relação se dá de diferentes formas. O estado de Riemann está releacionado aos números primos por seus coeficientes serem uma função dos zeros da função zeta de Riemann. Por outro lado, o estado Primo é uma superposição equiprovável de estados cujas codificações decimais são números primos.

10.5 Construção do circuito quântico Riemanniano

A partir da matriz unitária $k \times k$ dada na Equação (10.3), é sempre possível obter um circuito quântico que representa sua realização física. Sem perda de generalidade, será considerado o caso em que $k = 2^n$ para que se obtenha um circuito para n qubits. Diferentes procedimentos podem ser utilizados para obter o circuito quântico associado a uma matriz, em geral, procedimentos diferentes levarão a circuitos diferentes, ainda que equivalentes, um exemplo é a CSD (*Cosine-Sine Decomposition*) [119]. Seguramente é possível montar um circuito composto apenas de $CNOT$'s e portas de um qubit cujas parametrizações de rotações dependem dos zeros. Entretanto, optou-se por uma abordagem simples usando os autovetores

de U_R.

Figura 10.4: Circuito quântico de Riemann.



Os autoestados do circuito quântico mostrado na Figura 10.4 são os autovetores de U_R (o último qubit está sempre no estado 1 e, portanto, pode ser ignorado):

$$|\psi_k\rangle = |00...000\rangle \tag{10.18a}$$
$$|\psi_{k-1}\rangle = |00...001\rangle \tag{10.18b}$$
$$|\psi_{k-2}\rangle = |00...010\rangle \tag{10.18c}$$
$$|\psi_{k-3}\rangle = |00...011\rangle \tag{10.18d}$$
$$\vdots$$
$$|\psi_2\rangle = |11...11\rangle\,(-e^{i\pi/4}\,|0\rangle + |1\rangle)/\sqrt{2} \tag{10.18e}$$
$$|\psi_1\rangle = |11...11\rangle\,(|0\rangle + e^{i\pi/4}\,|1\rangle)/\sqrt{2}. \tag{10.18f}$$

Deste modo, a Figura 10.4 apresenta o circuito quântico que mostra como programar (uma vez que demanda o conhecimento acerca dos zeros) um computador quântico universal para funcionar como um sistema físico relacionado aos zeros da função zeta de Riemann.

10.6 Conclusão

Primeiramente, pode-se notar que a abordagem aqui apresentada é diferente daquela tradicionalmente encontrada na literatura em que se busca um sistema quântico relacionado aos infinitos zeros da função zeta de Riemann. Em geral, o potencial quântico usado em tais sistemas são difíceis de encontrar na natureza ou mesmo construir artificialmente. Em se-

gundo lugar, faz-se importante salientar que, embora tenha-se considerado os primeiros k zeros da função zeta de Riemann, a teoria aqui descrita pode ser aplicada para um valor arbitrário de k.

Deste modo, pode-se tomar qualquer quantidade finita de zeros, evidentemente na linha crítica, e construir o circuito quântico cujos autovalores estão relacionados aos zeros de uma maneira muito clara: cada autovalor depende exclusivamente de um zero da função. Assim, pode-se afirmar que todos os zeros da função zeta de Riemann são relacionados a um sistema físico. Portanto, a abordagem aqui descrita mostra como construir um sistema físico, com recursos finitos (número de portas quânticas), capaz de lidar com um conjunto de qualquer quantidade (finita) de zeros.

Este circuito quântico pode ser útil para algumas tarefas, por exemplo, para estudar as propriedades dos zeros da função em diferentes partes da linha crítica. Ainda, como o sistema físico em questão é um circuito quântico, ele pode ser, ao menos em princípio, programado em um computador quântico universal e, deste modo, implementado usando óptica, supercondutores, pontos quânticos ou outra tecnologia estudada na implementação de computadores quânticos.

Por outro lado, pode-se arguir que é fácil produzir uma matriz unitária e, consequentemente, um circuito quântico cujos autovalores estejam relacionados aos zeros da função zeta de Riemann. Por exemplo, uma matriz unitária $k \times k$ relacionada poderia ser montada como uma matriz diagonal cujos elementos seriam $\theta_j \forall j \in \{1, 2, \cdots, k\}$, em que θ_j seria o exposto na Equação (10.4). Neste caso, os autoestados seriam estados da base canônica. Contudo, considera-se esta abordagem demasiadamente artificial uma vez que a parte real dos zeros da função não são levadas em consideração em nenhum momento. Além disso, ela não decorreria da sugestão de Hilbert-Pólya que aponta para a busca de um operador do tipo $I/2 + iH$.

Capítulo 11

Conclusões e trabalhos futuros

11.1 Conclusões

Esta tese tratou essencialmente os temas da separabilidade, da teleportação de portas quânticas e sobre algumas conexões com a teoria dos números. Temas para os quais as conclusões são apresentadas, de modo agrupado, nas seções seguintes.

11.1.1 Separabilidade

- ◇ Foi demonstrado um teorema acerca da preservação da separabilidade sob conjugação para elementos em $U(4)$, ou seja, quando $U \cdot (V_A \otimes V_B) \cdot U^\dagger = V'_A \otimes V'_B$, em que $U \in U(4)$ e $V_A, V_B, V'_A, V'_B \in U(2)$.
- ◇ Foi demonstrado um teorema que define a forma geral de um elemento do grupo de Clifford.
- ◇ Foram formulados os critérios para separabilidade de estados quânticos em partições e dimensões arbitrárias.
- ◇ A noção de separabilidade de estados quânticos foi aplicada na busca por entrelaçadores universais achando alguns bons candidatos construídos a partir de portas quânticas largamente conhecidas.

11.1.2 Teleportabilidade

- ◇ Foi realizada uma formulação analítica que explicita o papel da base de medição na teleportação de um estado quântico arbitrário.
- ◇ Foi demonstrado o teorema da teleportabilidade que descreve as condições, necessárias e suficientes, sob as quais se obtém uma teleportação determinística de portas de dois qubits.

◇ Foram apresentadas a caracterização e algumas parametrizações de bases de medição úteis ao protocolo de teleportação de portas quânticas.

◇ Foi demonstrada a teleportação de portas quânticas fora do grupo de Clifford.

◇ Foi construída uma formulação analítica que descreve detalhadamente o papel do estado recurso no protocolo de teleportação de portas quânticas, incluindo a definição da classe de estados úteis ao processo.

11.1.3 Informação quântica e a teoria dos números

◇ Foram enunciado os estados quânticos sequências e realizadas análises acerca das propriedades de seu entrelaçamento e preparação usando o algoritmo de Grover.

◇ Foram apontadas algumas características dos estados sequências que sugerem contradições na literatura acerca da interpretação das propriedades do estado Primo.

◇ Foram propostas novas sequências de números inteiros inspiradas em estados quânticos e entrelaçamento.

◇ Foi formulado o circuito quântico de Riemann, uma realidade física associada aos zeros da função Zeta de Riemann.

◇ Foi apresentada uma discussão sobre o entrelaçamento do estado quântico de Riemann.

11.2 Trabalhos futuros

11.2.1 Separabilidade

◇ Avaliar a possibilidade de formulação de uma medida de entrelaçamento a partir dos critérios de separabilidade.

◇ Aplicar os critérios de separabilidade em parametrizações de vetores/matrizes unitárias [88, 89] para definir formas gerais, preferencialmente usando parâmetros reais, de vetores e matrizes, separáveis e não separáveis, para dimensões além de qubits.

◇ De posse das parametrizações alcançadas no item anterior, buscar aplicar estratégias [90–92] para solução de sistemas de equações polinomiais afim de buscar parametrizações para entrelaçadores universais.

11.2.2 Teleportabilidade

◇ Realizar um estudo mais elaborado sobre o comportamento do protocolo de teleportação de portas quânticas sob a ação do ruído em vários pontos do circuito e quando utilizado um estado arbitrário a ser teleportado.

◇ Analisar como o conhecimento gerado neste trabalho pode ser aplicado em outros protocolos de teleportação além do proposto por Gottesman e Chuang [1].

11.2.3 Informação quântica e a teoria dos números

◇ Buscar aplicações dos estados sequências na otimização/solução de problemas na teoria dos números.

◇ Buscar entender quais propriedades "clássicas" das sequências de números inteiros podem, de algum modo, estar associadas ao comportamento do entrelaçamento encontrado nos estados quânticos gerados a partir delas.

◇ Buscar novas aplicações na teoria dos números para o circuito quântico de Riemann.

◇ Estudar a possibilidade de generalização do circuito de Riemann para uma quantidade infinita de zeros da função Zeta de Riemann.

◇ Buscar melhor entender alguns indícios encontrados de que o comportamento do entrelaçamento de um estado sequência está mais diretamente ligado ao padrão de formação das sequências subjacentes que ao número de elementos presentes na interseção entre estas.

Referências Bibliográficas

[1] GOTTESMAN, D.; CHUANG, I. L. Quantum teleportation is a universal computational primitive. *Nature*, v. 402, p. 390–392, Aug 1999. Disponível em: <http://arxiv.org/abs/quant-ph/9908010>.

[2] XIN-WEI, Z.; GANG-LONG, M. Classification of four-qubit states by means of a stochastic local operation and the classical communication invariant. *Chinese Physics Letters*, v. 28, n. 2, p. 020301, 2011. Disponível em: <http://stacks.iop.org/0256-307X/28/i=2/a=020301>.

[3] US DOE. *Site – Human Genome Project Information*. 2009. Disponível em: <http://genomics.energy.gov>.

[4] US DOE. *Site – U.S. Department of Energy*. 2009. Acesso em: 12 dez. 2009. Disponível em: <http://www.energy.gov>.

[5] BENIOFF, P. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of Statistical Physics*, V22, n. 5, p. 563–591, May 1980. Disponível em: <http://dx.doi.org/10.1007/BF01011339>.

[6] FEYNMAN, R. P. Simulating physics with computers. *International Journal of Theoretical Physics*, v. 21, p. 6–7, 1982.

[7] DEUTSCH, D. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, v. 400, n. 1818, p. 97–117, 1985. Disponível em: <http://www.jstor.org/stable/2397601>.

[8] SHOR, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Symposium on Foundations of Computer Science*, v. 00, p. 00–00, jan 1994.

[9] GROVER, L. K. A fast quantum mechanical algorithm for database search. In: *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. New York, NY, USA: ACM, 1996. p. 212–219. ISBN 0-89791-785-5.

[10] DEUTSCH, D.; JOZSA, R. Rapid solution of problems by quantum computation. *Proc Roy Soc Lond A*, v. 439, p. 553–558, October 1992.

[11] ARORA, S.; BARAK, B. *Computational Complexity: A Modern Approach*. [S.l.]: Cambridge University Press, 2007. ISBN 0521424267, 9780521424264.

[12] SIMON, D. R. On the power of quantum computation. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. Los Alamitos, CA: Institute of Electrical and Electronic Engineers Computer Society Press, 1994. p. 116–123. Disponível em: <http://citeseer.ist.psu.edu/simon94power.html>.

[13] DEUTSCH, D. *The Fabric of Reality*. [S.l.]: Penguin, 1998. ISBN 014027541X, 9780140275414.

[14] BENNETT, C. H. et al. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, American Physical Society, v. 70, n. 13, p. 1895–1899, Mar 1993.

[15] EINSTEIN, A.; PODOLSKY, B.; ROSEN, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, American Physical Society, v. 47, n. 10, p. 777–780, May 1935.

[16] BRASSARD, G.; HORODECKI, P.; MOR, T. Telepovm – a generalized quantum teleportation scheme. *IBM J. Res. Dev.*, IBM Corp., Riverton, NJ, USA, v. 48, n. 1, p. 87–97, 2004. ISSN 0018-8646.

[17] BRASSARD, G.; BRAUNSTEIN, S. L.; CLEVE, R. Teleportation as a quantum computation. In: *PhysComp96: Proceedings of the fourth workshop on Physics and computation*. Amsterdam, The Netherlands, The Netherlands: Elsevier Science Publishers B. V., 1998. p. 43–47. ISBN 0167-2789.

[18] MENDES, F. V.; RAMOS, R. V. Schemes for teleportation of quantum gates. *Quantum Information Processing*, Springer US, v. 10, n. 2, p. 203–212, 2011. ISSN 1570-0755. Disponível em: <http://dx.doi.org/10.1007/s11128-010-0189-7>.

[19] YUAN, Z.-S. et al. Experimental demonstration of a bdcz quantum repeater node. *Nature*, Macmillan Publishers Limited, v. 454, p. 1098–1101, Aug 2008. ISSN 0028-0836.

[20] DUAN, R.; FENG, Y.; YING, M. Local distinguishability of multipartite unitary operations. *Phys. Rev. Lett.*, American Physical Society, v. 100, p. 020503, Jan 2008. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.100.020503>.

[21] YU, N.; DUAN, R.; YING, M. Optimal simulation of a perfect entangler. *Phys. Rev. A*, American Physical Society, v. 81, p. 032328, Mar 2010. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.81.032328>.

[22] BALAKRISHNAN, S.; SANKARANARAYANAN, R. Entangling power and local invariants of two-qubit gates. *Phys. Rev. A*, American Physical Society, v. 82, p. 034301, Sep 2010. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.82.034301>.

[23] CAMPBELL, E. T. Optimal entangling capacity of dynamical processes. *Phys. Rev. A*, American Physical Society, v. 82, p. 042314, Oct 2010. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.82.042314>.

[24] CHEN, J. et al. Existence of universal entangler. *Journal of Mathematical Physics*, v. 49, n. 1, p. –, 2008. Disponível em: <http://scitation.aip.org/content/aip/journal/jmp/49/1/10.1063/1.2829895>.

[25] BORISOV, A.; NATHANSON, M. B.; WANG, Y. Quantum integers and cyclotomy. *Journal of Number Theory*, v. 109, n. 1, p. 120 – 135, 2004. ISSN 0022-314X. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0022314X04001180>.

[26] TOKUO, K. Quantum number theory. *International Journal of Theoretical Physics*, Kluwer Academic Publishers-Plenum Publishers, v. 43, n. 12, p. 2461–2481, 2004. ISSN 0020-7748. Disponível em: <http://dx.doi.org/10.1007/s10773-004-7711-6>.

[27] KONTOROVICH, A. V.; NATHANSON, M. B. Quadratic addition rules for quantum integers. *Journal of Number Theory*, v. 117, n. 1, p. 1 – 13, 2006. ISSN 0022-314X. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0022314X05001058>.

[28] RAMOS, R. V.; MENDES, F. V. Riemannian quantum circuit. *Physics Letters A*, v. 378, n. 20, p. 1346 – 1349, 2014. ISSN 0375-9601. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0375960114001571>.

[29] Latorre, J. I.; Sierra, G. Quantum Computation of Prime Number Functions. *ArXiv e-prints*, fev. 2013.

[30] Latorre, J. I.; Sierra, G. There is entanglement in the primes. *ArXiv e-prints*, mar 2014.

[31] BOUWMEESTER, D. et al. Experimental quantum teleportation. *Nature*, Nature, v. 390, p. 575–579, Dec 1997.

[32] NIELSEN, M. A.; KNILL, E.; LAFLAMME, R. Complete quantum teleportation using nuclear magnetic resonance. *Nature*, Nature, v. 396, p. 52–55, Nov 1998.

[33] RIEBE, M. et al. Deterministic quantum teleportation with atoms. *Nature*, Nature Publishing Group, v. 429, n. 6993, p. 734–737, June 2004. ISSN 0028-0836. Disponível em: <http://dx.doi.org/10.1038/nature02570>.

[34] LI, D. et al. Quantum secure direct communication using w state. *Communications in Theoretical Physics*, v. 49, n. 6, p. 1495–1498, 2008. Disponível em: <http://stacks.iop.org/0253-6102/49/1495>.

[35] DONG, J.; TENG, J.; WANG, S. Multiparty controlled quantum secure direct communication of d-dimensional using ghz state. In: *IITA '08: Proceedings of the 2008 Second International Symposium on Intelligent Information Technology Application*. Washington, DC, USA: IEEE Computer Society, 2008. p. 551–555. ISBN 978-0-7695-3497-8.

[36] ZHAN-JUN, Z.; YI-MIN, L.; ZHONG-XIAO, M. Many-agent controlled teleportation of multi-qubit quantum information via quantum entanglement swapping. *Communications in Theoretical Physics*, v. 44, n. 5, p. 847–850, 2005. Disponível em: <http://stacks.iop.org/0253-6102/44/847>.

[37] MURAO, M. et al. Quantum telecloning and multiparticle entanglement. *Phys. Rev. A*, American Physical Society, v. 59, n. 1, p. 156–161, Jan 1999.

[38] CIRAC, J. I. et al. Distributed quantum computation over noisy channels. *Phys. Rev. A*, American Physical Society, v. 59, n. 6, p. 4249–4254, Jun 1999.

[39] CHEFLES, A.; GILSON, C. R.; BARNETT, S. M. Entanglement, information, and multiparticle quantum operations. *Phys. Rev. A*, American Physical Society, v. 63, n. 3, p. 032314, Feb 2001.

[40] METER, R. D. V. *Architecture of a Quantum Multicomputer Optimized for Shor's Factoring Algorithm*. 2006. Disponível em: <http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0607065>.

[41] CHEN, L.; LU, H.; CHEN, W. Constructing a universal set of quantum gates via probabilistic teleportation. *Chin. Opt. Lett.*, OSA, v. 3, n. 4, p. 240–243, 2005. Disponível em: <http://col.osa.org/abstract.cfm?URI=col-3-4-240>.

[42] NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. Paperback. Disponível em: <http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20{&}path=ASIN/0521635039>.

[43] PRESKILL, J. Reliable quantum computers. *Proc. Roy. Soc. Lond. A*, v. 454, p. 385, 1998. Disponível em: <http://arxiv.org/abs/quant-ph/9705031>.

[44] DIVINCENZO, D. P. Fault tolerant architectures for superconducting qubits. *Physica Scripta*, T137, p. 014020, May 2009. Disponível em: <http://stacks.iop.org/1402-4896/2009/i=T137/a=014020>.

[45] SHOR, P. W. Fault-tolerant quantum computation. In: *FOCS '96: Proceedings of the 37th Annual Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 1996. p. 56.

[46] KNILL RAYMOND LAFLAMME, W. H. Z. E. Resilient quantum computation. *Science*, v. 279, p. 342–345, 1998.

[47] GREENBERGER, D. M. et al. Bell's theorem without inequalities. *American Journal of Physics*, AAPT, v. 58, n. 12, p. 1131–1143, 1990. Disponível em: <http://link.aip.org/link/?AJP/58/1131/1>.

[48] SAMELSON, H. *Notes on Lie Algebras 2nd edition*. [S.l.]: Springer, 1990. ISBN 0387972641, 9780387972640.

[49] BARENCO, A. et al. Elementary gates for quantum computation. *Phys. Rev. A*, American Physical Society, v. 52, n. 5, p. 3457–3467, Nov 1995.

[50] KNILL, E. Group representations, error bases and quantum codes. In: *Los Alamos National Laboratory Report*. [s.n.], 1996. p. 96–2807. Disponível em: <http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/9608049>.

[51] GOTTESMAN, D. Fault-tolerant quantum computation with higher-dimensional systems. In: *QCQC '98: Selected papers from the First NASA International Conference on Quantum Computing and Quantum Communications*. London, UK: Springer-Verlag, 1998. p. 302–313. ISBN 3-540-65514-X.

[52] ALBER, G. et al. *Generalized quantum XOR-gate for quantum teleportation and state purification in arbitrary dimensional Hilbert spaces*. 2000. Disponível em: <http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0008022>.

[53] CHEN, G.; KAUFFMAN, L.; LOMONACO, S. J. *Mathematics of Quantum Computation and Quantum Technology*. [S.l.]: Chapman & Hall/CRC, 2007. ISBN 1584888997, 9781584888994.

[54] NAKAHARA, M.; RAHIMI, R.; SAITOH, A. *Mathematical Aspects of Quantum Computing 2007*. [S.l.]: World Scientific Publishing Company, 2007. ISBN 9812814477, 9789812814470.

[55] SHARMA, C. The kronecker product of two 2x2 matrices, lorentz transformations, and the structure of space-time in special relativity. *Annals of Physics*, v. 210, n. 2, p. 241 – 254, 1991. ISSN 0003-4916. Disponível em: <http://www.sciencedirect.com/science/article/pii/0003491691900449>.

[56] SZYMICZEK, K. *Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms*. [S.l.]: Taylor & Francis, 1997. (Algebra, logic, and applications). ISBN 9789056990763.

[57] Dutailly, J. C. *Mathematics for theoretical physics*. [s.n.], 2012. Disponível em: <http://adsabs.harvard.edu/abs/2012arXiv1209.5665D>.

[58] Tucci, R. R. An Introduction to Cartan's KAK Decomposition for QC Programmers. *eprint arXiv:quant-ph/0507171*, jul. 2005.

[59] VUJI?I?, J. S. M. *Linear Algebra Thoroughly Explained*. [S.l.]: Springer Berlin Heidelberg, 2008. ISBN 9783540746379.

[60] GILBERT, J.; GILBERT, L. *Linear Algebra and Matrix Theory*. [S.l.]: Academic Press, 1995. ISBN 9780122829703.

[61] LIPSCHUTZ, S.; LIPSON, M. *Schaum's Outline of Linear Algebra, 4ed*. [S.l.]: McGraw-Hill Education, 2008. (Schaum's Outline Series). ISBN 9780071543538.

[62] ISRAEL, R. *Private communication*. 2012.

[63] CLARK, S.; JOZSA, R.; LINDEN, N. Generalized clifford groups and simulation of associated quantum circuits. *Quantum Info. Comput.*, Rinton Press, Incorporated, Paramus, NJ, v. 8, n. 1, p. 106–126, jan. 2008. ISSN 1533-7146. Disponível em: <http://dl.acm.org/citation.cfm?id=2011752.2011760>.

[64] STENHOLM, S.; BARDROFF, P. J. Teleportation of N-dimensional states. *Phys. Rev. A*, American Physical Society, v. 58, p. 4373–4376, Dec 1998. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.58.4373>.

[65] SAN-RU HOU BO-YU, X. X.-Q. H.; RUI-HONG, Y. Quantum standard teleportation based on the generic measurement bases. *Communications in Theoretical Physics*, v. 40, p. 415–420, Oct 2003. Disponível em: <http://ctp.itp.ac.cn/EN/abstract/abstract9413.shtml>.

[66] TAPP, K. *Matrix Groups For Undergraduates*. American Mathematical Society, 2005. (Student Mathematical Library). ISBN 9780821837856. Disponível em: <http://books.google.com.br/books?id=Un_15Im3NhUC>.

[67] LUQUE, J.-G.; THIBON, J.-Y. Polynomial invariants of four qubits. *Phys. Rev. A*, American Physical Society, v. 67, p. 042303, Apr 2003. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.67.042303>.

[68] OLIVEIRA, D.; RAMOS, R. Residual entanglement with negativity for pure four-qubit quantum states. *Quantum Information Processing*, Springer US, v. 9, n. 4, p. 497–508, 2010. ISSN 1570-0755. Disponível em: <http://dx.doi.org/10.1007/s11128-009-0154-5>.

[69] Mendes, F. V.; Ramos, R. V. On the role of the basis of measurement in quantum gate teleportation. *ArXiv e-prints*, jul 2013. Disponível em: <http://arxiv.org/abs/1307.4750>.

[70] VERSTRAETE, F. et al. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, American Physical Society, v. 65, p. 052112, Apr 2002. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.65.052112>.

[71] YEO, Y.; CHUA, W. K. Teleportation and dense coding with genuine multipartite entanglement. *Phys. Rev. Lett.*, American Physical Society, v. 96, p. 060502, Feb 2006. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.96.060502>.

[72] MENDES, F. V.; RAMOS, R. V. Numerical search for universal entanglers in $\mathbb{C}^3 \otimes \mathbb{C}^4$ and $\mathbb{C}^4 \otimes \mathbb{C}^4$. *Physics Letters A*, v. 379, n. 4, p. 289 – 292, 2015. ISSN 0375-9601. Disponível em: <http://www.sciencedirect.com/science/article/pii/S037596011401216X>.

[73] NEUMANN, J. von. *Mathematical Foundations of Quantum Mechanics*. [S.l.]: Princeton Press, 1955. xii + 445 p. (Princeton landmarks in mathematics and physics series). Translated from the German edition by Robert T. Beyer. Original first edition published in German in 1932. ISBN 0-691-08003-8; 0-691-02893-1.

[74] WOOTTERS, W. K. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, American Physical Society, v. 80, p. 2245–2248, Mar 1998. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.80.2245>.

[75] HORODECKI PAWEL HORODECKI, R. H. M. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, v. 223, n. 1-2, p. 1 – 8, 1996. ISSN 0375-9601. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0375960196007062>.

[76] VIDAL, G.; WERNER, R. F. Computable measure of entanglement. *Phys. Rev. A*, American Physical Society, v. 65, p. 032314, Feb 2002. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.65.032314>.

[77] ZANARDI, P.; ZALKA, C.; FAORO, L. Entangling power of quantum evolutions. *Phys. Rev. A*, American Physical Society, v. 62, p. 030301, Aug 2000. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.62.030301>.

[78] KRAUS, B.; CIRAC, J. I. Optimal creation of entanglement using a two-qubit gate. *Phys. Rev. A*, American Physical Society, v. 63, p. 062309, May 2001. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.63.062309>.

[79] REZAKHANI, A. T. Characterization of two-qubit perfect entanglers. *Phys. Rev. A*, American Physical Society, v. 70, p. 052313, Nov 2004. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.70.052313>.

[80] Chen, J. et al. Minimum Entangling Power is Close to Its Maximum. *ArXiv e-prints*, out. 2012.

[81] KLASSEN, J.; CHEN, J.; ZENG, B. Universal Entanglers for Bosonic and Fermionic Systems. In: SEVERINI, S.; BRANDAO, F. (Ed.). *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2013. (Leibniz International Proceedings in Informatics (LIPIcs), v. 22), p. 35–49. ISBN 978-3-939897-55-2. ISSN 1868-8969. Disponível em: <http://drops.dagstuhl.de/opus/volltexte/2013/4322>.

[82] BATLE, J.; CASAS, M.; PLASTINO, A. Correlated multipartite quantum states. *Phys. Rev. A*, American Physical Society, v. 87, p. 032318, Mar 2013. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevA.87.032318>.

[83] Klassen, J.; Chen, J.; Zeng, B. Universal Entanglers for Bosonic and Fermionic Systems. *ArXiv e-prints, Presented at TQC 2013*, maio 2013.

[84] STORN, R.; PRICE, K. Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces. *J. of Global Optimization*, Kluwer Academic Publishers, Hingham, MA, USA, v. 11, n. 4, p. 341–359, dez. 1997. ISSN 0925-5001. Disponível em: <http://dx.doi.org/10.1023/A:1008202821328>.

[85] PRICE, K.; STORN, R. M.; LAMPINEN, J. A. *Differential Evolution: A Practical Approach to Global Optimization (Natural Computing Series)*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005. ISBN 3540209506.

[86] NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. Paperback. Disponível em: <http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20&path=ASIN/0521635039>.

[87] EDELMAN, A.; RAO, N. R. Random matrix theory. *Acta Numerica*, v. 14, p. 233–297, 5 2005. ISSN 1474-0508. Disponível em: <http://journals.cambridge.org/article_S0962492904000236>.

[88] LUNDBERG, M.; SVENSSON, L. The haar measure and the generation of random unitary matrices. In: *Sensor Array and Multichannel Signal Processing Workshop Proceedings, 2004*. [S.l.: s.n.], 2004. p. 114–118.

[89] JARLSKOG, C. A recursive parametrization of unitary matrices. *Journal of Mathematical Physics*, v. 46, n. 10, p. –, 2005. Disponível em: <http://scitation.aip.org/content/aip/journal/jmp/46/10/10.1063/1.2038607>.

[90] BUCHBERGER, B. Gröbner bases: A short introduction for systems theorists. In: MORENO-DíAZ, R.; BUCHBERGER, B.; FREIRE, J. L. (Ed.). *Computer Aided Systems Theory – EUROCAST 2001*. Springer Berlin Heidelberg, 2001, (Lecture Notes in Computer Science, v. 2178). p. 1–19. ISBN 978-3-540-42959-3. Disponível em: <http://dx.doi.org/10.1007/3-540-45654-6_1>.

[91] MANOCHA, D. Solving systems of polynomial equations. *Computer Graphics and Applications, IEEE*, v. 14, n. 2, p. 46–55, March 1994. ISSN 0272-1716.

[92] STURMFELS, B. *Solving Systems of Polynomial Equations (Cbms Regional Conference Series in Mathematics)*. American Mathematical Society, 2002. Paperback. ISBN 0821832514. Disponível em: <http://www.worldcat.org/isbn/0821832514>.

[93] Mendes, F. V.; Ramos, R. V. Quantum Sequence States. *ArXiv e-prints*, aug 2014. Disponível em: <http://arxiv.org/abs/1408.4838>.

[94] BROWN, I. D. K. et al. Searching for highly entangled multi-qubit states. *Journal of Physics A: Mathematical and General*, v. 38, n. 5, p. 1119, 2005. Disponível em: <http://stacks.iop.org/0305-4470/38/i=5/a=013>.

[95] BORRAS, A. et al. Multiqubit systems: highly entangled states and entanglement distribution. *Journal of Physics A: Mathematical and Theoretical*, v. 40, n. 44, p. 13407, 2007. Disponível em: <http://stacks.iop.org/1751-8121/40/i=44/a=018>.

[96] TAPIADOR, J. E. et al. Highly entangled multi-qubit states with simple algebraic structure. *Journal of Physics A: Mathematical and Theoretical*, v. 42, n. 41, p. 415301, 2009. Disponível em: <http://stacks.iop.org/1751-8121/42/i=41/a=415301>.

[97] OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences*. 2011. Disponível em: <http://oeis.org>.

[98] HIGUCHI, A.; SUDBERY, A. How entangled can two couples get? *Physics Letters A*, v. 273, n. 4, p. 213 – 217, 2000. ISSN 0375-9601. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0375960100004801>.

[99] GARDINER, V. et al. On certain sequences of integers defined by sieves. *Mathematics Magazine*, Mathematical Association of America, v. 29, n. 3, p. pp. 117–122, 1956. ISSN 0025570X. Disponível em: <http://www.jstor.org/stable/3029719>.

[100] HAWKINS, D.; BRIGGS, W. E. The lucky number theorem. *Mathematics Magazine*, Mathematical Association of America, v. 31, n. 2, p. pp. 81–84, 1957. ISSN 0025570X. Disponível em: <http://www.jstor.org/stable/3029213>.

[101] AGRAWAL, M.; KAYAL, N.; SAXENA, N. Primes is in p. *Annals of Mathematics*, Annals of Mathematics, v. 160, n. 2, p. pp. 781–793, 2004. ISSN 0003486X. Disponível em: <http://www.jstor.org/stable/3597229>.

[102] MILLER, G. L. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, v. 13, n. 3, p. 300 – 317, 1976. ISSN 0022-0000. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0022000076800438>.

[103] van Dam, W. Quantum Computing and Zeroes of Zeta Functions. *eprint arXiv:quant-ph/0405081*, maio 2004.

[104] DAM, W.; SHPARLINSKI, I. Classical and quantum algorithms for exponential congruences. Springer Berlin Heidelberg, v. 5106, p. 1–10, 2008. Disponível em: <http://dx.doi.org/10.1007/978-3-540-89304-2_1>.

[105] SCHUMAYER, D.; HUTCHINSON, D. A. W. *Colloquium* : Physics of the riemann hypothesis. *Rev. Mod. Phys.*, American Physical Society, v. 83, p. 307–330, Apr 2011. Disponível em: <http://link.aps.org/doi/10.1103/RevModPhys.83.307>.

[106] Ramos, R. V. Riemann Hypothesis as an Uncertainty Relation. *ArXiv e-prints*, abr. 2013.

[107] Wolf, M. Will a physicists prove the Riemann Hypothesis? *ArXiv e-prints*, out. 2014.

[108] SCHUMAYER, D.; ZYL, B. P. van; HUTCHINSON, D. A. W. Quantum mechanical potentials related to the prime numbers and riemann zeros. *Phys. Rev. E*, American Physical Society, v. 78, p. 056215, Nov 2008. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevE.78.056215>.

[109] BUNIMOVICH, L.; DETTMANN, C. Open circular billiards and the riemann hypothesis. *Phys. Rev. Lett.*, American Physical Society, v. 94, p. 100201, Mar 2005. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.94.100201>.

[110] BERRY, M.; KEATING, J. The riemann zeros and eigenvalue asymptotics. *SIAM Review*, v. 41, n. 2, p. 236–266, 1999. Disponível em: <http://dx.doi.org/10.1137/S0036144598347497>.

[111] MONTGOMERY, H. L. The pair correlation of zeros of the zeta function. In: *Analytic number theory – Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo.* Providence, R.I.: Amer. Math. Soc., 1973. p. 181–193.

[112] BOGOMOLNY, E. B.; KEATING, J. P. Random matrix theory and the riemann zeros ii: n - point correlations. *Nonlinearity*, v. 9, n. 4, p. 911, 1996. Disponível em: <http://stacks.iop.org/0951-7715/9/i=4/a=006>.

[113] BORWEIN, D.; BORWEIN, J. M.; TAYLOR, K. F. Convergence of lattice sums and madelung's constant. *Journal of Mathematical Physics*, v. 26, n. 11, p. 2999–3009, 1985. Disponível em: <http://scitation.aip.org/content/aip/journal/jmp/26/11/10.1063/1.526675>.

[114] CHEN, N.-x. Modified möbius inverse formula and its applications in physics. *Phys. Rev. Lett.*, American Physical Society, v. 64, p. 1193–1195, Mar 1990. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.64.1193>.

[115] BILLINGSLEY, P. Prime Numbers and Brownian Motion. *The American Mathematical Monthly*, Mathematical Association of America, v. 80, n. 10, 1973. ISSN 00029890. Disponível em: <http://dx.doi.org/10.2307/2318544>.

[116] VERDIèRE, Y. Colin de. Ergodicité et fonctions propres du laplacien. *Comm. Math. Phys.*, Springer, v. 102, n. 3, p. 497–502, 1985. Disponível em: <http://projecteuclid.org/euclid.cmp/1104114465>.

[117] ODLYZKO, A. *Tables of zeros of the Riemann zeta function*. 2014. Disponível em: <http://www.dtc.umn.edu/~odlyzko/zeta_tables/>.

[118] KAYE, P.; LAFLAMME, R.; MOSCA, M. *An Introduction to Quantum Computing*. New York, NY, USA: Oxford University Press, Inc., 2007. ISBN 0198570007.

[119] MÖTTÖNEN, M. et al. Quantum circuits for general multiqubit gates. *Phys. Rev. Lett.*, American Physical Society, v. 93, p. 130502, Sep 2004. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.93.130502>.

Apêndices

Apêndice A

Condições de separabilidade: casos particulares

Resumo

Este apêndice apresenta a aplicação da técnica sobre a separabilidade de estados quânticos desenvolvida no Capítulo 8 para vários casos particulares nas dimensões $2 \otimes n$, $3 \otimes n$ *e* $4 \otimes n$ *com* $n \in \{2, 3, 4, 5, 6, 7, 8\}$. *Para todos os casos, a separabilidade será verificada se, e somente se,* $\sum_i |\xi_i| = 0$.

A.1 Separabilidade de estados na forma $2 \otimes n$ com $n \in [2, 8]$

A.1.1 Espaço $2 \otimes 3$

$$\xi_1 = \alpha_{00} \cdot \alpha_{04} - \alpha_{01} \cdot \alpha_{03}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{05} - \alpha_{02} \cdot \alpha_{03}; \quad \xi_3 = \alpha_{01} \cdot \alpha_{05} - \alpha_{02} \cdot \alpha_{04}; \tag{A.1}$$

A.1.2 Espaço $2 \otimes 4$

$$\xi_1 = \alpha_{00} \cdot \alpha_{05} - \alpha_{01} \cdot \alpha_{04}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{06} - \alpha_{02} \cdot \alpha_{04}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{04}; \tag{A.2}$$

$$\xi_4 = \alpha_{01} \cdot \alpha_{06} - \alpha_{02} \cdot \alpha_{05}; \quad \xi_5 = \alpha_{01} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{05}; \quad \xi_6 = \alpha_{02} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{06}; \tag{A.3}$$

A.1.3 Espaço $2 \otimes 5$

$$\xi_1 = \alpha_{00} \cdot \alpha_{06} - \alpha_{01} \cdot \alpha_{05}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{07} - \alpha_{02} \cdot \alpha_{05}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{05}; \tag{A.4}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{05}; \quad \xi_5 = \alpha_{01} \cdot \alpha_{07} - \alpha_{02} \cdot \alpha_{06}; \quad \xi_6 = \alpha_{01} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{06}; \tag{A.5}$$

$$\xi_7 = \alpha_{01} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{06}; \quad \xi_8 = \alpha_{02} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{07}; \quad \xi_9 = \alpha_{02} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{07}; \tag{A.6}$$

$$\xi_{10} = \alpha_{03} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{08}; \tag{A.7}$$

A.1.4 Espaço $2 \otimes 6$

$$\xi_1 = \alpha_{00} \cdot \alpha_{07} - \alpha_{01} \cdot \alpha_{06}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{06}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{06}; \tag{A.8}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{06}; \quad \xi_5 = \alpha_{00} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{06}; \quad \xi_6 = \alpha_{01} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{07}; \tag{A.9}$$

$$\xi_7 = \alpha_{01} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{07}; \quad \xi_8 = \alpha_{01} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{07}; \quad \xi_9 = \alpha_{01} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{07}; \tag{A.10}$$

$$\xi_{10} = \alpha_{02} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{08}; \quad \xi_{11} = \alpha_{02} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_{12} = \alpha_{02} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{08}; \tag{A.11}$$

$$\xi_{13} = \alpha_{03} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{09}; \quad \xi_{14} = \alpha_{03} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{15} = \alpha_{04} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{10}; \tag{A.12}$$

A.1.5 Espaço $2 \otimes 7$

$$\xi_1 = \alpha_{00} \cdot \alpha_{08} - \alpha_{01} \cdot \alpha_{07}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{09} - \alpha_{02} \cdot \alpha_{07}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{07}; \tag{A.13}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{07}; \quad \xi_5 = \alpha_{00} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{07}; \quad \xi_6 = \alpha_{00} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{07}; \tag{A.14}$$

$$\xi_7 = \alpha_{01} \cdot \alpha_{09} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_8 = \alpha_{01} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{08}; \quad \xi_9 = \alpha_{01} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{08}; \tag{A.15}$$

$$\xi_{10} = \alpha_{01} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_{11} = \alpha_{01} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{08}; \quad \xi_{12} = \alpha_{02} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{09}; \tag{A.16}$$

$$\xi_{13} = \alpha_{02} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{09}; \quad \xi_{14} = \alpha_{02} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{15} = \alpha_{02} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{09}; \tag{A.17}$$

$$\xi_{16} = \alpha_{03} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{10}; \quad \xi_{17} = \alpha_{03} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{10}; \quad \xi_{18} = \alpha_{03} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{10}; \tag{A.18}$$

$$\xi_{19} = \alpha_{04} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{11}; \quad \xi_{20} = \alpha_{04} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{11}; \quad \xi_{21} = \alpha_{05} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{12}; \tag{A.19}$$

A.1.6 Espaço $2 \otimes 8$

$$\xi_1 = \alpha_{00} \cdot \alpha_{09} - \alpha_{01} \cdot \alpha_{08}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{08}; \tag{A.20}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_5 = \alpha_{00} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_6 = \alpha_{00} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{08}; \tag{A.21}$$

$$\xi_7 = \alpha_{00} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{08}; \quad \xi_8 = \alpha_{01} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{09}; \quad \xi_9 = \alpha_{01} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{09}; \tag{A.22}$$

$$\xi_{10} = \alpha_{01} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{09}; \quad \xi_{11} = \alpha_{01} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{12} = \alpha_{01} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{09}; \tag{A.23}$$

$$\xi_{13} = \alpha_{01} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{09}; \quad \xi_{14} = \alpha_{02} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{10}; \quad \xi_{15} = \alpha_{02} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{10}; \tag{A.24}$$

$$\xi_{16} = \alpha_{02} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{10}; \quad \xi_{17} = \alpha_{02} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{10}; \quad \xi_{18} = \alpha_{02} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{10}; \tag{A.25}$$

$$\xi_{19} = \alpha_{03} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{11}; \quad \xi_{20} = \alpha_{03} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{11}; \quad \xi_{21} = \alpha_{03} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{11}; \tag{A.26}$$

$$\xi_{22} = \alpha_{03} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{11}; \quad \xi_{23} = \alpha_{04} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{12}; \quad \xi_{24} = \alpha_{04} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{12}; \tag{A.27}$$

$$\xi_{25} = \alpha_{04} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{12}; \quad \xi_{26} = \alpha_{05} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{13}; \quad \xi_{27} = \alpha_{05} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{13}; \tag{A.28}$$

$$\xi_{28} = \alpha_{06} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{14}; \tag{A.29}$$

A.2 Separabilidade de estados na forma $3 \otimes n$ com $n \in [2, 8]$

A.2.1 Espaço $3 \otimes 2$

$$\xi_1 = \alpha_{00} \cdot \alpha_{03} - \alpha_{01} \cdot \alpha_{02}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{05} - \alpha_{01} \cdot \alpha_{04}; \quad \xi_3 = \alpha_{02} \cdot \alpha_{05} - \alpha_{03} \cdot \alpha_{04}; \tag{A.30}$$

A.2.2 Espaço $3 \otimes 3$

$$\xi_1 = \alpha_{00} \cdot \alpha_{04} - \alpha_{01} \cdot \alpha_{03}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{05} - \alpha_{02} \cdot \alpha_{03}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{07} - \alpha_{01} \cdot \alpha_{06}; \tag{A.31}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{06}; \quad \xi_5 = \alpha_{01} \cdot \alpha_{05} - \alpha_{02} \cdot \alpha_{04}; \quad \xi_6 = \alpha_{01} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{07}; \tag{A.32}$$

$$\xi_7 = \alpha_{03} \cdot \alpha_{07} - \alpha_{04} \cdot \alpha_{06}; \quad \xi_8 = \alpha_{03} \cdot \alpha_{08} - \alpha_{05} \cdot \alpha_{06}; \quad \xi_9 = \alpha_{04} \cdot \alpha_{08} - \alpha_{05} \cdot \alpha_{07}; \tag{A.33}$$

A.2.3 Espaço $3 \otimes 4$

$$\xi_1 = \alpha_{00} \cdot \alpha_{05} - \alpha_{01} \cdot \alpha_{04}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{06} - \alpha_{02} \cdot \alpha_{04}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{04}; \tag{A.34}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{09} - \alpha_{01} \cdot \alpha_{08}; \quad \xi_5 = \alpha_{00} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_6 = \alpha_{00} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{08}; \tag{A.35}$$

$$\xi_7 = \alpha_{01} \cdot \alpha_{06} - \alpha_{02} \cdot \alpha_{05}; \quad \xi_8 = \alpha_{01} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{05}; \quad \xi_9 = \alpha_{01} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{09}; \tag{A.36}$$

$$\xi_{10} = \alpha_{01} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{09}; \quad \xi_{11} = \alpha_{02} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{06}; \quad \xi_{12} = \alpha_{02} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{10}; \tag{A.37}$$

$$\xi_{13} = \alpha_{04} \cdot \alpha_{09} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_{14} = \alpha_{04} \cdot \alpha_{10} - \alpha_{06} \cdot \alpha_{08}; \quad \xi_{15} = \alpha_{04} \cdot \alpha_{11} - \alpha_{07} \cdot \alpha_{08}; \tag{A.38}$$

$$\xi_{16} = \alpha_{05} \cdot \alpha_{10} - \alpha_{06} \cdot \alpha_{09}; \quad \xi_{17} = \alpha_{05} \cdot \alpha_{11} - \alpha_{07} \cdot \alpha_{09}; \quad \xi_{18} = \alpha_{06} \cdot \alpha_{11} - \alpha_{07} \cdot \alpha_{10}; \tag{A.39}$$

A.2.4 Espaço $3 \otimes 5$

$$\xi_1 = \alpha_{00} \cdot \alpha_{06} - \alpha_{01} \cdot \alpha_{05}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{07} - \alpha_{02} \cdot \alpha_{05}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{05}; \tag{A.40}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{05}; \quad \xi_5 = \alpha_{00} \cdot \alpha_{11} - \alpha_{01} \cdot \alpha_{10}; \quad \xi_6 = \alpha_{00} \cdot \alpha_{12} - \alpha_{02} \cdot \alpha_{10}; \tag{A.41}$$

$$\xi_7 = \alpha_{00} \cdot \alpha_{13} - \alpha_{03} \cdot \alpha_{10}; \quad \xi_8 = \alpha_{00} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{10}; \quad \xi_9 = \alpha_{01} \cdot \alpha_{07} - \alpha_{02} \cdot \alpha_{06}; \tag{A.42}$$

$$\xi_{10} = \alpha_{01} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{06}; \quad \xi_{11} = \alpha_{01} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{06}; \quad \xi_{12} = \alpha_{01} \cdot \alpha_{12} - \alpha_{02} \cdot \alpha_{11}; \tag{A.43}$$

$$\xi_{13} = \alpha_{01} \cdot \alpha_{13} - \alpha_{03} \cdot \alpha_{11}; \quad \xi_{14} = \alpha_{01} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{11}; \quad \xi_{15} = \alpha_{02} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{07}; \tag{A.44}$$

$$\xi_{16} = \alpha_{02} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{07}; \quad \xi_{17} = \alpha_{02} \cdot \alpha_{13} - \alpha_{03} \cdot \alpha_{12}; \quad \xi_{18} = \alpha_{02} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{12}; \tag{A.45}$$

$$\xi_{19} = \alpha_{03} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_{20} = \alpha_{03} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{13}; \quad \xi_{21} = \alpha_{05} \cdot \alpha_{11} - \alpha_{06} \cdot \alpha_{10}; \tag{A.46}$$

$$\xi_{22} = \alpha_{05} \cdot \alpha_{12} - \alpha_{07} \cdot \alpha_{10}; \quad \xi_{23} = \alpha_{05} \cdot \alpha_{13} - \alpha_{08} \cdot \alpha_{10}; \quad \xi_{24} = \alpha_{05} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{10}; \tag{A.47}$$

$$\xi_{25} = \alpha_{06} \cdot \alpha_{12} - \alpha_{07} \cdot \alpha_{11}; \quad \xi_{26} = \alpha_{06} \cdot \alpha_{13} - \alpha_{08} \cdot \alpha_{11}; \quad \xi_{27} = \alpha_{06} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{11}; \tag{A.48}$$

$$\xi_{28} = \alpha_{07} \cdot \alpha_{13} - \alpha_{08} \cdot \alpha_{12}; \quad \xi_{29} = \alpha_{07} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{12}; \quad \xi_{30} = \alpha_{08} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{13}; \tag{A.49}$$

A.2.5 Espaço $3 \otimes 6$

$$\xi_1 = \alpha_{00} \cdot \alpha_{07} - \alpha_{01} \cdot \alpha_{06}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{06}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{06}; \tag{A.50}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{06}; \quad \xi_5 = \alpha_{00} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{06}; \quad \xi_6 = \alpha_{00} \cdot \alpha_{13} - \alpha_{01} \cdot \alpha_{12}; \tag{A.51}$$

$$\xi_7 = \alpha_{00} \cdot \alpha_{14} - \alpha_{02} \cdot \alpha_{12}; \quad \xi_8 = \alpha_{00} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{12}; \quad \xi_9 = \alpha_{00} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{12}; \tag{A.52}$$

$$\xi_{10} = \alpha_{00} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{12}; \quad \xi_{11} = \alpha_{01} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{07}; \quad \xi_{12} = \alpha_{01} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{07}; \tag{A.53}$$

$$\xi_{13} = \alpha_{01} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{07}; \quad \xi_{14} = \alpha_{01} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{07}; \quad \xi_{15} = \alpha_{01} \cdot \alpha_{14} - \alpha_{02} \cdot \alpha_{13}; \tag{A.54}$$

$$\xi_{16} = \alpha_{01} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{13}; \quad \xi_{17} = \alpha_{01} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{13}; \quad \xi_{18} = \alpha_{01} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{13}; \tag{A.55}$$

$$\xi_{19} = \alpha_{02} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{08}; \quad \xi_{20} = \alpha_{02} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_{21} = \alpha_{02} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{08}; \tag{A.56}$$

$$\xi_{22} = \alpha_{02} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{14}; \quad \xi_{23} = \alpha_{02} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{14}; \quad \xi_{24} = \alpha_{02} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{14}; \tag{A.57}$$

$$\xi_{25} = \alpha_{03} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{09}; \quad \xi_{26} = \alpha_{03} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{27} = \alpha_{03} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{15}; \tag{A.58}$$

$$\xi_{28} = \alpha_{03} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{15}; \quad \xi_{29} = \alpha_{04} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{10}; \quad \xi_{30} = \alpha_{04} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{16}; \tag{A.59}$$

$$\xi_{31} = \alpha_{06} \cdot \alpha_{13} - \alpha_{07} \cdot \alpha_{12}; \quad \xi_{32} = \alpha_{06} \cdot \alpha_{14} - \alpha_{08} \cdot \alpha_{12}; \quad \xi_{33} = \alpha_{06} \cdot \alpha_{15} - \alpha_{09} \cdot \alpha_{12}; \tag{A.60}$$

$$\xi_{34} = \alpha_{06} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{12}; \quad \xi_{35} = \alpha_{06} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{12}; \quad \xi_{36} = \alpha_{07} \cdot \alpha_{14} - \alpha_{08} \cdot \alpha_{13}; \tag{A.61}$$

$$\xi_{37} = \alpha_{07} \cdot \alpha_{15} - \alpha_{09} \cdot \alpha_{13}; \quad \xi_{38} = \alpha_{07} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{13}; \quad \xi_{39} = \alpha_{07} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{13}; \tag{A.62}$$

$$\xi_{40} = \alpha_{08} \cdot \alpha_{15} - \alpha_{09} \cdot \alpha_{14}; \quad \xi_{41} = \alpha_{08} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{14}; \quad \xi_{42} = \alpha_{08} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{14}; \tag{A.63}$$

$$\xi_{43} = \alpha_{09} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{15}; \quad \xi_{44} = \alpha_{09} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{15}; \quad \xi_{45} = \alpha_{10} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{16}; \tag{A.64}$$

A.2.6 Espaço $3 \otimes 7$

$$\xi_1 = \alpha_{00} \cdot \alpha_{08} - \alpha_{01} \cdot \alpha_{07}; \quad \xi_2 = \alpha_{00} \cdot \alpha_{09} - \alpha_{02} \cdot \alpha_{07}; \quad \xi_3 = \alpha_{00} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{07}; \tag{A.65}$$

$$\xi_4 = \alpha_{00} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{07}; \quad \xi_5 = \alpha_{00} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{07}; \quad \xi_6 = \alpha_{00} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{07}; \tag{A.66}$$

$$\xi_7 = \alpha_{00} \cdot \alpha_{15} - \alpha_{01} \cdot \alpha_{14}; \quad \xi_8 = \alpha_{00} \cdot \alpha_{16} - \alpha_{02} \cdot \alpha_{14}; \quad \xi_9 = \alpha_{00} \cdot \alpha_{17} - \alpha_{03} \cdot \alpha_{14}; \tag{A.67}$$

$$\xi_{10} = \alpha_{00} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{14}; \quad \xi_{11} = \alpha_{00} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{14}; \quad \xi_{12} = \alpha_{00} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{14}; \tag{A.68}$$

$$\xi_{13} = \alpha_{01} \cdot \alpha_{09} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_{14} = \alpha_{01} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{08}; \quad \xi_{15} = \alpha_{01} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{08}; \tag{A.69}$$

$$\xi_{16} = \alpha_{01} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_{17} = \alpha_{01} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{08}; \quad \xi_{18} = \alpha_{01} \cdot \alpha_{16} - \alpha_{02} \cdot \alpha_{15}; \tag{A.70}$$

$$\xi_{19} = \alpha_{01} \cdot \alpha_{17} - \alpha_{03} \cdot \alpha_{15}; \quad \xi_{20} = \alpha_{01} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{15}; \quad \xi_{21} = \alpha_{01} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{15}; \tag{A.71}$$

$$\xi_{22} = \alpha_{01} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{15}; \quad \xi_{23} = \alpha_{02} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{09}; \quad \xi_{24} = \alpha_{02} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{09}; \tag{A.72}$$

$$\xi_{25} = \alpha_{02} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{26} = \alpha_{02} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{09}; \quad \xi_{27} = \alpha_{02} \cdot \alpha_{17} - \alpha_{03} \cdot \alpha_{16}; \tag{A.73}$$

$$\xi_{28} = \alpha_{02} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{16}; \quad \xi_{29} = \alpha_{02} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{16}; \quad \xi_{30} = \alpha_{02} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{16}; \tag{A.74}$$

$$\xi_{31} = \alpha_{03} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{10}; \quad \xi_{32} = \alpha_{03} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{10}; \quad \xi_{33} = \alpha_{03} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{10}; \tag{A.75}$$

$$\xi_{34} = \alpha_{03} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{17}; \quad \xi_{35} = \alpha_{03} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{17}; \quad \xi_{36} = \alpha_{03} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{17}; \tag{A.76}$$

$$\xi_{37} = \alpha_{04} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{11}; \quad \xi_{38} = \alpha_{04} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{11}; \quad \xi_{39} = \alpha_{04} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{18}; \tag{A.77}$$

$$\xi_{40} = \alpha_{04} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{18}; \quad \xi_{41} = \alpha_{05} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{12}; \quad \xi_{42} = \alpha_{05} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{19}; \tag{A.78}$$

$$\xi_{43} = \alpha_{07} \cdot \alpha_{15} - \alpha_{08} \cdot \alpha_{14}; \quad \xi_{44} = \alpha_{07} \cdot \alpha_{16} - \alpha_{09} \cdot \alpha_{14}; \quad \xi_{45} = \alpha_{07} \cdot \alpha_{17} - \alpha_{10} \cdot \alpha_{14}; \tag{A.79}$$

$$\xi_{46} = \alpha_{07} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{14}; \quad \xi_{47} = \alpha_{07} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{14}; \quad \xi_{48} = \alpha_{07} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{14}; \tag{A.80}$$

$$\xi_{49} = \alpha_{08} \cdot \alpha_{16} - \alpha_{09} \cdot \alpha_{15}; \quad \xi_{50} = \alpha_{08} \cdot \alpha_{17} - \alpha_{10} \cdot \alpha_{15}; \quad \xi_{51} = \alpha_{08} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{15}; \tag{A.81}$$

$$\xi_{52} = \alpha_{08} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{15}; \quad \xi_{53} = \alpha_{08} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{15}; \quad \xi_{54} = \alpha_{09} \cdot \alpha_{17} - \alpha_{10} \cdot \alpha_{16}; \tag{A.82}$$

$$\xi_{55} = \alpha_{09} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{16}; \quad \xi_{56} = \alpha_{09} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{16}; \quad \xi_{57} = \alpha_{09} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{16}; \tag{A.83}$$

$$\xi_{58} = \alpha_{10} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{17}; \quad \xi_{59} = \alpha_{10} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{17}; \quad \xi_{60} = \alpha_{10} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{17}; \tag{A.84}$$

$$\xi_{61} = \alpha_{11} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{18}; \quad \xi_{62} = \alpha_{11} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{18}; \quad \xi_{63} = \alpha_{12} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{19}; \tag{A.85}$$

A.2.7 Espaço $3 \otimes 8$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{09} - \alpha_{01} \cdot \alpha_{08}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{08}; \tag{A.86}$$

$$\xi_{4} = \alpha_{00} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_{5} = \alpha_{00} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_{6} = \alpha_{00} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{08}; \tag{A.87}$$

$$\xi_{7} = \alpha_{00} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{08}; \quad \xi_{8} = \alpha_{00} \cdot \alpha_{17} - \alpha_{01} \cdot \alpha_{16}; \quad \xi_{9} = \alpha_{00} \cdot \alpha_{18} - \alpha_{02} \cdot \alpha_{16}; \tag{A.88}$$

$$\xi_{10} = \alpha_{00} \cdot \alpha_{19} - \alpha_{03} \cdot \alpha_{16}; \quad \xi_{11} = \alpha_{00} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{16}; \quad \xi_{12} = \alpha_{00} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{16}; \tag{A.89}$$

$$\xi_{13} = \alpha_{00} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{16}; \quad \xi_{14} = \alpha_{00} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{16}; \quad \xi_{15} = \alpha_{01} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{09}; \tag{A.90}$$

$$\xi_{16} = \alpha_{01} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{09}; \quad \xi_{17} = \alpha_{01} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{09}; \quad \xi_{18} = \alpha_{01} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{09}; \tag{A.91}$$

$$\xi_{19} = \alpha_{01} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{09}; \quad \xi_{20} = \alpha_{01} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{09}; \quad \xi_{21} = \alpha_{01} \cdot \alpha_{18} - \alpha_{02} \cdot \alpha_{17}; \tag{A.92}$$

$$\xi_{22} = \alpha_{01} \cdot \alpha_{19} - \alpha_{03} \cdot \alpha_{17}; \quad \xi_{23} = \alpha_{01} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{17}; \quad \xi_{24} = \alpha_{01} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{17}; \tag{A.93}$$

$$\xi_{25} = \alpha_{01} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{17}; \quad \xi_{26} = \alpha_{01} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{17}; \quad \xi_{27} = \alpha_{02} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{10}; \tag{A.94}$$

$$\xi_{28} = \alpha_{02} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{10}; \quad \xi_{29} = \alpha_{02} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{10}; \quad \xi_{30} = \alpha_{02} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{10}; \tag{A.95}$$

$$\xi_{31} = \alpha_{02} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{10}; \quad \xi_{32} = \alpha_{02} \cdot \alpha_{19} - \alpha_{03} \cdot \alpha_{18}; \quad \xi_{33} = \alpha_{02} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{18}; \tag{A.96}$$

$$\xi_{34} = \alpha_{02} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{18}; \quad \xi_{35} = \alpha_{02} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{18}; \quad \xi_{36} = \alpha_{02} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{18}; \tag{A.97}$$

$$\xi_{37} = \alpha_{03} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{11}; \quad \xi_{38} = \alpha_{03} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{11}; \quad \xi_{39} = \alpha_{03} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{11}; \tag{A.98}$$

$$\xi_{40} = \alpha_{03} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{11}; \quad \xi_{41} = \alpha_{03} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{19}; \quad \xi_{42} = \alpha_{03} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{19}; \tag{A.99}$$

$$\xi_{43} = \alpha_{03} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{19}; \quad \xi_{44} = \alpha_{03} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{19}; \quad \xi_{45} = \alpha_{04} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{12}; \tag{A.100}$$

$$\xi_{46} = \alpha_{04} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{12}; \quad \xi_{47} = \alpha_{04} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{12}; \quad \xi_{48} = \alpha_{04} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{20}; \tag{A.101}$$

$$\xi_{49} = \alpha_{04} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{20}; \quad \xi_{50} = \alpha_{04} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{20}; \quad \xi_{51} = \alpha_{05} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{13}; \tag{A.102}$$

$$\xi_{52} = \alpha_{05} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{13}; \quad \xi_{53} = \alpha_{05} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{21}; \quad \xi_{54} = \alpha_{05} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{21}; \tag{A.103}$$

$$\xi_{55} = \alpha_{06} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{14}; \quad \xi_{56} = \alpha_{06} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{22}; \quad \xi_{57} = \alpha_{08} \cdot \alpha_{17} - \alpha_{09} \cdot \alpha_{16}; \tag{A.104}$$

$$\xi_{58} = \alpha_{08} \cdot \alpha_{18} - \alpha_{10} \cdot \alpha_{16}; \quad \xi_{59} = \alpha_{08} \cdot \alpha_{19} - \alpha_{11} \cdot \alpha_{16}; \quad \xi_{60} = \alpha_{08} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{16}; \tag{A.105}$$

$$\xi_{61} = \alpha_{08} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{16}; \quad \xi_{62} = \alpha_{08} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{16}; \quad \xi_{63} = \alpha_{08} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{16}; \tag{A.106}$$

$$\xi_{64} = \alpha_{09} \cdot \alpha_{18} - \alpha_{10} \cdot \alpha_{17}; \quad \xi_{65} = \alpha_{09} \cdot \alpha_{19} - \alpha_{11} \cdot \alpha_{17}; \quad \xi_{66} = \alpha_{09} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{17}; \tag{A.107}$$

$$\xi_{67} = \alpha_{09} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{17}; \quad \xi_{68} = \alpha_{09} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{17}; \quad \xi_{69} = \alpha_{09} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{17}; \tag{A.108}$$

$$\xi_{70} = \alpha_{10} \cdot \alpha_{19} - \alpha_{11} \cdot \alpha_{18}; \quad \xi_{71} = \alpha_{10} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{18}; \quad \xi_{72} = \alpha_{10} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{18}; \tag{A.109}$$

$$\xi_{73} = \alpha_{10} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{18}; \quad \xi_{74} = \alpha_{10} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{18}; \quad \xi_{75} = \alpha_{11} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{19}; \tag{A.110}$$

$$\xi_{76} = \alpha_{11} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{19}; \quad \xi_{77} = \alpha_{11} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{19}; \quad \xi_{78} = \alpha_{11} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{19}; \tag{A.111}$$

$$\xi_{79} = \alpha_{12} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{20}; \quad \xi_{80} = \alpha_{12} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{20}; \quad \xi_{81} = \alpha_{12} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{20}; \tag{A.112}$$

$$\xi_{82} = \alpha_{13} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{21}; \quad \xi_{83} = \alpha_{13} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{21}; \quad \xi_{84} = \alpha_{14} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{22}; \tag{A.113}$$

A.3 Separabilidade de estados na forma $4 \otimes n$ com $n \in [2, 8]$

A.3.1 Espaço $4 \otimes 2$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{03} - \alpha_{01} \cdot \alpha_{02}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{05} - \alpha_{01} \cdot \alpha_{04}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{07} - \alpha_{01} \cdot \alpha_{06}; \tag{A.114}$$

$$\xi_{4} = \alpha_{02} \cdot \alpha_{05} - \alpha_{03} \cdot \alpha_{04}; \quad \xi_{5} = \alpha_{02} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{06}; \quad \xi_{6} = \alpha_{04} \cdot \alpha_{07} - \alpha_{05} \cdot \alpha_{06}; \tag{A.115}$$

A.3.2 Espaço $4 \otimes 3$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{04} - \alpha_{01} \cdot \alpha_{03}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{05} - \alpha_{02} \cdot \alpha_{03}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{07} - \alpha_{01} \cdot \alpha_{06}; \tag{A.116}$$

$$\xi_{4} = \alpha_{00} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{06}; \quad \xi_{5} = \alpha_{00} \cdot \alpha_{10} - \alpha_{01} \cdot \alpha_{09}; \quad \xi_{6} = \alpha_{00} \cdot \alpha_{11} - \alpha_{02} \cdot \alpha_{09}; \tag{A.117}$$

$$\xi_{7} = \alpha_{01} \cdot \alpha_{05} - \alpha_{02} \cdot \alpha_{04}; \quad \xi_{8} = \alpha_{01} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{07}; \quad \xi_{9} = \alpha_{01} \cdot \alpha_{11} - \alpha_{02} \cdot \alpha_{10}; \tag{A.118}$$

$$\xi_{10} = \alpha_{03} \cdot \alpha_{07} - \alpha_{04} \cdot \alpha_{06}; \quad \xi_{11} = \alpha_{03} \cdot \alpha_{08} - \alpha_{05} \cdot \alpha_{06}; \quad \xi_{12} = \alpha_{03} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{09}; \tag{A.119}$$

$$\xi_{13} = \alpha_{03} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{14} = \alpha_{04} \cdot \alpha_{08} - \alpha_{05} \cdot \alpha_{07}; \quad \xi_{15} = \alpha_{04} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{10}; \tag{A.120}$$

$$\xi_{16} = \alpha_{06} \cdot \alpha_{10} - \alpha_{07} \cdot \alpha_{09}; \quad \xi_{17} = \alpha_{06} \cdot \alpha_{11} - \alpha_{08} \cdot \alpha_{09}; \quad \xi_{18} = \alpha_{07} \cdot \alpha_{11} - \alpha_{08} \cdot \alpha_{10}; \tag{A.121}$$

A.3.3 Espaço $4 \otimes 4$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{05} - \alpha_{01} \cdot \alpha_{04}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{06} - \alpha_{02} \cdot \alpha_{04}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{04}; \tag{A.122}$$

$$\xi_{4} = \alpha_{00} \cdot \alpha_{09} - \alpha_{01} \cdot \alpha_{08}; \quad \xi_{5} = \alpha_{00} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_{6} = \alpha_{00} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{08}; \tag{A.123}$$

$$\xi_{7} = \alpha_{00} \cdot \alpha_{13} - \alpha_{01} \cdot \alpha_{12}; \quad \xi_{8} = \alpha_{00} \cdot \alpha_{14} - \alpha_{02} \cdot \alpha_{12}; \quad \xi_{9} = \alpha_{00} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{12}; \tag{A.124}$$

$$\xi_{10} = \alpha_{01} \cdot \alpha_{06} - \alpha_{02} \cdot \alpha_{05}; \quad \xi_{11} = \alpha_{01} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{05}; \quad \xi_{12} = \alpha_{01} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{09}; \tag{A.125}$$

$$\xi_{13} = \alpha_{01} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{09}; \quad \xi_{14} = \alpha_{01} \cdot \alpha_{14} - \alpha_{02} \cdot \alpha_{13}; \quad \xi_{15} = \alpha_{01} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{13}; \tag{A.126}$$

$$\xi_{16} = \alpha_{02} \cdot \alpha_{07} - \alpha_{03} \cdot \alpha_{06}; \quad \xi_{17} = \alpha_{02} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{10}; \quad \xi_{18} = \alpha_{02} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{14}; \tag{A.127}$$

$$\xi_{19} = \alpha_{04} \cdot \alpha_{09} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_{20} = \alpha_{04} \cdot \alpha_{10} - \alpha_{06} \cdot \alpha_{08}; \quad \xi_{21} = \alpha_{04} \cdot \alpha_{11} - \alpha_{07} \cdot \alpha_{08}; \tag{A.128}$$

$$\xi_{22} = \alpha_{04} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{12}; \quad \xi_{23} = \alpha_{04} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{12}; \quad \xi_{24} = \alpha_{04} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{12}; \tag{A.129}$$

$$\xi_{25} = \alpha_{05} \cdot \alpha_{10} - \alpha_{06} \cdot \alpha_{09}; \quad \xi_{26} = \alpha_{05} \cdot \alpha_{11} - \alpha_{07} \cdot \alpha_{09}; \quad \xi_{27} = \alpha_{05} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{13}; \tag{A.130}$$

$$\xi_{28} = \alpha_{05} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{13}; \quad \xi_{29} = \alpha_{06} \cdot \alpha_{11} - \alpha_{07} \cdot \alpha_{10}; \quad \xi_{30} = \alpha_{06} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{14}; \tag{A.131}$$

$$\xi_{31} = \alpha_{08} \cdot \alpha_{13} - \alpha_{09} \cdot \alpha_{12}; \quad \xi_{32} = \alpha_{08} \cdot \alpha_{14} - \alpha_{10} \cdot \alpha_{12}; \quad \xi_{33} = \alpha_{08} \cdot \alpha_{15} - \alpha_{11} \cdot \alpha_{12}; \tag{A.132}$$

$$\xi_{34} = \alpha_{09} \cdot \alpha_{14} - \alpha_{10} \cdot \alpha_{13}; \quad \xi_{35} = \alpha_{09} \cdot \alpha_{15} - \alpha_{11} \cdot \alpha_{13}; \quad \xi_{36} = \alpha_{10} \cdot \alpha_{15} - \alpha_{11} \cdot \alpha_{14}; \tag{A.133}$$

A.3.4 Espaço $4 \otimes 5$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{06} - \alpha_{01} \cdot \alpha_{05}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{07} - \alpha_{02} \cdot \alpha_{05}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{05}; \tag{A.134}$$

$$\xi_{4} = \alpha_{00} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{05}; \quad \xi_{5} = \alpha_{00} \cdot \alpha_{11} - \alpha_{01} \cdot \alpha_{10}; \quad \xi_{6} = \alpha_{00} \cdot \alpha_{12} - \alpha_{02} \cdot \alpha_{10}; \tag{A.135}$$

$$\xi_{7} = \alpha_{00} \cdot \alpha_{13} - \alpha_{03} \cdot \alpha_{10}; \quad \xi_{8} = \alpha_{00} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{10}; \quad \xi_{9} = \alpha_{00} \cdot \alpha_{16} - \alpha_{01} \cdot \alpha_{15}; \tag{A.136}$$

$$\xi_{10} = \alpha_{00} \cdot \alpha_{17} - \alpha_{02} \cdot \alpha_{15}; \quad \xi_{11} = \alpha_{00} \cdot \alpha_{18} - \alpha_{03} \cdot \alpha_{15}; \quad \xi_{12} = \alpha_{00} \cdot \alpha_{19} - \alpha_{04} \cdot \alpha_{15}; \tag{A.137}$$

$$\xi_{13} = \alpha_{01} \cdot \alpha_{07} - \alpha_{02} \cdot \alpha_{06}; \quad \xi_{14} = \alpha_{01} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{06}; \quad \xi_{15} = \alpha_{01} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{06}; \tag{A.138}$$

$$\xi_{16} = \alpha_{01} \cdot \alpha_{12} - \alpha_{02} \cdot \alpha_{11}; \quad \xi_{17} = \alpha_{01} \cdot \alpha_{13} - \alpha_{03} \cdot \alpha_{11}; \quad \xi_{18} = \alpha_{01} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{11}; \tag{A.139}$$

$$\xi_{19} = \alpha_{01} \cdot \alpha_{17} - \alpha_{02} \cdot \alpha_{16}; \quad \xi_{20} = \alpha_{01} \cdot \alpha_{18} - \alpha_{03} \cdot \alpha_{16}; \quad \xi_{21} = \alpha_{01} \cdot \alpha_{19} - \alpha_{04} \cdot \alpha_{16}; \tag{A.140}$$

$$\xi_{22} = \alpha_{02} \cdot \alpha_{08} - \alpha_{03} \cdot \alpha_{07}; \quad \xi_{23} = \alpha_{02} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{07}; \quad \xi_{24} = \alpha_{02} \cdot \alpha_{13} - \alpha_{03} \cdot \alpha_{12}; \tag{A.141}$$

$$\xi_{25} = \alpha_{02} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{12}; \quad \xi_{26} = \alpha_{02} \cdot \alpha_{18} - \alpha_{03} \cdot \alpha_{17}; \quad \xi_{27} = \alpha_{02} \cdot \alpha_{19} - \alpha_{04} \cdot \alpha_{17}; \tag{A.142}$$

$$\xi_{28} = \alpha_{03} \cdot \alpha_{09} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_{29} = \alpha_{03} \cdot \alpha_{14} - \alpha_{04} \cdot \alpha_{13}; \quad \xi_{30} = \alpha_{03} \cdot \alpha_{19} - \alpha_{04} \cdot \alpha_{18}; \tag{A.143}$$

$$\xi_{31} = \alpha_{05} \cdot \alpha_{11} - \alpha_{06} \cdot \alpha_{10}; \quad \xi_{32} = \alpha_{05} \cdot \alpha_{12} - \alpha_{07} \cdot \alpha_{10}; \quad \xi_{33} = \alpha_{05} \cdot \alpha_{13} - \alpha_{08} \cdot \alpha_{10}; \tag{A.144}$$

$$\xi_{34} = \alpha_{05} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{10}; \quad \xi_{35} = \alpha_{05} \cdot \alpha_{16} - \alpha_{06} \cdot \alpha_{15}; \quad \xi_{36} = \alpha_{05} \cdot \alpha_{17} - \alpha_{07} \cdot \alpha_{15}; \tag{A.145}$$

$$\xi_{37} = \alpha_{05} \cdot \alpha_{18} - \alpha_{08} \cdot \alpha_{15}; \quad \xi_{38} = \alpha_{05} \cdot \alpha_{19} - \alpha_{09} \cdot \alpha_{15}; \quad \xi_{39} = \alpha_{06} \cdot \alpha_{12} - \alpha_{07} \cdot \alpha_{11}; \tag{A.146}$$

$$\xi_{40} = \alpha_{06} \cdot \alpha_{13} - \alpha_{08} \cdot \alpha_{11}; \quad \xi_{41} = \alpha_{06} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{11}; \quad \xi_{42} = \alpha_{06} \cdot \alpha_{17} - \alpha_{07} \cdot \alpha_{16}; \tag{A.147}$$

$$\xi_{43} = \alpha_{06} \cdot \alpha_{18} - \alpha_{08} \cdot \alpha_{16}; \quad \xi_{44} = \alpha_{06} \cdot \alpha_{19} - \alpha_{09} \cdot \alpha_{16}; \quad \xi_{45} = \alpha_{07} \cdot \alpha_{13} - \alpha_{08} \cdot \alpha_{12}; \tag{A.148}$$

$$\xi_{46} = \alpha_{07} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{12}; \quad \xi_{47} = \alpha_{07} \cdot \alpha_{18} - \alpha_{08} \cdot \alpha_{17}; \quad \xi_{48} = \alpha_{07} \cdot \alpha_{19} - \alpha_{09} \cdot \alpha_{17}; \tag{A.149}$$

$$\xi_{49} = \alpha_{08} \cdot \alpha_{14} - \alpha_{09} \cdot \alpha_{13}; \quad \xi_{50} = \alpha_{08} \cdot \alpha_{19} - \alpha_{09} \cdot \alpha_{18}; \quad \xi_{51} = \alpha_{10} \cdot \alpha_{16} - \alpha_{11} \cdot \alpha_{15}; \tag{A.150}$$

$$\xi_{52} = \alpha_{10} \cdot \alpha_{17} - \alpha_{12} \cdot \alpha_{15}; \quad \xi_{53} = \alpha_{10} \cdot \alpha_{18} - \alpha_{13} \cdot \alpha_{15}; \quad \xi_{54} = \alpha_{10} \cdot \alpha_{19} - \alpha_{14} \cdot \alpha_{15}; \tag{A.151}$$

$$\xi_{55} = \alpha_{11} \cdot \alpha_{17} - \alpha_{12} \cdot \alpha_{16}; \quad \xi_{56} = \alpha_{11} \cdot \alpha_{18} - \alpha_{13} \cdot \alpha_{16}; \quad \xi_{57} = \alpha_{11} \cdot \alpha_{19} - \alpha_{14} \cdot \alpha_{16}; \tag{A.152}$$

$$\xi_{58} = \alpha_{12} \cdot \alpha_{18} - \alpha_{13} \cdot \alpha_{17}; \quad \xi_{59} = \alpha_{12} \cdot \alpha_{19} - \alpha_{14} \cdot \alpha_{17}; \quad \xi_{60} = \alpha_{13} \cdot \alpha_{19} - \alpha_{14} \cdot \alpha_{18}; \tag{A.153}$$

A.3.5 Espaço $4 \otimes 6$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{07} - \alpha_{01} \cdot \alpha_{06}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{06}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{06}; \tag{A.154}$$

$$\xi_{4} = \alpha_{00} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{06}; \quad \xi_{5} = \alpha_{00} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{06}; \quad \xi_{6} = \alpha_{00} \cdot \alpha_{13} - \alpha_{01} \cdot \alpha_{12}; \tag{A.155}$$

$$\xi_{7} = \alpha_{00} \cdot \alpha_{14} - \alpha_{02} \cdot \alpha_{12}; \quad \xi_{8} = \alpha_{00} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{12}; \quad \xi_{9} = \alpha_{00} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{12}; \tag{A.156}$$

$$\xi_{10} = \alpha_{00} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{12}; \quad \xi_{11} = \alpha_{00} \cdot \alpha_{19} - \alpha_{01} \cdot \alpha_{18}; \quad \xi_{12} = \alpha_{00} \cdot \alpha_{20} - \alpha_{02} \cdot \alpha_{18}; \tag{A.157}$$

$$\xi_{13} = \alpha_{00} \cdot \alpha_{21} - \alpha_{03} \cdot \alpha_{18}; \quad \xi_{14} = \alpha_{00} \cdot \alpha_{22} - \alpha_{04} \cdot \alpha_{18}; \quad \xi_{15} = \alpha_{00} \cdot \alpha_{23} - \alpha_{05} \cdot \alpha_{18}; \tag{A.158}$$

$$\xi_{16} = \alpha_{01} \cdot \alpha_{08} - \alpha_{02} \cdot \alpha_{07}; \quad \xi_{17} = \alpha_{01} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{07}; \quad \xi_{18} = \alpha_{01} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{07}; \tag{A.159}$$

$$\xi_{19} = \alpha_{01} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{07}; \quad \xi_{20} = \alpha_{01} \cdot \alpha_{14} - \alpha_{02} \cdot \alpha_{13}; \quad \xi_{21} = \alpha_{01} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{13}; \tag{A.160}$$

$$\xi_{22} = \alpha_{01} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{13}; \quad \xi_{23} = \alpha_{01} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{13}; \quad \xi_{24} = \alpha_{01} \cdot \alpha_{20} - \alpha_{02} \cdot \alpha_{19}; \tag{A.161}$$

$$\xi_{25} = \alpha_{01} \cdot \alpha_{21} - \alpha_{03} \cdot \alpha_{19}; \quad \xi_{26} = \alpha_{01} \cdot \alpha_{22} - \alpha_{04} \cdot \alpha_{19}; \quad \xi_{27} = \alpha_{01} \cdot \alpha_{23} - \alpha_{05} \cdot \alpha_{19}; \tag{A.162}$$

$$\xi_{28} = \alpha_{02} \cdot \alpha_{09} - \alpha_{03} \cdot \alpha_{08}; \quad \xi_{29} = \alpha_{02} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_{30} = \alpha_{02} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{08}; \tag{A.163}$$

$$\xi_{31} = \alpha_{02} \cdot \alpha_{15} - \alpha_{03} \cdot \alpha_{14}; \quad \xi_{32} = \alpha_{02} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{14}; \quad \xi_{33} = \alpha_{02} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{14}; \tag{A.164}$$

$$\xi_{34} = \alpha_{02} \cdot \alpha_{21} - \alpha_{03} \cdot \alpha_{20}; \quad \xi_{35} = \alpha_{02} \cdot \alpha_{22} - \alpha_{04} \cdot \alpha_{20}; \quad \xi_{36} = \alpha_{02} \cdot \alpha_{23} - \alpha_{05} \cdot \alpha_{20}; \tag{A.165}$$

$$\xi_{37} = \alpha_{03} \cdot \alpha_{10} - \alpha_{04} \cdot \alpha_{09}; \quad \xi_{38} = \alpha_{03} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{39} = \alpha_{03} \cdot \alpha_{16} - \alpha_{04} \cdot \alpha_{15}; \tag{A.166}$$

$$\xi_{40} = \alpha_{03} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{15}; \quad \xi_{41} = \alpha_{03} \cdot \alpha_{22} - \alpha_{04} \cdot \alpha_{21}; \quad \xi_{42} = \alpha_{03} \cdot \alpha_{23} - \alpha_{05} \cdot \alpha_{21}; \tag{A.167}$$

$$\xi_{43} = \alpha_{04} \cdot \alpha_{11} - \alpha_{05} \cdot \alpha_{10}; \quad \xi_{44} = \alpha_{04} \cdot \alpha_{17} - \alpha_{05} \cdot \alpha_{16}; \quad \xi_{45} = \alpha_{04} \cdot \alpha_{23} - \alpha_{05} \cdot \alpha_{22}; \tag{A.168}$$

$$\xi_{46} = \alpha_{06} \cdot \alpha_{13} - \alpha_{07} \cdot \alpha_{12}; \quad \xi_{47} = \alpha_{06} \cdot \alpha_{14} - \alpha_{08} \cdot \alpha_{12}; \quad \xi_{48} = \alpha_{06} \cdot \alpha_{15} - \alpha_{09} \cdot \alpha_{12}; \tag{A.169}$$

$$\xi_{49} = \alpha_{06} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{12}; \quad \xi_{50} = \alpha_{06} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{12}; \quad \xi_{51} = \alpha_{06} \cdot \alpha_{19} - \alpha_{07} \cdot \alpha_{18}; \tag{A.170}$$

$$\xi_{52} = \alpha_{06} \cdot \alpha_{20} - \alpha_{08} \cdot \alpha_{18}; \quad \xi_{53} = \alpha_{06} \cdot \alpha_{21} - \alpha_{09} \cdot \alpha_{18}; \quad \xi_{54} = \alpha_{06} \cdot \alpha_{22} - \alpha_{10} \cdot \alpha_{18}; \tag{A.171}$$

$$\xi_{55} = \alpha_{06} \cdot \alpha_{23} - \alpha_{11} \cdot \alpha_{18}; \quad \xi_{56} = \alpha_{07} \cdot \alpha_{14} - \alpha_{08} \cdot \alpha_{13}; \quad \xi_{57} = \alpha_{07} \cdot \alpha_{15} - \alpha_{09} \cdot \alpha_{13}; \tag{A.172}$$

$$\xi_{58} = \alpha_{07} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{13}; \quad \xi_{59} = \alpha_{07} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{13}; \quad \xi_{60} = \alpha_{07} \cdot \alpha_{20} - \alpha_{08} \cdot \alpha_{19}; \tag{A.173}$$

$$\xi_{61} = \alpha_{07} \cdot \alpha_{21} - \alpha_{09} \cdot \alpha_{19}; \quad \xi_{62} = \alpha_{07} \cdot \alpha_{22} - \alpha_{10} \cdot \alpha_{19}; \quad \xi_{63} = \alpha_{07} \cdot \alpha_{23} - \alpha_{11} \cdot \alpha_{19}; \tag{A.174}$$

$$\xi_{64} = \alpha_{08} \cdot \alpha_{15} - \alpha_{09} \cdot \alpha_{14}; \quad \xi_{65} = \alpha_{08} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{14}; \quad \xi_{66} = \alpha_{08} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{14}; \tag{A.175}$$

$$\xi_{67} = \alpha_{08} \cdot \alpha_{21} - \alpha_{09} \cdot \alpha_{20}; \quad \xi_{68} = \alpha_{08} \cdot \alpha_{22} - \alpha_{10} \cdot \alpha_{20}; \quad \xi_{69} = \alpha_{08} \cdot \alpha_{23} - \alpha_{11} \cdot \alpha_{20}; \tag{A.176}$$

$$\xi_{70} = \alpha_{09} \cdot \alpha_{16} - \alpha_{10} \cdot \alpha_{15}; \quad \xi_{71} = \alpha_{09} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{15}; \quad \xi_{72} = \alpha_{09} \cdot \alpha_{22} - \alpha_{10} \cdot \alpha_{21}; \tag{A.177}$$

$$\xi_{73} = \alpha_{09} \cdot \alpha_{23} - \alpha_{11} \cdot \alpha_{21}; \quad \xi_{74} = \alpha_{10} \cdot \alpha_{17} - \alpha_{11} \cdot \alpha_{16}; \quad \xi_{75} = \alpha_{10} \cdot \alpha_{23} - \alpha_{11} \cdot \alpha_{22}; \tag{A.178}$$

$$\xi_{76} = \alpha_{12} \cdot \alpha_{19} - \alpha_{13} \cdot \alpha_{18}; \quad \xi_{77} = \alpha_{12} \cdot \alpha_{20} - \alpha_{14} \cdot \alpha_{18}; \quad \xi_{78} = \alpha_{12} \cdot \alpha_{21} - \alpha_{15} \cdot \alpha_{18}; \tag{A.179}$$

$$\xi_{79} = \alpha_{12} \cdot \alpha_{22} - \alpha_{16} \cdot \alpha_{18}; \quad \xi_{80} = \alpha_{12} \cdot \alpha_{23} - \alpha_{17} \cdot \alpha_{18}; \quad \xi_{81} = \alpha_{13} \cdot \alpha_{20} - \alpha_{14} \cdot \alpha_{19}; \tag{A.180}$$

$$\xi_{82} = \alpha_{13} \cdot \alpha_{21} - \alpha_{15} \cdot \alpha_{19}; \quad \xi_{83} = \alpha_{13} \cdot \alpha_{22} - \alpha_{16} \cdot \alpha_{19}; \quad \xi_{84} = \alpha_{13} \cdot \alpha_{23} - \alpha_{17} \cdot \alpha_{19}; \tag{A.181}$$

$$\xi_{85} = \alpha_{14} \cdot \alpha_{21} - \alpha_{15} \cdot \alpha_{20}; \quad \xi_{86} = \alpha_{14} \cdot \alpha_{22} - \alpha_{16} \cdot \alpha_{20}; \quad \xi_{87} = \alpha_{14} \cdot \alpha_{23} - \alpha_{17} \cdot \alpha_{20}; \tag{A.182}$$

$$\xi_{88} = \alpha_{15} \cdot \alpha_{22} - \alpha_{16} \cdot \alpha_{21}; \quad \xi_{89} = \alpha_{15} \cdot \alpha_{23} - \alpha_{17} \cdot \alpha_{21}; \quad \xi_{90} = \alpha_{16} \cdot \alpha_{23} - \alpha_{17} \cdot \alpha_{22}; \tag{A.183}$$

A.3.6 Espaço $4 \otimes 7$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{08} - \alpha_{01} \cdot \alpha_{07}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{09} - \alpha_{02} \cdot \alpha_{07}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{07}; \tag{A.184}$$

$$\xi_{4} = \alpha_{00} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{07}; \quad \xi_{5} = \alpha_{00} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{07}; \quad \xi_{6} = \alpha_{00} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{07}; \tag{A.185}$$

$$\xi_{7} = \alpha_{00} \cdot \alpha_{15} - \alpha_{01} \cdot \alpha_{14}; \quad \xi_{8} = \alpha_{00} \cdot \alpha_{16} - \alpha_{02} \cdot \alpha_{14}; \quad \xi_{9} = \alpha_{00} \cdot \alpha_{17} - \alpha_{03} \cdot \alpha_{14}; \tag{A.186}$$

$$\xi_{10} = \alpha_{00} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{14}; \quad \xi_{11} = \alpha_{00} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{14}; \quad \xi_{12} = \alpha_{00} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{14}; \tag{A.187}$$

$$\xi_{13} = \alpha_{00} \cdot \alpha_{22} - \alpha_{01} \cdot \alpha_{21}; \quad \xi_{14} = \alpha_{00} \cdot \alpha_{23} - \alpha_{02} \cdot \alpha_{21}; \quad \xi_{15} = \alpha_{00} \cdot \alpha_{24} - \alpha_{03} \cdot \alpha_{21}; \tag{A.188}$$

$$\xi_{16} = \alpha_{00} \cdot \alpha_{25} - \alpha_{04} \cdot \alpha_{21}; \quad \xi_{17} = \alpha_{00} \cdot \alpha_{26} - \alpha_{05} \cdot \alpha_{21}; \quad \xi_{18} = \alpha_{00} \cdot \alpha_{27} - \alpha_{06} \cdot \alpha_{21}; \tag{A.189}$$

$$\xi_{19} = \alpha_{01} \cdot \alpha_{09} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_{20} = \alpha_{01} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{08}; \quad \xi_{21} = \alpha_{01} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{08}; \tag{A.190}$$

$$\xi_{22} = \alpha_{01} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_{23} = \alpha_{01} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{08}; \quad \xi_{24} = \alpha_{01} \cdot \alpha_{16} - \alpha_{02} \cdot \alpha_{15}; \tag{A.191}$$

$$\xi_{25} = \alpha_{01} \cdot \alpha_{17} - \alpha_{03} \cdot \alpha_{15}; \quad \xi_{26} = \alpha_{01} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{15}; \quad \xi_{27} = \alpha_{01} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{15}; \tag{A.192}$$

$$\xi_{28} = \alpha_{01} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{15}; \quad \xi_{29} = \alpha_{01} \cdot \alpha_{23} - \alpha_{02} \cdot \alpha_{22}; \quad \xi_{30} = \alpha_{01} \cdot \alpha_{24} - \alpha_{03} \cdot \alpha_{22}; \tag{A.193}$$

$$\xi_{31} = \alpha_{01} \cdot \alpha_{25} - \alpha_{04} \cdot \alpha_{22}; \quad \xi_{32} = \alpha_{01} \cdot \alpha_{26} - \alpha_{05} \cdot \alpha_{22}; \quad \xi_{33} = \alpha_{01} \cdot \alpha_{27} - \alpha_{06} \cdot \alpha_{22}; \tag{A.194}$$

$$\xi_{34} = \alpha_{02} \cdot \alpha_{10} - \alpha_{03} \cdot \alpha_{09}; \quad \xi_{35} = \alpha_{02} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{09}; \quad \xi_{36} = \alpha_{02} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{09}; \tag{A.195}$$

$$\xi_{37} = \alpha_{02} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{09}; \quad \xi_{38} = \alpha_{02} \cdot \alpha_{17} - \alpha_{03} \cdot \alpha_{16}; \quad \xi_{39} = \alpha_{02} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{16}; \tag{A.196}$$

$$\xi_{40} = \alpha_{02} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{16}; \quad \xi_{41} = \alpha_{02} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{16}; \quad \xi_{42} = \alpha_{02} \cdot \alpha_{24} - \alpha_{03} \cdot \alpha_{23}; \tag{A.197}$$

$$\xi_{43} = \alpha_{02} \cdot \alpha_{25} - \alpha_{04} \cdot \alpha_{23}; \quad \xi_{44} = \alpha_{02} \cdot \alpha_{26} - \alpha_{05} \cdot \alpha_{23}; \quad \xi_{45} = \alpha_{02} \cdot \alpha_{27} - \alpha_{06} \cdot \alpha_{23}; \tag{A.198}$$

$$\xi_{46} = \alpha_{03} \cdot \alpha_{11} - \alpha_{04} \cdot \alpha_{10}; \quad \xi_{47} = \alpha_{03} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{10}; \quad \xi_{48} = \alpha_{03} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{10}; \tag{A.199}$$

$$\xi_{49} = \alpha_{03} \cdot \alpha_{18} - \alpha_{04} \cdot \alpha_{17}; \quad \xi_{50} = \alpha_{03} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{17}; \quad \xi_{51} = \alpha_{03} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{17}; \tag{A.200}$$

$$\xi_{52} = \alpha_{03} \cdot \alpha_{25} - \alpha_{04} \cdot \alpha_{24}; \quad \xi_{53} = \alpha_{03} \cdot \alpha_{26} - \alpha_{05} \cdot \alpha_{24}; \quad \xi_{54} = \alpha_{03} \cdot \alpha_{27} - \alpha_{06} \cdot \alpha_{24}; \tag{A.201}$$

$$\xi_{55} = \alpha_{04} \cdot \alpha_{12} - \alpha_{05} \cdot \alpha_{11}; \quad \xi_{56} = \alpha_{04} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{11}; \quad \xi_{57} = \alpha_{04} \cdot \alpha_{19} - \alpha_{05} \cdot \alpha_{18}; \tag{A.202}$$

$$\xi_{58} = \alpha_{04} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{18}; \quad \xi_{59} = \alpha_{04} \cdot \alpha_{26} - \alpha_{05} \cdot \alpha_{25}; \quad \xi_{60} = \alpha_{04} \cdot \alpha_{27} - \alpha_{06} \cdot \alpha_{25}; \tag{A.203}$$

$$\xi_{61} = \alpha_{05} \cdot \alpha_{13} - \alpha_{06} \cdot \alpha_{12}; \quad \xi_{62} = \alpha_{05} \cdot \alpha_{20} - \alpha_{06} \cdot \alpha_{19}; \quad \xi_{63} = \alpha_{05} \cdot \alpha_{27} - \alpha_{06} \cdot \alpha_{26}; \tag{A.204}$$

$$\xi_{64} = \alpha_{07} \cdot \alpha_{15} - \alpha_{08} \cdot \alpha_{14}; \quad \xi_{65} = \alpha_{07} \cdot \alpha_{16} - \alpha_{09} \cdot \alpha_{14}; \quad \xi_{66} = \alpha_{07} \cdot \alpha_{17} - \alpha_{10} \cdot \alpha_{14}; \tag{A.205}$$

$$\xi_{67} = \alpha_{07} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{14}; \quad \xi_{68} = \alpha_{07} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{14}; \quad \xi_{69} = \alpha_{07} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{14}; \tag{A.206}$$

$$\xi_{70} = \alpha_{07} \cdot \alpha_{22} - \alpha_{08} \cdot \alpha_{21}; \quad \xi_{71} = \alpha_{07} \cdot \alpha_{23} - \alpha_{09} \cdot \alpha_{21}; \quad \xi_{72} = \alpha_{07} \cdot \alpha_{24} - \alpha_{10} \cdot \alpha_{21}; \tag{A.207}$$

$$\xi_{73} = \alpha_{07} \cdot \alpha_{25} - \alpha_{11} \cdot \alpha_{21}; \quad \xi_{74} = \alpha_{07} \cdot \alpha_{26} - \alpha_{12} \cdot \alpha_{21}; \quad \xi_{75} = \alpha_{07} \cdot \alpha_{27} - \alpha_{13} \cdot \alpha_{21}; \tag{A.208}$$

$$\xi_{76} = \alpha_{08} \cdot \alpha_{16} - \alpha_{09} \cdot \alpha_{15}; \quad \xi_{77} = \alpha_{08} \cdot \alpha_{17} - \alpha_{10} \cdot \alpha_{15}; \quad \xi_{78} = \alpha_{08} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{15}; \tag{A.209}$$

$$\xi_{79} = \alpha_{08} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{15}; \quad \xi_{80} = \alpha_{08} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{15}; \quad \xi_{81} = \alpha_{08} \cdot \alpha_{23} - \alpha_{09} \cdot \alpha_{22}; \tag{A.210}$$

$$\xi_{82} = \alpha_{08} \cdot \alpha_{24} - \alpha_{10} \cdot \alpha_{22}; \quad \xi_{83} = \alpha_{08} \cdot \alpha_{25} - \alpha_{11} \cdot \alpha_{22}; \quad \xi_{84} = \alpha_{08} \cdot \alpha_{26} - \alpha_{12} \cdot \alpha_{22}; \tag{A.211}$$

$$\xi_{85} = \alpha_{08} \cdot \alpha_{27} - \alpha_{13} \cdot \alpha_{22}; \quad \xi_{86} = \alpha_{09} \cdot \alpha_{17} - \alpha_{10} \cdot \alpha_{16}; \quad \xi_{87} = \alpha_{09} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{16}; \tag{A.212}$$

$$\xi_{88} = \alpha_{09} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{16}; \quad \xi_{89} = \alpha_{09} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{16}; \quad \xi_{90} = \alpha_{09} \cdot \alpha_{24} - \alpha_{10} \cdot \alpha_{23}; \tag{A.213}$$

$$\xi_{91} = \alpha_{09} \cdot \alpha_{25} - \alpha_{11} \cdot \alpha_{23}; \quad \xi_{92} = \alpha_{09} \cdot \alpha_{26} - \alpha_{12} \cdot \alpha_{23}; \quad \xi_{93} = \alpha_{09} \cdot \alpha_{27} - \alpha_{13} \cdot \alpha_{23}; \tag{A.214}$$

$$\xi_{94} = \alpha_{10} \cdot \alpha_{18} - \alpha_{11} \cdot \alpha_{17}; \quad \xi_{95} = \alpha_{10} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{17}; \quad \xi_{96} = \alpha_{10} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{17}; \tag{A.215}$$

$$\xi_{97} = \alpha_{10} \cdot \alpha_{25} - \alpha_{11} \cdot \alpha_{24}; \quad \xi_{98} = \alpha_{10} \cdot \alpha_{26} - \alpha_{12} \cdot \alpha_{24}; \quad \xi_{99} = \alpha_{10} \cdot \alpha_{27} - \alpha_{13} \cdot \alpha_{24}; \tag{A.216}$$

$$\xi_{100} = \alpha_{11} \cdot \alpha_{19} - \alpha_{12} \cdot \alpha_{18}; \quad \xi_{101} = \alpha_{11} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{18}; \quad \xi_{102} = \alpha_{11} \cdot \alpha_{26} - \alpha_{12} \cdot \alpha_{25}; \tag{A.217}$$

$$\xi_{103} = \alpha_{11} \cdot \alpha_{27} - \alpha_{13} \cdot \alpha_{25}; \quad \xi_{104} = \alpha_{12} \cdot \alpha_{20} - \alpha_{13} \cdot \alpha_{19}; \quad \xi_{105} = \alpha_{12} \cdot \alpha_{27} - \alpha_{13} \cdot \alpha_{26}; \tag{A.218}$$

$$\xi_{106} = \alpha_{14} \cdot \alpha_{22} - \alpha_{15} \cdot \alpha_{21}; \quad \xi_{107} = \alpha_{14} \cdot \alpha_{23} - \alpha_{16} \cdot \alpha_{21}; \quad \xi_{108} = \alpha_{14} \cdot \alpha_{24} - \alpha_{17} \cdot \alpha_{21}; \tag{A.219}$$

$$\xi_{109} = \alpha_{14} \cdot \alpha_{25} - \alpha_{18} \cdot \alpha_{21}; \quad \xi_{110} = \alpha_{14} \cdot \alpha_{26} - \alpha_{19} \cdot \alpha_{21}; \quad \xi_{111} = \alpha_{14} \cdot \alpha_{27} - \alpha_{20} \cdot \alpha_{21}; \tag{A.220}$$

$$\xi_{112} = \alpha_{15} \cdot \alpha_{23} - \alpha_{16} \cdot \alpha_{22}; \quad \xi_{113} = \alpha_{15} \cdot \alpha_{24} - \alpha_{17} \cdot \alpha_{22}; \quad \xi_{114} = \alpha_{15} \cdot \alpha_{25} - \alpha_{18} \cdot \alpha_{22}; \tag{A.221}$$

$$\xi_{115} = \alpha_{15} \cdot \alpha_{26} - \alpha_{19} \cdot \alpha_{22}; \quad \xi_{116} = \alpha_{15} \cdot \alpha_{27} - \alpha_{20} \cdot \alpha_{22}; \quad \xi_{117} = \alpha_{16} \cdot \alpha_{24} - \alpha_{17} \cdot \alpha_{23}; \tag{A.222}$$

$$\xi_{118} = \alpha_{16} \cdot \alpha_{25} - \alpha_{18} \cdot \alpha_{23}; \quad \xi_{119} = \alpha_{16} \cdot \alpha_{26} - \alpha_{19} \cdot \alpha_{23}; \quad \xi_{120} = \alpha_{16} \cdot \alpha_{27} - \alpha_{20} \cdot \alpha_{23}; \tag{A.223}$$

$$\xi_{121} = \alpha_{17} \cdot \alpha_{25} - \alpha_{18} \cdot \alpha_{24}; \quad \xi_{122} = \alpha_{17} \cdot \alpha_{26} - \alpha_{19} \cdot \alpha_{24}; \quad \xi_{123} = \alpha_{17} \cdot \alpha_{27} - \alpha_{20} \cdot \alpha_{24}; \tag{A.224}$$

$$\xi_{124} = \alpha_{18} \cdot \alpha_{26} - \alpha_{19} \cdot \alpha_{25}; \quad \xi_{125} = \alpha_{18} \cdot \alpha_{27} - \alpha_{20} \cdot \alpha_{25}; \quad \xi_{126} = \alpha_{19} \cdot \alpha_{27} - \alpha_{20} \cdot \alpha_{26}; \tag{A.225}$$

A.3.7 Espaço $4 \otimes 8$

$$\xi_{1} = \alpha_{00} \cdot \alpha_{09} - \alpha_{01} \cdot \alpha_{08}; \quad \xi_{2} = \alpha_{00} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{08}; \quad \xi_{3} = \alpha_{00} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{08}; \tag{A.226}$$

$$\xi_{4} = \alpha_{00} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{08}; \quad \xi_{5} = \alpha_{00} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{08}; \quad \xi_{6} = \alpha_{00} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{08}; \tag{A.227}$$

$$\xi_{7} = \alpha_{00} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{08}; \quad \xi_{8} = \alpha_{00} \cdot \alpha_{17} - \alpha_{01} \cdot \alpha_{16}; \quad \xi_{9} = \alpha_{00} \cdot \alpha_{18} - \alpha_{02} \cdot \alpha_{16}; \tag{A.228}$$

$$\xi_{10} = \alpha_{00} \cdot \alpha_{19} - \alpha_{03} \cdot \alpha_{16}; \quad \xi_{11} = \alpha_{00} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{16}; \quad \xi_{12} = \alpha_{00} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{16}; \tag{A.229}$$

$$\xi_{13} = \alpha_{00} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{16}; \quad \xi_{14} = \alpha_{00} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{16}; \quad \xi_{15} = \alpha_{00} \cdot \alpha_{25} - \alpha_{01} \cdot \alpha_{24}; \tag{A.230}$$

$$\xi_{16} = \alpha_{00} \cdot \alpha_{26} - \alpha_{02} \cdot \alpha_{24}; \quad \xi_{17} = \alpha_{00} \cdot \alpha_{27} - \alpha_{03} \cdot \alpha_{24}; \quad \xi_{18} = \alpha_{00} \cdot \alpha_{28} - \alpha_{04} \cdot \alpha_{24}; \tag{A.231}$$

$$\xi_{19} = \alpha_{00} \cdot \alpha_{29} - \alpha_{05} \cdot \alpha_{24}; \quad \xi_{20} = \alpha_{00} \cdot \alpha_{30} - \alpha_{06} \cdot \alpha_{24}; \quad \xi_{21} = \alpha_{00} \cdot \alpha_{31} - \alpha_{07} \cdot \alpha_{24}; \tag{A.232}$$

$$\xi_{22} = \alpha_{01} \cdot \alpha_{10} - \alpha_{02} \cdot \alpha_{09}; \quad \xi_{23} = \alpha_{01} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{09}; \quad \xi_{24} = \alpha_{01} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{09}; \tag{A.233}$$

$$\xi_{25} = \alpha_{01} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{09}; \quad \xi_{26} = \alpha_{01} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{09}; \quad \xi_{27} = \alpha_{01} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{09}; \tag{A.234}$$

$$\xi_{28} = \alpha_{01} \cdot \alpha_{18} - \alpha_{02} \cdot \alpha_{17}; \quad \xi_{29} = \alpha_{01} \cdot \alpha_{19} - \alpha_{03} \cdot \alpha_{17}; \quad \xi_{30} = \alpha_{01} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{17}; \tag{A.235}$$

$$\xi_{31} = \alpha_{01} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{17}; \quad \xi_{32} = \alpha_{01} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{17}; \quad \xi_{33} = \alpha_{01} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{17}; \tag{A.236}$$

$$\xi_{34} = \alpha_{01} \cdot \alpha_{26} - \alpha_{02} \cdot \alpha_{25}; \quad \xi_{35} = \alpha_{01} \cdot \alpha_{27} - \alpha_{03} \cdot \alpha_{25}; \quad \xi_{36} = \alpha_{01} \cdot \alpha_{28} - \alpha_{04} \cdot \alpha_{25}; \tag{A.237}$$

$$\xi_{37} = \alpha_{01} \cdot \alpha_{29} - \alpha_{05} \cdot \alpha_{25}; \quad \xi_{38} = \alpha_{01} \cdot \alpha_{30} - \alpha_{06} \cdot \alpha_{25}; \quad \xi_{39} = \alpha_{01} \cdot \alpha_{31} - \alpha_{07} \cdot \alpha_{25}; \tag{A.238}$$

$$\xi_{40} = \alpha_{02} \cdot \alpha_{11} - \alpha_{03} \cdot \alpha_{10}; \quad \xi_{41} = \alpha_{02} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{10}; \quad \xi_{42} = \alpha_{02} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{10}; \tag{A.239}$$

$$\xi_{43} = \alpha_{02} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{10}; \quad \xi_{44} = \alpha_{02} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{10}; \quad \xi_{45} = \alpha_{02} \cdot \alpha_{19} - \alpha_{03} \cdot \alpha_{18}; \tag{A.240}$$

$$\xi_{46} = \alpha_{02} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{18}; \quad \xi_{47} = \alpha_{02} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{18}; \quad \xi_{48} = \alpha_{02} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{18}; \tag{A.241}$$

$$\xi_{49} = \alpha_{02} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{18}; \quad \xi_{50} = \alpha_{02} \cdot \alpha_{27} - \alpha_{03} \cdot \alpha_{26}; \quad \xi_{51} = \alpha_{02} \cdot \alpha_{28} - \alpha_{04} \cdot \alpha_{26}; \tag{A.242}$$

$$\xi_{52} = \alpha_{02} \cdot \alpha_{29} - \alpha_{05} \cdot \alpha_{26}; \quad \xi_{53} = \alpha_{02} \cdot \alpha_{30} - \alpha_{06} \cdot \alpha_{26}; \quad \xi_{54} = \alpha_{02} \cdot \alpha_{31} - \alpha_{07} \cdot \alpha_{26}; \tag{A.243}$$

$$\xi_{55} = \alpha_{03} \cdot \alpha_{12} - \alpha_{04} \cdot \alpha_{11}; \quad \xi_{56} = \alpha_{03} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{11}; \quad \xi_{57} = \alpha_{03} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{11}; \tag{A.244}$$

$$\xi_{58} = \alpha_{03} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{11}; \quad \xi_{59} = \alpha_{03} \cdot \alpha_{20} - \alpha_{04} \cdot \alpha_{19}; \quad \xi_{60} = \alpha_{03} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{19}; \tag{A.245}$$

$$\xi_{61} = \alpha_{03} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{19}; \quad \xi_{62} = \alpha_{03} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{19}; \quad \xi_{63} = \alpha_{03} \cdot \alpha_{28} - \alpha_{04} \cdot \alpha_{27}; \tag{A.246}$$

$$\xi_{64} = \alpha_{03} \cdot \alpha_{29} - \alpha_{05} \cdot \alpha_{27}; \quad \xi_{65} = \alpha_{03} \cdot \alpha_{30} - \alpha_{06} \cdot \alpha_{27}; \quad \xi_{66} = \alpha_{03} \cdot \alpha_{31} - \alpha_{07} \cdot \alpha_{27}; \tag{A.247}$$

$$\xi_{67} = \alpha_{04} \cdot \alpha_{13} - \alpha_{05} \cdot \alpha_{12}; \quad \xi_{68} = \alpha_{04} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{12}; \quad \xi_{69} = \alpha_{04} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{12}; \tag{A.248}$$

$$\xi_{70} = \alpha_{04} \cdot \alpha_{21} - \alpha_{05} \cdot \alpha_{20}; \quad \xi_{71} = \alpha_{04} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{20}; \quad \xi_{72} = \alpha_{04} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{20}; \tag{A.249}$$

$$\xi_{73} = \alpha_{04} \cdot \alpha_{29} - \alpha_{05} \cdot \alpha_{28}; \quad \xi_{74} = \alpha_{04} \cdot \alpha_{30} - \alpha_{06} \cdot \alpha_{28}; \quad \xi_{75} = \alpha_{04} \cdot \alpha_{31} - \alpha_{07} \cdot \alpha_{28}; \tag{A.250}$$

$$\xi_{76} = \alpha_{05} \cdot \alpha_{14} - \alpha_{06} \cdot \alpha_{13}; \quad \xi_{77} = \alpha_{05} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{13}; \quad \xi_{78} = \alpha_{05} \cdot \alpha_{22} - \alpha_{06} \cdot \alpha_{21}; \tag{A.251}$$

$$\xi_{79} = \alpha_{05} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{21}; \quad \xi_{80} = \alpha_{05} \cdot \alpha_{30} - \alpha_{06} \cdot \alpha_{29}; \quad \xi_{81} = \alpha_{05} \cdot \alpha_{31} - \alpha_{07} \cdot \alpha_{29}; \tag{A.252}$$

$$\xi_{82} = \alpha_{06} \cdot \alpha_{15} - \alpha_{07} \cdot \alpha_{14}; \quad \xi_{83} = \alpha_{06} \cdot \alpha_{23} - \alpha_{07} \cdot \alpha_{22}; \quad \xi_{84} = \alpha_{06} \cdot \alpha_{31} - \alpha_{07} \cdot \alpha_{30}; \tag{A.253}$$

$$\xi_{85} = \alpha_{08} \cdot \alpha_{17} - \alpha_{09} \cdot \alpha_{16}; \quad \xi_{86} = \alpha_{08} \cdot \alpha_{18} - \alpha_{10} \cdot \alpha_{16}; \quad \xi_{87} = \alpha_{08} \cdot \alpha_{19} - \alpha_{11} \cdot \alpha_{16}; \tag{A.254}$$

$$\xi_{88} = \alpha_{08} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{16}; \quad \xi_{89} = \alpha_{08} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{16}; \quad \xi_{90} = \alpha_{08} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{16}; \tag{A.255}$$

$$\xi_{91} = \alpha_{08} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{16}; \quad \xi_{92} = \alpha_{08} \cdot \alpha_{25} - \alpha_{09} \cdot \alpha_{24}; \quad \xi_{93} = \alpha_{08} \cdot \alpha_{26} - \alpha_{10} \cdot \alpha_{24}; \tag{A.256}$$

$$\xi_{94} = \alpha_{08} \cdot \alpha_{27} - \alpha_{11} \cdot \alpha_{24}; \quad \xi_{95} = \alpha_{08} \cdot \alpha_{28} - \alpha_{12} \cdot \alpha_{24}; \quad \xi_{96} = \alpha_{08} \cdot \alpha_{29} - \alpha_{13} \cdot \alpha_{24}; \tag{A.257}$$

$$\xi_{97} = \alpha_{08} \cdot \alpha_{30} - \alpha_{14} \cdot \alpha_{24}; \quad \xi_{98} = \alpha_{08} \cdot \alpha_{31} - \alpha_{15} \cdot \alpha_{24}; \quad \xi_{99} = \alpha_{09} \cdot \alpha_{18} - \alpha_{10} \cdot \alpha_{17}; \tag{A.258}$$

$$\xi_{100} = \alpha_{09} \cdot \alpha_{19} - \alpha_{11} \cdot \alpha_{17}; \quad \xi_{101} = \alpha_{09} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{17}; \quad \xi_{102} = \alpha_{09} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{17}; \tag{A.259}$$

$$\xi_{103} = \alpha_{09} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{17}; \quad \xi_{104} = \alpha_{09} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{17}; \quad \xi_{105} = \alpha_{09} \cdot \alpha_{26} - \alpha_{10} \cdot \alpha_{25}; \tag{A.260}$$

$$\xi_{106} = \alpha_{09} \cdot \alpha_{27} - \alpha_{11} \cdot \alpha_{25}; \quad \xi_{107} = \alpha_{09} \cdot \alpha_{28} - \alpha_{12} \cdot \alpha_{25}; \quad \xi_{108} = \alpha_{09} \cdot \alpha_{29} - \alpha_{13} \cdot \alpha_{25}; \tag{A.261}$$

$$\xi_{109} = \alpha_{09} \cdot \alpha_{30} - \alpha_{14} \cdot \alpha_{25}; \quad \xi_{110} = \alpha_{09} \cdot \alpha_{31} - \alpha_{15} \cdot \alpha_{25}; \quad \xi_{111} = \alpha_{10} \cdot \alpha_{19} - \alpha_{11} \cdot \alpha_{18}; \tag{A.262}$$

$$\xi_{112} = \alpha_{10} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{18}; \quad \xi_{113} = \alpha_{10} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{18}; \quad \xi_{114} = \alpha_{10} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{18}; \tag{A.263}$$

$$\xi_{115} = \alpha_{10} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{18}; \quad \xi_{116} = \alpha_{10} \cdot \alpha_{27} - \alpha_{11} \cdot \alpha_{26}; \quad \xi_{117} = \alpha_{10} \cdot \alpha_{28} - \alpha_{12} \cdot \alpha_{26}; \tag{A.264}$$

$$\xi_{118} = \alpha_{10} \cdot \alpha_{29} - \alpha_{13} \cdot \alpha_{26}; \quad \xi_{119} = \alpha_{10} \cdot \alpha_{30} - \alpha_{14} \cdot \alpha_{26}; \quad \xi_{120} = \alpha_{10} \cdot \alpha_{31} - \alpha_{15} \cdot \alpha_{26}; \tag{A.265}$$

$$\xi_{121} = \alpha_{11} \cdot \alpha_{20} - \alpha_{12} \cdot \alpha_{19}; \quad \xi_{122} = \alpha_{11} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{19}; \quad \xi_{123} = \alpha_{11} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{19}; \tag{A.266}$$

$$\xi_{124} = \alpha_{11} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{19}; \quad \xi_{125} = \alpha_{11} \cdot \alpha_{28} - \alpha_{12} \cdot \alpha_{27}; \quad \xi_{126} = \alpha_{11} \cdot \alpha_{29} - \alpha_{13} \cdot \alpha_{27}; \tag{A.267}$$

$$\xi_{127} = \alpha_{11} \cdot \alpha_{30} - \alpha_{14} \cdot \alpha_{27}; \quad \xi_{128} = \alpha_{11} \cdot \alpha_{31} - \alpha_{15} \cdot \alpha_{27}; \quad \xi_{129} = \alpha_{12} \cdot \alpha_{21} - \alpha_{13} \cdot \alpha_{20}; \tag{A.268}$$

$$\xi_{130} = \alpha_{12} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{20}; \quad \xi_{131} = \alpha_{12} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{20}; \quad \xi_{132} = \alpha_{12} \cdot \alpha_{29} - \alpha_{13} \cdot \alpha_{28}; \tag{A.269}$$

$$\xi_{133} = \alpha_{12} \cdot \alpha_{30} - \alpha_{14} \cdot \alpha_{28}; \quad \xi_{134} = \alpha_{12} \cdot \alpha_{31} - \alpha_{15} \cdot \alpha_{28}; \quad \xi_{135} = \alpha_{13} \cdot \alpha_{22} - \alpha_{14} \cdot \alpha_{21}; \tag{A.270}$$

$$\xi_{136} = \alpha_{13} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{21}; \quad \xi_{137} = \alpha_{13} \cdot \alpha_{30} - \alpha_{14} \cdot \alpha_{29}; \quad \xi_{138} = \alpha_{13} \cdot \alpha_{31} - \alpha_{15} \cdot \alpha_{29}; \tag{A.271}$$

$$\xi_{139} = \alpha_{14} \cdot \alpha_{23} - \alpha_{15} \cdot \alpha_{22}; \quad \xi_{140} = \alpha_{14} \cdot \alpha_{31} - \alpha_{15} \cdot \alpha_{30}; \quad \xi_{141} = \alpha_{16} \cdot \alpha_{25} - \alpha_{17} \cdot \alpha_{24}; \tag{A.272}$$

$$\xi_{142} = \alpha_{16} \cdot \alpha_{26} - \alpha_{18} \cdot \alpha_{24}; \quad \xi_{143} = \alpha_{16} \cdot \alpha_{27} - \alpha_{19} \cdot \alpha_{24}; \quad \xi_{144} = \alpha_{16} \cdot \alpha_{28} - \alpha_{20} \cdot \alpha_{24}; \tag{A.273}$$

$$\xi_{145} = \alpha_{16} \cdot \alpha_{29} - \alpha_{21} \cdot \alpha_{24}; \quad \xi_{146} = \alpha_{16} \cdot \alpha_{30} - \alpha_{22} \cdot \alpha_{24}; \quad \xi_{147} = \alpha_{16} \cdot \alpha_{31} - \alpha_{23} \cdot \alpha_{24}; \tag{A.274}$$

$$\xi_{148} = \alpha_{17} \cdot \alpha_{26} - \alpha_{18} \cdot \alpha_{25}; \quad \xi_{149} = \alpha_{17} \cdot \alpha_{27} - \alpha_{19} \cdot \alpha_{25}; \quad \xi_{150} = \alpha_{17} \cdot \alpha_{28} - \alpha_{20} \cdot \alpha_{25}; \tag{A.275}$$

$$\xi_{151} = \alpha_{17} \cdot \alpha_{29} - \alpha_{21} \cdot \alpha_{25}; \quad \xi_{152} = \alpha_{17} \cdot \alpha_{30} - \alpha_{22} \cdot \alpha_{25}; \quad \xi_{153} = \alpha_{17} \cdot \alpha_{31} - \alpha_{23} \cdot \alpha_{25}; \tag{A.276}$$

$$\xi_{154} = \alpha_{18} \cdot \alpha_{27} - \alpha_{19} \cdot \alpha_{26}; \quad \xi_{155} = \alpha_{18} \cdot \alpha_{28} - \alpha_{20} \cdot \alpha_{26}; \quad \xi_{156} = \alpha_{18} \cdot \alpha_{29} - \alpha_{21} \cdot \alpha_{26}; \tag{A.277}$$

$$\xi_{157} = \alpha_{18} \cdot \alpha_{30} - \alpha_{22} \cdot \alpha_{26}; \quad \xi_{158} = \alpha_{18} \cdot \alpha_{31} - \alpha_{23} \cdot \alpha_{26}; \quad \xi_{159} = \alpha_{19} \cdot \alpha_{28} - \alpha_{20} \cdot \alpha_{27}; \tag{A.278}$$

$$\xi_{160} = \alpha_{19} \cdot \alpha_{29} - \alpha_{21} \cdot \alpha_{27}; \quad \xi_{161} = \alpha_{19} \cdot \alpha_{30} - \alpha_{22} \cdot \alpha_{27}; \quad \xi_{162} = \alpha_{19} \cdot \alpha_{31} - \alpha_{23} \cdot \alpha_{27}; \tag{A.279}$$

$$\xi_{163} = \alpha_{20} \cdot \alpha_{29} - \alpha_{21} \cdot \alpha_{28}; \quad \xi_{164} = \alpha_{20} \cdot \alpha_{30} - \alpha_{22} \cdot \alpha_{28}; \quad \xi_{165} = \alpha_{20} \cdot \alpha_{31} - \alpha_{23} \cdot \alpha_{28}; \tag{A.280}$$

$$\xi_{166} = \alpha_{21} \cdot \alpha_{30} - \alpha_{22} \cdot \alpha_{29}; \quad \xi_{167} = \alpha_{21} \cdot \alpha_{31} - \alpha_{23} \cdot \alpha_{29}; \quad \xi_{168} = \alpha_{22} \cdot \alpha_{31} - \alpha_{23} \cdot \alpha_{30}; \tag{A.281}$$

Anexos

Anexo I

Artigos e apresentações

Resumo

Neste anexo serão apresentados os artigos e apresentações decorrentes deste trabalho.

I.1 Artigos

1. **On the Role of the Basis of Measurement in Quantum Gate Teleportation**
   - ◇ Periódico: Quantum Information Processing
   - ◇ Data: 30/06/2014
   - ◇ Situação: Aceito

ON THE ROLE OF THE BASIS OF MEASUREMENT IN QUANTUM GATE TELEPORTATION

F. V. Mendes, R. V. Ramos

fernandovm@deti.ufc.br rubens@deti.ufc.br

Lab. of Quantum Information Technology, Department of Teleinformatic Engineering – Federal University of Ceara - DETI/UFC, C.P. 6007 – Campus do Pici - 60455-970 Fortaleza-Ce, Brazil.

Quantum teleportation is a powerful protocol with applications in several schemes of quantum communication, quantum cryptography and quantum computing. The present work shows the required conditions for a two-qubit quantum gate to be deterministically and probabilistically teleported by a quantum gate teleportation scheme using different bases of measurement. Additionally, we present examples of teleportation of two-qubit gates that do not belong to Clifford group as well the limitations of the quantum gate teleportation scheme employing a four-qubit state with genuine four-way entanglement. At last, we provide a general decomposition of Clifford operations.

Keywords: Quantum teleportation, Clifford group, separability of quantum gates.

1. Introduction

Since its proposal [1] quantum teleportation has played an increasing role in schemes of quantum communication, quantum cryptography and quantum computing [2-4]. In what concerns the teleportation of quantum gates (teleportation of the action of the quantum gate), a well known result is that gates belonging to Clifford group are deterministically teleported by a quantum teleportation scheme employing a pair of Bell states and Bell basis in the measurements, what results in error correction based on Pauli matrices [4,5]. This happens because Clifford group preserves Pauli group under conjugation. The quantum gate teleportation scheme proposed in [4] shows that quantum gates can be implemented using just previous entanglement and qubit teleportation. The crucial aspect of this important work is that it shows that a universal quantum computer can be built from entangled states, Bell measurements and single-qubit operations. In addition, it also shows how to build some gates in a fault-tolerant way. This scheme was experimentally demonstrated using linear optical [6,7] and, recently, in [8], using both high-fidelity six-photon interferometer and four-photon hyperentanglement.

Although some works have generalized the teleportation of quantum states [9], including the usage of generic bases in the measurement [10], to the best of our knowledge, this has not been done for quantum gate teleportation. In this direction, the present work discusses the role of the basis of measurement in a two-qubit quantum gate teleportation scheme, showing explicitly the conditions to be satisfied by the quantum gate and the basis of measurement in order to have deterministic teleportation. Additionally, we give examples of teleportation of quantum gates that do not belong to Clifford group. We also show the result of the teleportation of a two-qubit quantum gate when a four-qubit state with genuine four-way entanglement is used. At last, as a secondary result of our theorem about teleportability, we describe a general decomposition of Clifford ($U(4)$) gates.

The present work is outlined as follows: In Section 2 the role of the measurement basis on the teleportation of quantum states is discussed; in Section 3 the teleportation of quantum gates is reviewed; in Section 4 we describe the sufficient conditions for a two-qubit quantum gate to be teleported by a quantum teleportation scheme using a particular basis of measurement; Section 5 brings some examples of quantum gate teleportation with different basis, including examples of teleportation of quantum gates that do not belong to Clifford group; Section 6 discusses the quantum gate teleportation by a scheme employing a genuine four-way entangled state; Using the conditions required for successful teleportation, Section 7

describes a general decomposition of Clifford gates; at last, conclusions are drawn in Section 8.

2. Teleportation of Quantum States

The general circuit for teleportation of a single-qubit is shown in Fig. 1.

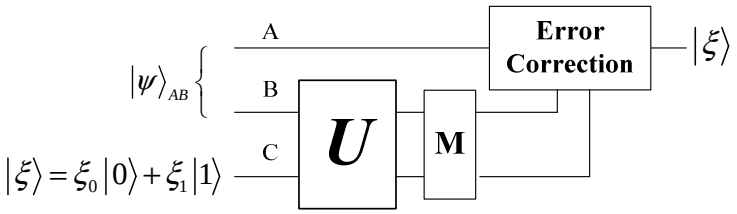


Fig. 1. General circuit for quantum teleportation of a single-qubit.

Basically, one qubit, let us say the second one, from the two-qubit state interacts with the single-qubit that will be teleported. After, measurements are realized and, according to the results obtained, a single-qubit error-correction is applied on the first qubit of the two-qubit state. If the teleportation is succeeded, that qubit will be exactly in the same quantum state that the input qubit was. The quantum state evolution expected for a useful teleportation, according to the circuit in Fig 1, is as follows:

$$(I \otimes U)|\psi\rangle_{AB}|\xi\rangle_C = \sum_{i=1}^{4} \sqrt{p_i} V_i |\xi\rangle_A |\beta_i\rangle_{BC}. \tag{1}$$

In order to have a successful teleportation the condition $\langle\beta_i|\beta_j\rangle=\delta_{ij}$ must be obeyed. Now, taking the inner product of $\langle\beta_j|$ with two last qubits of (1) one gets

$$\langle\beta_j|(I \otimes U)|\psi\rangle|\xi\rangle = \sum_{i=1}^{4} \sqrt{p_i} V_i |\xi\rangle \langle\beta_j|\beta_i\rangle = \sqrt{p_j} V_i |\xi\rangle. \tag{2}$$

Using $|\psi\rangle=\psi_{00}|00\rangle+\psi_{01}|01\rangle+\psi_{10}|10\rangle+\psi_{11}|11\rangle$ in (2) it results in

$$\langle\beta_j|(I \otimes U)(\psi_{00}|00\rangle|\xi\rangle + \psi_{01}|01\rangle|\xi\rangle + \psi_{10}|10\rangle|\xi\rangle + \psi_{11}|11\rangle|\xi\rangle) = \sqrt{p_j} V_j |\xi\rangle \tag{3}$$

$$\psi_{00}|0\rangle\langle\beta_j|U|0\xi\rangle + \psi_{01}|0\rangle\langle\beta_j|U|1\xi\rangle + \psi_{10}|1\rangle\langle\beta_j|U|0\xi\rangle + \psi_{11}|1\rangle\langle\beta_j|U|1\xi\rangle = \sqrt{p_j} V_j |\xi\rangle \tag{4}$$

$$\left(\psi_{00}\langle\beta_j|U|0\xi\rangle + \psi_{01}\langle\beta_j|U|1\xi\rangle\right)|0\rangle + \left(\psi_{10}\langle\beta_j|U|0\xi\rangle + \psi_{11}\langle\beta_j|U|1\xi\rangle\right)|1\rangle = \sqrt{p_j} V_j |\xi\rangle. \tag{5}$$

Substituting

$$|\xi\rangle = \xi_0|0\rangle + \xi_1|1\rangle \tag{6}$$

$$U|0\xi\rangle = \xi_0 U|00\rangle + \xi_1 U|01\rangle \tag{7}$$

$$U|1\xi\rangle = \xi_0 U|10\rangle + \xi_1 U|11\rangle \tag{8}$$

$$V_j = \begin{bmatrix} v_{11}^j & v_{12}^j \\ v_{21}^j & v_{22}^j \end{bmatrix} \tag{9}$$

in (5), one obtains

$$\left\{ \begin{bmatrix} \left(\psi_{00}\langle\beta_j|U|00\rangle + \psi_{01}\langle\beta_j|U|10\rangle\right)\xi_0 + \\ \left(\psi_{00}\langle\beta_j|U|01\rangle + \psi_{01}\langle\beta_j|U|11\rangle\right)\xi_1 \end{bmatrix} |0\rangle + \begin{bmatrix} \left(\psi_{10}\langle\beta_j|U|00\rangle + \psi_{11}\langle\beta_j|U|10\rangle\right)\xi_0 + \\ \left(\psi_{10}\langle\beta_j|U|01\rangle + \psi_{11}\langle\beta_j|U|11\rangle\right)\xi_1 \end{bmatrix} |1\rangle \right\} =$$

$$\left[\sqrt{p_j}\left(v_{11}^j\xi_0 + v_{12}^j\xi_1\right)|0\rangle + \sqrt{p_j}\left(v_{21}^j\xi_0 + v_{22}^j\xi_1\right)|1\rangle\right]. \tag{10}$$

Thus the V_j matrix can be directly obtained from (10):

$$V_j = \frac{1}{\sqrt{p_j}} \begin{bmatrix} \psi_{00}\langle\beta_j|U_{00}\rangle + \psi_{01}\langle\beta_j|U_{10}\rangle & \psi_{00}\langle\beta_j|U_{01}\rangle + \psi_{01}\langle\beta_j|U_{11}\rangle \\ \psi_{10}\langle\beta_j|U_{00}\rangle + \psi_{11}\langle\beta_j|U_{10}\rangle & \psi_{10}\langle\beta_j|U_{01}\rangle + \psi_{11}\langle\beta_j|U_{11}\rangle \end{bmatrix}, \tag{11}$$

where $U_{xy}=U|xy\rangle$ $x,y\in\{0,1\}$. Eq. (11) shows the relation between the two-qubit state used, the errors corrections required and the measurement basis used by Bob. It can be rewritten as

$$V_j = \frac{1}{\sqrt{p_j}}\psi\beta_U = \frac{1}{\sqrt{p_j}} \begin{bmatrix} \psi_{00} & \psi_{01} \\ \psi_{10} & \psi_{11} \end{bmatrix} \begin{bmatrix} \langle\beta_j|U_{00}\rangle & \langle\beta_j|U_{01}\rangle \\ \langle\beta_j|U_{10}\rangle & \langle\beta_j|U_{11}\rangle \end{bmatrix}. \tag{12}$$

It is well known that teleportation is possible only if there is entanglement. This can be directly seen from (12). Since V_j must belong to $U(2)$, one must have $|\det(V_j)|=1$. Hence $\det(\psi) = \psi_{00}\psi_{11}-\psi_{01}\psi_{10} \neq 0$. Note that $|\det(\psi)|^2$ is an entanglement measure (concurrence) for two-qubit pure states, hence the two-qubit state used cannot be disentangled. Now, let us consider the cases where the results obtained by Bob are equally probable, $p_j=1/4$, and the two-qubit state used is maximally entangled, $\psi_{00}=\psi_{11}=1/2^{1/2}$ and $\psi_{01}=\psi_{10}=0$. In this case Eq. (12) is simplified to

$$V_j = \sqrt{2} \begin{bmatrix} \langle\beta_j|U_{00}\rangle & \langle\beta_j|U_{01}\rangle \\ \langle\beta_j|U_{10}\rangle & \langle\beta_j|U_{11}\rangle \end{bmatrix}. \tag{13}$$

It can be easily checked that, for a given U, when the measurement basis is $\{(|U_{00}\rangle\pm|U_{11}\rangle)/2^{1/2}, (|U_{01}\rangle\pm|U_{10}\rangle)/2^{1/2}\}$ the V_j are the Pauli matrices. Note that a basis $\{|\beta_1\rangle,|\beta_2\rangle,|\beta_3\rangle,|\beta_4\rangle\}$ is useful for teleportation only if the matrices $V_1,..,V_4$ produced are unitary.

Now, as an example, let us consider $U=(H\otimes I)C_{\pi/8}$ (controlled-$\pi/8$) whose action in the canonical basis is given by

$$U_{x0} = U\left|x0\right\rangle = \left[\left|00\right\rangle + (-1)^x \left|10\right\rangle\right]\Big/\sqrt{2} \tag{14}$$

$$U_{x1} = U\left|x1\right\rangle = \left[\frac{(1+i)}{\sqrt{2}}\right]^x \left[\left|01\right\rangle + (-1)^x \left|11\right\rangle\right]\Big/\sqrt{2}. \tag{15}$$

Choosing $\{(|U_{00}\rangle \pm e^{i\pi/4}|U_{11}\rangle)/2^{1/2}, (|U_{01}\rangle \pm e^{i\pi/4}|U_{10}\rangle)/2^{1/2}\}$ as measurement basis, the error correction is realized by the single-qubit gates provided by Eq. (14): $V_1^\dagger = [\pi/8]Z$, $V_2^\dagger = [\pi/8]$, $V_3^\dagger = XSZ$, $V_4^\dagger = XS$, where

$$\pi/8 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix},\ S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{16}$$

3. Teleportation of quantum gates

The general scheme for teleportation of two-qubit quantum gate is shown in Fig. 2.

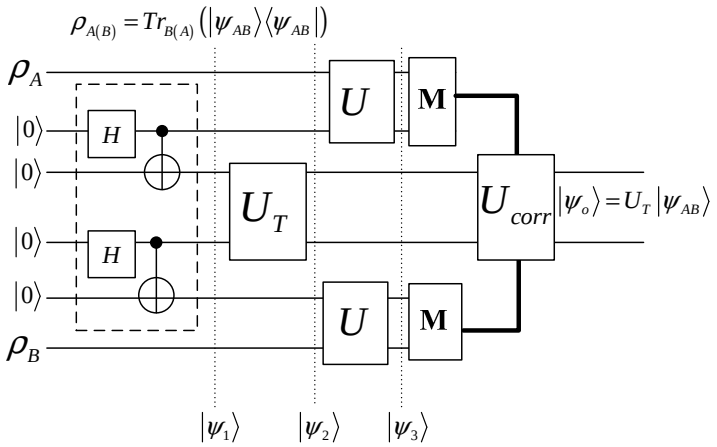


Fig. 2. General circuit for teleportation of the two-qubit quantum gate U_T.

As one may note comparing Figs. 1 and 2, quantum gate teleportation uses quantum state teleportation as a building block. Analyzing the quantum circuit in Fig. 2 for a successful teleportation, one has the following quantum state just before the measurements

$$\left|\psi_3\right\rangle = \frac{1}{2}\left[\begin{array}{l} \psi_{00}\begin{pmatrix} U\left|00\right\rangle U_T\left|00\right\rangle U\left|00\right\rangle + U\left|00\right\rangle U_T\left|01\right\rangle U\left|01\right\rangle \\ +U\left|01\right\rangle U_T\left|10\right\rangle U\left|00\right\rangle + U\left|01\right\rangle U_T\left|11\right\rangle U\left|01\right\rangle \end{pmatrix} + \psi_{01}\begin{pmatrix} U\left|00\right\rangle U_T\left|00\right\rangle U\left|10\right\rangle + U\left|00\right\rangle U_T\left|01\right\rangle U\left|11\right\rangle \\ +U\left|01\right\rangle U_T\left|10\right\rangle U\left|10\right\rangle + U\left|01\right\rangle U_T\left|11\right\rangle U\left|11\right\rangle \end{pmatrix} \\ +\psi_{10}\begin{pmatrix} U\left|10\right\rangle U_T\left|00\right\rangle U\left|00\right\rangle + U\left|10\right\rangle U_T\left|01\right\rangle U\left|01\right\rangle \\ +U\left|11\right\rangle U_T\left|10\right\rangle U\left|00\right\rangle + U\left|11\right\rangle U_T\left|11\right\rangle U\left|01\right\rangle \end{pmatrix} + \psi_{11}\begin{pmatrix} U\left|10\right\rangle U_T\left|00\right\rangle U\left|10\right\rangle + U\left|10\right\rangle U_T\left|01\right\rangle U\left|11\right\rangle \\ +U\left|11\right\rangle U_T\left|10\right\rangle U\left|10\right\rangle + U\left|11\right\rangle U_T\left|11\right\rangle U\left|11\right\rangle \end{pmatrix} \end{array}\right]$$

$$= \frac{1}{4}\sum_{n,m=0}^{3} V_{nm} U_T\left[\psi_{00}\left|00\right\rangle + \psi_{01}\left|01\right\rangle + \psi_{10}\left|10\right\rangle + \psi_{11}\left|11\right\rangle\right]\left|\beta_n\right\rangle\left|\beta_m\right\rangle. \tag{17}$$

Now, taking the inner product of $\langle\beta_j|$ with the first two-qubits of (17) and $\langle\beta_k|$ with the last two-qubits of (17) one gets

$$\begin{aligned}
&\frac{1}{2}\left[\begin{array}{l}
\left(\begin{array}{l}\langle\beta_j|U_{00}\rangle\langle\beta_k|U_{00}\rangle U_T\psi_{00}|00\rangle+\langle\beta_j|U_{00}\rangle\langle\beta_k|U_{01}\rangle U_T\psi_{00}|01\rangle\\ +\langle\beta_j|U_{01}\rangle\langle\beta_k|U_{00}\rangle U_T\psi_{00}|10\rangle+\langle\beta_j|U_{01}\rangle\langle\beta_k|U_{01}\rangle U_T\psi_{00}|11\rangle\end{array}\right)\\
+\left(\begin{array}{l}\langle\beta_j|U_{00}\rangle\langle\beta_k|U_{10}\rangle U_T\psi_{01}|00\rangle+\langle\beta_j|U_{00}\rangle\langle\beta_k|U_{11}\rangle U_T\psi_{01}|01\rangle\\ +\langle\beta_j|U_{01}\rangle\langle\beta_k|U_{10}\rangle U_T\psi_{01}|10\rangle+\langle\beta_j|U_{01}\rangle\langle\beta_k|U_{11}\rangle U_T\psi_{01}|11\rangle\end{array}\right)\\
+\left(\begin{array}{l}\langle\beta_j|U_{10}\rangle\langle\beta_k|U_{00}\rangle U_T\psi_{10}|00\rangle+\langle\beta_j|U_{10}\rangle\langle\beta_k|U_{01}\rangle U_T\psi_{10}|01\rangle\\ +\langle\beta_j|U_{11}\rangle\langle\beta_k|U_{00}\rangle U_T\psi_{10}|10\rangle+\langle\beta_j|U_{11}\rangle\langle\beta_k|U_{01}\rangle U_T\psi_{10}|11\rangle\end{array}\right)\\
+\left(\begin{array}{l}\langle\beta_j|U_{10}\rangle\langle\beta_k|U_{10}\rangle U_T\psi_{11}|00\rangle+\langle\beta_j|U_{10}\rangle\langle\beta_k|U_{11}\rangle U_T\psi_{11}|01\rangle\\ +\langle\beta_j|U_{11}\rangle\langle\beta_k|U_{10}\rangle U_T\psi_{11}|10\rangle+\langle\beta_j|U_{11}\rangle\langle\beta_k|U_{11}\rangle U_T\psi_{11}|11\rangle\end{array}\right)
\end{array}\right]\\
&=\frac{1}{4}V_{jk}U_T\left[\psi_{00}|00\rangle+\psi_{01}|01\rangle+\psi_{10}|10\rangle+\psi_{11}|11\rangle\right],
\end{aligned} \tag{18}$$

In order to get (18) from (17) we did, for example, $\langle\beta_j|\langle\beta_k|(\psi_{00}U|00\rangle U_T|01\rangle U|01\rangle) = \langle\beta_j|U|00\rangle\langle\beta_k|U|01\rangle U_T\psi_{00}|01\rangle = \langle\beta_j|U_{00}\rangle\langle\beta_k|U_{01}\rangle U_T\psi_{00}|01\rangle$. Equation (18) can be rewritten as

$$U_T\beta_{jk}|\psi_{AB}\rangle = V_{jk}U_T|\psi_{AB}\rangle \tag{19}$$

$$\beta_{jk}=\beta_j\otimes\beta_k=\sqrt{2}\begin{bmatrix}\langle\beta_j|U_{00}\rangle & \langle\beta_j|U_{10}\rangle\\ \langle\beta_j|U_{01}\rangle & \langle\beta_j|U_{11}\rangle\end{bmatrix}\otimes\sqrt{2}\begin{bmatrix}\langle\beta_k|U_{00}\rangle & \langle\beta_k|U_{10}\rangle\\ \langle\beta_k|U_{01}\rangle & \langle\beta_k|U_{11}\rangle\end{bmatrix} \tag{20}$$

$$|\psi_{AB}\rangle=\psi_{00}|00\rangle+\psi_{01}|01\rangle+\psi_{10}|10\rangle+\psi_{11}|11\rangle. \tag{21}$$

Equations (19)-(21) tell us that the quantum gate U_T can be teleported only if the quantum gate U and the measurement basis are chosen in such way that $U_T\beta_{jk}=V_{jk}U_T$ where, if the error correction must be local, V_{jk} is decomposable in the tensor product of single-qubit gates. In other words, given U and a measurement basis, there exist a specific set of quantum gates that can be teleported. For example, if $U=I$ and the measurement basis is the Bell basis, then we have the well known result that the error correction gates are Pauli matrices and the quantum gates belonging to Clifford group can be teleported.

Following the same procedure as before, for a two-qudit gate one has

$$U_T\beta|\psi_{AB}\rangle = V_{jk}U_T|\psi_{AB}\rangle \tag{22}$$

$$\beta=\sqrt{d}\begin{bmatrix}\langle\beta_j|U_{00}\rangle & \langle\beta_j|U_{10}\rangle & \cdots & \langle\beta_j|U_{(d-1)0}\rangle\\ \langle\beta_j|U_{01}\rangle & \langle\beta_j|U_{11}\rangle & \cdots & \langle\beta_j|U_{(d-1)1}\rangle\\ \vdots & \vdots & & \vdots\\ \langle\beta_j|U_{0(d-1)}\rangle & \langle\beta_j|U_{1(d-1)}\rangle & \cdots & \langle\beta_j|U_{(d-1)(d-1)}\rangle\end{bmatrix}\otimes\sqrt{d}\begin{bmatrix}\langle\beta_k|U_{00}\rangle & \langle\beta_k|U_{10}\rangle & \cdots & \langle\beta_k|U_{(d-1)0}\rangle\\ \langle\beta_k|U_{01}\rangle & \langle\beta_k|U_{11}\rangle & \cdots & \langle\beta_k|U_{(d-1)1}\rangle\\ \vdots & \vdots & & \vdots\\ \langle\beta_k|U_{0(d-1)}\rangle & \langle\beta_k|U_{1(d-1)}\rangle & \cdots & \langle\beta_k|U_{(d-1)(d-1)}\rangle\end{bmatrix} \tag{23}$$

$$|\psi_{AB}\rangle=\sum_{n,m=0}^{d-1}\psi_{nm}|nm\rangle, \tag{24}$$

while for a n-qubit gate one obtains

$$U_T\beta\left|\psi_{12\ldots N}\right\rangle = V_{j_1\ldots_N}U_T\left|\psi_{12\ldots N}\right\rangle \tag{25}$$

$$\beta = \prod_{j=1}^{N}\otimes\sqrt{2}\begin{bmatrix}\left\langle\beta_j\middle|U_{00}\right\rangle & \left\langle\beta_j\middle|U_{10}\right\rangle\\ \left\langle\beta_j\middle|U_{01}\right\rangle & \left\langle\beta_j\middle|U_{11}\right\rangle\end{bmatrix} \tag{26}$$

$$\left|\psi_{12\ldots N}\right\rangle = \psi_{00\ldots00}\left|00\ldots.0\right\rangle + \psi_{00\ldots01}\left|00\ldots01\right\rangle + \psi_{00\ldots10}\left|00\ldots10\right\rangle + \psi_{11\ldots11}\left|11\ldots11\right\rangle. \tag{27}$$

4. Preservation of separability under conjugation and the teleportation of two-qubit gates

In this section we will discuss the conditions required for a basis to be useful for teleportation of a two-qubit gate or, alternatively, the conditions required for a gate to be teleported by a given basis. Firstly, let us assume the following notation: $\sigma_\mu = \mu$ and $\sigma_\upsilon = \upsilon$ are Pauli matrices: $\mu,\upsilon \in \{I, X, Y, Z\}$. Furthermore, $\sigma_{\mu\upsilon} = \sigma_\mu \otimes \sigma_\upsilon$. Now, one has that

$$\left[\sigma_{\mu\mu},\sigma_{\upsilon\upsilon}\right] = \left[\sigma_{\mu\mu},\sigma_{I\mu}\right] = \left[\sigma_{\mu\mu},\sigma_{\mu I}\right] = \left[\sigma_{\mu I},\sigma_{I\upsilon}\right] = \left[\sigma_{I\mu},\sigma_{\upsilon I}\right] = 0. \tag{28}$$

As it is well know, a general single-qubit gate and a separable two-qubit gate can be represented, respectively, as

$$U_\Lambda = e^{-i\left(\frac{\lambda_1}{2}\sigma_Z\right)}e^{-i\left(\frac{\lambda_2}{2}\sigma_Y\right)}e^{-i\left(\frac{\lambda_3}{2}\sigma_Z\right)} \tag{29}$$

$$U_{\Lambda\Omega} = \left[e^{-i\left(\frac{\lambda_1}{2}\sigma_Z\right)}\otimes e^{-i\left(\frac{\omega_1}{2}\sigma_Z\right)}\right]\left[e^{-i\left(\frac{\lambda_2}{2}\sigma_Y\right)}\otimes e^{-i\left(\frac{\omega_2}{2}\sigma_Y\right)}\right]\left[e^{-i\left(\frac{\lambda_3}{2}\sigma_Z\right)}\otimes e^{-i\left(\frac{\omega_3}{2}\sigma_Z\right)}\right]. \tag{30}$$

Now, using

$$e^A\otimes e^B = e^{A\oplus B} \tag{31}$$

$$A\oplus B = A\otimes I + I\otimes B \tag{32}$$

in (30) one gets

$$U_{\Lambda\Omega} = e^{-i\left(\frac{\lambda_1}{2}\sigma_{ZI}+\frac{\omega_1}{2}\sigma_{IZ}\right)}e^{-i\left(\frac{\lambda_2}{2}\sigma_{YI}+\frac{\omega_2}{2}\sigma_{IY}\right)}e^{-i\left(\frac{\lambda_3}{2}\sigma_{ZI}+\frac{\omega_3}{2}\sigma_{IZ}\right)}. \tag{33}$$

Now, according to KAK decomposition [11], a general two-qubit quantum gate is decomposed as

$$U = \left(U_A\otimes U_B\right)U_{NL}\left(U_C\otimes U_D\right) \tag{34}$$

$$U_{NL} = e^{i\left(\theta_1\sigma_{XX}+\theta_2\sigma_{YY}+\theta_3\sigma_{ZZ}\right)} = e^{i\left(\theta_1\sigma_{XX}\right)}e^{i\left(\theta_2\sigma_{YY}\right)}e^{i\left(\theta_3\sigma_{ZZ}\right)}, \tag{35}$$

where U_A, U_B, U_C and U_D are local single-qubit gates and U_{NL} is the non-local part. Using (33) in (34)-(35), one obtains

$$U = e^{-i\left(\frac{\lambda_1}{2}\sigma_{ZI}+\frac{\omega_1}{2}\sigma_{IZ}\right)} e^{-i\left(\frac{\lambda_2}{2}\sigma_{YI}+\frac{\omega_2}{2}\sigma_{IY}\right)} e^{-i\left(\frac{\lambda_3}{2}\sigma_{ZI}+\frac{\omega_3}{2}\sigma_{IZ}\right)} e^{i(\theta_1\sigma_{XX})} e^{i(\theta_2\sigma_{YY})} e^{i(\theta_3\sigma_{ZZ})} e^{-i\left(\frac{\xi_1}{2}\sigma_{ZI}+\frac{\mu_1}{2}\sigma_{IZ}\right)} e^{-i\left(\frac{\xi_2}{2}\sigma_{YI}+\frac{\mu_2}{2}\sigma_{IY}\right)} e^{-i\left(\frac{\xi_3}{2}\sigma_{ZI}+\frac{\mu_3}{2}\sigma_{IZ}\right)}. \quad (36)$$

Considering again the two-qubit quantum gate teleportation, one has that teleportation with local error correction is possible if $U_T \beta_{jk} U_T^\dagger = V_{jk}$. Using the KAK decomposition of U_T, the left side can be rewritten as $\left[\left(U_A \otimes U_B\right) U_{NL} \left(U_C \otimes U_D\right)\right] \beta_{jk} \left[\left(U_C^\dagger \otimes U_D^\dagger\right) U_{NL}^\dagger \left(U_A^\dagger \otimes U_B^\dagger\right)\right]$ hence, the teleportation is possible if $W = U_{NL} \beta'_{jk} U_{NL}^\dagger$, where $\beta'_{jk} = \left(U_C \otimes U_D\right) \beta_{jk} \left(U_C^\dagger \otimes U_D^\dagger\right)$, is separable. Using (33) and (35) W can be written as

$$W = e^{i(\theta_1\sigma_{XX})} e^{i(\theta_2\sigma_{YY})} e^{i(\theta_3\sigma_{ZZ})} e^{-i\left(\frac{\lambda_1}{2}\sigma_{ZI}+\frac{\omega_1}{2}\sigma_{IZ}\right)} e^{-i\left(\frac{\lambda_2}{2}\sigma_{YI}+\frac{\omega_2}{2}\sigma_{IY}\right)} e^{-i\left(\frac{\lambda_3}{2}\sigma_{ZI}+\frac{\omega_3}{2}\sigma_{IZ}\right)} e^{-i(\theta_3\sigma_{ZZ})} e^{-i(\theta_2\sigma_{YY})} e^{-i(\theta_1\sigma_{XX})}. \quad (37)$$

Using the commutation relations given in (28), one gets

$$W = e^{i(\theta_1\sigma_{XX}+\theta_2\sigma_{YY})} e^{-i\left(\frac{\lambda_1}{2}\sigma_{ZI}+\frac{\omega_1}{2}\sigma_{IZ}\right)} e^{-i(\theta_1\sigma_{XX}+\theta_2\sigma_{YY})} e^{i(\theta_1\sigma_{XX}+\theta_3\sigma_{ZZ})} e^{-i\left(\frac{\lambda_2}{2}\sigma_{YI}+\frac{\omega_2}{2}\sigma_{IY}\right)} e^{-i(\theta_1\sigma_{XX}+\theta_3\sigma_{ZZ})} e^{i(\theta_1\sigma_{XX}+\theta_2\sigma_{YY})} e^{-i\left(\frac{\lambda_3}{2}\sigma_{ZI}+\frac{\omega_3}{2}\sigma_{IZ}\right)} e^{-i(\theta_1\sigma_{XX}+\theta_2\sigma_{YY})}. \quad (38)$$

Therefore, W is separable only if the unitary matrices

$$W_1 = e^{i(\theta\sigma_{\mu\mu})} e^{-i\left(\frac{\lambda}{2}\sigma_{ZI}\right)} e^{-i(\theta\sigma_{\mu\mu})} \quad (39)$$

$$W_2 = e^{i(\theta\sigma_{\mu\mu})} e^{-i\left(\frac{\lambda}{2}\sigma_{IZ}\right)} e^{-i(\theta\sigma_{\mu\mu})} \quad (40)$$

$$W_3 = e^{i(\theta\sigma_{\upsilon\upsilon})} e^{-i\left(\frac{\lambda}{2}\sigma_{YI}\right)} e^{-i(\theta\sigma_{\upsilon\upsilon})} \quad (41)$$

$$W_4 = e^{i(\theta\sigma_{\upsilon\upsilon})} e^{-i\left(\frac{\lambda}{2}\sigma_{IY}\right)} e^{-i(\theta\sigma_{\upsilon\upsilon})} \quad (42)$$

are also separable, where $\mu \in \{X,Y\}$ and $\upsilon \in \{X,Z\}$. After some algebra, one can find that the unitary matrices $W_1,\ldots,W_4$ are separable if the following condition is satisfied

$$\sin\left(\frac{\lambda}{2}\right)\sin(2\theta)\left[e^{i\frac{\lambda}{2}}\sin^2(\theta)+e^{-i\frac{\lambda}{2}}\cos^2(\theta)\right]=0. \quad (43)$$

The solutions of (43) are $(\theta,\lambda) \in \{(k\pi/2,x);(x,2k\pi);((2k+1)\pi/4,n\pi)\}$ where $x \in R$ while k and $n \in$ Z. The first two solutions are not interesting because $\exp(i(k\pi/2)\sigma_{\mu\mu})$ is separable and $\exp(ik\pi\sigma_{\mu l}) = \exp(ik\pi\sigma_{l\mu})=I$. Therefore, the non-trivial separability preservation occurs according to Theorem 1:

Theorem 1: Given a two-qubit quantum gate U_T with KAK decomposition $U_T = (U_A\otimes U_B)U_{NL}(U_C\otimes U_D)$, and a two-qubit basis $\{|\beta_1\rangle,|\beta_2\rangle,|\beta_3\rangle,|\beta_4\rangle\}$, the quantum gate U_T can be deterministically teleported if the following conditions are satisfied:

$$U_{NL} = e^{i\left[\varepsilon_x(2k_x+1)\frac{\pi}{4}\sigma_{XX}+\varepsilon_y(2k_y+1)\frac{\pi}{4}\sigma_{YY}+\varepsilon_z(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]}$$

$$\left(U_C\otimes U_D\right)\beta_{jk}\left(U_C^{\dagger}\otimes U_D^{\dagger}\right)=v_{jk}=v_j\otimes v_k$$

$$v_j = e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})n_1\pi+(\varepsilon_s+\varepsilon_{xy})\lambda_1}{2}\sigma_Z\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xz})n_2\pi+(\varepsilon_s+\varepsilon_{xz})\lambda_2}{2}\sigma_Y\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})n_3\pi+(\varepsilon_s+\varepsilon_{xy})\lambda_3}{2}\sigma_Z\right)}$$

$$v_k = e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})m_1\pi+(\varepsilon_s+\varepsilon_{xy})\omega_1}{2}\sigma_Z\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xz})m_2\pi+(\varepsilon_s+\varepsilon_{xz})\omega_2}{2}\sigma_Y\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})m_3\pi+(\varepsilon_s+\varepsilon_{xy})\omega_3}{2}\sigma_Z\right)}$$

$$\varepsilon_{ab}=(1-\varepsilon_a)(1-\varepsilon_b);\ \varepsilon_s=\delta(1-\varepsilon_x\varepsilon_y\varepsilon_z)\delta(k_x)\delta(k_y)\delta(k_z)$$

where

$$\beta_j\otimes\beta_k=\sqrt{2}\begin{bmatrix}\langle\beta_j|00\rangle & \langle\beta_j|10\rangle\\ \langle\beta_j|01\rangle & \langle\beta_j|11\rangle\end{bmatrix}\otimes\sqrt{2}\begin{bmatrix}\langle\beta_k|00\rangle & \langle\beta_k|10\rangle\\ \langle\beta_k|01\rangle & \langle\beta_k|11\rangle\end{bmatrix}$$

$$\varepsilon_{x,y,z}=0,1$$

$$k_{x,y,z}, n_{1,2,3}, m_{1,2,3}=0,\pm1,\pm2,\ldots$$

$$\lambda_{1,2,3},\omega_{1,2,3}\in R$$

$$j,k=1,2,3,4$$

These conditions are summarized in Table 1.

$U_{NL} = e^{i\left[\varepsilon_x(2k_x+1)\frac{\pi}{4}\sigma_{XX}+\varepsilon_y(2k_y+1)\frac{\pi}{4}\sigma_{YY}+\varepsilon_z(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]}$	$\left(U_C\otimes U_D\right)\beta_{jk}\left(U_C^{\dagger}\otimes U_D^{\dagger}\right)=e^{-\frac{i}{2}(\phi_1\sigma_{ZI}+\phi_2\sigma_{IZ})}e^{-\frac{i}{2}(\phi_3\sigma_{YI}+\phi_4\sigma_{IY})}e^{-\frac{i}{2}(\phi_5\sigma_{ZI}+\phi_6\sigma_{IZ})}$
($\varepsilon_x = 0$, $\varepsilon_y = 1$, $\varepsilon_z = 1$) ,($\varepsilon_x = 1$, $\varepsilon_y = 0$, $\varepsilon_z = 0$) , ($\varepsilon_x = 1$, $\varepsilon_y = 0$, $\varepsilon_z = 1$), ($\varepsilon_x = 1$, $\varepsilon_y = 1$, $\varepsilon_z = 0$), ($\varepsilon_x = 1$, $\varepsilon_y = 1$, $\varepsilon_z = 1$) & ($k_x \neq k_y$ and/or $k_x \neq k_z$)	$\phi_1=n_1\pi$, $\phi_2=n_2\pi$, $\phi_3=n_3\pi$, $\phi_4=n_4\pi$, $\phi_5=n_5\pi$, $\phi_6=n_6\pi$
($\varepsilon_x = 0$, $\varepsilon_y = 0$, $\varepsilon_z = 1$)	$\phi_1=\lambda_1$, $\phi_2=\lambda_2$, $\phi_3=n_3\pi$, $\phi_4=n_4\pi$, $\phi_5=\lambda_5$, $\phi_6=\lambda_6$
($\varepsilon_x = 0$, $\varepsilon_y = 1$, $\varepsilon_z = 0$)	$\phi_1=n_1\pi$, $\phi_2=n_2\pi$, $\phi_3=\lambda_3$, $\phi_4=\lambda_4$, $\phi_5=n_5\pi$, $\phi_6=n_6\pi$
($\varepsilon_x = 1$, $\varepsilon_y = 1$, $\varepsilon_z = 1$) & ($k_x = k_y = k_z$)	$\phi_1=\lambda_1$, $\phi_2=\lambda_2$, $\phi_3=\lambda_3$, $\phi_4=\lambda_4$, $\phi_5=\lambda_5$, $\phi_6=\lambda_6$

Table 1. Conditions for deterministic teleportation according to Theorem 1: $n_{1\ldots6}$ are integer numbers while $\lambda_{1\ldots6}$ are real numbers.

Without loss of generality, we have considered $U = I$ in scheme in Fig. 2. Note that, if Theorem 1 is only partially satisfied (the tensor product is not satisfied for all values of (j,k)) then a probabilistic teleportation takes place. In this case the success probability is $N(j,k)/16$, where $N(j,k)$ is the number of pairs (j,k) that satisfies the tensor product.

5. Examples of quantum gate teleportation with different bases

In this section we show some examples of teleportation with different bases. For all examples here considered we used $U = I$ in Fig. 2. Firstly, let us consider the real basis β_{ab} and its corresponding matrices β_j, j=1,…,4:

$$\beta_{ab} = \left\{ \begin{pmatrix} -a \\ b \\ b \\ a \end{pmatrix}, \begin{pmatrix} -b \\ a \\ -a \\ -b \end{pmatrix}, \begin{pmatrix} -a \\ -b \\ b \\ -a \end{pmatrix}, \begin{pmatrix} b \\ a \\ a \\ -b \end{pmatrix} \right\} \tag{44}$$

$$\beta_1 = \sqrt{2}\begin{bmatrix} a & -b \\ -b & -a \end{bmatrix}, \beta_2 = \sqrt{2}\begin{bmatrix} b & a \\ -a & b \end{bmatrix}, \beta_3 = \sqrt{2}\begin{bmatrix} a & -b \\ b & a \end{bmatrix}, \beta_4 = \sqrt{2}\begin{bmatrix} -b & -a \\ -a & b \end{bmatrix} \tag{45}$$

$$a^2 + b^2 = 1/2. \tag{46}$$

An example of such basis is

$$M_1 = \left\{ \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \right\}. \tag{47}$$

The second basis to be considered is obtained taking the columns of the unitary matrix U_{NL} given in (35):

$$\beta_{NL} = \left\{ \begin{pmatrix} \cos(\theta_1 - \theta_2)e^{i\theta_3} \\ 0 \\ 0 \\ \sin(\theta_1 - \theta_2)ie^{i\theta_3} \end{pmatrix}, \begin{pmatrix} 0 \\ \cos(\theta_1 + \theta_2)e^{-i\theta_3} \\ \sin(\theta_1 + \theta_2)ie^{-i\theta_3} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \sin(\theta_1 + \theta_2)ie^{-i\theta_3} \\ \cos(\theta_1 + \theta_2)e^{-i\theta_3} \\ 0 \end{pmatrix}, \begin{pmatrix} \sin(\theta_1 - \theta_2)ie^{i\theta_3} \\ 0 \\ 0 \\ \cos(\theta_1 - \theta_2)e^{i\theta_3} \end{pmatrix} \right\} \tag{48}$$

$$(\theta_1, \theta_2) = \begin{cases} \left(0, \pm\frac{\pi}{4}\right), \left(\pm\frac{\pi}{4}, 0\right), \left(0, \pm\frac{3\pi}{4}\right), \left(\pm\frac{3\pi}{4}, 0\right), \left(\pi, \frac{\pi}{4}\right), \left(\frac{\pi}{4}, \pi\right) \\ \left(\pm\frac{\pi}{2}, \pm\frac{\pi}{4}\right), \left(\pm\frac{\pi}{4}, \pm\frac{\pi}{2}\right), \left(\pm\frac{\pi}{2}, \pm\frac{3\pi}{4}\right), \left(\pm\frac{3\pi}{4}, \pm\frac{\pi}{2}\right) \end{cases} \tag{49}$$

The angle θ_3 can assume any real value. Note that taking values for θ_1 and θ_2 different from those values shown in (49) will result in a non valid basis since the matrices β_j will not be unitary. Two examples of this class are the bases

$$M_{Bell} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \right\} \tag{50}$$

$$M_2 = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 0 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -i \\ i \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ i \end{pmatrix} \right\}. \tag{51}$$

After some algebra, one can easily check that the CNOT can be deterministically teleported by the scheme in Fig. 2 if the basis M_{Bell} is used, it can be probabilistically teleported if the basis M_2 is used and it cannot be teleported if the basis M_1 is used. Table 2 shows the probability of successful teleportation for a small set of gates when the basis M_{Bell}, M_1 and M_2 are considered.

Gate	$\boldsymbol{M_{Bell}}$	$\boldsymbol{M_1}$	$\boldsymbol{M_2}$
CNOT	1	0	0.5
$C_{\pi/8}$	0.5	0	0.5
$\text{CNOT}^{1/2}$	0.5	0	0.25
$\text{SWAP}^{1/2}$	0.25	0.25	0.25
$\exp(i\pi/4\sigma_{YY})$	1	1	0.25

Table 2. Probability of successful teleportation according to the basis used: M_{Bell}, M_1 and M_2.

Now, let us consider the quantum gate T that is deterministically teleported by M_{BELL} and M_2 but it is not teleported by M_1.

$$G(\phi,\xi) = \begin{bmatrix} i & 0 & 0 & 0 \\ 0 & e^{i\phi} & 0 & 0 \\ 0 & 0 & e^{i\xi} & 0 \\ 0 & 0 & 0 & ie^{i(\phi+\xi)} \end{bmatrix}. \tag{52}$$

Considering the basis M_2 one has

$$\beta_1 = -iS = \begin{bmatrix} -i & 0 \\ 0 & 1 \end{bmatrix}, \beta_2 = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \beta_3 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \beta_4 = S\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} \tag{53}$$

and the results for $G(\beta_j \otimes \beta_k)G^{\dagger}$ shown in Table 3.

j	k	$G(\beta_j\otimes\beta_k)G^\dagger$	j	k	$G(\beta_j\otimes\beta_k)G^\dagger$
1	1	$S\otimes -S$	3	1	$V_\xi\otimes iS\sigma_Z$
1	2	$S\sigma_Z\otimes -V_\phi\sigma_Z$	3	2	$-V_\xi\sigma_Z\otimes iV_\phi$
1	3	$S\sigma_Z\otimes iV_\phi$	3	3	$V_\xi\sigma_Z\otimes -V_\phi\sigma_Z$
1	4	$S\otimes S\sigma_Y\sigma_X$	3	4	$-V_\xi\otimes S$
2	1	$-V_\xi\sigma_Z\otimes S\sigma_Z$	4	1	$P\sigma_Y\sigma_X\otimes S$
2	2	$V_\xi\otimes V_\phi$	4	2	$-V_\phi\sigma_Z\otimes iS$
2	3	$V_\xi\otimes -V_\phi\sigma_Z$	4	3	$S\otimes -V_\phi$
2	4	$-V_\xi\sigma_Z\otimes iS$	4	4	$S\sigma_Z\otimes S\sigma_Z$
$V_{\phi,\xi}=\begin{bmatrix} 0 & -ie^{-i\phi,\xi} \\ ie^{i\phi,\xi} & 0 \end{bmatrix}$					

Table 3. Results of $G(\beta_j\otimes\beta_k)G^\dagger$ for teleportation of G in (52) when basis M_2 is used .

Hence, the gate $G(\phi,\xi)$ is deterministically teleportable for any values for ϕ and ξ when the basis M_2 is used (the same happens if M_{Bell} is used). Two interesting cases are $G(\phi=\pi/8,\ \xi=\pi/8)$ and $G(\phi=\pi/7,\ \xi=\pi/13)$. They are deterministically teleportable but both of them do not belong to Clifford group. This is remarkable since up to now, from the best of our knowledge, none explicit example of a non-Clifford quantum gate teleportation was presented.

In order to generalize a procedure to deterministically teleport gates out of Clifford group, let us consider the set of gates of the type $F=(U_A\otimes U_B)U_{NL}(U_R\otimes U_R)$ with U_{NL} obeying the Theorem 1. This kind of gate can always be teleported by the basis (j=1,…,4)

$$\left|\beta_j\right\rangle=\sum_{n,m=0}^{1}\frac{\left\langle n\left|\beta_j\right|m\right\rangle}{\sqrt{2}}\left|nm\right\rangle \tag{54}$$

$$\beta_j=U_R^\dagger\sigma_j U_R. \tag{55}$$

Note that $\beta_j\beta_k=\beta_m$. If at least one of the gates U_A, U_B or U_R does not preserve Pauli under conjugation, then F does not belong to Clifford group. Thus, there is infinity of gates out of Clifford group that can be teleported deterministically. All of those gates are only probabilistically teleported if the Bell basis is used. A special case of F gates are the gates $R_k=\left(U_R^\dagger\otimes U_R^\dagger\right)U_{NL}^k\left(U_R\otimes U_R\right)$. It can be checked that $R_kR_s=R_t$ where $U_{NL}^t=U_{NL}^kU_{NL}^s$ and $R_k\beta_{jk}R_k^\dagger=\beta_{nm}$. Hence, the set of gates R_k forms a group that preserves the group β_j under conjugation. As an example, let us consider $U_R=T=\mathrm{diag}\{i,(1+i)/2^{1/2}\}$. The basis obtained from (54)-(55) is

$$M_T=\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\\0\\1\end{pmatrix},\begin{pmatrix}0\\(1+i)/\sqrt{2}\\(1-i)/\sqrt{2}\\0\end{pmatrix},\begin{pmatrix}0\\(1-i)/\sqrt{2}\\(1+i)/\sqrt{2}\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}\right\}. \tag{56}$$

The basis M_T given in (56) can be used to teleport deterministically any gate of the form $(U_A \otimes U_B)\cdot\exp\{i[\varepsilon_x(2k_x+1)\pi/4\sigma_{XX} + \varepsilon_y(2k_y+1)\pi/4\sigma_{YY} + \varepsilon_z(2k_z+1)\pi/4\sigma_{ZZ}]\}\cdot (T\otimes T)$.

6. Quantum gate teleportation with a genuine four-way entangled state

At last, in this section we consider the two-qubit quantum gate teleportation using a genuine four-way entangled state instead of a pair of Bell states. The four-qubit quantum state used is [12]

$$|\chi\rangle = \left(|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle\right)/8. \tag{57}$$

Following the steps described in (17)-(21), one gets the following quantum state before error correction

$$|\psi\rangle = \frac{\left(U_T U_1 \sigma_{XX} \beta_{jk} |\psi_{AB}\rangle + U_T U_1 \sigma_{ZZ} \beta_{jk} |\psi_{AB}\rangle\right)}{\sqrt{2}} \tag{58}$$

$$U_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{59}$$

Due to the superposition in (58), a successful teleportation of the two-qubit state $U_T|\psi_{AB}\rangle$ can never be achieved. However, using $U=U_T U_1$ in (58), it can be rewritten as

$$|\psi\rangle = \frac{\left(U\sigma_{XX}\beta_{jk}U^\dagger\right)U|\psi_{AB}\rangle + \left(U\sigma_{ZZ}\beta_{jk}U^\dagger\right)U|\psi_{AB}\rangle}{\sqrt{2}}, \tag{60}$$

what shows that a superposition of $U|\psi_{AB}\rangle$ with local errors is realized if $(U\sigma_{XX}\beta_{jk}U^\dagger)$ and $(U\sigma_{ZZ}\beta_{jk}U^\dagger)$ are separable. In particular, if Bell basis is used (hence β_j is a Pauli matrix), U belongs to Clifford group and $|\psi_{AB}\rangle = U^\dagger|00\rangle$, then one has

$$|\psi\rangle = \frac{\sigma_{nm}|00\rangle + \sigma_{rs}|00\rangle}{\sqrt{2}}. \tag{61}$$

In this case, the quantum gate teleportation schemes works as non–local quantum circuit whose input is $U^\dagger|00\rangle$ and the output is (probabilistically) one of the Bell states.

7. General decomposition of two-qubit Clifford gates

An immediate consequence of Theorem 1 is the Lemma 1:

Lemma 1: Any Clifford gate has a decomposition of the form $(U_A\otimes U_B)\cdot\exp\{i[\varepsilon_x(2k_x+1)\pi/4\sigma_{XX} + \varepsilon_y(2k_y+1)\pi/4\sigma_{YY} + \varepsilon_z(2k_z+1)\pi/4\sigma_{ZZ}]\}\cdot(U_C\otimes U_D)$, where the gates U_A, U_B, U_C and U_D preserve Pauli under conjugation.

In order to prove this statement, let us start by the following definitions (see for example [13] for a review):

1) The Pauli group P_1 is the closure of the set $\{I, X, Y, Z\}$ under multiplication, with multiplicative factors $\{\pm1,\pm i\}$. The Pauli group on two qubits, P_2, consists of all tensor products of Pauli and identity matrices with phase factors $\{\pm1,\pm i\}$: $P_2=\{\lambda\sigma_\mu\otimes\sigma_\nu |\ \lambda\in\{\pm1,\pm i\}$ and $\sigma_\mu,\sigma_\upsilon\in\{I, X, Y, Z\}\}$.

2) The Clifford group on one qubit, C_1, is the group of gates U belonging to $U(2)$ which normalize P_1: $C_1=\{U\in U(2)|\ \forall\ \sigma_\mu \in P_1: U\sigma_\mu U^\dagger\in P_1\}$. The single-qubit Hadamard (H) and phase (S) gates are generators of C_1: $C_1=\langle H, S\rangle$. Similarly, the Clifford group on two qubits, C_2, is the group of gates U belonging to $U(4)$ which normalize P_2: $C_2=\{U\in U(4)|\ \forall\ \sigma_\mu\otimes\sigma_\nu\in P_2: U\sigma_\mu\otimes\sigma_\nu U^\dagger\in P_2\}$. The two-qubit controlled-not and the single-qubit Hadamard (H) and phase (S) gates are generators of C_2: $C_2=\langle H, S, \mathrm{CNOT}\rangle$.

Now, let $U=(U_A\otimes U_B)U_{NL}(U_C\otimes U_D)$ to be the KAK decomposition of the two-qubit Clifford gate U. Then one has that

$$\left[\left(U_A\otimes U_B\right)U_{NL}\left(U_C\otimes U_D\right)\right]\left(\sigma_\mu\otimes\sigma_\upsilon\right)\left[\left(U_C^\dagger\otimes U_D^\dagger\right)U_{NL}^\dagger\left(U_A^\dagger\otimes U_B^\dagger\right)\right]=\left(\sigma_\alpha\otimes\sigma_\beta\right) \tag{62}$$

In order to (62) to be true, $U_{NL}\left(U_C\otimes U_D\right)\left(\sigma_\mu\otimes\sigma_\upsilon\right)\left(U_C^\dagger\otimes U_D^\dagger\right)U_{NL}^\dagger$ must be separable. Hence, it must obey the separabilitity condition given by (43) and, hence, it must obey the Theorem 1 too. Thus

$$U_{NL}=e^{i\left[\varepsilon_x(2k_x+1)\frac{\pi}{4}\sigma_{XX}+\varepsilon_y(2k_y+1)\frac{\pi}{4}\sigma_{YY}+\varepsilon_z(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]} \tag{63}$$

$$\left(U_C\otimes U_D\right)\left(\sigma_\mu\otimes\sigma_\upsilon\right)\left(U_C^\dagger\otimes U_D^\dagger\right)=w_j\otimes w_k \tag{64}$$

$$w_j=e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})n_1\pi+(\varepsilon_s+\varepsilon_{xy})\lambda_1}{2}\sigma_Z\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xz})n_2\pi+(\varepsilon_s+\varepsilon_{xz})\lambda_2}{2}\sigma_Y\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})n_3\pi+(\varepsilon_s+\varepsilon_{xy})\lambda_3}{2}\sigma_Z\right)} \tag{65}$$

$$w_k=e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})m_1\pi+(\varepsilon_s+\varepsilon_{xy})\omega_1}{2}\sigma_Z\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xz})m_2\pi+(\varepsilon_s+\varepsilon_{xz})\omega_2}{2}\sigma_Y\right)}e^{-i\left(\frac{(1-\varepsilon_s)(1-\varepsilon_{xy})m_3\pi+(\varepsilon_s+\varepsilon_{xy})\omega_3}{2}\sigma_Z\right)} \tag{66}$$

or, as shown in Table 4.

$U_{NL}=e^{i\left[\varepsilon_x(2k_x+1)\frac{\pi}{4}\sigma_{XX}+\varepsilon_y(2k_y+1)\frac{\pi}{4}\sigma_{YY}+\varepsilon_z(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]}$	$\left(U_C\otimes U_D\right)\left(\sigma_\mu\otimes\sigma_\upsilon\right)\left(U_C^\dagger\otimes U_D^\dagger\right)=w_j\otimes w_k$
($\varepsilon_x=0$, $\varepsilon_y=1$, $\varepsilon_z=1$) ,($\varepsilon_x=1$, $\varepsilon_y=0$, $\varepsilon_z=0$) , ($\varepsilon_x=1$, $\varepsilon_y=0$, $\varepsilon_z=1$), ($\varepsilon_x=1$, $\varepsilon_y=1$, $\varepsilon_z=0$), ($\varepsilon_x=1$, $\varepsilon_y=1$, $\varepsilon_z=1$)&($k_x\neq k_y$ and/or $k_x\neq k_z$)	$e^{-\frac{i}{2}(n_1\pi\sigma_Z)}e^{-\frac{i}{2}(n_2\pi\sigma_Y)}e^{-\frac{i}{2}(n_3\pi\sigma_Z)}\otimes e^{-\frac{i}{2}(m_1\pi\sigma_Z)}e^{-\frac{i}{2}(m_2\pi\sigma_Y)}e^{-\frac{i}{2}(m_3\pi\sigma_Z)}$
($\varepsilon_x=0$, $\varepsilon_y=0$, $\varepsilon_z=1$)	$e^{-\frac{i}{2}(\lambda_1\sigma_Z)}e^{-\frac{i}{2}(n_2\pi\sigma_Y)}e^{-\frac{i}{2}(\lambda_3\sigma_Z)}\otimes e^{-\frac{i}{2}(\omega_1\sigma_Z)}e^{-\frac{i}{2}(m_2\pi\sigma_Y)}e^{-\frac{i}{2}(\omega_3\sigma_Z)}$
($\varepsilon_x=0$, $\varepsilon_y=1$, $\varepsilon_z=0$)	$e^{-\frac{i}{2}(n_1\pi\sigma_Z)}e^{-\frac{i}{2}(\lambda_2\sigma_Y)}e^{-\frac{i}{2}(n_3\pi\sigma_Z)}\otimes e^{-\frac{i}{2}(m_1\pi\sigma_Z)}e^{-\frac{i}{2}(\omega_2\sigma_Y)}e^{-\frac{i}{2}(m_3\pi\sigma_Z)}$
($\varepsilon_x=1$, $\varepsilon_y=1$, $\varepsilon_z=1$) & ($k_x=k_y=k_z$)	$e^{-\frac{i}{2}(\lambda_1\sigma_Z)}e^{-\frac{i}{2}(\lambda_2\sigma_Y)}e^{-\frac{i}{2}(\lambda_3\sigma_Z)}\otimes e^{-\frac{i}{2}(\omega_1\sigma_Z)}e^{-\frac{i}{2}(\omega_2\sigma_Y)}e^{-\frac{i}{2}(\omega_3\sigma_Z)}$

Table 4. Conditions of separability for $U_{NL}\left(U_C\otimes U_D\right)\left(\sigma_\mu\otimes\sigma_\upsilon\right)\left(U_C^\dagger\otimes U_D^\dagger\right)U_{NL}^\dagger$.

Now let us to analyze each case in Table 4. Hereafter we will use the term P_1 to designate any element of Pauli group. Thus, for example, $P_1 \otimes P_1$ means the tensor product of two (not necessarily equal) Pauli matrices.

7.1 ($\varepsilon_x = 0$, $\varepsilon_y = 1$, $\varepsilon_z = 1$) ,($\varepsilon_x = 1$, $\varepsilon_y = 0$, $\varepsilon_z = 0$) , ($\varepsilon_x = 1$, $\varepsilon_y = 0$, $\varepsilon_z = 1$), ($\varepsilon_x = 1$, $\varepsilon_y = 1$, $\varepsilon_z = 0$), ($\varepsilon_x = 1$, $\varepsilon_y = 1$, $\varepsilon_z = 1$) & ($k_x \neq k_y$ and/or $k_x \neq k_z$).

In these cases, the possible values for U_{NL} are

$$U_{NL} \in \left\{ e^{i\left[(2k_x+1)\frac{\pi}{4}\sigma_{XX}\right]}, e^{i\left[(2k_x+1)\frac{\pi}{4}\sigma_{XX}+(2k_y+1)\frac{\pi}{4}\sigma_{YY}\right]}, e^{i\left[(2k_x+1)\frac{\pi}{4}\sigma_{XX}+(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]}, e^{i\left[(2k_x+1)\frac{\pi}{4}\sigma_{XX}+(2k_y+1)\frac{\pi}{4}\sigma_{YY}+(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]}, e^{i\left[(2k_y+1)\frac{\pi}{4}\sigma_{YY}+(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]} \right\} \quad (67)$$

Furthermore, since $\exp(-in\pi\sigma_\mu)$ is an identity matrix (if n is even) or a Pauli matrix (if n is odd) (multiplied by $\pm i$ or ± 1), from Table 4 one has that

$$\left(U_C \otimes U_D\right)\left(\sigma_\mu \otimes \sigma_\upsilon\right)\left(U_C^\dagger \otimes U_D^\dagger\right) = e^{-\frac{i}{2}(n_1\pi\sigma_Z)} e^{-\frac{i}{2}(n_2\pi\sigma_Y)} e^{-\frac{i}{2}(n_3\pi\sigma_Z)} \otimes e^{-\frac{i}{2}(m_1\pi\sigma_Z)} e^{-\frac{i}{2}(m_2\pi\sigma_Y)} e^{-\frac{i}{2}(m_3\pi\sigma_Z)} = P_1 \otimes P_1 \Rightarrow \quad (68)$$

$$U_C \sigma_\mu U_C^\dagger \otimes U_D \sigma_\upsilon U_D^\dagger = P_1 \otimes P_1 \quad (69)$$

From (69) one has that U_C and $U_D \in C_1$. Moreover, one can easily check that

$$U_{NL} P_1 \otimes P_1 U_{NL}^\dagger = P_1 \otimes P_1. \quad (70)$$

Hence,

$$\left[\left(U_A \otimes U_B\right) U_{NL} \left(U_C \otimes U_D\right)\right]\left(\sigma_\mu \otimes \sigma_\nu\right)\left[\left(U_C^\dagger \otimes U_D^\dagger\right) U_{NL}^\dagger \left(U_A^\dagger \otimes U_B^\dagger\right)\right] = \left(U_A \otimes U_B\right)\left(P_1 \otimes P_1\right)\left(U_A^\dagger \otimes U_B^\dagger\right), \quad (71)$$

Implying that U_A and $U_B \in C_1$.

7.2 ($\varepsilon_x = 0$, $\varepsilon_y = 0$, $\varepsilon_z = 1$)

In this case, one has

$$U_{NL} = e^{i(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}} \quad (72)$$

$$\left(U_C \otimes U_D\right)\left(\sigma_\mu \otimes \sigma_\upsilon\right)\left(U_C^\dagger \otimes U_D^\dagger\right) = e^{-\frac{i}{2}(\lambda_1\sigma_Z)} P_1 e^{-\frac{i}{2}(\lambda_3\sigma_Z)} \otimes e^{-\frac{i}{2}(\omega_1\sigma_Z)} P_1 e^{-\frac{i}{2}(\omega_3\sigma_Z)}, \quad (73)$$

hence,

$$U_{NL}\left(U_C\otimes U_D\right)\left(\sigma_\mu\otimes\sigma_\nu\right)\left(U_C^\dagger\otimes U_D^\dagger\right)U_{NL}^\dagger = U_{NL}e^{-\frac{i}{2}(\lambda_1\sigma_{ZI}+\omega_1\sigma_{IZ})}\left(P_1\otimes P_1\right)e^{-\frac{i}{2}(\lambda_3\sigma_{ZI}+\omega_3\sigma_{IZ})}U_{NL}^\dagger = \tag{74}$$

$$e^{-\frac{i}{2}(\lambda_1\sigma_{ZI}+\omega_1\sigma_{IZ})}U_{NL}\left(P_1\otimes P_1\right)U_{NL}^\dagger e^{-\frac{i}{2}(\lambda_3\sigma_{ZI}+\omega_3\sigma_{IZ})} = e^{-\frac{i}{2}(\lambda_1\sigma_{ZI}+\omega_1\sigma_{IZ})}\left(P_1\otimes P_1\right)e^{-\frac{i}{2}(\lambda_3\sigma_{ZI}+\omega_3\sigma_{IZ})}. \tag{75}$$

In (75) we used $[\exp(i\theta\sigma_{ZZ}),\exp(-i/2(\lambda\sigma_{ZI}+\omega\sigma_{IZ}))] = 0$, for any θ, λ, and ω. At last,

$$\left[\left(U_A\otimes U_B\right)U_{NL}\left(U_C\otimes U_D\right)\right]\left(\sigma_\mu\otimes\sigma_\nu\right)\left[\left(U_C^\dagger\otimes U_D^\dagger\right)U_{NL}^\dagger\left(U_A^\dagger\otimes U_B^\dagger\right)\right] = \tag{76}$$

$$\left(U_A\otimes U_B\right)\left[e^{-\frac{i}{2}(\lambda_1\sigma_{ZI}+\omega_1\sigma_{IZ})}\left(P_1\otimes P_1\right)e^{-\frac{i}{2}(\lambda_3\sigma_{ZI}+\omega_3\sigma_{IZ})}\right]\left(U_A^\dagger\otimes U_B^\dagger\right) = \tag{77}$$

$$\left[\left(U_A\otimes U_B\right)e^{-\frac{i}{2}(\lambda_1\sigma_{ZI}+\omega_1\sigma_{IZ})}\left(U_A^\dagger\otimes U_B^\dagger\right)\right]\left[\left(U_A\otimes U_B\right)\left(P_1\otimes P_1\right)\left(U_A^\dagger\otimes U_B^\dagger\right)\right]\left[\left(U_A\otimes U_B\right)e^{-\frac{i}{2}(\lambda_3\sigma_{ZI}+\omega_3\sigma_{IZ})}\left(U_A^\dagger\otimes U_B^\dagger\right)\right] = \tag{78}$$

$$\left(U_Ae^{-\frac{i}{2}(\lambda_1\sigma_Z)}U_A^\dagger\right)\left(U_AP_1U_A^\dagger\right)\left(U_Ae^{-\frac{i}{2}(\lambda_3\sigma_Z)}U_A^\dagger\right)\otimes\left(U_Be^{-\frac{i}{2}(\omega_1\sigma_Z)}U_B^\dagger\right)\left(U_BP_1U_B^\dagger\right)\left(U_Be^{-\frac{i}{2}(\omega_3\sigma_Z)}U_B^\dagger\right). \tag{79}$$

Since, in general, $\lambda_1\neq\lambda_3$ and $\omega_1\neq\omega_3$, (79) is equal to a tensor product of two Pauli gates if U_A and $U_B\in C_1$ and $\lambda_{1,3} = n_{1,3}\pi$ and $\omega_{1,3} = m_{1,3}\pi$ ($n_{1,3}$ and $m_{1,3}$ are integer numbers), hence, the exponentials in (79) are also Pauli gates. Now, returning to (73) one readily sees that U_C and $U_D\in C_1$.

7.3 ($\varepsilon_x = 0$, $\varepsilon_y = 1$, $\varepsilon_z = 0$)

In this case, one has

$$U_{NL} = e^{i(2k_Y+1)\frac{\pi}{4}\sigma_{YY}} \tag{80}$$

$$\left(U_C\otimes U_D\right)\left(\sigma_\mu\otimes\sigma_\nu\right)\left(U_C^\dagger\otimes U_D^\dagger\right) = P_1e^{-\frac{i}{2}(\lambda_2\sigma_Y)}P_1\otimes P_1e^{-\frac{i}{2}(\omega_2\sigma_Y)}P_1, \tag{81}$$

hence,

$$U_{NL}\left(U_C\otimes U_D\right)\left(\sigma_\mu\otimes\sigma_\nu\right)\left(U_C^\dagger\otimes U_D^\dagger\right)U_{NL}^\dagger = U_{NL}P_1e^{-\frac{i}{2}(\lambda_2\sigma_Y)}P_1\otimes P_1e^{-\frac{i}{2}(\omega_2\sigma_Y)}P_1U_{NL}^\dagger = \tag{82}$$

$$U_{NL}\left[\left(P_1\otimes P_1\right)\left(e^{-\frac{i}{2}(\lambda_2\sigma_Y)}\otimes e^{-\frac{i}{2}(\omega_2\sigma_Y)}\right)\left(P_1\otimes P\right)_1\right]U_{NL}^\dagger = \tag{83}$$

$$\left[U_{NL}\left(P_1\otimes P_1\right)U_{NL}^\dagger\right]\left(e^{-\frac{i}{2}(\lambda_2\sigma_Y)}\otimes e^{-\frac{i}{2}(\omega_2\sigma_Y)}\right)\left[U_{NL}\left(P_1\otimes P_1\right)U_{NL}^\dagger\right] = \left(P_1\otimes P_1\right)\left(e^{-\frac{i}{2}(\lambda_2\sigma_Y)}\otimes e^{-\frac{i}{2}(\omega_2\sigma_Y)}\right)\left(P_1\otimes P_1\right). \tag{84}$$

At last,

$$\left[\left(U_A\otimes U_B\right)U_{NL}\left(U_C\otimes U_D\right)\right]\left(\sigma_\mu\otimes\sigma_\upsilon\right)\left[\left(U_C^\dagger\otimes U_D^\dagger\right)U_{NL}^\dagger\left(U_A^\dagger\otimes U_B^\dagger\right)\right]= \tag{85}$$

$$\left(U_A\otimes U_B\right)\left[\left(P_1\otimes P_1\right)\left(e^{-\frac{i}{2}(\lambda_2\sigma_Y)}\otimes e^{-\frac{i}{2}(\omega_2\sigma_Y)}\right)\left(P_1\otimes P_1\right)\right]\left(U_A^\dagger\otimes U_B^\dagger\right)= \tag{86}$$

$$\left[\left(U_A\otimes U_B\right)\left(P_1\otimes P_1\right)\left(U_A^\dagger\otimes U_B^\dagger\right)\right]\left[\left(U_A\otimes U_B\right)\left(e^{-\frac{i}{2}(\lambda_2\sigma_Y)}\otimes e^{-\frac{i}{2}(\omega_2\sigma_Y)}\right)\left(U_A^\dagger\otimes U_B^\dagger\right)\right]\left[\left(U_A\otimes U_B\right)\left(P_1\otimes P_1\right)\left(U_A^\dagger\otimes U_B^\dagger\right)\right]= \tag{87}$$

$$\left(U_AP_1U_A^\dagger\right)\left(U_Ae^{-\frac{i}{2}(\lambda_2\sigma_Y)}U_A^\dagger\right)\left(U_AP_1U_A^\dagger\right)\otimes\left(U_BP_1U_B^\dagger\right)\left(U_Be^{-\frac{i}{2}(\omega_2\sigma_Y)}U_B^\dagger\right)\left(U_BP_1U_B^\dagger\right). \tag{88}$$

Equation (88) is equal to a tensor product of two Pauli gates if U_A and $U_B\in C_1$ and $\lambda_2 = n_2\pi$ and $\omega_2 = m_2\pi$ (n_2 and m_2 are integer numbers), hence, the exponentials in (88) are also Pauli gates. Now, returning to (81) one readily sees that U_C and $U_D \in C_1$.

7.4 ($\varepsilon_x = 1$, $\varepsilon_y = 1$, $\varepsilon_z = 1$) & ($k_x = k_y = k_z$)

In this case, one has

$$U_{NL} = e^{i(2k+1)\frac{\pi}{4}\sigma_{XX}+(2k+1)\frac{\pi}{4}\sigma_{YY}+(2k+1)\frac{\pi}{4}\sigma_{ZZ}}. \tag{89}$$

The gate U_{NL} given in (89) is the SWAP gate (multiplied by ±1 or ±i), hence,

$$\left(U_A\otimes U_B\right)U_{NL}\left(U_C\otimes U_D\right)=\left(U_DU_A\otimes U_CU_B\right)U_{NL}=\left(U_A'\otimes U_B'\right)U_{NL}. \tag{90}$$

Thus,

$$\left(U_A'\otimes U_B'\right)U_{NL}\left(\sigma_\mu\otimes\sigma_\nu\right)U_{NL}^\dagger\left(U_A'^\dagger\otimes U_B'^\dagger\right)=\left(U_A'\otimes U_B'\right)\left(P_1\otimes P_1\right)\left(U_A'^\dagger\otimes U_B'^\dagger\right). \tag{91}$$

Equation (91) is equal to a tensor product of two Pauli gates if U_A' and $U_B'\in C_1$.

Summarizing, a (non-separable) two-qubit Clifford gate has a decomposition formed by a non-local part given by (63) and local parts by C_1 gates. Now, one has that a single-qubit gate belongs to C_1 if (the ±1 or ±i factor in the right side was not considered)

$$e^{-\frac{i}{2}\lambda_1\sigma_\mu}e^{-\frac{i}{2}\lambda_2\sigma_\upsilon}e^{-\frac{i}{2}\lambda_3\sigma_\mu}\sigma_\xi e^{\frac{i}{2}\lambda_3\sigma_\mu}e^{\frac{i}{2}\lambda_2\sigma_\upsilon}e^{\frac{i}{2}\lambda_1\sigma_\mu}=\sigma_\eta. \tag{92}$$

However, it can be checked that

$$e^{-\frac{i}{2}\lambda\sigma_\mu}\sigma_\upsilon e^{\frac{i}{2}\lambda\sigma_\mu}=\sigma_\eta\ \forall\ \mu,\upsilon,\eta\in\{X,Y,Z\},\mu\neq\upsilon,\ \Rightarrow\lambda=k\pi/2, \tag{93}$$

where k is an integer number. The cases $\lambda = 0$ and $\mu = \upsilon$ have trivial solution. Hence, any C_1 gate has a decomposition of the form

$$e^{i\theta} e^{-\frac{i}{2}\left(k_1\frac{\pi}{2}\right)\sigma_\mu} e^{-\frac{i}{2}\left(k_2\frac{\pi}{2}\right)\sigma_\upsilon} e^{-\frac{i}{2}\left(k_3\frac{\pi}{2}\right)\sigma_\mu}, \tag{94}$$

where θ is a global phase. Finally, any (C_2) Clifford gate has a decomposition of the form

$$\begin{aligned} U = {} & e^{-\frac{i}{2}\left[\left(n_1\frac{\pi}{2}\right)\sigma_{\mu I}+\left(n_2\frac{\pi}{2}\right)\sigma_{I\mu}\right]} e^{-\frac{i}{2}\left[\left(n_3\frac{\pi}{2}\right)\sigma_{\upsilon I}+\left(n_4\frac{\pi}{2}\right)\sigma_{I\upsilon}\right]} e^{-\frac{i}{2}\left[\left(n_5\frac{\pi}{2}\right)\sigma_{\mu I}+\left(n_6\frac{\pi}{2}\right)\sigma_{I\mu}\right]} \\ & e^{i\left[\varepsilon_x(2k_x+1)\frac{\pi}{4}\sigma_{XX}+\varepsilon_y(2k_y+1)\frac{\pi}{4}\sigma_{YY}+\varepsilon_z(2k_z+1)\frac{\pi}{4}\sigma_{ZZ}\right]} \\ & e^{-\frac{i}{2}\left[\left(m_1\frac{\pi}{2}\right)\sigma_{\mu I}+\left(m_2\frac{\pi}{2}\right)\sigma_{I\mu}\right]} e^{-\frac{i}{2}\left[\left(m_3\frac{\pi}{2}\right)\sigma_{\upsilon I}+\left(m_4\frac{\pi}{2}\right)\sigma_{I\upsilon}\right]} e^{-\frac{i}{2}\left[\left(m_5\frac{\pi}{2}\right)\sigma_{\mu I}+\left(m_6\frac{\pi}{2}\right)\sigma_{I\mu}\right]} \\ & \varepsilon_{x,y,z} = 0,1;\ k_{x,y,z}, n_{1,\ldots,6}, m_{1,\ldots,6} = 0, \pm1, \pm2, \ldots \end{aligned} \tag{95}$$

Obviously, one expects to find decompositions of the generators of C_1 and C_2 in the forms given, respectively, by (94) and (95). In fact such decompositions are

$$CNOT = e^{-\frac{i}{2}\left(-\frac{3\pi}{2}\sigma_{ZI}+\frac{\pi}{2}\sigma_{IZ}\right)} e^{-\frac{i}{2}\left(\frac{3\pi}{2}\sigma_{YI}+\frac{3\pi}{2}\sigma_{IY}\right)} e^{-\frac{i}{2}\left(-\frac{\pi}{2}\sigma_{IZ}\right)} \left(e^{i\frac{\pi}{4}} e^{i\frac{\pi}{4}\sigma_{XX}} \right) e^{-\frac{i}{2}(\pi\sigma_{IZ})} e^{-\frac{i}{2}\left(\frac{\pi}{2}\sigma_{YI}\right)} e^{-\frac{i}{2}(-2\pi\sigma_{ZI}-\pi\sigma_{IZ})} \tag{96}$$

$$H = e^{i\frac{\pi}{2}} e^{-\frac{i}{2}\left(\frac{\pi}{2}\sigma_Y\right)} e^{-\frac{i}{2}(\pi\sigma_Z)} \tag{97}$$

$$S = e^{i\frac{\pi}{4}} e^{-\frac{i}{2}(\pi\sigma_Z)} e^{-\frac{i}{2}\left(-\frac{\pi}{2}\sigma_Y\right)} e^{-\frac{i}{2}(-\pi\sigma_Z)}. \tag{98}$$

Using (96)-(98), it can be shown that any two-qubit gate constructed using the gates CNOT, H and S will have the decomposition given by (95).

At last, in the supplementary material of [14] it was shown that the two-qubit Clifford operations can be divided in four classes. These classes are divided according to the use of C_1 gates and the two-qubit gates CNOT, SWAP and ISWAP. The decomposition of SWAP and ISWAP gates are

$$SWAP = e^{-i\frac{\pi}{4}} e^{i\left(\frac{\pi}{4}\sigma_{XX}+\frac{\pi}{4}\sigma_{YY}+\frac{\pi}{4}\sigma_{ZZ}\right)} \tag{99}$$

$$ISWAP = e^{-\frac{i}{2}\left(-\frac{\pi}{2}\sigma_{IZ}\right)} e^{-\frac{i}{2}(-\pi\sigma_{YI}+\pi\sigma_{IY})} e^{-\frac{i}{2}\left(-\frac{\pi}{2}\sigma_{ZI}-\frac{\pi}{2}\sigma_{IZ}\right)} e^{i\left(\frac{\pi}{4}\sigma_{XX}+\frac{\pi}{4}\sigma_{YY}\right)} e^{-\frac{i}{2}\left(-\frac{\pi}{2}\sigma_{ZI}-\frac{\pi}{2}\sigma_{IZ}\right)} e^{-\frac{i}{2}(-\pi\sigma_{YI}+\pi\sigma_{IY})} e^{-\frac{i}{2}\left(-\frac{\pi}{2}\sigma_{ZI}-\pi\sigma_{IZ}\right)}, \tag{100}$$

showing that this result is also in agreement with our Clifford decomposition given by (95).

8. Conclusions

Summarizing, this work discussed: I) the sufficient conditions for a two-qubit quantum gate to be teleported by a quantum circuit having as resource two bell states and a given basis of measurement; II) the teleportation of gates out of

Clifford group; III) the quantum gate teleportation using a four-qubit state with genuine four-way entanglement. From the work done, we conclude that:

1. The Theorem 1 gives the sufficient conditions for a quantum gate U_T to be teleported when a given basis is used. In particular, from the best of our knowledge, the teleportation of gates out of Clifford group was demonstrated by the first time.

2. The basis used in the measurement plays a crucial role. Two important points are: 1) Any basis that produces a unitary matrix $\beta_j = I$ (like the Bell basis), has teleportation capability larger than zero. In this case, the lowest success probability is 1/16; 2) Any basis having at least one disentangled state has teleportation capability equal to zero: if the basis' state $|\beta_j\rangle$ is disentangled, then $\det(\beta_j) = 0$ and β_j is, obviously, not unitary.

3. From Theorem 1 one gets that any Clifford gate has non-local part with angles $(2k+1)\pi/4$ (k is an integer number) and local single-qubits gates belonging to C_1. Any two-qubit Clifford gate has decomposition as given by equation (95). From the best of our knowledge this is the first time that a formula for construction of Clifford gates is provided.

Acknowledgment

This work was supported by the Brazilian agency CNPq via Grant no. 303514/2008-6. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

1. Bennet, C. H., Brassard, G., Crépeau, C., Josza, R., peres, A., and Wooters, W. K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett., 70, 13, 1895 (1993).
2. Zhan-Jun, Z., Yu-Min, L., and Zhong-Xiao, M.: Many-agent controlled teleportation of multi-qubit quantum information via quantum entanglement swapping, Comm. in Theor. Phys., 44, 5, 847 (2005).
3. Chen, L., Lu, H., and Chen, W.: Constructing a universal set of quantum gates via probabilistic teleportation, Chin. Opt. Lett., 3, 4, 240 (2005).
4. Gottesman, D., and Chuang, I. L.: Quantum teleportation is a universal computational primitive, Nature, 402, 390 (1999).
5. Mendes F. V., and Ramos, R. V.: Schemes for teleportation of quantum gates, Quant. Inf. Process., 10, 203 (2011).
6. Huang, Y.-F., Ren, X.-F., Zhang, Y.-S., Duan, L.-M., and Guo, G.-C.: Experimental Teleportation of a Quantum Controlled-NOT Gate, Phys. Rev. Lett., 93, 240501 (2004).
7. Slodička, L., Ježek, M., and Fiurášek, J.: Experimental demonstration of a teleportation-based programmable quantum gate, Phys. Rev. A, 79, 050304R (2009).
8. Gaoa, W.-B., Goebelb, A. M., Lua, C.-Y., Daia, H.-N., Wagenknechtb, C., Zhanga, Q., Zhaoa, B., Penga, C.-Z., Chena, Z.-B., Chena, Y.-A., and Pan. J.-W.: Teleportation-based realization of an optical quantum two-qubit entangling gate, PNAS, 107, 49, 20869-20874 (2010).
9. Stenholm, S., and Bardroff, P. J.: Teleportation of N-dimensional states, Phys. Rev. A, 58, 4373 (1998).
10. Xi, X.-Q., Hao, S.-R., Hou, B.-Y., and Yue, R. H.: Quantum standard teleportation based on generic measurement bases, Comm. in Theor. Phys., 40, 415 (2003).
11. Tucci, R. R.: An introduction to Cartan's KAK decomposition for QC programmers, arXiv:quant-ph/0507171 (2005).
12. Yeo, Y. and Chua W. K.: Teleportation and dense coding with genuine multipartite entanglement, Phys. Rev. Lett. 96, 060502/1-4 (2006).
13. Backens, M.: The ZX-calculus is complete for stabilizers quantum mechanics, arXiv:quant-ph/13077025 (2013).
14. Córcoles, A. D., Gambetta, J. M., Chow, J. M., and Smolin, J. A: Process verification of two-qubit quantum gates by randomized benchmarking, Phys. Rev. A 87, 030301 (2013).

2. **On the Role of the Four-Qubit State in Two-Qubit Gate Teleportation**

   - ◇ Periódico: Quantum Information Processing
   - ◇ Data: 20/05/2014
   - ◇ Situação: Submetido

On the Role of the Four-Qubit State in Two-Qubit Gate Teleportation

P. R. M. Sousa, F. V. Mendes and R. V. Ramos
pauloregisms@gmail.com fernandovm@gmail.com rubens.viana@pq.cnpq.br

Lab. of Quantum Information Technology, Department of Teleinformatic Engineering – Federal University of Ceara - DETI/UFC, C.P. 6007 – Campus do Pici - 60455-970 Fortaleza-Ce, Brazil.

The complete understanding of circuits for quantum protocols requires the knowledge of the role of the quantum states, bases of measurement and quantum unitary operations involved. In what concerns the famous two-qubit quantum gate teleportation protocol, the role of the basis of measurement has been considered in a recent work by Mendes and Ramos. In this work, we analyze the role of the four-qubit state used as resource. We show that using different types of four-qubit states, the teleportation of the action of a two-qubit gate in a given two-qubit state changes for a probabilistic teleportation of the action of a two-qubit gate in a set of states.

1. Introduction

Two-qubit quantum gate teleportation is an important quantum protocol proposed by Gottesmann and Chuang [1]. In their work, they proved that any Clifford gate is deterministically teleported by a quantum teleportation scheme employing a pair of Bell states and Bell basis in the measurements, what results in error correction based on Pauli matrices. More recently, the role of the basis of measurement in two-qubit quantum gate teleportation was investigated and the conditions for a deterministic teleportation, including gates out of Clifford group, were established [2]. In that work, however, the quantum sate used as resource was still a pair of Bell states.

In the present work, we analyze the two-qubit quantum teleportation circuit using as resource a general four-qubit state. It is shown how the two-qubit gate teleported and the protocol's result depend on the four-qubit state used. In particular, we present the case where the probabilistic teleportation of the action of the two-qubit gate in the canonical basis ($|00\rangle$,$|01\rangle$,$|10\rangle$,$|11\rangle$) is achieved. Furthermore, some specific examples using maximally entangled four-qubit states found in the literature are presented.

The rest of the present work is outlined as follows: In Section 2 it is introduced the Υ matrix that is responsible for the definition of the gate to be teleported; In Section 3 the two-qubit gate teleportation using a general four-qubit state is described and several examples of teleportation are presented; At last, the conclusions are drawn in Section 4.

2. The matrix Υ

Let $|\sigma\rangle$ be a general four-qubit state,

$$|\sigma\rangle = \sum_{k,l,m,n=0}^{1} \sigma_{klmn} |klmn\rangle = \sum_{i=0}^{15} \sigma_i |i\rangle. \quad (1)$$

Using the coefficients of $|\sigma\rangle$ one can get the Υ matrix

$$\Upsilon = \begin{bmatrix} \sigma_0 & \sigma_1 & \sigma_8 & \sigma_9 \\ \sigma_2 & \sigma_3 & \sigma_{10} & \sigma_{11} \\ \sigma_4 & \sigma_5 & \sigma_{12} & \sigma_{13} \\ \sigma_6 & \sigma_7 & \sigma_{14} & \sigma_{15} \end{bmatrix}. \quad (2)$$

Considering the use of (1) in two-qubit gate teleportation, we are interested in two situations: 1) $\Upsilon = 1/2U_\sigma$, where U_σ is a unitary matrix; 2) Υ is normal ($[\Upsilon,\Upsilon^\dagger]=0$) but 2Υ is not unitary or Υ is not normal. It will be shown latter that the type of teleportation achieved depends on the type of Υ matrix. The determinant of Υ is an invariant [3] that can be used (together with other invariants) to define classes of four-qubit states. For example, according to the classification given in [4] there are 16 classes: 1, 2a, 2b, 2c, 2d, 3a, 3b, 3c, 3d, 3e, 3f, 4a, 4b, 4c, 4d and 5. Table 1 shows, for each one of these classes, the canonical state, its four-way entanglement measured by π_4 [5], the type of Υ matrix and the value of det(Υ).

Class	State	π_4	Type	det(Υ)
1	$\lvert\psi_1\rangle = 1/\sqrt{2}\left(\lvert0000\rangle + \lvert0111\rangle\right)$	0	Ñ	0
2a	$\lvert\psi_{2a}\rangle = 1/\sqrt{2}\left(\lvert0000\rangle + \lvert1111\rangle\right)$	1	N	0
2b	$\lvert\psi_{2b}\rangle = 1/2\left(\lvert0000\rangle + \lvert0101\rangle + \lvert1010\rangle - \lvert1111\rangle\right)$	1	U	1/16
2c	$\lvert\psi_{2c}\rangle = 1/2\left(\lvert0000\rangle + \lvert0110\rangle + \lvert1001\rangle - \lvert1111\rangle\right)$	1	N	1/16
2d	$\lvert\psi_{2d}\rangle = 1/\sqrt{6}\left(\lvert0001\rangle + \lvert0010\rangle + \lvert0100\rangle + \lvert1000\rangle + \sqrt{2}\lvert1111\rangle\right)$	1	N	0
3a	$\lvert\psi_{3a}\rangle = 1/2\left(\lvert0000\rangle + \lvert0101\rangle + \lvert1010\rangle + \lvert1111\rangle\right)$	0	U	-1/16
3b	$\lvert\psi_{3b}\rangle = 1/2\left(\lvert0000\rangle + \lvert0011\rangle + \lvert1100\rangle + \lvert1111\rangle\right)$	0	U	1/16
3c	$\lvert\psi_{3c}\rangle = 1/\sqrt{6}\left(\lvert0000\rangle + \lvert0101\rangle + \lvert0110\rangle + \lvert1001\rangle + \lvert1010\rangle + \lvert1111\rangle\right)$	0.1975	N	0
3d	$\lvert\psi_{3d}\rangle = \frac{1}{\sqrt{8}}\left(\begin{array}{l}\lvert0000\rangle - \lvert0011\rangle + \lvert0101\rangle + \lvert0110\rangle + \\ \lvert1001\rangle - \lvert1010\rangle + \lvert1100\rangle + \lvert1111\rangle\end{array}\right)$	1	Ñ	0
3e	$\lvert\psi_{3e}\rangle = 1/3\left(\lvert0000\rangle + \lvert0101\rangle - 2\lvert0110\rangle + \lvert1001\rangle + \lvert1010\rangle + \lvert1111\rangle\right)$	0.6243	Ñ	-1/27
3f	$\lvert\psi_{3f}\rangle = 1/3\left(\lvert0000\rangle + \lvert0011\rangle - 2\lvert0101\rangle + \lvert1010\rangle + \lvert1100\rangle + \lvert1111\rangle\right)$	0.6243	Ñ	1/27
4a	$\lvert\psi_{4a}\rangle = 1/\sqrt{17}\left(\lvert0000\rangle + \lvert0011\rangle + 3\lvert0101\rangle + \lvert1010\rangle - 2\lvert1100\rangle + \lvert1111\rangle\right)$	0.1217	Ñ	-5/289
4b	$\lvert\psi_{4b}\rangle = 1/\sqrt{12}\left(\lvert0000\rangle + 2\lvert0011\rangle + \lvert0101\rangle + \lvert1010\rangle + 2\lvert1100\rangle + \lvert1111\rangle\right)$	0.0625	N	1/48
4c	$\lvert\psi_{4c}\rangle = 1/\sqrt{12}\left(\lvert0000\rangle + \lvert0011\rangle + 2\lvert0101\rangle + 2\lvert1010\rangle + \lvert1100\rangle + \lvert1111\rangle\right)$	0.0625	N	-1/48
4d	$\lvert\psi_{4d}\rangle = 1/3\left(2\lvert0000\rangle - \lvert0011\rangle - \lvert0101\rangle + \lvert1010\rangle + \lvert1100\rangle + \lvert1111\rangle\right)$	0.6243	Ñ	0
5	$\lvert\psi_5\rangle = 1/\sqrt{12}\left(\lvert0000\rangle + \lvert0011\rangle + \lvert0101\rangle + 2\lvert1010\rangle + 2\lvert1100\rangle + \lvert1111\rangle\right)$	0.0560	Ñ	0

Table 1 - Type of Υ matrix for the canonical states of the classification of four-qubit states given in [4]. U - 2Υ is unitary; N – Υ is normal but 2Υ is not unitary; Ñ - Υ is not normal.

An interesting question that may arise is about the distribution of the four-way entanglement, measured by π_4, of the four-qubit state $|\sigma\rangle$ that comes from Υ when the last is randomly obtained. Let us consider two cases: 1) $\Upsilon = 1/2U_\sigma$ and 2) Υ is normal but 2Υ is not unitary. For the first case, we estimate that distribution by using a million of U_σ gates obtained from an ensemble of random unitary matrices. This ensemble consists of all unitary matrices with the natural Haar measure on the group $U(4)$. Such matrices are produced in the following way [6-8]:

$$U_\sigma = U^{(1,2)}(\varphi_{12},\psi_{12},\theta_{12})U^{(2,3)}(\varphi_{23},\psi_{23},0)U^{(1,3)}(\varphi_{13},\psi_{13},\theta_{13})U^{(3,4)}(\varphi_{34},\psi_{34},0)\times \\ U^{(2,4)}(\varphi_{24},\psi_{24},0)U^{(1,4)}(\varphi_{14},\psi_{14},\theta_{14}) \tag{3}$$

where $U^{(i,j)}$, i,j=1,2,3,4, are complex matrices with three real parameters, ϕ,ψ and θ. Their rule of formation is:

$$U_{kl}^{(i,j)}(\phi,\psi,\theta) = \begin{cases} 1, & k=l, k\neq i, j \\ \sin(\phi)e^{i\theta}, & k=i, l=j \\ \cos(\phi)e^{i\psi}, & k=l=i \\ \cos(\phi)e^{-i\psi}, & k=l=j \\ -\sin(\phi)e^{-i\theta}, & k=j, l=i \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

The angles ψ and θ are random variables uniformly distributed in the interval $[0,2\pi)$, while the angles ϕ are obtained from $\phi_{ij} = \arcsin\left(\varepsilon^{1/(2i)}\right)$, i=1,2,3, where ε is a random variable uniformly distributed in the interval [0,1). The relative frequency of $\pi_4(|\sigma\rangle)$ can be seen in Fig. 1.

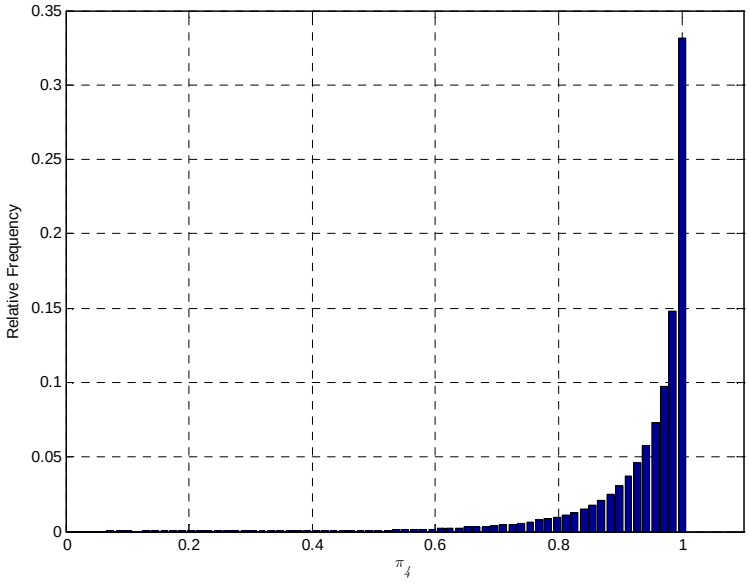


Fig. 1. Relative frequency of $\pi_4(|\sigma\rangle)$, for U_σ taken from an ensemble of random (4x4) unitary matrices.

As it can be noted in Fig. 1, most of the four-qubit states obtained are highly entangled state.

Now we turn to the second case. Since Υ is normal it can be diagonalized, $\Upsilon = U^\dagger DU$, where D is a diagonal matrix having as entries the eigenvalues of Υ. By using (2) one can easily note that

$$Tr\left(\Upsilon\Upsilon^{\dagger}\right)=\sum_{i=0}^{15}\left|\sigma_i\right|^2=Tr\left(DD^{\dagger}\right)=1 \tag{5}$$

and, hence, $\sum_{i=0}^{3}\left|\lambda_i\right|^2=1$, where λ_i (i = 0,1,2,3) are the eigenvalues of Υ. We estimate the distribution of the four-way entanglement π_4 by using a million of four-qubit states $|\sigma\rangle$ obtained from $\Upsilon = U^{\dagger}DU$, where once more U is chosen randomly from the ensemble of all unitary matrices with the natural Haar measure on the group $U(4)$, as explained before, and the matrix D is a diagonal matrix whose elements are $D_{kk} = (d_{kk})^{1/2}\exp(i\theta_k)$ (k = 1, 2 and 3), where θ_k is uniformly distributed in the interval $[-\pi,\pi]$ and

$$d_{11}=1-\xi_1^{1/3} \tag{6}$$
$$d_{22}=\left(1-\xi_2^{1/2}\right)(1-d_{11}) \tag{7}$$
$$d_{33}=\left(1-\xi_3\right)(1-d_{11}-d_{22}) \tag{8}$$
$$d_{44}=1-d_{11}-d_{22}-d_{33}. \tag{9}$$

In (6)-(8) $\xi_{1\text{-}3}$ are also random variables distributed uniformly in the interval [0,1). Equations (6)-(9) ensure the D's elements are uniformly distributed on the manifold defined by $\sum_i\left|D_{ii}\right|^2=1$ [6-8]. The plot of the relative frequency of $\pi_4(|\sigma\rangle)$ is shown in Fig. 2.

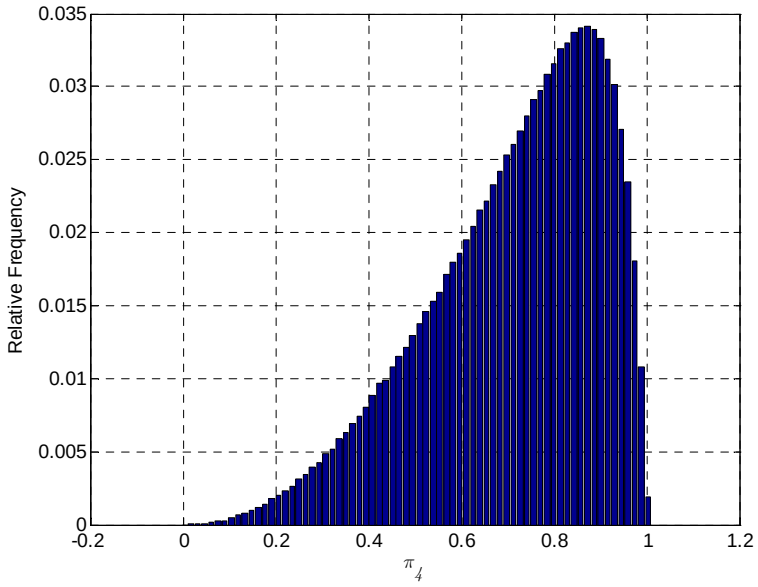


Fig. 2. Relative frequency of $\pi_4(|\sigma\rangle)$, where σ is obtained from matrices $\Upsilon = U^{\dagger}DU$ randomly obtained.

3. Teleportation of two-qubit quantum gates

The scheme for teleportation of two-qubit quantum gates considering a general four-qubit state is shown in Fig. 3.

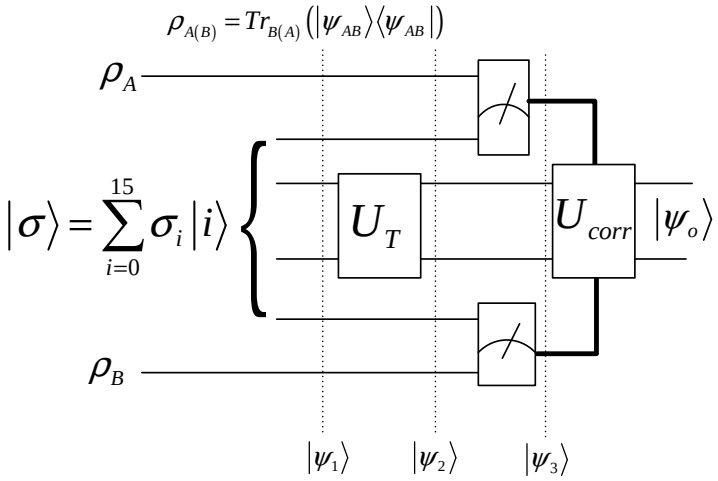


Fig. 3. Circuit for teleportation of a two-qubit quantum gate using a general four-qubit state.

The four-qubit state $|\sigma\rangle$ carries the entanglement required for the teleportation protocol. Following the procedure used in [2], after some algebra one can get that the output state before error correction is

$$|\psi_o\rangle = \sum_{j,k=0}^{3} \frac{1}{2} U_T \Upsilon \beta_{jk} |\psi_{AB}\rangle \tag{10}$$

$$\beta_{jk} = \beta_j \otimes \beta_k = \sqrt{2}\begin{bmatrix} \langle\beta_j|00\rangle & \langle\beta_j|10\rangle \\ \langle\beta_j|01\rangle & \langle\beta_j|11\rangle \end{bmatrix} \otimes \sqrt{2}\begin{bmatrix} \langle\beta_k|00\rangle & \langle\beta_k|10\rangle \\ \langle\beta_k|01\rangle & \langle\beta_k|11\rangle \end{bmatrix}. \tag{11}$$

In (10)-(11) $\{|\beta_1\rangle,|\beta_2\rangle,|\beta_3\rangle,|\beta_4\rangle\}$ is the used basis of measurement. The newness in the present work is the presence of the matrix Υ discussed in Section 2. Let us start by considering the case where $\Upsilon = 1/2U_\sigma$. In this case, one has

$$|\psi_o\rangle = \sum_{j,k=0}^{3} \frac{1}{4} U_T U_\sigma \beta_{jk} |\psi_{AB}\rangle, \tag{12}$$

and a teleportation succeeds if

$$|\psi_o\rangle = \sum_{j,k=0}^{3} \frac{1}{4} U_T U_\sigma \beta_{jk} |\psi_{AB}\rangle = \sum_{j,k=0}^{3} \frac{1}{4} \left(U_T U_\sigma \beta_{jk} U_\sigma^\dagger U_T^\dagger\right) U_T U_\sigma |\psi_{AB}\rangle = \sum_{j,k=0}^{3} \frac{1}{4} \left(V_j \otimes V_k\right) U_T U_\sigma |\psi_{AB}\rangle, \tag{13}$$

where V_j and V_k are single-qubit gates. Applying the error correction $U_{corr} = \left(V_j^\dagger \otimes V_k^\dagger\right)$ one gets as output state $U_T U_\sigma |\psi_{AB}\rangle$. Equation (13) makes clear the role of the four-qubit state in the final result of the teleportation: the teleported gate is $U_T U_\sigma$ where $U_\sigma = 2\Upsilon$ depends on the four-qubit state. Equation (13) also gives us another point of view about the two-qubit gate teleportation: one can make $U_T = I$ and get a desired quantum gate teleportation by choosing the suitable four-qubit state. The probability of success of the teleportation will depend on the basis of measurement used, as explained by Theorem 1 of [2]. Hence, hereafter we will consider $U_T = I$. It can be easily shown that the four-qubit state required for teleportation of the gate U_σ is the state

$$|\sigma\rangle = (I \otimes U_\sigma \otimes I)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right). \quad (14)$$

.

According to KAK decomposition [9], one has that

$$U_\sigma = (U_A \otimes U_B) U_{NL} (U_C \otimes U_D) \quad (15)$$

$$U_{NL} = e^{i(\theta_x \sigma_{XX} + \theta_y \sigma_{YY} + \theta_z \sigma_{ZZ})}, \quad (16)$$

where U_A, U_B, U_C and U_D are local single-qubit gates, U_{NL} is the non-local part and $\sigma_{jj}=\sigma_j \otimes \sigma_j$ ($j=X, Y, Z$) is the tensor product of two Pauli matrices. The following statements follow directly from (14)-(16):

1. The four-way entanglement of $|\sigma\rangle$, measured by π_4, depends only on the non-local part of U_σ. In particular, if the four-qubit state $|\sigma\rangle$ has zero four-way entanglement, then the gate U_σ has $\theta_x = \theta_y = \theta_z = 0$, and, hence, it is separable in the tensor product of two single-qubit gates.
2. According to Theorem 1 in [2], the quantum gate U_σ can be deterministically teleported only if each angle θ_x, θ_y and θ_z is equal to 0 or $(2k+1)\pi/4$ (k is an integer number). However, in this situation (except in the obvious case where $\theta_x = \theta_y = \theta_z = 0$) $|\sigma\rangle$ is maximally entangled ($\pi_4 = 1$), hence, a necessary (but not sufficient) condition for deterministic teleportation of U_σ is that it comes from a maximally four-way entangled state $|\sigma\rangle$. On the other hand, as it will be seen latter, a maximally four-way entangled state $|\sigma\rangle$ does not always generates a deterministically teleportable quantum gate U_σ.

The case $\Upsilon = 1/2U_\sigma$ is the classical case considered in [1], where the four-qubit state is the tensor product of the two Bell states $|\sigma\rangle=(|00\rangle+|11\rangle)/2^{1/2}\otimes(|00\rangle+|11\rangle)/2^{1/2}$, what makes $U_\sigma = I$ (identity gate) and, hence, the gate teleported, as shown in Fig. 1, is U_T via the state $(I\otimes U_T\otimes I)$ $(|00\rangle+|11\rangle)/2^{1/2}\otimes(|00\rangle+|11\rangle)/2^{1/2}$.

Now, we turn to the case where 2Υ is not unitary but Υ is normal, hence, $\Upsilon = UDU^\dagger$. The output state is

$$\rho_o = \sum_{j,k=0}^{3} \frac{1}{4} |\psi_0^{jk}\rangle\langle\psi_0^{jk}| = \sum_{j,k=0}^{3} \frac{1}{4} \frac{\Upsilon\beta_{jk}|\psi_{ab}\rangle\langle\psi_{ab}|\beta_{jk}^\dagger\Upsilon^\dagger}{\langle\psi_{ab}|\beta_{jk}^\dagger\Upsilon^\dagger\Upsilon\beta_{jk}|\psi_{ab}\rangle} \quad (17)$$

$$|\psi_0^{jk}\rangle = \frac{1}{\sqrt{\langle\psi_{ab}|\beta_{jk}^\dagger U \begin{bmatrix} |\lambda_0|^2 & 0 & 0 & 0 \\ 0 & |\lambda_1|^2 & 0 & 0 \\ 0 & 0 & |\lambda_2|^2 & 0 \\ 0 & 0 & 0 & |\lambda_3|^2 \end{bmatrix} U^\dagger \beta_{jk}|\psi_{ab}\rangle}} U \begin{bmatrix} \lambda_0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 \\ 0 & 0 & 0 & \lambda_3 \end{bmatrix} U^\dagger \beta_{jk}|\psi_{ab}\rangle \Rightarrow \quad (18)$$

$$|\psi_0^{jk}\rangle = U\left(\frac{\lambda_0\langle 00|U^\dagger\beta_{jk}|\psi_{ab}\rangle|00\rangle + \lambda_1\langle 01|U^\dagger\beta_{jk}|\psi_{ab}\rangle|01\rangle + \lambda_2\langle 10|U^\dagger\beta_{jk}|\psi_{ab}\rangle|10\rangle + \lambda_3\langle 11|U^\dagger\beta_{jk}|\psi_{ab}\rangle|11\rangle}{\sqrt{|\lambda_0\langle 00|U^\dagger\beta_{jk}|\psi_{ab}\rangle|^2 + |\lambda_1\langle 01|U^\dagger\beta_{jk}|\psi_{ab}\rangle|^2 + |\lambda_2\langle 10|U^\dagger\beta_{jk}|\psi_{ab}\rangle|^2 + |\lambda_3\langle 11|U^\dagger\beta_{jk}|\psi_{ab}\rangle|^2}}\right). \quad (19)$$

In (18)-(19), λ_i (i = 0,1,2,3,4) are the eigenvalues of Υ. Equation (19) can still be rewritten as

$$\left|\psi_0^{jk}\right\rangle = U\left(\frac{\lambda_0\langle 00|V_{jk}U^\dagger|\psi_{ab}\rangle|00\rangle + \lambda_1\langle 01|V_{jk}U^\dagger|\psi_{ab}\rangle|01\rangle + \lambda_2\langle 10|V_{jk}U^\dagger|\psi_{ab}\rangle|10\rangle + \lambda_3\langle 11|V_{jk}U^\dagger|\psi_{ab}\rangle|11\rangle}{\sqrt{\left|\lambda_0\langle 00|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2 + \left|\lambda_1\langle 01|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2 + \left|\lambda_2\langle 10|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2 + \left|\lambda_3\langle 11|V_{jk}U^\dagger|\psi_{ab}\rangle\right|^2}}\right). \quad (20)$$

where $V_{jk} = U^\dagger \beta_{jk} U$. Now, let us to consider the special case: 1) The Bell basis is used in the measurements and, hence, β_{jk} is the tensor product of two Pauli matrices. 2) U belongs to Clifford group. 3) The input state is such that $U^\dagger|\psi_{ab}\rangle = |00\rangle$. In this case (20) becomes

$$\left|\psi_0^{jk}\right\rangle = U\left(\frac{\lambda_0\langle 00|\sigma_{jk}|00\rangle|00\rangle + \lambda_1\langle 01|\sigma_{jk}|00\rangle|01\rangle + \lambda_2\langle 10|\sigma_{jk}|00\rangle|10\rangle + \lambda_3\langle 11|\sigma_{jk}|00\rangle|11\rangle}{\sqrt{\left|\lambda_0\langle 00|\sigma_{jk}|00\rangle\right|^2 + \left|\lambda_1\langle 01|\sigma_{jk}|00\rangle\right|^2 + \left|\lambda_2\langle 10|\sigma_{jk}|00\rangle\right|^2 + \left|\lambda_3\langle 11|\sigma_{jk}|00\rangle\right|^2}}\right). \quad (21)$$

The Table 2 shows the possible output states when $\lambda_i \neq 0$ (i = 0,..,3), according to the results of the measurements.

σ_{jk}	$\left\|\psi_0^{jk}\right\rangle$	σ_{jk}	$\left\|\psi_0^{jk}\right\rangle$
$I\otimes I$	$\left\|\psi_0^{jk}\right\rangle = U\|00\rangle$	$\sigma_Y\otimes I$	$\left\|\psi_0^{jk}\right\rangle = iU\|10\rangle$
$I\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = U\|01\rangle$	$\sigma_Y\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = iU\|11\rangle$
$I\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = iU\|01\rangle$	$\sigma_Y\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = -U\|11\rangle$
$I\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = U\|00\rangle$	$\sigma_Y\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = iU\|10\rangle$
$\sigma_X\otimes I$	$\left\|\psi_0^{jk}\right\rangle = U\|10\rangle$	$\sigma_Z\otimes I$	$\left\|\psi_0^{jk}\right\rangle = U\|00\rangle$
$\sigma_X\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = U\|11\rangle$	$\sigma_Z\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = U\|01\rangle$
$\sigma_X\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = iU\|11\rangle$	$\sigma_Z\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = iU\|01\rangle$
$\sigma_X\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = U\|10\rangle$	$\sigma_Z\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = U\|00\rangle$

Table 2 - Output states (Eq. (21)) according to the results of the measurements using the Bell basis.

As can be noted in Table 2, the output state is not the teleportation of a unitary operation applied to the input state $|\psi_{ab}\rangle$. The output state is (ignoring the global phase), probabilistically, one of the states: $U|00\rangle$, $U|01\rangle$, $U|10\rangle$ and $U|11\rangle$, where U comes from the decomposition of Υ and, hence, depends on the four-qubit state. Thus, what is teleported is the action of U in the canonical basis. One may also note that error correction is not necessary. This happens because one cannot choose the state to be teleported, the result is probabilistic. As another example, let us consider the following maximally entangled four-qubit state

$$\left|\xi\right\rangle = \left(\left|0000\right\rangle + \left|0011\right\rangle + \left|0101\right\rangle + \left|0110\right\rangle + \left|1001\right\rangle + \left|1010\right\rangle + \left|1100\right\rangle + \left|1111\right\rangle\right)/\sqrt{8}. \quad (22)$$

For such state one has

$$\Upsilon = \frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = U \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 0 \\ 0 & 0 & 0 & 1/\sqrt{2} \end{bmatrix} U^{\dagger} \tag{23}$$

$$U = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{bmatrix}. \tag{24}$$

Hence, (19) is reduced to

$$\left|\psi_0^{jk}\right\rangle = U\left(\frac{\left(\langle 00|\beta_{jk}|\psi_{ab}\rangle + \langle 11|\beta_{jk}|\psi_{ab}\rangle\right)|10\rangle + \left(\langle 01|\beta_{jk}|\psi_{ab}\rangle + \langle 10|\beta_{jk}|\psi_{ab}\rangle\right)|11\rangle}{\sqrt{\left|\left(\langle 00|\beta_{jk}|\psi_{ab}\rangle + \langle 11|\beta_{jk}|\psi_{ab}\rangle\right)\right|^2 + \left|\langle 01|\beta_{jk}|\psi_{ab}\rangle + \langle 10|\beta_{jk}|\psi_{ab}\rangle\right|^2}}\right). \tag{25}$$

Choosing again the Bell basis for measurement and $|\psi_{ab}\rangle = |00\rangle$, one gets the results shown in Table 3

σ_{jk}	$\left\|\psi_0^{jk}\right\rangle$	σ_{jk}	$\left\|\psi_0^{jk}\right\rangle$
$I\otimes I$	$\left\|\psi_0^{jk}\right\rangle = U\|10\rangle$	$\sigma_Y\otimes I$	$\left\|\psi_0^{jk}\right\rangle = iU\|11\rangle$
$I\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = U\|11\rangle$	$\sigma_Y\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = iU\|10\rangle$
$I\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = iU\|11\rangle$	$\sigma_Y\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = -U\|10\rangle$
$I\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = U\|10\rangle$	$\sigma_Y\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = iU\|11\rangle$
$\sigma_X\otimes I$	$\left\|\psi_0^{jk}\right\rangle = U\|11\rangle$	$\sigma_Z\otimes I$	$\left\|\psi_0^{jk}\right\rangle = U\|10\rangle$
$\sigma_X\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = U\|10\rangle$	$\sigma_Z\otimes\sigma_X$	$\left\|\psi_0^{jk}\right\rangle = U\|11\rangle$
$\sigma_X\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = iU\|10\rangle$	$\sigma_Z\otimes\sigma_Y$	$\left\|\psi_0^{jk}\right\rangle = iU\|11\rangle$
$\sigma_X\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = U\|11\rangle$	$\sigma_Z\otimes\sigma_Z$	$\left\|\psi_0^{jk}\right\rangle = U\|10\rangle$
$U\|10\rangle = \left(\|00\rangle - \|11\rangle\right)/\sqrt{2}$; $U\|11\rangle = \left(\|01\rangle + \|10\rangle\right)/\sqrt{2}$			

Table 3 - Output states (Eq. (25)) according to the results of the measurements using the Bell basis.

As shown in Table 3, only the action of U in two states of the canonical basis is teleported. This happens because Υ in (23) has two eigenvalues equal to zero.

In general, states of the type $a|0000\rangle+b|0011\rangle+c|0101\rangle+d|0110\rangle+d|1001\rangle+c|1010\rangle+b|1100\rangle+a|1111\rangle$ [10] produces a normal Υ matrix.

At last, we consider states for which Υ is not normal. Although not being normal, a diagonalisation with different unitary matrices is possible. Applying firstly the Polar decomposition, one has $\Upsilon = UH$, where U is unitary and H is Hermitean. Now, the Hermitean matrix is decomposed as $H = VDV^\dagger$, hence, $\Upsilon = UVDV^\dagger = WDV^\dagger$, where D is a diagonal matrix whose elements are the eigenvalues of H. The output state is

$$\rho_o = \sum_{j,k=0}^{3} \frac{1}{4} \left|\psi_0^{jk}\right\rangle\left\langle\psi_0^{jk}\right| = \sum_{j,k=0}^{3} \frac{1}{4} \frac{\Upsilon\beta_{jk}\left|\psi_{ab}\right\rangle\left\langle\psi_{ab}\right|\beta_{jk}^\dagger\Upsilon^\dagger}{\left\langle\psi_{ab}\right|\beta_{jk}^\dagger\Upsilon^\dagger\Upsilon\beta_{jk}\left|\psi_{ab}\right\rangle} \tag{26}$$

$$\left|\psi_0^{jk}\right\rangle = \frac{1}{\sqrt{\left\langle\psi_{ab}\right|\beta_{jk}^\dagger V \begin{bmatrix} |\lambda_0|^2 & 0 & 0 & 0 \\ 0 & |\lambda_1|^2 & 0 & 0 \\ 0 & 0 & |\lambda_2|^2 & 0 \\ 0 & 0 & 0 & |\lambda_3|^2 \end{bmatrix} V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle}} W \begin{bmatrix} \lambda_0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 \\ 0 & 0 & 0 & \lambda_3 \end{bmatrix} V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle \Rightarrow \tag{27}$$

$$\left|\psi_0^{jk}\right\rangle = W\left(\frac{\lambda_0\left\langle 00\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\left|00\right\rangle + \lambda_1\left\langle 01\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\left|01\right\rangle + \lambda_2\left\langle 10\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\left|10\right\rangle + \lambda_3\left\langle 11\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\left|11\right\rangle}{\sqrt{\left|\lambda_0\left\langle 00\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\right|^2 + \left|\lambda_1\left\langle 01\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\right|^2 + \left|\lambda_2\left\langle 10\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\right|^2 + \left|\lambda_3\left\langle 11\right|V^\dagger\beta_{jk}\left|\psi_{ab}\right\rangle\right|^2}}\right). \tag{28}$$

This result is similar to that one in (19), but now λ_i (i = 0,1,2,3,4) are eigenvalues of H instead of Υ. Furthermore, using (5) one has that $\mathrm{Tr}(\Upsilon\Upsilon^\dagger) = \mathrm{Tr}(HH^\dagger) = 1$ and, hence, $\sum_i|\lambda_i|^2 = 1$. Now, considering that the Bell basis is used in the measurements, that V belongs to Clifford group and the input state is such that $V^\dagger|\psi_{ab}\rangle = |00\rangle$, (28) is reduced to.

$$\left|\psi_0^{jk}\right\rangle = W\left(\frac{\lambda_0\left\langle 00\right|\sigma_{jk}\left|00\right\rangle\left|00\right\rangle + \lambda_1\left\langle 01\right|\sigma_{jk}\left|00\right\rangle\left|01\right\rangle + \lambda_2\left\langle 10\right|\sigma_{jk}\left|00\right\rangle\left|10\right\rangle + \lambda_3\left\langle 11\right|\sigma_{jk}\left|00\right\rangle\left|11\right\rangle}{\sqrt{\left|\lambda_0\left\langle 00\right|\sigma_{jk}\left|00\right\rangle\right|^2 + \left|\lambda_1\left\langle 01\right|\sigma_{jk}\left|00\right\rangle\right|^2 + \left|\lambda_2\left\langle 10\right|\sigma_{jk}\left|00\right\rangle\right|^2 + \left|\lambda_3\left\langle 11\right|\sigma_{jk}\left|00\right\rangle\right|^2}}\right). \tag{29}$$

Observing (29), one can see the teleportation of the action of W in a set of states, however, here W may not belong to Clifford group.

Another possibility for a not normal Υ matrix is to use the Schur decomposition, $\Upsilon = UTU^\dagger$, where T is an upper triangular matrix. Let us consider, for example, the following four-qubit state [11]

$$\left|\chi\right\rangle = \left(\left|0000\right\rangle - \left|0011\right\rangle - \left|0101\right\rangle + \left|0110\right\rangle + \left|1001\right\rangle + \left|1010\right\rangle + \left|1100\right\rangle + \left|1111\right\rangle\right)/\sqrt{8}. \tag{30}$$

For such state one has the following Schur decomposition:

$$\Upsilon = \frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = UTU^\dagger = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1/\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/\sqrt{2} \\ 0 & 0 & 0 & 0 \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \end{bmatrix}^\dagger \tag{31}$$

The output state of the teleportation protocol is

$$\rho_o = \sum_{j,k=0}^{3} \frac{1}{4} \left|\psi_0^{jk}\right\rangle \left\langle\psi_0^{jk}\right| = \sum_{j,k=0}^{3} \frac{1}{4} \frac{\Upsilon\beta_{jk} \left|\psi_{ab}\right\rangle \left\langle\psi_{ab}\right| \beta_{jk}^{\dagger} \Upsilon^{\dagger}}{\left\langle\psi_{ab}\right| \beta_{jk}^{\dagger} \Upsilon^{\dagger} \Upsilon \beta_{jk} \left|\psi_{ab}\right\rangle} \tag{32}$$

$$\left|\psi_0^{jk}\right\rangle = \frac{U\left(\left|00\right\rangle\left\langle 00\right| + \left|10\right\rangle\left\langle 11\right|\right) U^{\dagger} \beta_{jk} \left|\psi_{ab}\right\rangle}{\sqrt{2}} = \tag{33}$$

$$\left|\psi_0^{jk}\right\rangle = U \frac{\left(\left\langle 00\right| \beta_{jk} \left|\psi_{ab}\right\rangle + \left\langle 11\right| \beta_{jk} \left|\psi_{ab}\right\rangle\right)\left|00\right\rangle + \left(\left\langle 10\right| \beta_{jk} \left|\psi_{ab}\right\rangle - \left\langle 01\right| \beta_{jk} \left|\psi_{ab}\right\rangle\right)\left|10\right\rangle}{\sqrt{\left|\left\langle 00\right| \beta_{jk} \left|\psi_{ab}\right\rangle + \left\langle 11\right| \beta_{jk} \left|\psi_{ab}\right\rangle\right|^2 + \left|\left\langle 10\right| \beta_{jk} \left|\psi_{ab}\right\rangle - \left\langle 01\right| \beta_{jk} \left|\psi_{ab}\right\rangle\right|^2}} \tag{34}$$

Choosing again the Bell basis for measurement and $|\psi_{ab}\rangle = |00\rangle$, one gets the results shown in Table 4

σ_{jk}	$\left\|\psi_0^{jk}\right\rangle$	σ_{jk}	$\left\|\psi_0^{jk}\right\rangle$
$I\otimes I$	$U\left\|00\right\rangle$	$\sigma_Y \otimes I$	$iU\left\|10\right\rangle$
$I\otimes\sigma_X$	$-U\left\|10\right\rangle$	$\sigma_Y \otimes \sigma_X$	$iU\left\|00\right\rangle$
$I\otimes\sigma_Y$	$-iU\left\|10\right\rangle$	$\sigma_Y \otimes \sigma_Y$	$-U\left\|00\right\rangle$
$I\otimes\sigma_Z$	$U\left\|00\right\rangle$	$\sigma_Y \otimes \sigma_Z$	$U\left\|10\right\rangle$
$\sigma_X\otimes I$	$U\left\|10\right\rangle$	$\sigma_Z\otimes I$	$U\left\|00\right\rangle$
$\sigma_X\otimes\sigma_X$	$U\left\|00\right\rangle$	$\sigma_Z\otimes\sigma_X$	$-U\left\|10\right\rangle$
$\sigma_X\otimes\sigma_Y$	$iU\left\|00\right\rangle$	$\sigma_Z\otimes\sigma_Y$	$-iU\left\|10\right\rangle$
$\sigma_X\otimes\sigma_Z$	$U\left\|10\right\rangle$	$\sigma_Z \otimes\sigma_Z$	$U\left\|00\right\rangle$
$U\left\|10\right\rangle = \left(\left\|01\right\rangle + \left\|10\right\rangle\right)/\sqrt{2}$; $U\left\|00\right\rangle = \left(\left\|00\right\rangle + \left\|11\right\rangle\right)/\sqrt{2}$			

Table 4 - Output states (Eq. (34)) according to the results of the measurements using the Bell basis.

As can be seen in Table 4, only the action of U in two states of the canonical basis is teleported.

4. Conclusions

In what concerns the role of the four-qubit state in two-qubit gate teleportation, one may define two classes of states: 1) the set of four-qubit states for which $\Upsilon = 1/2U_\sigma$ and 2) the set of four-qubit states for which Υ is normal but 2Υ is not unitary or Υ is not normal. The main differences in the two-qubit gate teleportation protocol when states of both classes are used are:

For class 1,

1. The basis of measurement is important to define the probability of success of the teleportation and the error correction.
2. A deterministic teleportation is achieved only if the four-qubit state used is maximally entangled.
3. The state teleported is the action of U in the input two-qubit state.

For class 2,

1. The action of U in a set of states is probabilistically teleported.
2. The basis of measurement and the input two-qubit state are used to define the set of states to be teleported.
3. There is no error correction.

Additionally, it was shown the probabilistic teleportation of the canonical basis by a two-qubit gate that belongs to Clifford group if Υ is normal, or does not belong to Clifford group is Υ is not normal. In the particular cases where the four-qubit states (22) and (30) are used, the result of the teleportation is, probabilistically, a Bell state.

Acknowledgment

This work was supported by the Brazilian agency CNPq via Grant no. 303514/2008-6. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

1. Gottesman, D., and Chuang, I. L.: Quantum teleportation is a universal computational primitive, Nature, 402, 390 (1999).
2. Mendes, F. V, and Ramos, R. V.: On the role of the basis of measurement in quantum gate teleportation, Arxiv:1307.4750 (2013).
3. Luque, J.-G., and Thibon, J.-Y.: Polynomial invariants of four qubits, Phys. Rev. A, 67, 042303 (2003).
4. Zha X.-W., and Ma, G.-L.: Classification of four-qubit states by means of a stochastic local operation and the classical communication invariant, Chin. Phys. Lett., 28, 2, 020301 (2011).
5. Oliveira, D. S. and Ramos, R. V.: Residual entanglement with negativity for pure four-qubit quantum states, Quant. Inf. Process., 9, 497 (2010).
6. Eisert, J., and Plenio, M. B.: A Comparison of Entanglement Measures, quant-ph/9807034 (1999).
7. Zyczkowski, K., and Kus, M.: Random unitary matrices, J. Phys. A: Math. Gen., 27, 4235 (1994).
8. Pozniak, M., Zyczkowski, K., and Kus, M.: Composed ensembles of random unitary matrices, J. Phys. A: Math. Gen., 31, 1059 (1998).
9. Tucci, R. R.: An introduction to Cartan's KAK decomposition for QC programmers, arXiv:quant-ph/0507171 (2005).
10. Verstraete, F., Dehaene, J., Moor, B. De , and Verschelde. H.: Four qubits can be entangled in nine different ways, Phys. Rev. A 65, 052112 (2002).
11. Yeo, Y. and Chua, W. K.: Teleportation and dense coding with genuine multipartite entanglement, Phys. Rev. Lett. 96, 060502/1-4 (2006).

3. **Numerical search for universal entanglers in $\mathbb{C}^3 \otimes \mathbb{C}^4$ and $\mathbb{C}^4 \otimes \mathbb{C}^4$**

   - ◇ Periódico: Physics Letters A
   - ◇ Data: 28/11/2014
   - ◇ Situação: Aceito

Physics Letters A ••• (••••) •••–•••

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Numerical search for universal entanglers in $C^3 \otimes C^4$ and $C^4 \otimes C^4$

F.V. Mendes *, R.V. Ramos

Lab. of Quantum Information Technology, Department of Teleinformatic Engineering, Federal University of Ceara - DETI/UFC, C.P. 6007, Campus do Pici, 60455-970 Fortaleza-Ce, Brazil

ARTICLE INFO

Article history:
Received 3 September 2014
Received in revised form 27 November 2014
Accepted 28 November 2014
Available online xxxx
Communicated by P.R. Holland

ABSTRACT

A universal entangler is quantum gate able to transform any disentangled state into an entangled state. Although universal entanglers are abundant in arbitrary high dimensional spaces, to verify if a quantum gate is a universal entangler is a hard task since it is not known which property of the unitary matrix is responsible for such behavior. In this direction, the present work shows the results of an algorithm based on differential evolution that tests universal entanglers in $C^3 \otimes C^4$ and $C^4 \otimes C^4$. We present two good candidates for each cited space and we show that a candidate found in the literature is not a universal entangler.

1. Introduction

Quantum entanglement plays a fundamental role in many interesting tasks such as quantum teleportation, quantum dense coding and other quantum cryptography protocols [1,2], so that techniques for its generation [3–5] and preservation [6–10] are essential. In this context, a relevant attention has been devoted to the study of entanglers [11–14], aiming to understand their properties, construction and applications. A particularly interesting class of entanglers is the universal entangler, a quantum gate able to transform any disentangled state (belonging to the appropriated Hilbert space) into an entangled state. Although universal entanglers are known to be abundant, it is not an easy task to affirm that a given quantum gate is a universal entangler since, in general, it is not known which property of the unitary matrix is responsible for such behavior. Furthermore, due to the dimensions of the spaces considered, a brute-force checking is not viable. An alternative is to use some heuristic in order to implement an intelligent search for universal entanglers. Although such heuristics are not able to confirm that a given gate is in fact a universal entangler, the use of heuristics has two interesting advantages: 1) It can find good candidates for universal entanglers. 2) It can be useful to discard pseudo-good candidates. In this direction, the present work shows the results obtained by an algorithm based on differential evolution that tests universal entanglers. We provide two good candidates for $C^3 \otimes C^4$ and two good candidates for $C^4 \otimes C^4$. Moreover, we also show that a candidate for a universal entangler presented in the literature is not a universal entangler.

2. Separability

In the core of the proposed algorithm are the separability test of normal matrices and the entanglement measure of pure bipartite states. There are good bipartite entangled measures like partial von Neumann entropy [15], concurrence [16], positive partial transpose (PPT) [17], negativity [18] among others. In this work only the entanglement measure based on the von Neumann entropy will be used. Given an entangled pure bipartite state $|\varphi\rangle_{AB}$, its entanglement is given by

$$E_{VN}(|\varphi\rangle_{AB}\langle\varphi|) = S_{VN}\big(Tr_A(|\varphi\rangle_{AB}\langle\varphi|)\big) = S_{VN}\big(Tr_B(|\varphi\rangle_{AB}\langle\varphi|)\big) \quad (1)$$

$$S_{VN}(\rho) = -Tr\big[\rho \ln(\rho)\big]. \quad (2)$$

In what concerns the separability, one says that a given normal matrix $N \in C^{m\cdot n}$ is separable if it can be described as the Kronecker product of two other normal matrices, $N = N_A \otimes N_B$, where $N_A \in C^m$ and $N_B \in C^n$. However, since the Kronecker product is a bilinear form, one can define the map $\gamma : C^m \times C^n \to C$ as

$$\gamma(\vec{p}, \vec{q}, \vec{r}, \vec{s}) = (\vec{p} \otimes \vec{r})^\dagger N (\vec{q} \otimes \vec{s}). \quad (3)$$

In (3) the column vectors $\vec{p}, \vec{q} \in C^m$ while the column vectors $\vec{r}, \vec{s} \in C^n$. Thus, a necessary and sufficient condition to have N decomposable in the Kronecker product $N_A \otimes N_B$ is

* Corresponding author.
E-mail addresses: fernandovm@gmail.com (F.V. Mendes), rubens.viana@pq.cnpq.br (R.V. Ramos).

http://dx.doi.org/10.1016/j.physleta.2014.11.056
0375-9601/

Please cite this article in press as: F.V. Mendes, R.V. Ramos, Numerical search for universal entanglers in $C^3 \otimes C^4$ and $C^4 \otimes C^4$, Phys. Lett. A (2015), http://dx.doi.org/10.1016/j.physleta.2014.11.056

$$\gamma(\vec{p}_1,\vec{q}_1,\vec{r}_1,\vec{s}_1)\cdot\gamma(\vec{p}_2,\vec{q}_2,\vec{r}_2,\vec{s}_2) = \gamma(\vec{p}_1,\vec{q}_1,\vec{r}_2,\vec{s}_2)\cdot\gamma(\vec{p}_2,\vec{q}_2,\vec{r}_1,\vec{s}_1) \quad (4)$$

to be true for all vectors $\vec{p}_i$, $\vec{q}_i$ in a basis of C^m and $\vec{r}_j$, $\vec{s}_j$ in a basis of C^n. This approach is an application of the Plücker coordinates, due to Julius Plücker dated 1865. It was also used in [19], for unitary matrices, in order to determine the conditions of separability preservation under conjugation of two-qubit quantum gates. When (3)–(4) are used to test the separability of the Hermitean matrix corresponding to a general two-qubit state, $\alpha_1|00\rangle+\alpha_2|01\rangle+\alpha_3|10\rangle+\alpha_4|11\rangle$, the known result $|\alpha_1\alpha_4-\alpha_2\alpha_3|=0$ is obtained. In general, the usage of (3)–(4) to check the biseparability of quantum states results in a set of polynomial equations in the states' coefficients that have to be identically null. If anyone of them is not equal to zero, then the state is not biseparable. Fort example, it was affirmed in [20] that the three-qutrit state

$$|\kappa\rangle=\frac{1}{\sqrt{6}}\big(|000\rangle-|011\rangle-|112\rangle+|120\rangle-|202\rangle+|221\rangle\big)_{ABC} \quad (5)$$

is biseparable. However, using (3)–(4), the conditions of biseparability of a general three-qutrit state $\alpha_1|000\rangle+\alpha_2|001\rangle+\alpha_3|002\rangle+\cdots+\alpha_{27}|222\rangle$ include the following equations

$$\alpha_1\cdot\alpha_{15}-\alpha_6\cdot\alpha_{10}=0 \quad \text{for A\_BC} \quad (6)$$

$$\alpha_1\cdot\alpha_{11}-\alpha_2\cdot\alpha_{10}=0 \quad \text{for B\_AC} \quad (7)$$

$$\alpha_1\cdot\alpha_{13}-\alpha_4\cdot\alpha_{10}=0 \quad \text{for AB\_C.} \quad (8)$$

Using $\alpha=1/6^{1/2}$ in (6)–(8), one gets for the three cases the value $-1/6$, hence, the state in (5) is not biseparable.

3. Universal entanglers

Any quantum gate able to generate entanglement between two separable states is considered an entangler. The concept of entangling power was developed in [21] aiming to characterize how good entangler is a particular quantum gate. In [13] it was established a connection between entangling power and the invariants of two-qubit gates. In [22] it was introduced the perfect entangler concept: perfect entanglers are entangler gates able to generate maximally entangled states from separable states. Another entangler class was defined in [23] aiming to respond the question: Does there exist any perfect entangler which can maximally entangle a full separable basis? This particular class has received the name of the especial perfect entanglers. A still more general definition about entanglers was introduced in [24], named universal entangler, in response to the question: Does there exist an entangler able to entangle any separable state? Formally, a universal entangler is a quantum gate U such that $E_{VN}(U(|\varphi\rangle_m|\psi\rangle_n))>0$, where $|\varphi\rangle_m$ and $|\psi\rangle_n$ are arbitrary one qudit states of dimensions m and n, respectively. In [24] it was established that a universal entangler exists if, and only if, $\min(m,n)\geq 3$ and $(m,n)\neq(3,3)$. Furthermore, how explicitly to construct universal entanglers to operate over an arbitrary bipartite $C^m\otimes C^n$ system is a question that remains opened. An explicit example of perfect entangler for $C^3\otimes C^4$ was given in [25] (which will be discussed in detail later), and in [26] two universal entanglers class applicable to bosonic/fermionic systems were provided.

Although does not exist an analytical formula to determine if a given unitary matrix is a universal entangler or not, there are some hints that can be followed to discard bad candidates. For example, we prove here the following lemma:

Lemma 1. *If an $n\times n$ unitary matrix U is an universal entangler then all of its n columns are non-separable vectors.*

Proof. Let $|u_i\rangle$, a separable state, be the i-th column of the $n\times n$ unitary matrix U, and $|v_i\rangle$ is the i-th state of the canonical basis and, hence, it is also separable. Then $U|v_i\rangle=|u_i\rangle$, that is separable, therefore, U is not a universal entangler. □

A direct consequence from Lemma 1 is that controlled gates cannot be universal entanglers. From the best of our knowledge, the only example of universal entangler in $C^3\otimes C^4$ was proposed in [25] and corroborated in [26,27], it is the quantum gate

$$U_H=\begin{bmatrix}
+ & - & - & - & - & - & - & - & - & - & - \\
+ & + & - & + & - & - & - & + & + & + & - & + \\
+ & + & + & - & + & - & - & - & + & + & + & - \\
+ & - & + & + & - & + & - & - & - & + & + & + \\
+ & + & - & + & + & - & + & - & - & - & + & + \\
+ & + & + & - & + & + & - & + & - & - & - & + \\
+ & + & + & + & - & + & + & - & + & - & - & - \\
+ & - & + & + & + & - & + & + & - & + & - & - \\
+ & - & - & + & + & + & - & + & + & - & + & - \\
+ & - & - & - & + & + & + & - & + & + & - & + \\
+ & + & - & - & - & + & + & + & - & + & + & - \\
+ & - & + & - & - & - & + & + & + & - & + & +
\end{bmatrix} \quad (9)$$

where the symbols + and − means, respectively, $12^{-1/2}$ and $-12^{-1/2}$. However, from Lemma 1 one can see that U_H cannot be a universal entangler. In fact it is easy to check that

$$U_H\big(|0\rangle_3\otimes|0\rangle_4\big)=F_3|0\rangle_3\otimes F_4|0\rangle_4. \quad (10)$$

In (10), F_d is the single-qudit Hadamard gate in C^d ($d=3,4$), $|0\rangle_3$ is the first state of the canonical basis of a qutrit $\{|0\rangle_3,|1\rangle_3,|2\rangle_3\}$, and $|0\rangle_4$ is the first state of the canonical basis of a qudit ($d=4$)$\{|0\rangle_4,|1\rangle_4,|2\rangle_4,|3\rangle_4\}$.

4. Candidates for universal entanglers in $C^3\otimes C^4$ and $C^4\otimes C^4$

To verify whether or not a given quantum gate is a universal entangler is an intractable problem; this arises from the fact that solving a system of polynomial equations is, in general, NP-hard. However, in practice, to find a counterexample that proves that a given gate is not a universal entangler is more feasible. In this work we used a Differential Evolution algorithm to enhance the ability to find counterexamples that invalidate universal entanglers' candidates. Here we considered only the spaces $C^3\otimes C^4$ and $C^4\otimes C^4$. According to (3)–(4), a general state in $C^3\otimes C^4$, $|\alpha_{34}\rangle=\alpha_1|00\rangle+\alpha_2|01\rangle+\alpha_3|02\rangle+\alpha_4|03\rangle+\cdots+\alpha_{12}|23\rangle$ is separable if

$$S_{3\otimes4}\big(|\alpha_{34}\rangle\big)\equiv\sum_{i=1}^{18}|\zeta_i|=0 \quad (11)$$

where

$$\begin{aligned}
&\zeta_1=\alpha_1\alpha_6-\alpha_2\alpha_5; && \zeta_2=\alpha_1\alpha_7-\alpha_3\alpha_5;\\
&\zeta_3=\alpha_1\alpha_8-\alpha_4\alpha_5; && \zeta_4=\alpha_1\alpha_{10}-\alpha_2\alpha_9;\\
&\zeta_5=\alpha_1\alpha_{11}-\alpha_3\alpha_9; && \zeta_6=\alpha_1\alpha_{12}-\alpha_4\alpha_9;\\
&\zeta_7=\alpha_2\alpha_7-\alpha_3\alpha_6; && \zeta_8=\alpha_2\alpha_8-\alpha_4\alpha_6;\\
&\zeta_9=\alpha_2\alpha_{11}-\alpha_3\alpha_{10}; && \zeta_{10}=\alpha_2\alpha_{12}-\alpha_4\alpha_{10};\\
&\zeta_{11}=\alpha_3\alpha_8-\alpha_4\alpha_7; && \zeta_{12}=\alpha_3\alpha_{12}-\alpha_4\alpha_{11};\\
&\zeta_{13}=\alpha_5\alpha_{10}-\alpha_6\alpha_9; && \zeta_{14}=\alpha_5\alpha_{11}-\alpha_7\alpha_9;\\
&\zeta_{15}=\alpha_5\alpha_{12}-\alpha_8\alpha_9; && \zeta_{16}=\alpha_6\alpha_{11}-\alpha_7\alpha_{10};\\
&\zeta_{17}=\alpha_6\alpha_{12}-\alpha_8\alpha_{10}; && \zeta_{18}=\alpha_7\alpha_{12}-\alpha_8\alpha_{11}.
\end{aligned} \quad (12)$$

Please cite this article in press as: F.V. Mendes, R.V. Ramos, Numerical search for universal entanglers in $C^3\otimes C^4$ and $C^4\otimes C^4$, Phys. Lett. A (2015), http://dx.doi.org/10.1016/j.physleta.2014.11.056

On the other hand, according to (3)–(4), a general state in $C^4 \otimes C^4$, $|\alpha_{44}\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|02\rangle + \alpha_4|03\rangle + \cdots + \alpha_{16}|33\rangle$ is separable if

$$S_{4\otimes 4}\left(|\alpha_{44}\rangle\right) \equiv \sum_{i=1}^{36} |\xi_i| = 0 \tag{13}$$

where

$$\begin{aligned}
&\xi_1 = \alpha_1\alpha_6 - \alpha_2\alpha_5; \quad && \xi_2 = \alpha_1\alpha_7 - \alpha_3\alpha_5;\\
&\xi_3 = \alpha_1\alpha_8 - \alpha_4\alpha_5; && \xi_4 = \alpha_1\alpha_{10} - \alpha_2\alpha_9;\\
&\xi_5 = \alpha_1\alpha_{11} - \alpha_3\alpha_9; && \xi_6 = \alpha_1\alpha_{12} - \alpha_4\alpha_9;\\
&\xi_7 = \alpha_1\alpha_{14} - \alpha_2\alpha_{13}; && \xi_8 = \alpha_1\alpha_{15} - \alpha_3\alpha_{13};\\
&\xi_9 = \alpha_1\alpha_{16} - \alpha_4\alpha_{13}; && \xi_{10} = \alpha_2\alpha_7 - \alpha_3\alpha_6;\\
&\xi_{11} = \alpha_2\alpha_8 - \alpha_4\alpha_6; && \xi_{12} = \alpha_2\alpha_{11} - \alpha_3\alpha_{10};\\
&\xi_{13} = \alpha_2\alpha_{12} - \alpha_4\alpha_{10}; && \xi_{14} = \alpha_2\alpha_{15} - \alpha_3\alpha_{14};\\
&\xi_{15} = \alpha_2\alpha_{16} - \alpha_4\alpha_{14}; && \xi_{16} = \alpha_3\alpha_8 - \alpha_4\alpha_7;\\
&\xi_{17} = \alpha_3\alpha_{12} - \alpha_4\alpha_{11}; && \xi_{18} = \alpha_3\alpha_{16} - \alpha_4\alpha_{15};\\
&\xi_{19} = \alpha_5\alpha_{10} - \alpha_6\alpha_9; && \xi_{20} = \alpha_5\alpha_{11} - \alpha_7\alpha_9;\\
&\xi_{21} = \alpha_5\alpha_{12} - \alpha_8\alpha_9; && \xi_{22} = \alpha_5\alpha_{14} - \alpha_6\alpha_{13};\\
&\xi_{23} = \alpha_5\alpha_{15} - \alpha_7\alpha_{13}; && \xi_{24} = \alpha_5\alpha_{16} - \alpha_8\alpha_{13};\\
&\xi_{25} = \alpha_6\alpha_{11} - \alpha_7\alpha_{10}; && \xi_{26} = \alpha_6\alpha_{12} - \alpha_8\alpha_{10};\\
&\xi_{27} = \alpha_6\alpha_{15} - \alpha_7\alpha_{14}; && \xi_{28} = \alpha_6\alpha_{16} - \alpha_8\alpha_{14};\\
&\xi_{29} = \alpha_7\alpha_{12} - \alpha_8\alpha_{11}; && \xi_{30} = \alpha_7\alpha_{16} - \alpha_8\alpha_{15};\\
&\xi_{31} = \alpha_9\alpha_{14} - \alpha_{10}\alpha_{13}; && \xi_{32} = \alpha_9\alpha_{15} - \alpha_{11}\alpha_{13};\\
&\xi_{33} = \alpha_9\alpha_{16} - \alpha_{12}\alpha_{13}; && \xi_{34} = \alpha_{10}\alpha_{15} - \alpha_{11}\alpha_{14};\\
&\xi_{35} = \alpha_{10}\alpha_{16} - \alpha_{12}\alpha_{14}; && \xi_{36} = \alpha_{11}\alpha_{16} - \alpha_{12}\alpha_{15}.
\end{aligned} \tag{14}$$

Let U_{34} to be a two-qudit quantum gate in $C^3 \otimes C^4$. If U_{34} is a universal entangler, the global minimum of the function $S_{3\otimes 4}(U_{34}|\alpha\rangle)$ is larger than zero, $S_{3\otimes 4}(U_{34}|\alpha_{min}\rangle) > 0$, where $|\alpha_{min}\rangle$ is the quantum state that minimizes the separability condition given in (11). On the other hand, if U_{34} is not a universal entangler, then the global minimum of the function $S_{3\otimes 4}(U_{34}|\alpha\rangle)$ is equal to zero, $S_{3\otimes 4}(U_{34}|\alpha_{min}\rangle) = 0$. An equivalent statement can be done considering a two-qudit quantum gate in $C^4 \otimes C^4$, U_{44}, and the function $S_{4\otimes 4}(U_{44}|\alpha\rangle)$. So, given a two-qudit gate in $C^3 \otimes C^4 (C^4 \otimes C^4)$, U, the goal of our algorithm is to find the global minimum of $S_{3\otimes 4}(U|\alpha\rangle))(S_{4\otimes 4}(U|\alpha\rangle))$. For example, our algorithm took only few seconds to show that U_H in (9) is not a universal entangler, finding the quantum state $|0\rangle_3|0\rangle_4$ as a counterexample, as can be seen in (10): $S_{3\otimes 4}(U_H|0\rangle_3|0\rangle_4) = 0$. Due to the intrinsic characteristic of the heuristic used, one can be sure that the global minimum was found only when the tested quantum gate is not a universal entangler gate, since in this case the minimum value of the separability condition (Eqs. (11) or (13)) is known to be zero. In other words, when we are testing a gate U and the algorithm converges to separability condition equal to zero, we can be sure that U is not a universal entangler. Similarly, one says that a good candidate for universal entangler was found only when the algorithm does not converge to separability condition equal to zero.

Although for high dimensions, as it was pointed in [25], a random unitary is almost surely a universal entangler, to build it from more familiar gates can be useful. Thus, our main goal in this work is to find good universal entanglers candidates using known gates. Here we try F_{12}, X_{12}, Y_{12} and Z_{12} operating over the product states $|\psi_A\rangle_3 \otimes |\psi_B\rangle_4$ and F_{16}, X_{16}, Y_{16} and Z_{16} operating over the product states $|\varphi_A\rangle_4 \otimes |\varphi_B\rangle_4$. The definitions of these quantum gates are

$$X_d|k\rangle = \left|(k+1) \bmod d\right\rangle \tag{15}$$

$$Z_d|k\rangle = e^{i2\pi k/d}|k\rangle \tag{16}$$

$$Y_d = iX_dZ_d \tag{17}$$

$$F_d|k\rangle = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} e^{(i2\pi kl/d)}|l\rangle. \tag{18}$$

The elements of their matrix representations are given by

$$(X_d)_{mn} = \begin{cases} 1 & \text{if } m = (n+1) \bmod d \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

$$(Z_d)_{mn} = \begin{cases} e^{(2\pi i/d)^{m-1}} & \text{if } m = n \\ 0 & \text{if } m \neq n \end{cases} \tag{20}$$

$$(F_d)_{mn} = e^{(2\pi i/d)^{mn}}/\sqrt{d}. \tag{21}$$

Although all these gates are non-separable in $C^3 \otimes C^4$ (for $d = 12$) and $C^4 \otimes C^4$ (for $d = 16$), they are not universal entanglers. Our algorithm takes only few seconds to find counterexamples. The same happens to $(X_d)^{1/2}$ and $(Z_d)^{1/2}$. On the other hand, good universal entanglers' candidates are

$$U_{E1} = \sqrt{Y_{12}} \tag{22}$$

$$U_{E2} = \sqrt{Y_{16}} \tag{23}$$

$$U_{E3} = \sqrt{X_{12}}^{\dagger} \cdot F_{12} \cdot \sqrt{X_{12}} \tag{24}$$

$$U_{E4} = \sqrt{X_{16}}^{\dagger} \cdot F_{16} \cdot \sqrt{X_{16}}. \tag{25}$$

After fifteen days looking for counterexamples for U_{E1}, U_{E2}, U_{E3} and U_{E4}, our algorithm was not able to find anyone. The minimal entanglement values created by them can be seen in Table 1.

Hence, our simulation results suggest Conjecture 1.

Table 1
Minimum entanglement generated by gates U_{E1}, U_{E2}, U_{E3} and U_{E4} after several days running the algorithm based on Differential Evolution.

Quantum gate	Minimum entanglement
U_{E1}	0.000016199687
U_{E2}	0.000057325250
U_{E3}	0.005023555953
U_{E4}	0.000130825518

Conjecture 1. *The gates $\sqrt{Y_{12}}$ and $\sqrt{X_{12}}^{\dagger} \cdot F_{12} \cdot \sqrt{X_{12}}$ are universal entanglers in $C^3 \otimes C^4$ while $\sqrt{Y_{16}}$ and $\sqrt{X_{16}}^{\dagger} \cdot F_{16} \cdot \sqrt{X_{16}}$ are universal entanglers in $C^4 \otimes C^4$.*

At last, we calculated the entanglement generated by the gates U_H, U_{E1} and U_{E3} when they are applied to a hundred thousand quantum states randomly chosen [28]. The estimated distributions of the entanglement values obtained are shown in Fig. 1.

The mean values of the entanglements are 0.9925, 1.0062 and 1.1096 for U_H, U_{E1} and U_{E3}, respectively.

5. Conclusions

Using the separability conditions provided by (3)–(4) as fitness function, we constructed an algorithm based on Differential Evolution that tests if a particular quantum gate is a universal entangler. Obviously one could use an entanglement measure to test the separability, however, this requires the calculation of eigenvalues and

Please cite this article in press as: F.V. Mendes, R.V. Ramos, Numerical search for universal entanglers in $C^3 \otimes C^4$ and $C^4 \otimes C^4$, Phys. Lett. A (2015), http://dx.doi.org/10.1016/j.physleta.2014.11.056

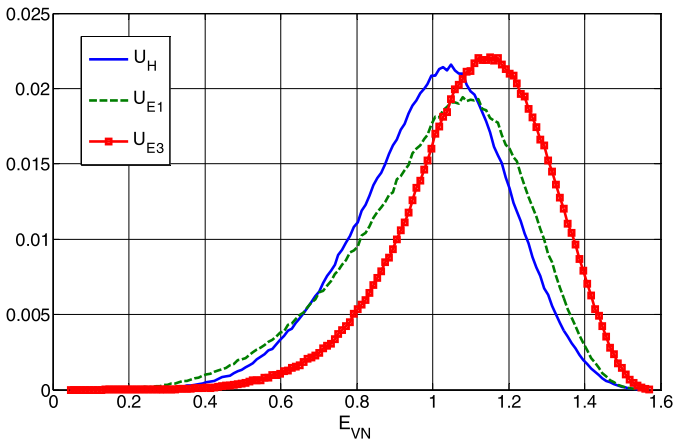


Fig. 1. Distribution of the entanglement generated by gates U_H, U_{E1} and U_{E3} when they are applied to a hundred thousand quantum states randomly chosen.

their logarithms. Evaluating the separability using only the coefficients of the states requires a lower computational effort. The proposed algorithm showed that a candidate to universal entangler in $C^3 \otimes C^4$ found in the literature is a not a universal entangler, what can also be observed analytically by Lemma 1. Furthermore, our algorithm provided two good candidates in $C^3 \otimes C^4$ $(d = 12)$ and $C^4 \otimes C^4$ $(d = 16)$: $\sqrt{Y_d}$ and $\sqrt{X_d}^{\dagger} \cdot F_d \cdot \sqrt{X_d}$. Although it is not known an analytical approach to build arbitrary universal entanglers, the knowledge of some examples based on common gates, like generalized Pauli gates, can be useful for some investigations. For example, which properties the candidates $\sqrt{Y_d}$ and $\sqrt{X_d}^{\dagger} \cdot F_d \cdot \sqrt{X_d}$ have in common or yet, why $\sqrt{Y_d}$ is a good candidate while $\sqrt{X_d}$ and $\sqrt{Z_d}$ are not, are questions that arise naturally.

Acknowledgements

This work was supported by the Brazilian agency CNPq Grant No. 303514/2008-6. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

[1] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels, Phys. Rev. Lett. 70 (13) (1993) 1895–1899, http://dx.doi.org/10.1103/PhysRevLett.70.1895.

[2] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, J.-W. Pan, Experimental demonstration of a BDCZ quantum repeater node, Nature 454 (2008) 1098–1101, http://dx.doi.org/10.1038/nature07241.

[3] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Quantum entanglement (review), Rev. Mod. Phys. 81 (2009) 865–942.

[4] F. Mintert, A.R.R. Carvalho, M. Kus, A. Buchleitner, Measures and dynamics of entangled states, Phys. Rep. 415 (2005) 207–259.

[5] V. Vedral, Quantum entanglement (review), Nat. Phys. 10 (2014) 256.

[6] R. Lo Franco, B. Bellomo, S. Maniscalco, G. Compagno, Dynamics of quantum correlations in two-qubit systems within non-Markovian environments (review), Int. J. Mod. Phys. B 27 (2013) 1345053.

[7] J.-S. Xu, et al., Experimental recovery of quantum correlations in absence of system-environment back-action, Nat. Commun. 4 (2013) 2851.

[8] A. D'Arrigo, R. Lo Franco, G. Benenti, E. Paladino, G. Falci, Recovering entanglement by local operations, Ann. Phys. 350 (2014) 211–224.

[9] A. Orieux, et al., Experimental on-demand recovery of quantum entanglement by local operations within non-Markovian dynamics, arXiv:1410.3678, 2014.

[10] R. Lo Franco, A. D'Arrigo, G. Falci, G. Compagno, E. Paladino, Preserving entanglement and nonlocality in solid-state qubits by dynamical decoupling, Phys. Rev. B 90 (2014) 054304.

[11] R. Duan, Y. Feng, M. Ying, Local distinguishability of multipartite unitary operations, Phys. Rev. Lett. 100 (2008) 020503, http://dx.doi.org/10.1103/PhysRevLett.100.020503.

[12] N. Yu, R. Duan, M. Ying, Optimal simulation of a perfect entangler, Phys. Rev. A 81 (2010) 032328, http://dx.doi.org/10.1103/PhysRevA.81.032328.

[13] S. Balakrishnan, R. Sankaranarayanan, Entangling power and local invariants of two-qubit gates, Phys. Rev. A 82 (2010) 034301, http://dx.doi.org/10.1103/PhysRevA.82.034301.

[14] E.T. Campbell, Optimal entangling capacity of dynamical processes, Phys. Rev. A 82 (2010) 042314, http://dx.doi.org/10.1103/PhysRevA.82.042314.

[15] J. von Neumann, Mathematical Foundations of Quantum Mechanics, Princeton Landmarks in Mathematics and Physics Series, Princeton Press, 1955, translated from the German edition by Robert T. Beyer. Original first edition published in German in 1932.

[16] W.K. Wootters, Entanglement of formation of an arbitrary state of two qubits, Phys. Rev. Lett. 80 (1998) 2245–2248, http://dx.doi.org/10.1103/PhysRevLett.80.2245.

[17] M. Horodecki, P. Horodecki, R. Horodecki, Separability of mixed states: necessary and sufficient conditions, Phys. Lett. A 223 (1–2) (1996) 1–8, http://dx.doi.org/10.1016/S0375-9601(96)00706-2.

[18] G. Vidal, R.F. Werner, Computable measure of entanglement, Phys. Rev. A 65 (2002) 032314, http://dx.doi.org/10.1103/PhysRevA.65.032314.

[19] F.V. Mendes, R.V. Ramos, On the role of the basis of measurement in quantum gate teleportation, arXiv:1307.4750.

[20] J. Batle, M. Casas, A. Plastino, Correlated multipartite quantum states, Phys. Rev. A 87 (2013) 032318, http://dx.doi.org/10.1103/PhysRevA.87.032318.

[21] P. Zanardi, C. Zalka, L. Faoro, Entangling power of quantum evolutions, Phys. Rev. A 62 (2000) 030301, http://dx.doi.org/10.1103/PhysRevA.62.030301.

[22] B. Kraus, J.I. Cirac, Optimal creation of entanglement using a two-qubit gate, Phys. Rev. A 63 (2001) 062309, http://dx.doi.org/10.1103/PhysRevA.63.062309.

[23] A.T. Rezakhani, Characterization of two-qubit perfect entanglers, Phys. Rev. A 70 (2004) 052313, http://dx.doi.org/10.1103/PhysRevA.70.052313.

[24] J. Chen, R. Duan, Z. Ji, M. Ying, J. Yu, Existence of universal entangler, J. Math. Phys. 49 (1) (2008), http://dx.doi.org/10.1063/1.2829895.

[25] J. Chen, Z. Ji, D.W. Kribs, B. Zeng, Minimum entangling power is close to its maximum, arXiv:1210.1296.

[26] J. Klassen, J. Chen, B. Zeng, Universal entanglers for bosonic and fermionic systems, in: S. Severini, F. Brandao (Eds.), 8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2013, in: Leibniz International Proceedings in Informatics (LIPIcs), vol. 22, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2013, pp. 35–49.

[27] J. Klassen, J. Chen, B. Zeng, Universal entanglers for bosonic and fermionic systems, presented at TQC 2013, arXiv:1305.7489.

[28] M. Lundberg, L. Svensson, The Haar measure and the generation of random unitary matrices, in: Sensor Array and Multichannel Signal Processing Workshop Proceedings, 2004, pp. 114–118.

Please cite this article in press as: F.V. Mendes, R.V. Ramos, Numerical search for universal entanglers in $C^3 \otimes C^4$ and $C^4 \otimes C^4$, Phys. Lett. A (2015), http://dx.doi.org/10.1016/j.physleta.2014.11.056

4. **Quantum Sequence States**

   - ◇ Periódico: Quantum Information Processing
   - ◇ Situação: Submetido

QUANTUM SEQUENCE STATES

F. V. Mendes, R. V. Ramos

Lab. of Quantum Information Technology, Department of Teleinformatic Engineering – Federal University of Ceara - DETI/UFC, C.P. 6007 – Campus do Pici - 60455-970 Fortaleza-Ce, Brazil.

In a recent paper it has been shown how to create a quantum state related to the prime number sequence using Grover's algorithm. Moreover, its multiqubit entanglement was analyzed. In the present work, we compare the multiqubit entanglement of several quantum sequence states as well we study the feasibility of producing such states using Grover's algorithm.

1. Introduction

In the mid-2000s some works connecting quantum information and number theory were reported [1-3] and, more recently, works showing that quantum information is a fertile environment to develop and testing number theory theorems were published [4-6]. In particular, in [5] and [6] Sierra and Latorre showed how to construct the quantum prime state, a quantum sequence state based on the sequence of prime numbers, using Grover's quantum search algorithm. They also studied its multiqubit entanglement. From the best of our knowledge, this is the unique quantum sequence state studied up to now. In this work we consider several different quantum sequence states. We make comparison between their entanglements and study the feasibility of their generation using Grover's quantum algorithm. Furthermore, we introduce a new sequence of integer numbers for which the related quantum sequence state has an entanglement that changes the sign of its slope every time a new qubit is added showing, hence, an oscillatory behavior with period of one qubit.

This paper is outlined as follows. The notation and the quantum sequence states used in this work are presented in Section 2. Section 3 brings the analysis of the entanglement of the quantum sequence states considered. In Section 4, we discuss the feasibility of producing quantum sequence states using Grover's algorithm. At last, Section 5 brings the conclusions.

2. Quantum sequence states

From an arbitrary finite integer sequence one can build the related quantum sequence state as follows. Let $S = \{s_1,s_2,s_3,\ldots,s_k\}$ be a set containing the first k elements of an infinite integer sequence, then, a n-qubit sequence state related to S with $s_k \leq 2^n$-1, is defined as

$$|S_n\rangle = \left(1/\sqrt{\tau\left(2^n\right)}\right)\sum_{i=1}^{k}|s_i\rangle. \qquad (1)$$

In (1) τ is the sequence counting function of S, which returns the sum of the squares of the quantities of each element in the sequence. In the case of a sequence having not repeated elements, the corresponding quantum sequence state is just an equally weighted superposition of the sequence's elements, hence, $\tau(2^n)$ returns the number of elements of S between 0 and 2^n-1. In this work we will consider the following integer sequences [7]: Fibonacci (A000045), Happy (A007770), Lucky (A000959), Abundant (A005101), Triangular (A000217), Lazy (A000124), Padovan (A000931), Prime (A000040), SPrime (A005097) and $PA^{[r]}$ that is a sequence generated by an arithmetic progression starting from zero and having ration equal to r. For example, the four qubit Fibonacci, Happy, Lucky and Prime sequences are

$$\left|Fib_4\right\rangle = \frac{1}{\sqrt{10}}\left(\left|0000\right\rangle + 2\left|0001\right\rangle + \left|0010\right\rangle + \left|0011\right\rangle + \left|0101\right\rangle + \left|1000\right\rangle + \left|1101\right\rangle\right) \tag{2.a}$$

$$\left|Hpy_4\right\rangle = \frac{1}{2}\left(\left|0001\right\rangle + \left|0111\right\rangle + \left|1010\right\rangle + \left|1101\right\rangle\right) \tag{2.b}$$

$$\left|Lck_4\right\rangle = \frac{1}{\sqrt{6}}\left(\left|0001\right\rangle + \left|0011\right\rangle + \left|0111\right\rangle + \left|1001\right\rangle + \left|1101\right\rangle + \left|1111\right\rangle\right) \tag{2.c}$$

$$\left|P_4\right\rangle = \frac{1}{\sqrt{6}}\left(\left|0010\right\rangle + \left|0011\right\rangle + \left|0101\right\rangle + \left|0111\right\rangle + \left|1011\right\rangle + \left|1101\right\rangle\right). \tag{2.d}$$

3. Entanglement analysis of sequence states

Since there is not a genuine entanglement measure for a quantum state of arbitrary dimension, in order to analyze the entanglement of the quantum sequence states we will adopt the same strategy used in [5, 8-10]: Given a n-qubit quantum state, there are 2^{n-1}-1 different partial transposes that are relevant to the entanglement measure. The bipartite entanglement of the i-th bipartition is given by

$$E_i\left(\left|s_n\right\rangle\right) = S_{VN}\left[Tr_j\left(\left|s_n\right\rangle\left\langle s_n\right|\right)\right]. \tag{3}$$

In (3) S_{VN} is the von Neumann entropy, $S_{VN}(\rho)$=Tr[ρlog(ρ)], and j represents the set of qubits traced out. The total amount of entanglement is simply given by the sum of the bipartite entanglement of all relevant bipartitions

$$E_{sum}\left(\left|s_n\right\rangle\right) = \sum_{i=1}^{2^{n-1}-1} E_i\left(\left|s_n\right\rangle\right) \tag{4}$$

or its average value

$$E_{avg}^{all}\left(\left|s_n\right\rangle\right)=\frac{E_{sum}\left(\left|s_n\right\rangle\right)}{2^{n-1}-1}. \tag{5}$$

However, the calculation of (5) requires a considerable computational effort when the number of qubits grows. An alternative and easier to calculate entanglement measure is the average between the entanglement of bipartitions formed by one qubit and *n*-1 qubits (hence, only *n* bipartitions are used). We use the upper level index to indicate these particular bipartitions. Thus, for an *n*-qubit state one has

$$E^1\left(\left|s_n\right\rangle\right)=S_{VN}\left[Tr_1\left(\left|s_n\right\rangle\left\langle s_n\right|\right)\right],E^2\left(\left|s_n\right\rangle\right)=S_{VN}\left[Tr_2\left(\left|s_n\right\rangle\left\langle s_n\right|\right)\right],...,E^n\left(\left|s_n\right\rangle\right)=S_{VN}\left[Tr_n\left(\left|s_n\right\rangle\left\langle s_n\right|\right)\right] \tag{6}$$

$$E_{avg}^{th}\left(\left|s_n\right\rangle\right)=\frac{1}{n}\sum_{i=1}^{n}E^i\left(\left|s_n\right\rangle\right). \tag{7}$$

Figure 1 shows E^i for six sequence states of 28 qubits.

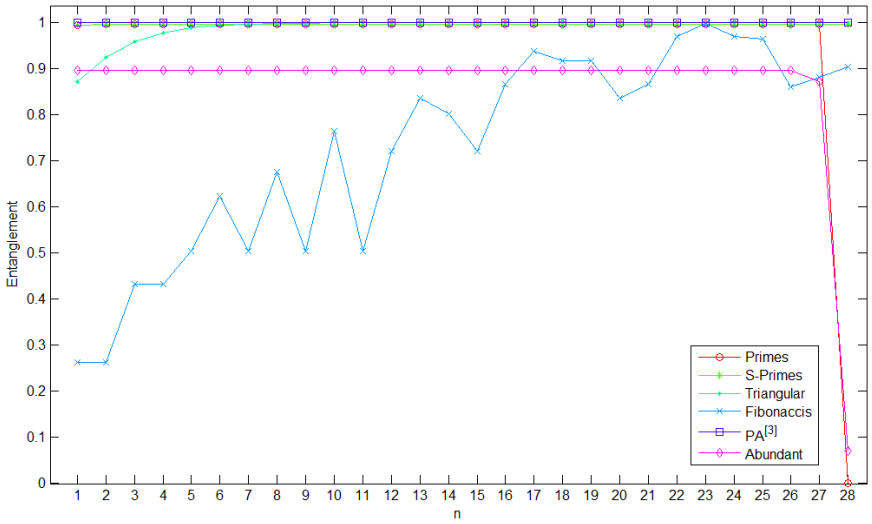


Figure 1: E^i versus *i*, for Prime, S-prime, Triangular, Fibonacci, PA[3] and abudant sequences.

Observing Fig.1, one can note that the entanglement of each individual qubit with the others 27 qubits of the Abundant and Prime states has a similar behavior: with exception of the last

qubit that has low entanglement with the others (zero in the case of the Prime state), all the others are highly entangled with the rest of the state. The explanation given in [5] associates this behavior with the fact that the Prime sequence is formed almost exclusively by odd numbers. This explanation cannot be used for the Abundant state that has a significant amount of both, odd and even numbers. The Fibonacci state, by its turn, shows a very different behavior, there is a low entanglement between the first qubits and the rest, furthermore, the value of E^i changes in a non-regular way when i grows. A resume of average entanglement values given by (7) is shown in Table 1.

Table 1: E_{avg}^{th} for 28-qubits quantum sequence states.

State	E_{avg}^{th}	State	E_{avg}^{th}
Prime	0.9606	Triangular	0.9897
SPrime	0.9964	Abundant	0.8660
Fibonacci	0.7302	PA[3]	1.0000

The entanglement of the quantum sequences SPrime, Triangular, Abundant and PA[3] overcomes the entanglement of the Prime state. In particular, the sequence PA[3] shows the maximal entanglement value, hence, each individual qubit of PA[3] is in the maximally mixed state. The relation between the entanglement of the series changes when the average between all bipartitions is taken into account. Figure 2 shows the comparison of E_{avg}^{th} and E_{avg}^{all} between PA[3] and Fibonacci states.

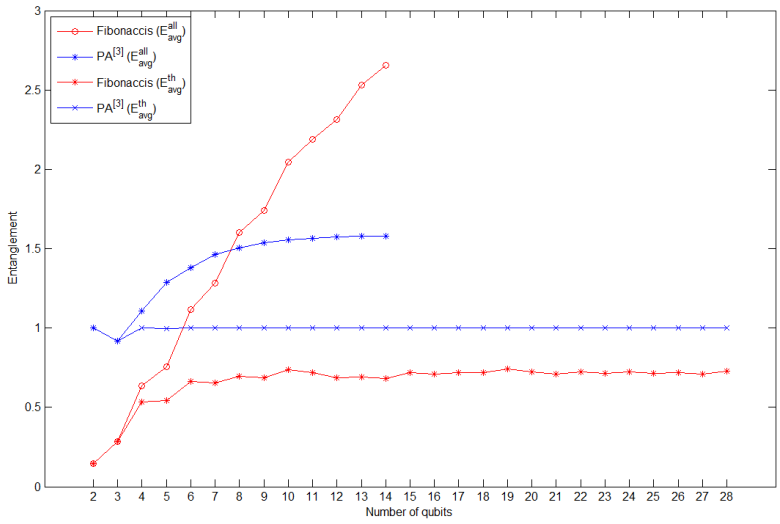


Figure 2: Comparison of E_{avg}^{th} and E_{avg}^{all} between Fibonacci and PA[3] states.

As it can be seen in Fig. 2, one has $E_{avg}^{th}\left(\left|PA_n^{[3]}\right\rangle\right) > E_{avg}^{th}\left(\left|Fib_n\right\rangle\right)$ for any number of qubits up to 28, while $E_{avg}^{all}\left(\left|PA_n^{[3]}\right\rangle\right) < E_{avg}^{all}\left(\left|Fib_n\right\rangle\right)$ for sequence states having more than six qubits.

It is not an easy task to understand for which reason a sequence state shows a large amount of entanglement. A supposition made in [5] is that the entanglement of the Prime state emerges from intrinsic randomness of prime numbers. However, as it can be seen in Fig. 1 and Tab. 1, using E_{avg}^{th} as reference, there are quantum sequence states originated from deterministic sequences whose entanglement is larger than the entanglement of the Prime state. The more regular of them is the $\mathrm{PA}^{[r]}$ state. In Fig. 3 one can see the entanglements E_{avg}^{th} and E_{avg}^{all} of $\mathrm{PA}^{[r]}$ for r = 3,5,7,9.

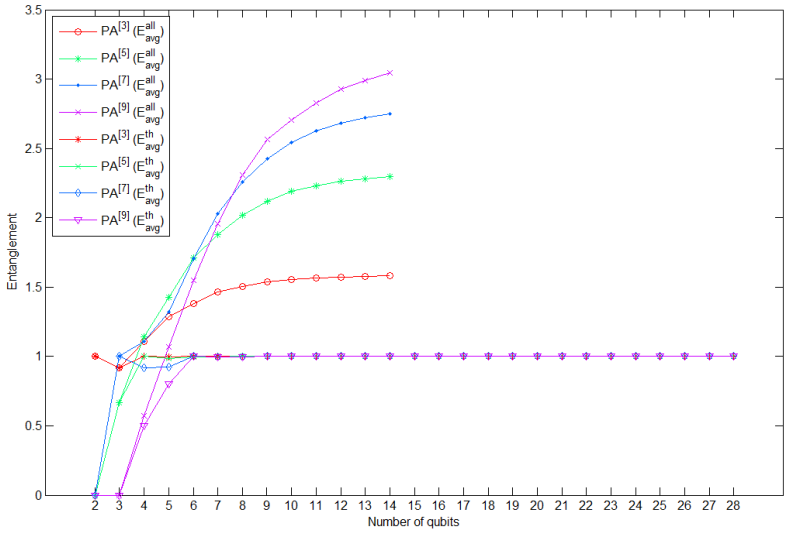


Figure 3: E_{avg}^{th} (up to 28 qubits) and E_{avg}^{all} (14 qubits) for $\mathrm{PA}^{[r]}$, r = 3,5,7,9.

Observing Fig. 3, one can note that the $\mathrm{PA}^{[r]}$ state tends to have most qubits maximally entangled with the others. Furthermore, for the set of values of r considered, after the seventh qubit, the larger the value of r the larger is E_{avg}^{all}. On the other hand, it is not hard to see that $\mathrm{PA}^{[r]}$ states do not have any entanglement when r is a power of two. This fact can be seen in Fig. 4 that shows $E_{avg}^{all}\left(\left|PA_{14}^{[r]}\right\rangle\right)$ versus r for a quantum state with 14 qubits. In fact, for $r = 2^k$ one has the following (completely disentangled) sequence state:

$$\left|PA_n^{\left[r=2^k\right]}\right\rangle = \begin{cases} \left|0\right\rangle^{\otimes n} & n < k \\ \left(H\left|0\right\rangle\right)^{\otimes(n-k)} \otimes \left|0\right\rangle^{\otimes k} & n \geq k \end{cases}. \tag{8}$$

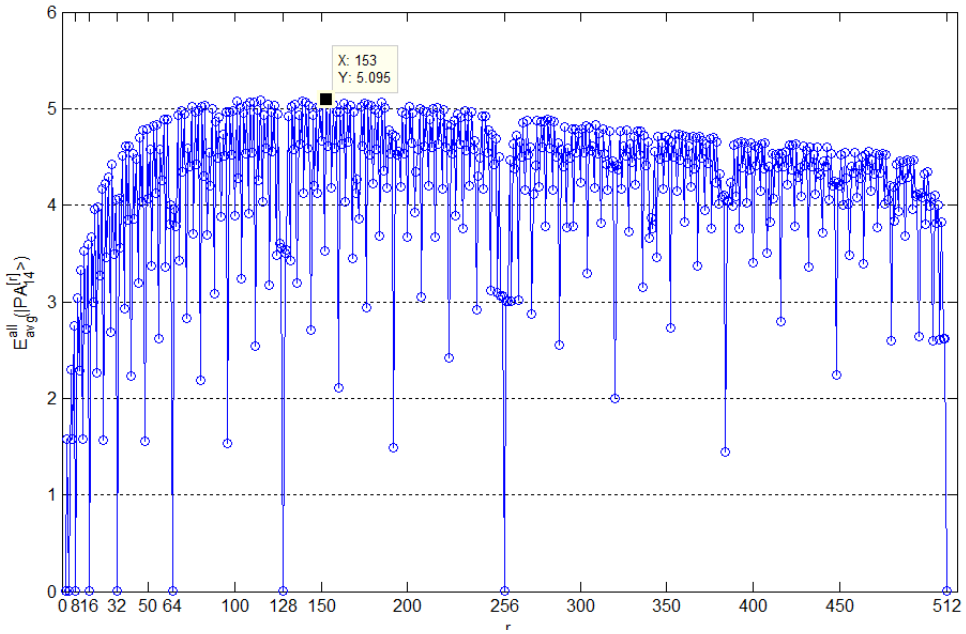


Figure 4: $E_{avg}^{all}\left(\left|PA_{14}^{[r]}\right\rangle\right)$ verus r.

In [5,6] is pointed out that the Prime state carries a large amount of entanglement but, in fact, how near from a maximally entangled (using (4)) n-qubit state is the n-qubit Prime state? Figure 5 shows E_{avg}^{all} for five different quantum sequence states.

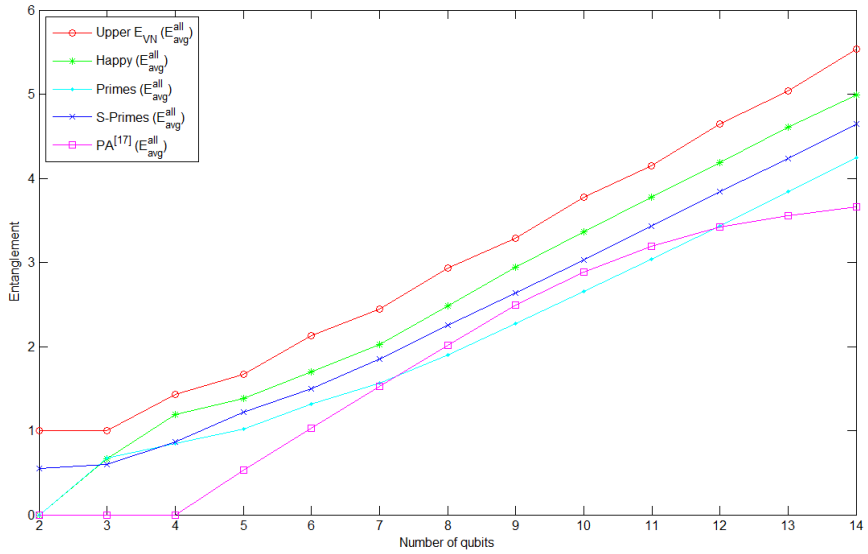


Figure 5: E_{avg}^{all} versus number of qubits and its comparison with the maximal value reacheable by the measure. Happy, Prime, Sprime and $PA^{[17]}$ sequences.

Analyzing Fig. 5, one can see that, inside the short search space observed, the entanglement of the states SPrime and Happy overcomes the Prime state's entanglement. While the Prime state reaches nearly 68% of predicted upper bound, the SPrime and Happy states reach, respectively, 74% and 78%. On the other hand, the entanglement of the PA[17] state overcome the Prime state's entanglement only in a short range, after, it begins to move away from the upper bound. In Fig. 6 other sequence states are shown.

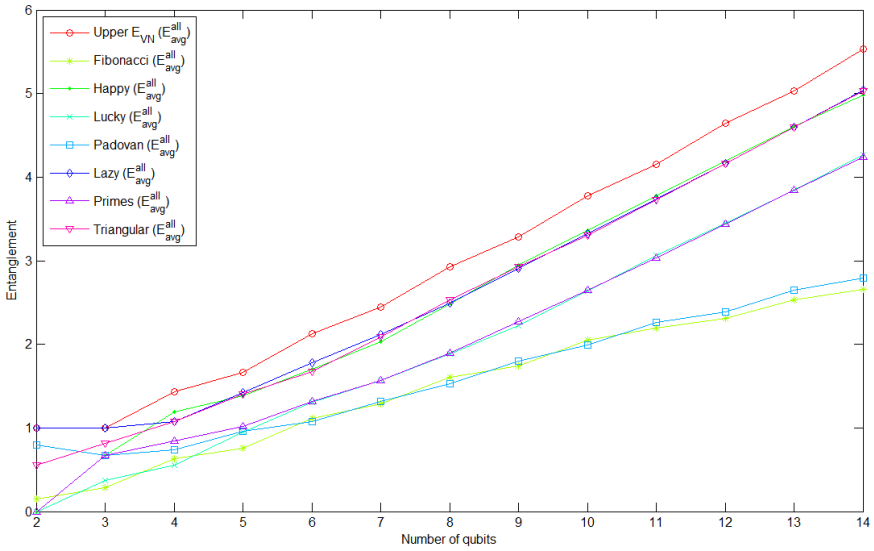


Figure 6: E^{all}_{avg} versus number of qubits and its comparison with the maximal value reacheable by the measure. Fibonacci, Happy, Lucky, Padovan, Lazy, Primes and Triangular sequences.

The Fibonacci and Padovan states follow a similar behavior and they have only five common elements (~7%). Similarly, the Lucky and Prime states follow a similar behavior and they have only ~7% of common elements. Furthermore, the Happy, Lazy and Triangular states also have a common entanglement behavior.

Now, let us introduce a new sequence, hereafter named *S*. In order to construct *S* we start with the sequence $S = \{0,3\}$. The sequence *S* is obtained iteratively according to the following steps ($k = 2,3,4,\ldots, n\text{-}1$):

- If k is even, then $S = S \cup \max(\{1,2,\ldots,2^k\text{-}1\}\text{-}S)$ and $k = k+1$. This step adds only one number to the sequence.
- If k is odd, then $S = S \cup \text{bitxor}(S,2^{k+1}\text{-}1)$ and $k = k+1$. If X is the set $\{x_1,x_2,x_3,\ldots,x_n\}$ and Y is just a number, then $bitxor(X,Y)$ is the set $\{\text{Dec}(\text{Bin}(x_1)\oplus\text{Bin}(Y)), \text{Dec}(\text{Bin}(x_2)\oplus\text{Bin}(Y)),\ldots,$

Dec(Bin(x_n)⊕Bin(Y))}. Here Dec and Bin are functions that return, respectively, the decimal and binary value of the argument.

For example, let us construct the sequence that finishes at k = 6.

k=2	S = {0, 3} ∪ max({1, 2, 3} – {0, 3}) → S = {0, 3} ∪ max({1, 2}) → S = {0, 3} ∪ {2} → S = {0, 2, 3}. k = 2 + 1.
k=3	S = {0, 2, 3} ∪ bitxor({0, 2, 3}, 15) → S = {0, 2, 3, 12, 13, 15}. k = 3 + 1. bitxor({0, 2, 3}, 15) = {(0⊕15), (2⊕15), (3⊕15)} = {15, 13, 12}
k=4	S = {0, 2, 3, 12, 13, 15} ∪ max({1, 2, 3, …, 15} – {0, 2, 3, 12, 13, 15}) → S = {0, 2, 3, 12, 13, 15} ∪ max({1, 4, …, 11, 14}) → S = {0, 2, 3, 12, 13, 15} ∪ {14} → S = {0, 2, 3, 12, 13, 14, 15}. k = 4 + 1.
k=5	S = {0, 2, 3, 12, 13, 14, 15} ∪ bitxor({0, 2, 3, 12, 13, 14, 15}, 63) → S = {0, 2, 3, 12, 13, 14, 15} ∪ {48, 49, 50, 51, 60, 61, 63}→ S ={0, 2, 3, 12, 13, 14, 15, 48, 49, 50, 51, 60, 61, 63}. k = 5+1. bitxor{0,2,3,12,13,14,15},63) = {(0⊕63), (2⊕63), (3⊕63), (12⊕63), (13⊕63), (14⊕63), (15⊕63)} = {48, 49, 50, 51, 60, 61, 63}
k=6	The procedure ends.

Hence, the sequence generated in this example is S = {0,2,3,12,13,14,15,48,49,50,51,60,61, 63}. The quantum sequence state $|S\rangle$ has an interesting behavior, its entanglement shows an oscillation with period of one qubit. In Figs. 7 and 8 one can see, respectively, the oscillatory behavior of E_{avg}^{th} for $|S_{28}\rangle$ and E_{avg}^{all} for $|S_{14}\rangle$.

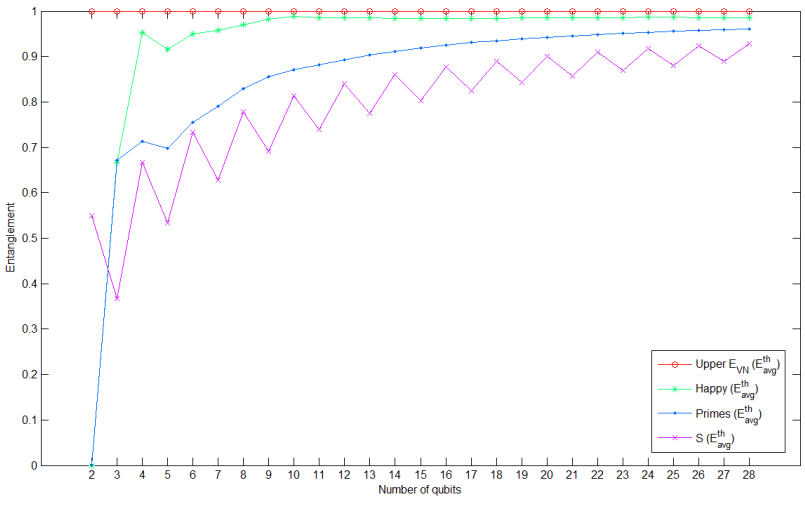


Figure 7: E_{avg}^{th} versus number of qubits for $|S_{28}\rangle$.

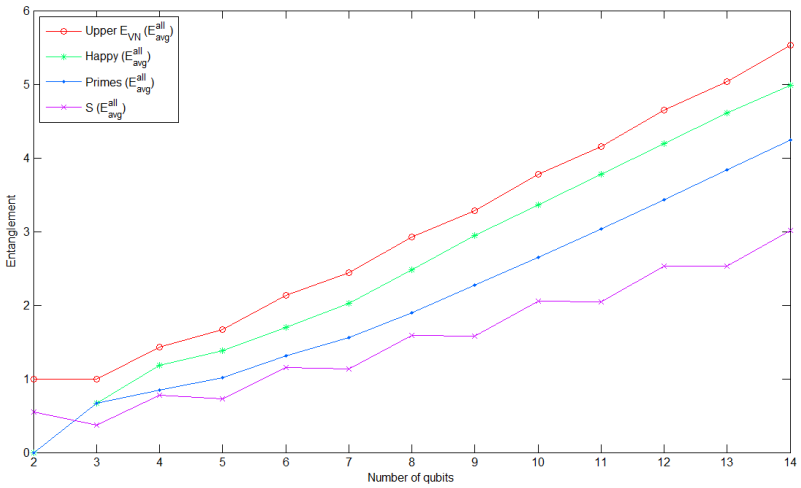


Figure 8: E_{avg}^{all} versus number of qubits for $|S_{14}\rangle$.

4. Quantum sequence state preparation with Grover's quantum search

The approach proposed to prepare the Prime state in [5] can also be used to prepare other quantum sequence states, provided that there is an oracle able to check whether a given element belongs to the considered sequence. Basically, the algorithm searches for $\tau(2^n)$ items within a set of 2^n elements. Grover's algorithm accomplishes this in $O((\tau(2^n)/2^n)^{1/2})$. The optimal value of iterations is given by

$$G(n) = \frac{\pi}{4\arcsin\left(\sqrt{\frac{\tau(2^n)}{2^n}}\right)} - \frac{1}{2}. \qquad 9$$

Hence, the feasibility of the sequence state generation using quantum search depends on how $G(n)$ grows when n (the number of qubits) increases. Figure 9 shows the curve of $G(n)$ versus n for Fibonacci, Lucky, Padovan, Lazy and Triangular quantum sequence states.

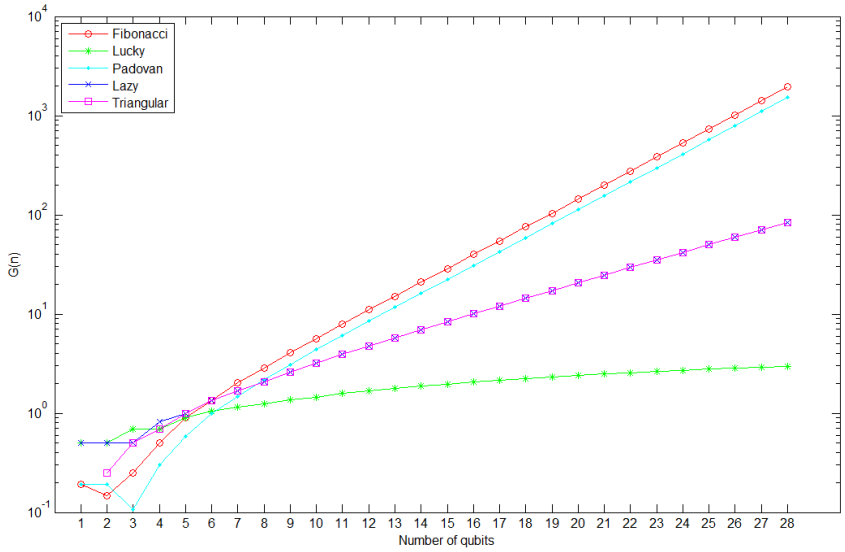


Figure 9: Number of Grover's iterations versus number of qubits for Fibonacci, Lucky, Padovan, Lazy and Triangular quantum sequence states.

Figure 10 shows a similar plot for Abundant, Happy, Hashard, Lucky, Prime and SPrime sequence states. The Abundant and Happy sequence states seem to assume a constant behavior ($\pi(2^n)/2^n$ remains roughly constant). The efficiency of generation of the SPrime state overcomes the efficiency of generation of the Prime state.

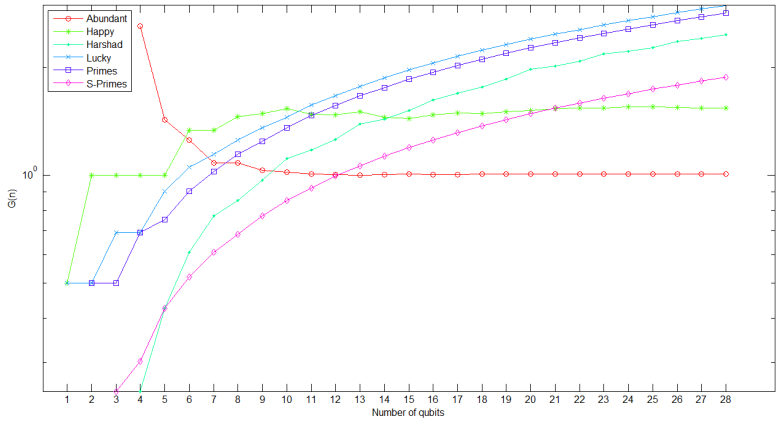


Figure 10: Number of Grover's iterations versus number of qubits for Abundant, Happy, Hashard, Lucky, Prime and SPrime sequence states.

Regarding the PA states, after a growing initial part, a constant behavior appears, as can be seen in Fig. 11.

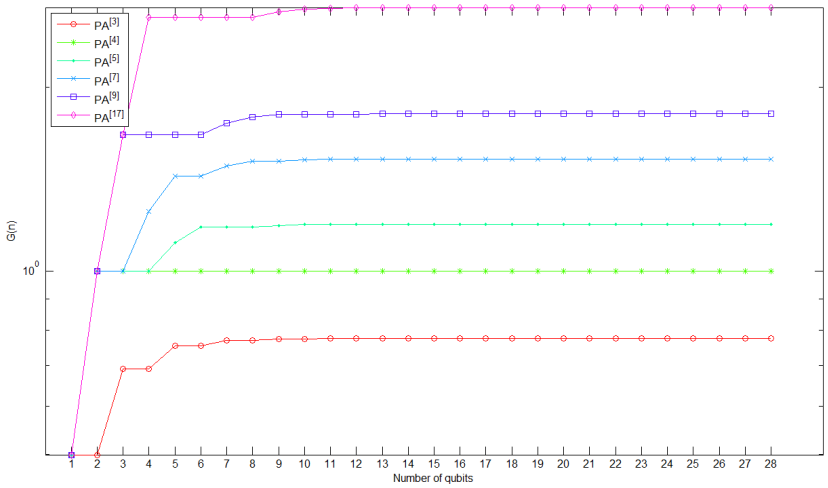


Figure 11: Number of Grover's iterations versus number of qubits for $PA^{[r]}$ sequences, $r \in \{3,4,5,7,9,17\}$.

At last, the curve of $G(n)$ for the state $|S\rangle$ with oscillatory entanglement can be seen in Fig. 12.

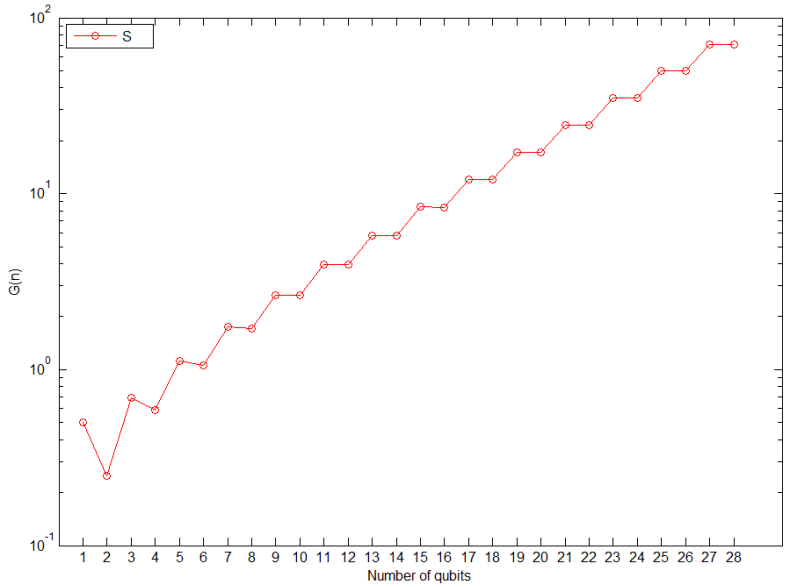


Figure 12: Number of Grover's iterations versus number of qubits for the sequence state $|S\rangle$.

Moebius state

$$\left|\ddot{m}\right\rangle = \frac{1}{\sqrt{\sum_{n=0}^{2^N-1}\left[\mu(n)\right]^2}} \sum_{n=0}^{2^N-1} \mu(n)\left|n\right\rangle$$

$$\left|\ddot{m}^2\right\rangle = \frac{1}{\sqrt{\sum_{n=0}^{2^N-1}\left[\mu(n)\right]^2}} \sum_{n=0}^{2^N-1} \left[\mu(n)\right]^2\left|n\right\rangle$$

$$\left|\left\langle \ddot{m}^2 \middle| \ddot{m}\right\rangle\right| = \frac{\left|M\left(2^N\right)\right|}{\sum_{n=0}^{2^N-1}\left[\mu(n)\right]^2} = \left|\frac{1}{2} - \frac{l\left(\left|\ddot{m}\right\rangle\right)}{2^N}\right|$$

$$L\left(2^N\right) = \sum_{n=0}^{2^N-1}\left[\mu(n)\right]^2 \sim 1 + \frac{6}{\pi^2}\left(2^N\right) + O\left(\sqrt{2^N}\right)$$

5. Conclusions

The analysis of the entanglement of sequence states is a hard task. Sequences states with similar entanglement behavior may have a common pattern but such pattern is not readily observed just looking at their elements. Prime and Lucky states are good examples, as well Fibonacci and Padovan states.

The Prime state has the charm of being related to prime numbers that play a crucial role in number theory. However, the Prime state is not the most entangled sequence state (for example, the Happy and SPrime sequences have more entanglement) as well it is not efficiently produced by quantum search.

Trying to connect entanglement with a pseudo-randomness of the numbers that make-up the sequence seems not to be a fruitful path since there are sequence states that emerge from a trivial increment pattern, which can carry a significant amount of entanglement. In particular, the sequence state PA[3] has maximal entanglement between each individual qubit and the rest *n*-1 qubits.

The way in which the entanglement changes when a qubit is added depends on the sequence considered. All sequences obtained from [7] showed a (growing) smooth behavior of E_{avg}^{all}. However, this is not a rule. In order to show this, we created a sequence whose related quantum state shows an (growing) oscillatory behavior of E_{avg}^{all}.

The feasibility of sequence state preparation using Grover's algorithm depends on the relation $\pi(2^n)/2^n$: if the number of integers that belong to the series grows in a rate lower than 2 when a qubit is added, then the use of Grover's algorithm is not viable for large values of *n*. This happens for Fibonacci, Lucky, Lazy, Padovan, Triangular, Sprime, Prime and the introduced *S* series. On the other hand, the Abundant, Happy and PA series can be efficiently produced with Grover's algorithm.

Acknowledgments

This work was supported by the Brazilian agency CNPq Grant no. 303514/2008-6. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

[1] A. Borisov, M. B. Nathanson, Y. Wang, Quantum integers and cyclotomy, Journal of Number Theory 109 (1) (2004) 120 – 135. doi:http://dx.doi.org/10.1016/j.jnt.2004.06.015.

[2] K. Tokuo, Quantum number theory, International Journal of Theoretical Physics 43 (12) (2004) 2461–2481. doi:10.1007/s10773-004-7711-6.

[3] A. V. Kontorovich, M. B. Nathanson, Quadratic addition rules for quantum integers, Journal of Number Theory 117 (1) (2006) 1 – 13. doi:http://dx.doi.org/10.1016/j.jnt.2005.04.015.

[4] R. V. Ramos, F. V. Mendes, Riemannian quantum circuit, Physics Letters A 378 (20) (2014) 1346 – 1349. doi:http://dx.doi.org/10.1016/j.physleta.2014.02.008.

[5] J. I. Latorre, G. Sierra, Quantum Computation of Prime Number Functions, Quantum Information & Compoutation 14 (2014) 577–588. arXiv:1302.6245.

[6] J. I. Latorre, G. Sierra, There is entanglement in the primes, ArXiv e-printsarXiv:1403.4765.

[7] OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences (2011). Avaliable at http://oeis.org.

[8] I. D. K. Brown, S. Stepney, A. Sudbery, S. L. Braunstein, Searching for highly entangled multi-qubit states, Journal of Physics A: Mathematical and General 38 (5) (2005) 1119.

[9] A. Borras, A. R. Plastino, J. Batle, C. Zander, M. Casas, A. Plastino, Multiqubit systems: highly entangled states and entanglement distribution, Journal of Physics A: Mathematical and Theoretical 40 (44) (2007) 13407.

[10] J. E. Tapiador, J. C. Hernandez-Castro, J. A. Clark, S. Stepney, Highly entangled multi-qubit states with simple algebraic structure, Journal of Physics A: Mathematical and Theoretical 42 (41) (2009) 415301.

[11] A. Higuchi, A. Sudbery, How entangled can two couples get? , Physics Letters A 273 (4) (2000) 213 – 217. doi:http://dx.doi.org/10.1016/S0375-9601(00)00480-1.

5. **Riemannian quantum circuit**

   - ◇ Periódico: Physics Letters A
   - ◇ Data: 10/02/2014
   - ◇ Situação: Aceito

Physics Letters A 378 (2014) 1346–1349

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Riemannian quantum circuit

R.V. Ramos, F.V. Mendes

Laboratory of Quantum Information Technology, Department of Teleinformatic Engineering, Federal University of Ceara, DETI/UFC, C.P. 6007, Campus do Pici, 60455-970 Fortaleza, Ce, Brazil

ARTICLE INFO

Article history:
Received 20 November 2013
Received in revised form 5 February 2014
Accepted 10 February 2014
Available online 12 February 2014
Communicated by P.R. Holland

ABSTRACT

Number theory is an abstract mathematical field that has found a fertile environment for development in theoretical physics. In particular, several physical systems were related to the zeros of the Riemann-zeta function. In this work we present the theory of a unitary matrix related to a finite number of zeros of the Riemann-zeta function. The equivalent quantum circuit and the calculation of the entanglement of a multipartite quantum state produced by the Riemannian quantum circuit are also shown.

1. Introduction

Recently, there has been a growing interest in quantum systems related to number theory problems [1–3]. Such interest comes from the early days of quantum mechanics, when Hilbert and Pólya discussed a possible physical solution for Riemann's hypothesis: the zeros of the Riemann-zeta function could be the spectrum of an operator $R = I/2 + iH$, where H is self-adjoint and interpreted as a Hamiltonian. Nowadays, several physical systems related to the zeros of the Riemann-zeta function have been discussed [4,5]. In particular, in [6] the authors, having a finite number of zeros of the Riemann-zeta function, used a numerical method for finding a quantum potential able to reproduce those zeros as energy eigenvalues.

In this work, we show how to construct a quantum circuit, hereafter named Riemannian quantum circuit, whose equivalent unitary matrix has eigenvalues related to the zeros (the amount of zeros considered is equal to the dimension of the unitary matrix) of the Riemann-zeta function. The existence of such quantum circuit implies that, at least in principle, it is always possible to construct a physical system related to any finite amount of zeros using a quantum computer. Additionally, we also show a quantum algorithm based on the Riemannian quantum circuit and we briefly discuss the amount of bipartite entanglement generated by the Riemannian quantum circuit for a particular state having up to 16 qubits.

The present work is outlined as follows: Section 2 brings the procedure for building a unitary matrix whose eigenvalues are related to the zeros of the Riemann-zeta function; Section 3 discusses some applications of the Riemannian quantum circuit; Section 4 shows a quantum circuit related to the unitary matrix obtained in Section 2; at last, conclusions are drawn in Section 5.

2. Procedure to construct the Riemannian unitary matrix

Let s_1, s_2, $s_3, \ldots, s_k$, be a set of the first k non-trivial zeros of the Riemann-zeta function, a function of a complex variable s that analytically continues the sum of the infinite series $\zeta(s) = \sum_n (1/n^s)$. A well known globally convergent analytic continuation of $\zeta(s)$ to the entire complex plane, except $s = 1$, is given by $\zeta(s) = (1 - 2^{1-s})^{-1} \sum_n (1/2^{n+1}) \sum_{k=0}^{n} -1^k \binom{n}{k} (k+1)^{-s}$. It is always possible to build a $(k \times k)$ unitary matrix whose eigenvalues are s_j^*/s_j for $j = 1, \ldots, k$. Initially, let us introduce the $(k \times k)$ matrix G,

$$G = \begin{bmatrix} s_k & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & s_{k-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & s_{k-2} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & s_3 & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & (s_1+s_2)/2 & (s_1-s_2)/2 \\ 0 & 0 & 0 & 0 & \cdots & (s_1-s_2)/2 & (s_1+s_2)/2 \end{bmatrix}. \tag{1}$$

The k eigenvalues of G are the zeros s_1, s_2, $s_3, \ldots, s_k$. Writing the zeros in the form $s_j = a + ib_j$, where both a (as it will be explained latter, the proposed method works only for zeros with the same real part) and b_j are real numbers, the G matrix can be rewritten as the sum of two matrices, $G = aI + iB$,

E-mail addresses: rubens@deti.ufc.br (R.V. Ramos), fernandovm@deti.ufc.br (F.V. Mendes).

http://dx.doi.org/10.1016/j.physleta.2014.02.008
0375-9601/

$$G = aI + iB$$
$$= a\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$
$$+ i\begin{bmatrix} b_k & 0 & 0 & \cdots & 0 \\ 0 & b_{k-1} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & (b_1+b_2)/2 & (b_1-b_2)/2 \\ 0 & 0 & \cdots & (b_1-b_2)/2 & (b_1+b_2)/2 \end{bmatrix}. \quad (2)$$

The matrix $G' = (1/a)G = I + i(1/a)B$ has eigenvalues $(1/a)s_1$, $(1/a)s_2$, $(1/a)s_3, \ldots, (1/a)s_k$, while the matrix $G'^{\dagger} = I - i(1/a)B$ has eigenvalues $(1/a)s_1^*, (1/a)s_2^*, \ldots, (1/a)s_k^*$. Since B/a is Hermitean, the Riemannian unitary matrix is simply obtained by

$$U_R = G'^{\dagger}/G' = \big[I - i(1/a)B\big]\big/\big[I + i(1/a)B\big]. \quad (3)$$

The eigenvalues of U_R are exactly $e^{i\theta_j} = s_j^*/s_j$, for $j = 1, \ldots, k$. As it can be noted, the procedure just described works only for zeros with the same real part, hence, hereafter we will consider $a = 1/2$. In fact, one may note that, if instead of G given by (1) we had chosen G as a diagonal matrix whose elements are $s_1, \ldots, s_k$, zeros with different real parts (if they exist!) could be used. However, in this case, G' with an identity part could not be obtained and, hence, the unitary matrix U_R could not be constructed. Since $a = 1/2$, one has

$$\theta_j = -\pi + \tan^{-1}\big[-b_j\big/\big(1/4 - b_j^2\big)\big]. \quad (4)$$

Some information about the angles θ_j in (4) can be obtained from the Riemann–von Mangoldt formula: the number of Riemann-zeta function zeros $a + ib$ with $0 < b \leqslant T$ is asymptotically given by $N(T) = (T/2\pi)\log(T/2\pi e) + O(\log(T))$. Now, let us consider the following approximation:

$$\theta_j = -\pi + \tan^{-1}\big[-b_j\big/\big(1/4 - b_j^2\big)\big]$$
$$\approx -\pi + \tan^{-1}(1/b_j) \approx -\pi + 1/b_j. \quad (5)$$

For example, for the lowest zero at the critical line ($b_1 \sim 14.134725142000001$) one has $|\theta_1 - (-\pi + 1/b_1)| \sim 3 \cdot 10^{-5}$. The amount of θ's in the range $[\theta_1, \theta_1 - \varepsilon]$ (where $\varepsilon \ll \theta_1$ is a very small angle) is asymptotically given by Riemann–von Mangoldt formula with $T = 1/\varepsilon$. The spacing between two consecutive angles θ_j and θ_{j+1} is $\Delta\theta_j \sim (1/b_j) - (1/b_{j+1}) = (b_{j+1} - b_j)/(b_{j+1}b_j) \sim (\Delta b_j)(\pi + \theta_{j+1})(\pi + \theta_j)$. However, the spacing between the imaginary part of two consecutive zeros, Δb_j, is asymptotically given by $2\pi/\log(j)$, hence, $\Delta\theta_j \sim (2\pi/\log(j))(\pi + \theta_{j+1})(\pi + \theta_j)$. A plot of $\Delta\theta$ versus θ can be seen in Fig. 1. The curve I is obtained using zeros with $b \in [101.3178510060000,\ 120000.3764067760]$ while the curve II is the analytical formula $(2\pi/\log(j))(\pi + \theta_{j+1})(\pi + \theta_j)$ using $j \in [30,\ 169165]$ (the 30th zero is $1/2 + i101.3178510060000$ and the 169 165th zeros is $1/2 + i120000.3764067760$).

At last, since b_j grows when j grows, θ_j gets closer to $-\pi$ when j grows. However, the value of $\sum_{j=1}^{\infty}(\pi + \theta_j)$ seems not to converge (A numerical check using the first 2 001 052 zeros provided by Odlyzko [7] can be easily done). This can be understood if one takes into account that, for large values of j, $b_j \sim 2\pi j/\log(j)$ and, hence, $\sum_j 1/b_j$ does not converge since it is larger than the harmonic series.

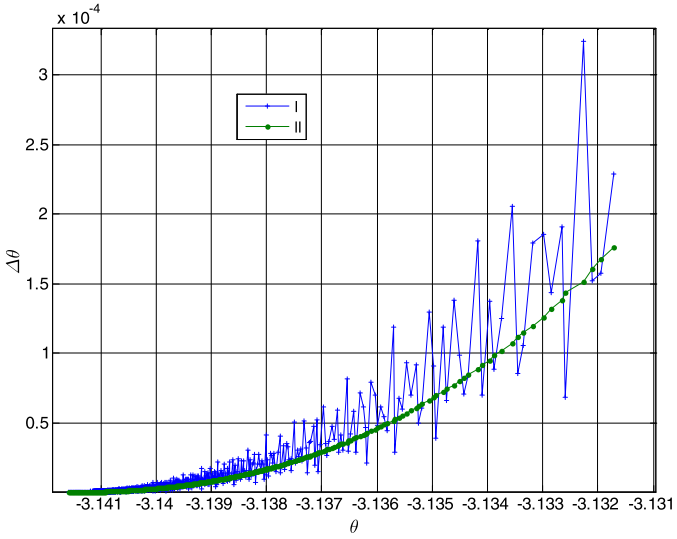


Fig. 1. Spacing between two consecutive θ's versus θ: (I) Obtained using zeros with $b \in [101.3178510060000,\ 120000.3764067760]$. (II) $(2\pi/\log(j))(\pi + \theta_{j+1})(\pi + \theta_j)$ for $j \in [30,\ 169165]$.

3. Applications of the Riemannian quantum circuit

Since the term $-\pi$ in (4) will appear as a global phase in the quantum states, hereafter it will not be taken into account anymore. Thus, one has that $\theta_j \sim 1/b_j$. Now, let us consider $|\psi_1\rangle, \ldots, |\psi_k\rangle$ the set of eigenvectors of $U_R(k \times k)$, where $|\psi_j\rangle$ is the eigenvector associated to the eigenvalue $\exp(i\theta_j)$. Now, let us describe a quantum algorithm for finding the value of $\sum_{j=1}^{k}\theta_j$, where k is the number of zeros. Firstly, we define the quantum translation operator T that shifts the eigenstates by one unity, that is,

$$T|\psi_j\rangle = |\psi_{j+1}\rangle \quad \forall 1 \leqslant j < k, \quad (6)$$
$$T|\psi_k\rangle = |\psi_1\rangle. \quad (7)$$

Furthermore, we define the Riemannian state as

$$|\psi_R\rangle = U_R \sum_{j=1}^{k} \frac{1}{\sqrt{k}}|\psi_j\rangle = \sum_{j=1}^{k} \frac{1}{\sqrt{k}} e^{i\theta_j}|\psi_j\rangle. \quad (8)$$

Using (6)–(8) it is straightforward to check that

$$(TU_R)^k \sum_{j=1}^{k} \frac{1}{\sqrt{k}}|\psi_j\rangle = e^{i(\sum_{m=1}^{k}\theta_m)} \sum_{j=1}^{k} \frac{1}{\sqrt{k}}|\psi_j\rangle. \quad (9)$$

Hence, the quantum state $(1/\sqrt{k})\sum_{j=1}^{k}|\psi_j\rangle$ is an eigenvector of the operator $(TU_R)^k$ with eigenvalue $e^{i(\sum_{m=1}^{k}\theta_m)}$. Thus, the quantum eigenvalue estimation algorithm [8] can be used to get an estimation of $\sum_{m=1}^{k}\theta_m$. Similarly, one can develop a quantum algorithm for estimating the value of $\sum_{m=1}^{k-1}\Delta_{m+1,m}$, where $\Delta_{m+1,m}$ is the difference of the angles of two consecutive eigenvalues: $\theta_{m+1} - \theta_m$ (and, hence, $(\sum_{m=1}^{k-1}\Delta_{m+1,m} = \theta_k - \theta_1)$. In this case, one should firstly note that $R|\psi_j\rangle = \exp(\theta_{j+1} - \theta_j)|\psi_j\rangle$, where $R = (TU_R)^{\dagger}(U_R T)$. Thus, $T(TR)^{k-1}|\psi_1\rangle = e^{i(\sum_{m=1}^{k}\Delta_{m+1,m})}|\psi_1\rangle$ and, hence, $\sum_{m=1}^{k-1}\Delta_{m+1,m}$ can be estimated by using the quantum eigenvalue estimation algorithm.

At last, let us to check the multipartite entanglement of the Riemannian state given in Eq. (8), whose representation in the canonical basis (the basis whose vectors are the columns of the identity matrix: $\{|00\ldots00\rangle, |00\ldots01\rangle, |00\ldots10\rangle, \ldots, |11\ldots10\rangle, |11\ldots11\rangle\}$) is

$$|\psi_R\rangle = \frac{1}{\sqrt{k}}\begin{bmatrix} e^{i\theta_k}|00...00\rangle + e^{i\theta_{k-1}}|00...01\rangle + \cdots \\ + \sqrt{2}e^{i(\frac{\theta_2+\theta_1}{2})}\cos(\frac{\theta_2-\theta_1}{2})|11...10\rangle \\ + i\sqrt{2}e^{i(\frac{\theta_2+\theta_1}{2})}\sin(\frac{\theta_2-\theta_1}{2})|11...11\rangle \end{bmatrix}. \quad (10)$$

In (10) one has $k = 2^n$, where n is the number of qubits. The Riemannian state $|\psi_R\rangle$ carries information about the first k zeros of the Riemann-zeta function. In order to measure its multipartite entanglement, we are going to use the average bipartite entanglement between all bipartitions of the Riemannian state, E_1, and the average bipartite entanglement considering only those bipartitions where one of the parts has only one qubit, E_2:

$$E_1 = \frac{1}{2^{n-1}-1}\sum_{k=1}^{2^{n-1}-1} E(\rho_{\Omega_k \Omega-\Omega_k}), \quad (11)$$

$$E_2 = \frac{1}{n}\sum_{k=1}^{n} E(\rho_{\omega_k \Omega-\omega_k}). \quad (12)$$

In (11)–(12), Ω represents the full set of n qubits, Ω_k represents a particular subset and $\Omega - \Omega_k$ is the subset of Ω whose elements do not belong to Ω_k. Moreover, ω_k represents a set of only one qubit and $\Omega - \omega_k$, with $n-1$ elements, is the subset of Ω whose elements do not belong to ω_k. For instance, for a Riemann state with four qubits one has $\Omega = \{A, B, C, D\}$ and the average entanglements are:

$$E_1 = \frac{1}{7}\begin{bmatrix} E(\rho_{A\_BCD}) + E(\rho_{B\_ACD}) + E(\rho_{C\_ABD}) + E(\rho_{D\_ABC}) \\ + E(\rho_{AB\_CD}) + E(\rho_{AC\_BD}) + E(\rho_{AD\_BC}) \end{bmatrix} \quad (13)$$

$$E_2 = \frac{1}{4}\left[E(\rho_{A\_BCD}) + E(\rho_{B\_ACD}) + E(\rho_{C\_ABD}) + E(\rho_{D\_ABC})\right] \quad (14)$$

The entanglements of $|\psi_R\rangle$ versus number of qubits (up to 16 qubits) are shown in Fig. 2. There, Ent_1 and Ent_3 are obtained from (13) and (14), respectively, by using the von Neumann entropy as bipartite entanglement measure: $E(\rho_{x\_y}) = S_{\mathrm{VN}}(\rho_x) = -\mathrm{Tr}[\rho_x \log(\rho_x)]$, where $\rho_x = \mathrm{Tr}_y(\rho_{x\_y})$ and Tr means the partial trace operation. Similarly, Ent_2 and Ent_4 are obtained from (13) and (14), respectively, by using the linear entropy as bipartite entanglement measure: $E(\rho_{x\_y}) = S_L(\rho_x) = 2\{1 - \mathrm{Tr}[(\rho_x)^2]\}$. For example, considering the von Neumann entropy, for the four qubit case one has $E(\rho_{A\_BCD}) = S_{\mathrm{VN}}(\rho_A) = S_{\mathrm{VN}}(\mathrm{Tr}_{BCD}(|\psi_R\rangle\langle_R\psi|))$ and $E(\rho_{AB\_CD}) = S_{\mathrm{VN}}(\rho_{AB}) = S_{\mathrm{VN}}(\mathrm{Tr}_{CD}(|\psi_R\rangle\langle_R\psi|))$.

As it can be noted, the larger the number of qubits (n) the lower is the average entanglement. In order to understand this behavior, let us consider the distance between the Riemann state and the disentangled state $H^{\otimes n}|0\rangle^{\otimes n} = 1/\sqrt{2^n}\sum_{x=00...0}^{11...1}|x\rangle$: the smaller the distance the lower is the entanglement. Since both of them are pure states, the distance can be simply given by the fidelity: $F = |\langle\psi_R|H^{\otimes n}|0\rangle^{\otimes n}|^2$, with $k = 2^n$. We are going to show that F tends to the value 1 (meaning that they are indistinguishable) when n grows. Firstly, one can note that

$$\left|\sum_{j=0}^{k} e^{i\theta_j}\right|^2 = \sum_{j,l=1}^{k} e^{i(\theta_j-\theta_l)} = \sum_{j=1}^{k} 1 + 2\sum_{\substack{j,l=1 \\ j>l}}^{k} \cos(\theta_j - \theta_l)$$

$$\approx k + 2\sum_{\substack{j,l=0 \\ j>l}}^{k} \cos\left(\frac{1}{b_j} - \frac{1}{b_l}\right)$$

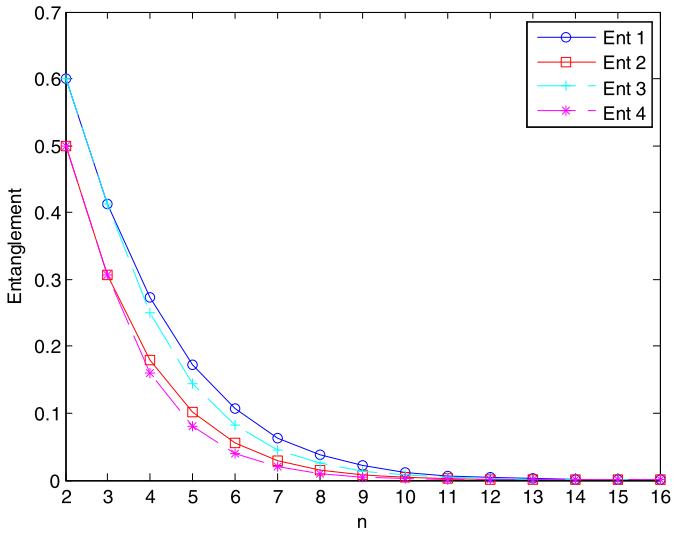


Fig. 2. Average bipartite entanglements versus number of qubits for the Riemannian state given in (10).

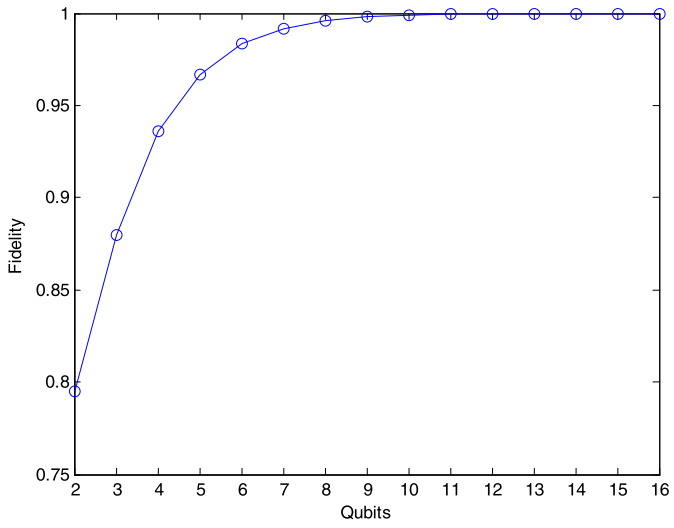


Fig. 3. Fidelity versus number of qubits. $F = |\langle\psi_R|H^{\otimes n}|0\rangle^{\otimes n}|^2$.

$$\approx k + 2\sum_{\substack{j,l=0 \\ j>l}}^{k} \left(1 - \frac{(b_j^{-1} - b_l^{-1})^2}{2}\right)$$

$$\approx k + 2\sum_{\substack{j,l=0 \\ j>l}}^{k} 1 = k + 2\frac{k(k-1)}{2} = k^2. \quad (15)$$

In (15) we used $\cos(\phi) \sim 1 - \phi^2/2 \sim 1$, since $\varphi = (b_j^{-1} - b_l^{-1})$ is very small. Now, returning to the fidelity, after some algebra one has that

$$F = \left|\langle 0^{\otimes n}|H^{\otimes n}|\psi_R\rangle\right|^2 = \frac{1}{k^2}\left|\sum_{j=1}^{k} e^{i\theta_j} - e^{i\theta_2} + (\sqrt{2}-1)e^{i\theta_1}\right|^2. \quad (16)$$

When k grows, the term out of the summation remains constant while the summation grows and become dominant. Hence, using (15) one has that $F \sim 1$ when k is large enough, what means that, for a large number of qubits, $|\psi_R\rangle$ is arbitrarily close to a

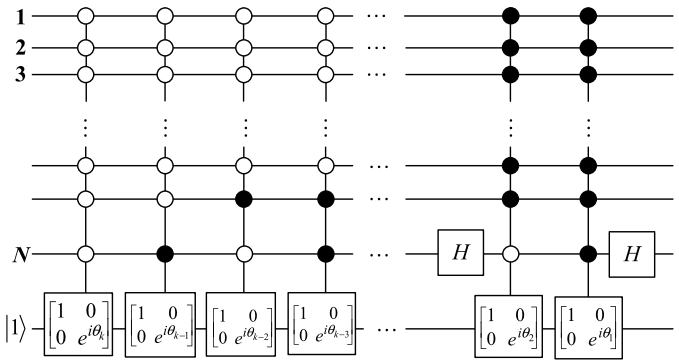


Fig. 4. Riemannian quantum circuit.

disentangled state, hence, it must have low entanglement. This behavior can be seen in Fig. 3 that shows $|\langle\psi_R|H^{\otimes n}|0\rangle^{\otimes n}|^2$ versus number of qubits (up to 16 qubits).

4. Procedure to build the Riemannian quantum circuit

Having the $(k \times k)$ unitary matrix given in (3), it is always possible to obtain a quantum circuit that represents its physical realization. For simplicity, here we consider the number of zeros $k = 2^N$ in order to have a quantum circuit for N qubits.

One can use different procedures in order to obtain a quantum circuit from a unitary matrix, for example the sin–cos decomposition [9]. In general, different procedures will result in different quantum circuits. For the Riemannian quantum circuit, one is expected to obtain a quantum circuit with several CNOTs and single-qubit gates whose parameters' values depend on the values of the zeros of Riemann-zeta function. Here we adopt a simpler approach, based on sin–cos decomposition, using the eigenvectors of U_R: the N qubits of the eigenvectors act as controllers in a N-qubit controlled gate. Using this, the quantum circuit for U_R is as shown in Fig. 4.

In Fig. 4, H is the Hadamard gate:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{17}$$

The eigenstates of the quantum circuit shown in Fig. 4 are the eigenvectors of U_R (the last qubit is always in the state $|1\rangle$ and it is not considered):

$$|\psi_k\rangle = |00\ldots000\rangle,$$
$$|\psi_{k-1}\rangle = |00\ldots001\rangle,$$
$$|\psi_{k-2}\rangle = |00\ldots010\rangle,$$
$$|\psi_{k-3}\rangle = |00\ldots011\rangle,$$
$$\vdots$$
$$|\psi_2\rangle = |11\ldots11\rangle(|0\rangle + |1\rangle)/2^{1/2},$$
$$|\psi_1\rangle = |11\ldots11\rangle(|0\rangle - |1\rangle)/2^{1/2}.$$

The quantum circuit in Fig. 4 shows how to program (hence it requires the knowledge of the used zeros) a universal quantum computer for working as a physical system related to a finite set of zeros of the Riemann-zeta function.

5. Conclusions

Firstly, one can note that our approach is different from the traditional approach found in the literature where people look for a quantum system related to all infinite zeros. In general, the quantum potentials used in such quantum systems are hard to find in nature or to construct artificially. Secondly, we would like to stress that, although we had always considered the first k zeros of the Riemann-zeta function, the theory here described works for any set of k zeros. Hence, we can take any finite number of zeros, anywhere in the critical line, and build a quantum circuit whose eigenvalues are related to them in a very clear way: each eigenvalue depends on only one zero. Hence, one can say that all zeros of the Riemann-zeta function are related to a physical system. In other words, our approach shows how to construct a physical system, with finite resources (finite number of quantum gates), able to work with any (finite) set of different zeros. Furthermore, since this physical system is a quantum circuit, it can be (at least in principle) programmed in a universal quantum computer and physically implemented with optics, superconductor, quantum dots or any other technology for quantum computer implementation.

It can be argued that it is easy to produce a unitary matrix and, consequently, a quantum circuit whose eigenvalues are related to the zeros of the Riemann-zeta function. For example, a $(k \times k)$ unitary matrix related to the zeros could be a diagonal matrix whose elements are $e^{i\theta_j}\, j = 1, \ldots, k$, where θ_j is as given in (4). In this case, the eigenstates are the states of the canonical basis. However, we consider this is not a natural path since the real part of the zeros is not taken into account in any moment. Furthermore, it does not follow the Hilbert-Pólya suggestion of searching for an operator of the type $I/2 + iH$. In our approach, the term $I/2$ comes naturally from the zeros.

Acknowledgements

This work was supported by the Brazilian agency CNPq via Grant No. 303514/2008-6. This work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

[1] W. van Dam, Quantum computing and zeroes of zeta functions, arXiv:quant-ph/0405081, 2004.
[2] W. van Dam, E. Shparlinski, Classical and quantum algorithms for exponential congruences, in: Proceedings of the 3rd Workshop on Theory of Quantum Computation, Communication and Cryptography (TQC 2008), in: Lecture Notes in Computer Science, vol. 5106, 2008, pp. 1–10.
[3] J.I. Latorre, G. Sierra, Quantum computation of prime number functions, arXiv:1302.6245v2 [quant-ph], 2013.
[4] D. Schumayer, D.A.W. Hutchinson, Physics of the Riemann hypothesis, Rev. Mod. Phys. 83 (2011).
[5] R.V. Ramos, Riemann hypothesis as an uncertainty relation, arXiv:1304.2435 [math-ph], 2013.
[6] D. Schumayer, B.P. van Zyl, D.A.W. Hutchinson, Quantum mechanical potentials related to the prime numbers and Riemann zeros, Phys. Rev. E 78 (5) (2008) 056215.
[7] A. Odlyzko, Tables of zeros of the Riemann zeta function, available at http://www.dtc.umn.edu~odlyzko/zeta_tables/, 2014.
[8] P. Kaye, R. Laflamme, M. Mosca, An Introduction to Quantum Computing, 1st ed., Oxford University Press, 2007.
[9] M. Mottonen, J.J. Vartiainen, V. Bergholm, M.M. Salomaa, Quantum circuits for general multiqubit gates, Phys. Rev. Lett. 93 (2004) 130502.