COPPE UFRJ
Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia

ANALISANDO O DESEMPENHO DO CÓDIGO DE STEANE USANDO RANDOMIZED BENCHMARKING

Anderson de Souza Barbosa

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Engenharia de Sistemas e Computação, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia de Sistemas e Computação.

Orientadores: Franklin de Lima Marquezino
Renato Portugal

Rio de Janeiro
Março de 2022

ANALISANDO O DESEMPENHO DO CÓDIGO DE STEANE USANDO RANDOMIZED BENCHMARKING

Anderson de Souza Barbosa

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Orientadores: Franklin de Lima Marquezino
Renato Portugal

Aprovada por: Prof. Franklin de Lima Marquezino
Prof. Renato Portugal
Prof. Celina Miraglia Herrera de Figueiredo
Prof. Carlile Campos Lavor

RIO DE JANEIRO, RJ – BRASIL
MARÇO DE 2022

Barbosa, Anderson de Souza

Analisando o Desempenho do Código de Steane Usando Randomized Benchmarking/Anderson de Souza Barbosa. – Rio de Janeiro: UFRJ/COPPE, 2022.

XI, 53 p.: il.; 29, 7cm.

Orientadores: Franklin de Lima Marquezino
Renato Portugal

Dissertação (mestrado) – UFRJ/COPPE/Programa de Engenharia de Sistemas e Computação, 2022.

Referências Bibliográficas: p. 48 – 51.

1. Correção de erros quânticos. 2. Código de Steane. 3. Randomized benchmarking. I. Marquezino, Franklin de Lima *et al.* II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia de Sistemas e Computação. III. Título.

Dedico este trabalho aos meus pais, Leci e Jorgito. Sem eles nada seria possível.

Agradecimentos

Agradeço primeiro a Deus por ter me dado saúde e forças para superar todas as dificuldades que surgiram ao longo do desenvolvimento deste trabalho, especialmente nos últimos dois anos, que foram tão difíceis para todos.

Agradeço aos meus pais, Leci e Jorgito, por todo o amor e apoio que me deram durante toda a minha vida e pelo esforço investido na minha educação.

Agradeço aos professores Franklin e Renato pela orientação ao longo deste trabalho.

Agradeço aos professores Celina e Carlile por terem aceitado participar da minha banca de mestrado.

Agradeço ao CNPq pela bolsa de estudos que possibilitou a minha dedicação integral ao PESC.

Também quero agradecer à COPPE e a todos os seus professores pela elevada qualidade do ensino oferecido.

Por fim, agradeço a todos os demais que direta ou indiretamente contribuíram para a realização deste trabalho.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

ANALISANDO O DESEMPENHO DO CÓDIGO DE STEANE USANDO RANDOMIZED BENCHMARKING

Anderson de Souza Barbosa

Março/2022

Orientadores: Franklin de Lima Marquezino
Renato Portugal

Programa: Engenharia de Sistemas e Computação

Computadores quânticos prometem resolver determinados problemas exponencialmente mais rápido que computadores clássicos com os melhores algoritmos disponíveis. No entanto, devido à grande presença de ruídos nesses dispositivos, ainda não é possível aproveitar esse potencial para resolver problemas do mundo real. Códigos quânticos de correção de erros (CQCE) são usados para proteger a informação quântica de ruídos e são essenciais para alcançar a computação quântica tolerante a falhas. Nesta dissertação, analisamos o desempenho do código de Steane, um importante CQCE, usando um protocolo de *randomized benchmarking* (RB). Protocolos RB permitem caracterizar parcialmente a qualidade da implementação de um conjunto de portas quânticas ao fornecer uma estimativa da fidelidade entre o ruído médio e o canal identidade. Usando simuladores quânticos com modelos de ruído personalizados, mostramos um cenário em que o uso do código de Steane, com 1 qubit lógico, resulta em uma maior fidelidade do que com 1 qubit físico. Além disso, analisamos situações com ruído em diferentes números de qubits com circuitos codificados e não codificados.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

ANALYZING STEANE CODE PERFORMANCE USING RANDOMIZED BENCHMARKING

Anderson de Souza Barbosa

March/2022

Advisors: Franklin de Lima Marquezino
Renato Portugal

Department: Systems Engineering and Computer Science

Quantum computers promise to solve certain problems exponentially faster than classical computers with the best algorithms available. However, due to the large presence of noise in these devices, it is still not possible to take advantage of this potential to solve real-world problems. Quantum error-correcting codes (QECC) are used to protect quantum information from noise and are essential to achieve fault-tolerant quantum computing. In this dissertation, we analyze the performance of Steane code, an important QECC, using a *randomized benchmarking* (RB) protocol. RB protocols allow to partially characterize the quality of the implementation of a set of quantum gates by providing an estimate of the fidelity between the average noise and the identity channel. Using quantum simulators with custom noise models, we show a scenario where using Steane code, with 1 logical qubit, results in higher fidelity than with 1 physical qubit. In addition, we analyze situations with noise on different numbers of qubits with encoded and unencoded circuits.

Sumário

Lista de Figuras **x**

Lista de Tabelas **xi**

1 Introdução **1**

1.1 Trabalhos relacionados 3

2 Conceitos básicos **5**

2.1 Introdução à computação quântica 5

2.1.1 A esfera de Bloch 7

2.2 Os postulados da mecânica quântica 8

2.2.1 Espaço de estados 9

2.2.2 Evolução 10

2.2.3 Medição quântica 10

2.2.4 Sistemas compostos 12

2.3 O operador densidade 12

2.4 Teoria dos grupos 13

2.5 Designs unitários 14

2.5.1 O grupo de Clifford 15

2.6 Correção de erros quânticos 16

2.6.1 Códigos lineares clássicos 16

2.6.2 Códigos Calderbank-Shor-Steane 17

2.6.3 Formalismo estabilizador 18

2.6.4 Código de Steane 20

2.7 Randomized benchmarking 21

2.7.1 Randomized benchmarking lógico 24

2.8 Canais quânticos 25

2.8.1 Canal despolarizador 25

2.8.2 Atenuação de amplitude 26

2.8.3 Atenuação de fase 28

3 Metodologia **31**
3.1 Modelos de ruído 32
3.2 Método experimental 33
3.2.1 Implementação do código de Steane 34
3.2.2 Experimentos com qubits auxiliares livres de ruído 35

4 Resultados **37**
4.1 Canal despolarizador 37
4.2 Atenuação de amplitude 38
4.3 Atenuação de fase 41
4.4 Discussão comparativa 41

5 Conclusões **45**
5.1 Trabalhos futuros 46

Referências Bibliográficas **48**

Índice Remissivo **52**

Lista de Figuras

2.1 Representação de um qubit na esfera de Bloch 9
2.2 Exemplo de circuito para uma sequência de tamanho m 25
2.3 Efeito do canal despolarizador na esfera de Bloch para $p = 0{,}5$ 26
2.4 Efeito da atenuação de amplitude na esfera de Bloch para $\lambda = 0{,}5$ . . 27
2.5 Efeito da atenuação de fase na esfera de Bloch para $\lambda = 0{,}5$ 29

3.1 Exemplo de modelo de ruído com erro despolarizador 33
3.2 Exemplo de modelo de ruído com erro atenuação de amplitude 33
3.3 Exemplo de modelo de ruído com erro atenuação de fase 34
3.4 Circuito utilizado na codificação no código de Steane 34
3.5 Circuito para medição dos geradores do código de Steane 35

4.1 Gráficos com os resultados dos experimentos com modelos de ruído do canal despolarizador 39
4.2 Gráficos com os resultados dos experimentos com modelos de ruído da atenuação de amplitude 40
4.3 Gráficos com os resultados dos experimentos com modelos de ruído da atenuação de fase 42
4.4 Limiar em função do número de qubits com ruído para cada canal . . 43

Lista de Tabelas

2.1 Ação das portas quânticas de 1 qubit sobre os estados da base computacional 6
2.2 Principais portas do grupo de Clifford codificadas no código de Steane 21

3.1 Conjunto de erros corrigíveis utilizado 36

4.1 Funções ajustadas aos pontos da Figura 4.4 43
4.2 Fidelidades médias encontradas 44

Capítulo 1

Introdução

Alguns algoritmos quânticos proporcionam uma aceleração exponencial sobre os melhores algoritmos clássicos conhecidos para alguns problemas como fatoração de inteiros [1], resolução de sistemas lineares de equações [2] e simulação de sistemas físicos [3, 4]. Para exemplificar a importância disso, considere o sistema de criptografia de chave pública RSA, que se baseia no fato de que é preciso um enorme esforço computacional para encontrar os fatores primos de um número grande usando computadores clássicos [5]. O algoritmo quântico proposto por Peter Shor em 1994 realiza essa tarefa em tempo polinomial.

Entretanto, ainda não é possível tirar proveito desses algoritmos, pois os computadores quânticos atuais sofrem com uma quantidade grande de ruído, o que faz com que grande parte ou toda a informação seja perdida durante o processamento. Para armazenar e processar informação usando um sistema quântico de forma confiável é preciso mantê-lo quase perfeitamente isolado do ambiente externo. No entanto, precisamos que os qubits interajam fortemente para processar informação [6]. Além disso, o sistema precisa ser controlado de fora e precisamos ler os qubits para obter o resultado da computação. É muito difícil atingir todos esses objetivos sem gerar muito ruído, por isso a computação quântica é tão desafiadora. Grandes empresas como IBM, Google, Microsoft e Intel tem trabalhado intensamente para criar computadores quânticos com cada vez mais qubits e menos ruído e estão em uma corrida para desenvolver o primeiro computador quântico universal de larga escala [7].

Uma maneira de tentar contornar ruídos em computadores quânticos é o uso de códigos quânticos de detecção e correção de erros. Esses códigos buscam proteger a informação criando redundâncias, ou seja, codificando cada qubit em vários outros, algo similar ao que é feito por códigos clássicos. No entanto, não é possível simplesmente criar cópias dos qubits a serem protegidos como é possível fazer com bits. Os códigos quânticos ainda não são utilizados pois seriam necessários mais qubits do que os disponíveis nos dispositivos atuais. Embora esses códigos ainda não sejam uma solução definitiva, cada vez mais avanços são feitos na área, que também se

beneficia do desenvolvimento de dispositivos quânticos com cada vez menos ruído.

Para criar dispositivos e códigos quânticos mais eficientes, é importante caracterizar os ruídos que afetam os computadores quânticos atuais. A tomografia de processo quântico é uma técnica que permite a caracterização completa do ruído, no entanto, ela não é escalável, o que dificulta o seu uso [8]. Magesan *et al.* [9] descreveram um protocolo de randomized benchmarking que, embora permita apenas uma caracterização parcial do ruído, é escalável.

O protocolo de randomized benchmarking descrito é adequado para caracterizar ruído em qubits físicos, mas, para avaliar um dispositivo quando é utilizado um código de correção de erros, é necessária uma abordagem que possa caracterizar ruído nos qubits lógicos criados. Com esse objetivo, Combes *et al.* [10] descreveram um randomized benchmarking lógico, que leva em consideração as peculiaridades de circuitos quânticos codificados, como a codificação, a recuperação, a decodificação e o uso de qubits auxiliares.

Harper e Flammia [11] desenvolveram um estudo em que buscaram estimar como a fidelidade entre o canal identidade e o ruído médio do conjunto de portas seria alterada ao usar um código quântico de detecção de erros $[[4, 2, 2]]$ em um computador quântico da IBM. Como resultado encontraram que sem a utilização de nenhum código a fidelidade é de 94,2% e com o código $[[4, 2, 2]]$, ela sobe para 99,4%. Eles utilizaram uma versão modificada do randomized benchmarking apresentada por Hashagen *et al.* [12], que pode ser executada usando apenas portas do grupo de Clifford real. Assim, foi possível obter resultados usando apenas o limitado conjunto de portas do código $[[4, 2, 2]]$, que não possui a porta de fase, por exemplo.

O objetivo deste trabalho foi realizar um estudo similar ao de Harper e Flammia [11] utilizando o código de Steane $[[7, 1, 3]]$ [13]. Por este ser um código de correção de erros, utilizamos a versão do randomized benchmarking descrita por Combes *et al.* [10]. Os experimentos deste trabalho foram realizados utilizando a plataforma IBM Quantum [14]. Como até o início deste trabalho os dispositivos quânticos da IBM não dispunham das instruções necessárias para executar todas as etapas de um código quântico de correção de erros (CQCE), optamos por executar os experimentos em simuladores disponíveis na plataforma e no Qiskit [15], nos quais utilizamos modelos de ruído personalizados. Para obter resultados com mais rapidez, os experimentos foram executados a partir do IBM Quantum Lab. No entanto, isto gerou uma limitação na quantidade de memória que poderia ser usada.

Utilizamos modelos de ruído baseados no canal despolarizador, na atenuação de amplitude e na atenuação de fase. Foram feitos experimentos com ruído em diferentes números de qubits para cada um destes canais. O objetivo foi determinar um limiar para os seus parâmetros em que as curvas de decaimento de fidelidade de experimentos codificados e não codificados fossem aproximadamente iguais, para

cada número de qubits com ruído. Desta forma, para valores abaixo do limiar, experimentos codificados terão um desempenho melhor que os físicos. Devido a limitação de memória supracitada, optamos por colocar ruído apenas nos qubits do código, deixando livres os qubits auxiliares, pois, caso contrário, estimamos que seria necessária uma quantidade de portas da ordem de dezenas de milhares para encontrar o limiar, o que exigiria uma quantidade de memória acima da disponível no IBM Quantum Lab.

Nossos resultados mostram que esses limiares podem ser alcançados, indicando que, sob certas circunstâncias, vale a pena usar o código de Steane, pois uma melhor fidelidade é obtida. Como esperado, quanto maior o número de qubits com ruído, menor foi o limiar, e mostramos que existe uma função que permite calcular o limiar a partir deste número. No entanto, é esperado que o comportamento seja diferente ao avançar em direção ao qubits auxiliares, pois o padrão das portas que atuam neles é diferente daqueles das portas que atuam nos qubits do código. A maior contribuição deste trabalho foi mostrar que em um cenário sem ruído nos qubits auxiliares e com ruído suficientemente baixo baixo nos qubits do bloco do código, obtemos melhores resultados para computações em 1 qubit se usarmos o código de Steane.

1.1 Trabalhos relacionados

Nesta seção apresentaremos alguns trabalhos relacionados ao tema desta dissertação além dos já citados nesta introdução. O randomized benchmarking tem sido bastante estudado nos últimos anos e muitas mudanças no protocolo original tem sido propostas para se adaptar a situações específicas. Por exemplo, um trabalho recente de Morvan *et al.* [16] estende o RB para ser capaz de analisar qutrits (sistemas de três níveis), que oferecem vantagens computacionais sobre qubits convencionais. Eles utilizaram a extensão proposta em um processador de cinco qutrits e encontraram uma infidelidade de portas de um qutrit de $2{,}38 \times 10^{-3}$.

A execução do RB padrão necessita de um conjunto de portas que seja um 2-design unitário, que pode não estar disponível em determinadas situações. Para tentar contornar esse problema, Brown e Eastin [17] examinaram protocolos RB baseados em subgrupos do grupo de Clifford que não formam um 2-design unitário. Eles propuseram um método para analisar esses protocolos e o aplicaram a dois interessantes subgrupos do grupo de Clifford: um gerado pelas portas de Pauli, CNOT e Hadamard e outro gerado apenas pelas portas de Pauli e Hadamard.

O protocolo de randomized benchmarking proposto por em [9] permite estimar o erro médio sobre todo o conjunto de portas do dispositivo sendo analisado, mas não permite estimar o erro médio sobre portas individuais. Pensando nisso, Magesan *et*

al. [18] propuseram um novo protocolo, que chamaram de randomized benchmarking intercalado, para analisar portas quânticas individuais. Ele consiste basicamente de intercalar portas de Clifford aleatórias com a porta de interesse e assim como o protocolo original, ele é escalável no tamanho do sistema quântico.

Uma outra limitação do protocolo RB padrão é a necessidade de compilar portas de Clifford de n qubits, para n grande, em grandes circuitos compostos pelas portas de 1 e 2 qubits nativas do dispositivo a ser analisado. Para contornar esse problema, Proctor *et al.* [19] propuseram um protocolo RB *direto*, que em sua maior parte evita a compilação. A ideia básica desse protocolo é gerar circuitos aleatórios como no RB padrão, mas, ao invés usar portas de Clifford, usar as portas nativas em um dispositivo. Eles testaram o protocolo no dispositivo IBMQX5, da IBM Quantum.

A estrutura do restante desta dissertação é apresentada a seguir. O Capítulo 2 apresenta os conceitos básicos de computação quântica e correção de erros necessários para o entendimento do trabalho, além de explicar o funcionamento do randomized benchmarking. O Capítulo 3 apresenta a metodologia utilizada, explicando como os modelos de ruído e os circuitos foram criados e como os experimentos foram executados. O Capítulo 4 apresenta e analisa os resultados obtidos. Por fim, o Capítulo 5 apresenta as conclusões e trabalhos futuros.

Capítulo 2

Conceitos básicos

Este capítulo apresenta a base teórica de computação quântica necessária para o entendimento do conteúdo deste trabalho. Apresentamos desde princípios básicos da computação quântica até assuntos mais específicos, como correção de erros e randomized benchmarking. Além disso, apresentamos os conceitos de grupos e de designs unitários, que são estruturas matemáticas importantes pra o tema desta dissertação.

2.1 Introdução à computação quântica

Na computação clássica, a informação é codificada em sequências compostas de 0s e 1s para ser armazenada e processada. Na computação quântica, por outro lado, representamos a informação através dos vetores $|0\rangle$ e $|1\rangle$, chamados de qubits e dados por

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.1}$$

e

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.2}$$

A diferença é que um qubit, diferente de um bit, pode estar em uma sobreposição destes vetores, isto é, um qubit genérico $|\psi\rangle$ é dado por

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.3}$$

onde α e β são números complexos e $|\alpha|^2 + |\beta|^2 = 1$.

Na computação clássica, o processo de transformação do estado de entrada no de saída é feito através de um circuito, que é composto por fios, que carregam a informação através dele, e por portas lógicas, que transformam a informação ao longo do circuito. Na computação quântica, a informação é transformada através de

portas quânticas, cujo efeito nos qubits é representado através de matrizes unitárias. As portas de 1 qubit mais comuns na computação quântica são as portas de Pauli, X, Y, Z, I, a porta de Hadamard, H, a porta de fase, S, e a porta $\pi/8$, T, que são dadas por

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{2.4}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \tag{2.5}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2.6}$$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tag{2.7}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{2.8}$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{2.9}$$

e

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}. \tag{2.10}$$

A Tabela 2.1 mostra a ação destas portas de 1 qubit sobre os estados da base computacional, $|0\rangle$ e $|1\rangle$. Observe que a ação da porta X é análoga à da porta lógica clássica NOT. A porta de Hadamard, por sua vez, gera uma superposição dos estados $|0\rangle$ e $|1\rangle$, uma característica única da computação quântica.

Tabela 2.1: Ação das portas quânticas de 1 qubit sobre os estados da base computacional

Porta	Ação sobre $\|0\rangle$	Ação sobre $\|1\rangle$
X	$X\|0\rangle = \|1\rangle$	$X\|1\rangle = \|0\rangle$
Y	$Y\|0\rangle = i\|1\rangle$	$Y\|1\rangle = -i\|0\rangle$
Z	$Z\|0\rangle = \|0\rangle$	$Z\|1\rangle = -\|1\rangle$
I	$I\|0\rangle = \|0\rangle$	$I\|1\rangle = \|1\rangle$
H	$H\|1\rangle = \frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$H\|1\rangle = \frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$
S	$S\|0\rangle = \|0\rangle$	$S\|1\rangle = i\|1\rangle$
T	$T\|0\rangle = \|0\rangle$	$T\|1\rangle = e^{i\frac{\pi}{4}}\|1\rangle$

Com relação às portas de 2 qubits, a mais importante é a porta $CNOT$. A ação dela é inverter o segundo qubit caso o primeiro seja $|1\rangle$. Sua representação matricial

é

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.11}$$

Além destas, um outro conjunto de portas foi importante no desenvolvimento deste trabalho. Ele consiste das portas $U1$, $U2$ e $U3$, que são dadas por

$$U1(\lambda) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{bmatrix}, \tag{2.12}$$

$$U2(\phi, \lambda) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -e^{i\lambda} \\ e^{i\phi} & e^{i(\lambda+\phi)} \end{bmatrix} \tag{2.13}$$

e

$$U3(\theta, \phi, \lambda) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda} \operatorname{sen}\left(\frac{\theta}{2}\right) \\ e^{i\phi} \operatorname{sen}\left(\frac{\theta}{2}\right) & e^{i(\lambda+\phi)} \cos\left(\frac{\theta}{2}\right) \end{bmatrix}. \tag{2.14}$$

Este é um conjunto genérico de portas, ao ajustar os parâmetros θ, ϕ e λ é possível obter qualquer porta de 1 qubit a partir dele. Por exemplo, a partir de $U3$, podemos obter a porta de Hadamard com $\theta = \pi/2$, $\phi = 0$ e $\lambda = \pi$ e a porta X com $\theta = \pi$, $\phi = 0$ e $\lambda = \pi$. A partir de $U1$, podemos obter a porta Z com $\lambda = \pi$ e a porta S com $\lambda = \pi/2$. É importante notar também que as portas $U1$ e $U2$ podem ser obtidas a partir da porta $U3$. Temos que $U1(\lambda) = U3(0, 0, \lambda)$ e $U2(\phi, \lambda) = U3(\pi/2, \phi, \lambda)$.

Para obtermos um resultado de um processamento quântico, é necessário realizar uma medição ao final. Considere um qubit genérico como o apresentado na Equação 2.3. A medição causará o colapso do estado do qubit, que ficará $|0\rangle$, com probabilidade $|\alpha|^2$, ou $|1\rangle$, com probabilidade $|\beta|^2$. Agora, considere o estado genérico de n qubits

$$|\psi_n\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle. \tag{2.15}$$

Neste caso, a medição fará com que $|\psi_n\rangle$ colapse para o estado $|x\rangle$ com probabilidade $|\alpha_x|^2$. Essa é uma medição na base computacional, na Seção 2.2 apresentaremos o postulado da medição da mecânica quântica, em que explicaremos a medição quântica mais formalmente e mostraremos que ela pode ser feita com outras bases.

2.1.1 A esfera de Bloch

A esfera de Bloch é uma representação alternativa do estado de um qubit. Considere a representação da Equação 2.3 e α e β em suas formas polares, $\alpha = |\alpha|e^{i\gamma}$ e

$\beta = |\beta| e^{i(\gamma+\varphi)}$. Além disso, considere um ângulo θ tal que

$$\cos\left(\frac{\theta}{2}\right) = |\alpha| \tag{2.16}$$

e

$$\operatorname{sen}\left(\frac{\theta}{2}\right) = |\beta|. \tag{2.17}$$

Assim, podemos reescrever a Equação 2.3 como

$$\begin{aligned} |\psi\rangle &= \cos\left(\frac{\theta}{2}\right) e^{i\gamma} |0\rangle + \operatorname{sen}\left(\frac{\theta}{2}\right) e^{i(\gamma+\varphi)} |1\rangle \\ &= e^{i\gamma} \left[\cos\left(\frac{\theta}{2}\right) |0\rangle + \operatorname{sen}\left(\frac{\theta}{2}\right) e^{i\varphi} |1\rangle\right] \end{aligned} \tag{2.18}$$

O termo $e^{i\gamma}$ é uma fase global e pode ser desconsiderado, pois não interfere nas estatísticas de medição. Desta forma, podemos representar o estado de um qubit usando apenas dois valores, θ e φ, no lugar dos quatro valores que compõem as amplitudes de $|0\rangle$ e $|1\rangle$. Podemos usar θ e φ para representar um ponto em uma esfera unitária centrada na origem através da equação

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \cos\varphi \operatorname{sen}\theta \\ \operatorname{sen}\varphi \operatorname{sen}\theta \\ \cos\theta \end{bmatrix}. \tag{2.19}$$

Essa esfera é chamada de esfera de Bloch e esse ponto é a representação do qubit correspondente nela. A Figura 2.1 mostra um exemplo de um qubit representado na esfera de Bloch. Note que o estado $|0\rangle$ corresponde ao vetor $\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ e o estado $|1\rangle$ ao vetor $\begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$.

2.2 Os postulados da mecânica quântica

A mecânica quântica é uma teoria da física que fornece uma descrição do comportamento da matéria nas escalas atômica e subatômica, logo, ela é essencial para o entendimento dos conceitos da computação quântica, pois ela fornece a estrutura necessária para o desenvolvimento das leis que um sistema físico deve obedecer [20]. Nesta seção, apresentaremos os quatro postulados básicos da mecânica quântica, que foram derivados após um longo processo de tentativa e erro. Alguns dos postulados reforçam o que já discutimos na seção 2.1 para qubits, mas se referem a sistemas

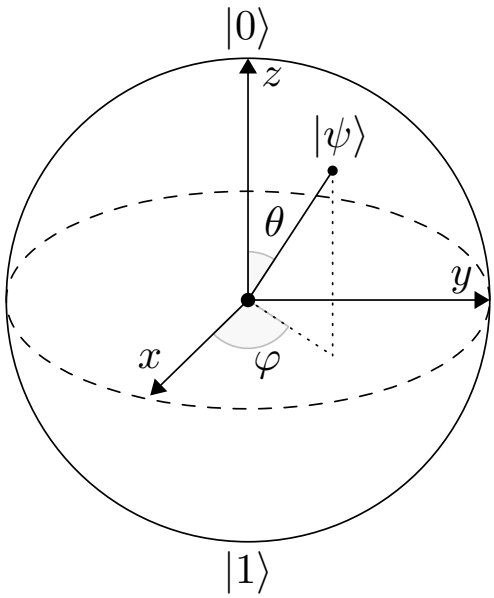


Figura 2.1: Representação de um qubit na esfera de Bloch

físicos em geral.

2.2.1 Espaço de estados

Apresentamos abaixo o postulado que define como o estado de um sistema isolado é descrito. Na seção 2.1, apresentamos o qubit e explicamos como seu estado é descrito. O Postulado 1 define isso de maneira formal para sistemas físicos isolados em geral.

> **Postulado 1:** Todo sistema físico isolado é descrito por um vetor de estados, que é um vetor unitário em um espaço de Hilbert.

O exemplo mais simples de um sistema quântico é justamente o qubit, que, como vimos na seção 2.1, tem seu estado descrito por um vetor bidimensional $\begin{bmatrix}\alpha & \beta\end{bmatrix}^T$, onde α e β são números complexos tais que $|\alpha|^2+|\beta|^2 = 1$. Além disso, $|0\rangle = \begin{bmatrix}1 & 0\end{bmatrix}^T$ e $|1\rangle = \begin{bmatrix}0 & 1\end{bmatrix}^T$ formam uma base para o espaço de Hilbert associado.

O espaço de Hilbert pode ser de dimensão infinita dependendo do grau de liberdade do sistema a que ele está associado. Por exemplo, considere uma partícula que é livre para ocupar qualquer ponto em uma região do espaço. O espaço de Hilbert associado ao seu estado é geralmente considerado um espaço contínuo e, portanto, de dimensão infinita [21].

2.2.2 Evolução

Como o estado de um sistema físico muda com o tempo, o seu vetor de estados $|\psi\rangle$ é uma função do tempo $|\psi(t)\rangle$ [21]. O Postulado 2 define como ela é descrita.

> **Postulado 2:** A evolução de um sistema fechado é descrita por uma transformação unitária.

A afirmação do postulado 2 significa que o estado $|\psi_1\rangle$ do sistema no instante t_1 está relacionado ao estado $|\psi_2\rangle$ no instante t_2 através de um operador unitário U que depende apenas de t_1 e t_2, isto é, $|\psi_1\rangle = U|\psi_2\rangle$. As portas quânticas apresentadas na Seção 2.1 são exemplos de operadores unitários quando o sistema considerado é um qubit.

2.2.3 Medição quântica

O Postulado 2 nos diz como descrever a evolução temporal de um sistema físico. No entanto, ele considera sistemas fechados, isto é, sem interação com o ambiente externo. Ao realizarmos uma computação quântica, em algum momento precisaremos medir o sistema para obter informações úteis. O problema é que, para que a medição seja feita, é preciso que haja interação entre o sistema e equipamento de medição, fazendo com que o sistema deixe de ser fechado e tornando o Postulado 2 inadequado para descrever a evolução de seu estado. O Postulado 3 define como as medições são descritas e como elas influenciam a evolução de sistemas físicos.

> **Postulado 3:** Medições quânticas são descritas por um conjunto $\{M_m\}$ de operadores de medição que atuam no espaço de estados do sistema sendo medido e que satisfazem a equação de completude, isto é
>
> $$\sum_m M_m^\dagger M_m = I. \tag{2.20}$$
>
> Se um sistema estiver no estado $|\psi\rangle$ imediatamente antes de ser medido, a probabilidade $p(m)$ de medir o estado m é
>
> $$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle. \tag{2.21}$$
>
> Após a medição, o estado do sistema é
>
> $$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{2.22}$$

Um importante caso especial do Postulado 3 são as *medições projetivas*. Uma medição projetiva é descrita por um observável O, um operador hermitiano no espaço

de estados do sistema sendo medido. O observável O possui decomposição espectral

$$O = \sum_m mP(m) \tag{2.23}$$

onde $P(m)$ é o projetor no autoespaço de O com autovalor m. Os autovalores de O correspondem aos possíveis resultados da medição. Se um sistema está no estado $|\psi\rangle$ imediatamente antes da medição, a probabilidade $p(m)$ de obter o resultado m é

$$p(m) = \langle\psi| P_m |\psi\rangle \tag{2.24}$$

e o estado do sistema após a medição é

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \tag{2.25}$$

Um exemplo de medição projetiva é a medição na base computacional, que utiliza como observável o operador Z, cuja decomposição espectral é dada por

$$Z = P_0 - P_1 \tag{2.26}$$

onde

$$P_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{2.27}$$

e

$$P_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \tag{2.28}$$

Uma ferramenta matemática útil para aplicações em que o maior interesse são as probabilidades dos diferentes resultados da medição e não o estado do sistema após a medição, é o formalismo POVM (POVM vem de *Positive Operator-Valued Measure*, cuja tradução é Medida com Operador Positivo Valorizado), que é uma consequência do Postulado 3 [20]. Considere uma medição descrita por operadores M_m e

$$E_m = M_m^\dagger M_m. \tag{2.29}$$

Do Postulado 3, temos que

$$\sum_m E_m = I \tag{2.30}$$

e

$$p(m) = \langle\psi| E_m |\psi\rangle \tag{2.31}$$

Os operadores E_m são chamados de elementos POVM e o conjunto $\{E_m\}$ é chamado de POVM.

2.2.4 Sistemas compostos

Com o Postulado 1 podemos entender como representar o estado de um qubit, mas para estudar computações potencialmente úteis, precisamos entender como a mecânica quântica funciona para sistemas compostos por vários qubits interagindo. O Postulado 4 define como é descrito o estado de um sistema composto.

> **Postulado 4:** O espaço de estados de um sistema composto é o produto tensorial dos espaços de estados dos sistemas que o compõem.

Para entender o que significa o Postulado 4, vamos considerar um sistemas composto por dois qubits. Suponha que um sistema de dois qubits seja composto pelos qubits $|\psi_1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ e $|\psi_2\rangle = |0\rangle$. Então, o estado $|\psi\rangle$ deste sistema é

$$\begin{aligned} |\psi\rangle &= |\psi_1\rangle\,|\psi_2\rangle \\ &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |0\rangle \\ &= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}. \end{aligned} \tag{2.32}$$

2.3 O operador densidade

O operador densidade é uma maneira alternativa de descrever sistemas quânticos. Ele é especialmente conveniente para situações em que o estado de um sistema não é completamente conhecido. Suponha que exista um conjunto de estados $\{|\psi_i\rangle\}$ em que um determinado sistema possa estar, cada um com probabilidade p_i. Neste caso, o operador densidade que descreve o sistema é dado por

$$\rho = \sum_i p_i\,|\psi_i\rangle\,\langle\psi_i|\,. \tag{2.33}$$

Para exemplificar, considere o estado $\psi = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. O seu operador densidade é dado por

$$\rho_\psi = |\psi\rangle\,\langle\psi| = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}. \tag{2.34}$$

O estado $|\psi\rangle$ é um exemplo de *estado puro*, que é aquele que é conhecido com exatidão e cujo operador densidade, considerando a representação da equação 2.33, é formado por um somatório de apenas uma parcela. Por outro lado, os estados não totalmente conhecidos são chamados de *estados misturados*. Por exemplo, considere que um sistema quântico está no estado $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ com probabilidade 0,7 e no estado $|1\rangle$

com probabilidade 0,3. O operador densidade que representa o estado deste sistema é dado por

$$\begin{aligned}\rho &= 0{,}7\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right) + 0{,}3\,|1\rangle\langle 1| \\ &= 0{,}7\begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{1}{2} & \frac{1}{2}\end{bmatrix} + 0{,}3\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix} \\ &= \begin{bmatrix}0{,}35 & 0{,}35\\ 0{,}35 & 0{,}65\end{bmatrix}.\end{aligned} \tag{2.35}$$

2.4 Teoria dos grupos

Os grupos são uma estrutura muito importante no estudo da computação quântica e, em especial, no estudo de códigos estabilizadores, como o código de Steane. Nesta seção, apresentaremos o conceito de grupo e algumas de suas propriedades.

Um *grupo* $(G, *)$ é um conjunto não vazio G combinado com uma operação binária "$*$" com as seguintes propriedades:

- **Fechamento:** $g_1 * g_2 \in G$ para todo $g_1, g_2 \in G$
- **Associatividade:** $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ para todo $g_1, g_2, g_3 \in G$
- **Identidade:** Existe $e \in G$ tal que para todo $g \in G$, $g * e = e * g = g$
- **Inversos:** Para todo $g \in G$, existe g^{-1} tal que $g * g^{-1} = g^{-1} * g = e$

Um grupo é *finito* se o seu conjunto subjacente possui um número finito de elementos. Um *subgrupo* de um grupo $(G, *)$ é um grupo $(H, *)$ tal que H é subconjunto não vazio de G.

Um importante exemplo de grupo presente no estudo da computação quântica é o grupo unitário, que é formado pelo conjunto de matrizes unitárias, que são as matrizes U tais que $UU^\dagger = U^\dagger U = I$, junto com a multiplicação matricial. Para reforçar as propriedades acima, vamos mostrar que o grupo unitário as satisfaz.

- **Fechamento:** Sejam A e B duas matrizes unitárias. Por definição, sabemos que $AA^\dagger = I$ e $BB^\dagger = I$. Precisamos mostrar que $(AB)(AB)^\dagger = I$. Temos que

$$(AB)(AB)^\dagger = ABB^\dagger A^\dagger \tag{2.36}$$
$$= AA^\dagger \tag{2.37}$$
$$= I, \tag{2.38}$$

logo, o grupo unitário satisfaz a propriedade do fechamento.

- **Associatividade:** A multiplicação matricial é uma operação associativa, e como ela é a operação binária do grupo unitário, este satisfaz a propriedade da associatividade.

- **Identidade:** O grupo unitário claramente tem como elemento a matriz identidade, satisfazendo assim esta propriedade.

- **Inversos:** É fácil ver que se U é uma matriz unitária, $U^\dagger$ também é, logo, o grupo unitário satisfaz a propriedade dos inversos.

O *gerador* de um grupo G é um subconjunto de seus elementos $g_1, g_2, \ldots, g_l$ tal que todo elemento de G pode ser obtido por uma sequência de operações "$*$" entre elementos desse subconjunto, possivelmente repetidos e escrevemos $G = \langle g_1, g_2, \ldots, g_l \rangle$. Considere, por exemplo, o grupo de Pauli de 1 qubit, que é dado por

$$P_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \tag{2.39}$$

e também tem como operação binária a multiplicação matricial. Note que todos os elementos de P_1 podem ser escritos como um produto das matrizes X, Z e iI, logo, elas formam um gerador para o grupo de Pauli de 1 qubit e escrevemos $P_1 = \langle X, Z, iI \rangle$. Os fatores multiplicativos ± 1 e $\pm i$ garantem que P_1 seja fechado sob multiplicação.

Se H é um subgrupo de G, uma *coclasse à esquerda* de H em G, para algum $g \in G$, é definida por $g * H = \{g * h | h \in H\}$. Uma *coclasse à direita* é definida de maneira análoga. A seguir é apresentado o teorema de Lagrange, que define o número de diferentes coclasses à esquerda de um determinado subgrupo

> **Teorema de Lagrange:** Seja G um grupo finito e H um subgrupo de G. O número $[G : H]$ de diferentes coclasses à esquerda de H em G é dado por $|G|/|H|$.

2.5 Designs unitários

Um conceito importante para entender o funcionamento do protocolo Randomized Benchmarking, apresentado na Seção 2.7 é o de t-design unitário. Ele descreve um conjunto de matrizes unitárias tal que a média de qualquer polinômio de ordem t sobre ele é igual à média sobre o grupo unitário inteiro [22]. Seja $U(d)$ o grupo de matrizes unitárias e $p(U)$ um polinômio em $2d^2$ variáveis, sendo elas os elementos de U e seus complexos conjugados. Formalmente, um t-design unitário é um subconjunto $\mathcal{S} = \{U_K\}_{1,\ldots,K}$ de $U(d)$ tal que, para todo p homogêneo de grau no máximo

t,

$$\frac{1}{K}\sum_{j=1}^{K} p(U_j) = \int_{U(d)} p(U)dU, \tag{2.40}$$

onde a integral é com relação à medida de Haar [23].

No caso $t = 2$, a condição se reduz a

$$\frac{1}{K}\sum_{j=1}^{K} U_j^\dagger \Lambda(U_j \rho U_j^\dagger) U_j = \int_{U(d)} U^\dagger \Lambda(U\rho U^\dagger) U dU \tag{2.41}$$

para todo canal quântico Λ.

2.5.1 O grupo de Clifford

O grupo de Clifford é um conjunto de portas quânticas que forma um 2-design unitário. Ele é o conjunto de matrizes unitárias que normaliza o grupo de Pauli. Mais formalmente, o grupo de Clifford C_n é definido como

$$C_n = \{V \in U_{2^n} \mid VP_nV^\dagger = P_n\}, \tag{2.42}$$

onde U_{2^n} é o conjunto de matrizes unitárias.

Para mostrar que o grupo de Clifford é 2-design unitário, e necessário provar que

$$\frac{1}{|\mathcal{C}_n|}\sum_{k=1}^{|\mathcal{C}_n|} C_k^\dagger \Lambda(C_k \rho C_k^\dagger) C_k = \int_{U(d)} U^\dagger \Lambda(U\rho U^\dagger) U dU. \tag{2.43}$$

Emerson *et al.* [24] avaliaram o lado direto da equação 2.43, que tem forma fechada dada por

$$\begin{aligned}\int_{U(d)} U^\dagger \Lambda(U\rho U^\dagger) U dU = &\frac{\mathrm{Tr}(AB)\mathrm{Tr}(\rho)}{d}\frac{I}{d} \\ &+ \left(\frac{d\mathrm{Tr}(A)\mathrm{Tr}(B) - \mathrm{Tr}(AB)}{d(d^2-1)}\right)\left(\rho - \mathrm{Tr}(\rho)\frac{I}{d}\right),\end{aligned} \tag{2.44}$$

onde A e B são operadores lineares tais que $\Lambda(\rho) = A\rho B$ e "Tr" representa o *traço*, que é a soma dos elementos da diagonal principal de uma matriz quadrada. Uma prova de que o lado esquerdo da equação 2.43 tem a mesma forma fechada pode ser encontrada em [25].

2.6 Correção de erros quânticos

Assim como sua contraparte clássica, códigos quânticos de correção de erros buscam criar redundâncias com o objetivo de preservar a informação caso um pequeno número de qubits seja alterado por ruídos. Para explicar a ideia por trás disso, primeiro apresentaremos um exemplo simples de código clássico de correção de erros.

Considere um código que codifique 1 bit em 3 simplesmente criando três cópias dele. Assim, o bit 0 se torna 000 e o bit 1 se torna 111. A correção de erros neste código é feita de voto de maioria, ou seja, considera-se que o valor correto do bit é aquele que aparece mais vezes na sequência de três bits. Assim, a sequência 001 seria corrigida para 000 e 101 para 111, por exemplo. Agora considere que um bit deve ser enviado através de um canal ruidoso que inverte o bit com probabilidade $p > 0$ e o mantem inalterado com probabilidade $1 - p$. A probabilidade de um erro não ser corrigido é a de dois ou mais bits serem invertidos, isto é, $3p^2 - 2p^3$.

2.6.1 Códigos lineares clássicos

Códigos lineares clássicos surgiram da necessidade de se a confiabilidade da comunicação através de um canal ruidoso [26] e possui muitas aplicações nesta área, mas a teoria envolvida também é de grande importância no desenvolvimento de vários códigos quânticos de correção de erros [20], portanto, apresentaremos uma breve introdução a essa classe de códigos.

Um código linear C que codifica k bits de informação em n bits é descrito por uma matriz geradora G n por k cujas entradas são 0's e 1's. Para codificar uma sequência x de k bits usando o código C, calculamos a multiplicação Gx. Considere, por exemplo, o código de repetição de 3 bits citado anteriormente. A matriz geradora para este código é dada por

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}. \tag{2.45}$$

Temos que $G\begin{bmatrix} 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}^T$ e $G\begin{bmatrix} 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^T$, que é a codificação esperada.

Uma maneira alternativa de definir um código linear é através da sua matriz de verificação de paridade, que possui dimensão $n - k$ por k. Um código com matriz de verificação de paridade H consiste de todos os vetores de n elementos tais que

$$Hx = 0. \tag{2.46}$$

Uma característica fundamental de um código linear é a sua *distância*. Sua definição depende do conceito de distância de Hamming. Suponha que x e y são

duas sequências de n bits cada. A distância de Hamming $d(x, y)$ entre x e y é o número de posições em que x e y diferem. Por exemplo $d(0110, 1100) = 2$, pois, da esquerda para a direita, o primeiro e o terceiro bits são diferentes e os demais são iguais. A *distância* de um código é definida como a distância de Hamming mínima entre quaisquer duas palavras-código, ou seja,

$$d(C) = \min_{x,y \in C, x \neq y} d(x, y). \tag{2.47}$$

A distância de um código é útil para determinar quantos erros ele é capaz de corrigir. Um código com distância de no mínimo $2t + 1$, para algum inteiro t, pode corrigir erros em até t bits. Dizemos que um código que codifica k bits em n e possui distância d é um código $[n, k, d]$.

Um conceito importante na construção de códigos CSS, que serão apresentados na próxima seção, é o de código dual. Considere um código C com matriz geradora G e matriz de verificação de paridade H. O código dual de C, denotado $C^{\perp}$, possui matriz geradora H^T e matriz de verificação de paridade G^T. É equivalente dizer que $C^{\perp}$ consiste de todas as palavras-código que são ortogonais a todas as palavras-código de C.

2.6.2 Códigos Calderbank-Shor-Steane

Códigos Calderbank-Shor-Steane (CSS) são uma importante classe de códigos quânticos de correção de erros com algumas propriedades especiais. Ela foi descoberta por Calderbank e Shor [27] e Steane [28], por isso recebe esse nome. Suponha que C_1 e C_2 são códigos lineares que codificam, respectivamente, k_1 e k_2 bits de informação em n bits tal que $C_2 \subset C_1$ e que C_1 e $C_2^{\perp}$ corrijam t erros. Considere as coclasses de C_2 em C_1 $c_1 + C_2, c_2 + C_2, \ldots, c_N + C_2$, onde $c_1, c_2, \ldots, c_N \in C_1$. Pelo teorema de Lagrange, sabemos que $N = 2^{k_1}/2^{k_2} = 2^{k_1 - k_2}$. Para cada coclasse identificada por c_i, definimos uma palavra-código base dada por

$$|c_i\rangle = \frac{1}{\sqrt{2^{k_2}}} \sum_{c \in C_2} |c_i + c\rangle \,. \tag{2.48}$$

Se $e \in C$ e $f \in C_1$ pertencem à mesma coclasse de C_2, elas definem a mesma palavra-código base, isto é, $|e\rangle = |f\rangle$. Para provar isso, perceba que, se e e f pertencem à mesma coclasse, então existe $h \in C_2$ tal que $e = f + h$. Pela equação 2.48, temos

que

$$
\begin{aligned}
|e\rangle &= \frac{1}{\sqrt{2^{k_2}}} \sum_{c \in C_2} |e + c\rangle \\
&= \frac{1}{\sqrt{2^{k_2}}} \sum_{c \in C_2} |f + h + c\rangle \\
&= \frac{1}{\sqrt{2^{k_2}}} \sum_{h' \in C_2} |f + h'\rangle \\
&= |f\rangle
\end{aligned}
\tag{2.49}
$$

onde $h' = h + c \in C_2$. Perceba que a equação 2.49 é válida porque, se c assume todo os valores de C_2, então $h + c$ também.

Assim, um código CSS construído a partir dos códigos C_1 e C_2 tem N estados base (os estados $|c_i\rangle$) e codificam $k_1 - k_2$ qubits em n qubits. Uma das propriedades mais úteis é dos códigos CSS é que todas as portas do grupo de Clifford codificadas neles podem ser implementadas de forma transversal [29], isto é, de forma tal que cada porta física que a compõe atue em no máximo 1 qubit físico de cada qubit lógico. Assim, se um única porta falhar, vai gerar apenas um erro por qubit lógico, que será corrigido pelo código.

2.6.3 Formalismo estabilizador

O formalismo estabilizador é uma maneira alternativa de representar estados quânticos. Considere, por exemplo, o estado de Bell

$$
|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.50}
$$

Este estado satisfaz as identidades $X_1X_2\,|\psi\rangle = |\psi\rangle$ e $Z_1Z_2\,|\psi\rangle = |\psi\rangle$. Dizemos que o estado $|\psi\rangle$ é estabilizado por X_1X_2 e por Z_1Z_2 e, a menos de uma fase global, é o único. A ideia do formalismo estabilizador é descrever o estado $|\psi\rangle$ pelo conjunto $\{X_1X_2, Z_1Z_2\}$.

De modo geral, o formalismo estabilizador descreve estados de n qubits como subgrupos do grupo de Pauli P_n. O grupo de Pauli de 1 qubit foi apresentado na equação 2.39. Para n qubits, o grupo de Pauli é formado pelo conjunto de todos os produtos tensoriais de n matrizes de Pauli com fatores multiplicativos ± 1 e $\pm i$. Seja S um subgrupo de P_n e V_s o conjunto de todos os estados de n qubits estabilizados por todos os elementos de S. Dizemos que V_s é o *espaço vetorial estabilizado por* S e que este é o estabilizador de V_s.

Precisamos agora definir como aplicar um operador unitário a um estado no formalismo estabilizador. Seja U um operador unitário qualquer e g um operador

que estabiliza o estado $|\psi\rangle$. Temos que

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle\,, \tag{2.51}$$

logo, o operador $UgU^\dagger$ estabiliza o estado $U|\psi\rangle$. Isso significa que, se S é o estabilizador de $|\psi\rangle$, então $S' = \{UgU^\dagger | g \in S\}$ é o estabilizador de $U|\psi\rangle$. Além disso, se $S = \langle g_1, g_2, \ldots, g_l\rangle$, $S' = \langle Ug_1U^\dagger, Ug_2U^\dagger, \ldots, Ug_l, U^\dagger\rangle$, ou seja, para computarmos uma operação unitária usando o formalismo estabilizador, basta calcularmos como ele afeta os geradores do estabilizador do estado a ser modificado. Portanto, vemos que no formalismo estabilizador podemos aplicar qualquer operador unitário U tal que $UgU^\dagger \in P_n$ e, como vimos na Seção 2.5.1, esta é exatamente a definição grupo de Clifford.

A partir deste formalismo, definimos os *códigos estabilizadores*, que são CQCEs cujo conjunto de palavras-código, isto é, seu espaço de código, pode ser gerado por um estabilizador. A maneira usual de descrever um código estabilizador de n qubits é através de um subconjunto P_n que seja gerador do estabilizador de seu espaço de código.

Assim como para códigos clássicos, podemos definir a noção de *distância* para códigos quânticos, mas antes precisamos de outras duas definições. O *peso* de um erro $E \in P_n$ é o número de elementos diferentes da identidade no produto tensorial que o forma. Seja S um grupo estabilizador. O *normalizador* de S em P_n, denotado por $N(S)$, é o conjunto de todos os elementos E de P_n tal que $EgE^\dagger \in S$ para todo $g \in S$. A distância de um código estabilizador é o peso mínimo de um elemento de $N(S) - S$. Se um código estabilizador codifica k qubits em n e possui distância d, dizemos que ele é um código $[[n, k, d]]$. Note que nesta descrição utilizamos colchetes duplos, diferentemente da descrição equivalente para códigos clássicos, em que utilizamos colchetes simples. De forma análoga a um código clássico, um código estabilizador com distância de no mínimo $2t + 1$ é capaz de corrigir erros arbitrários em quaisquer t qubits [20].

Alguns dos mais importantes códigos estabilizadores são o código de Steane [13], o código de 5 qubits [30, 31], que é o menor código quântico capaz de proteger contra erros arbitrários de 1 qubit, e o código de Shor [32]. Embora todos eles sejam códigos muito interessantes, escolhemos utilizar neste trabalho o código de Steane, pois destes três ele é o único que é um código CSS, o que torna a sua implementação bem mais fácil que a dos outros dois.

O formalismo estabilizador possui uma série de vantagens, como o fornecimento de uma descrição compacta de códigos quânticos de correção de erros [33]. Além disso, processamento quântico pode ser eficientemente simulado em um computador clássico usando este formalismo. É importante dizer, no entanto, que apenas um

grupo restrito de estados quânticos podem ser representados através do formalismo estabilizador, o que limita essa capacidade de simulação.

2.6.4 Código de Steane

O código de Steane é um *código estabilizador* que foi apresentado por Andrew Steane em 1996 [13]. Se trata de um código CSS e, consequentemente, podemos codificar nele todas as portas do grupo de Clifford de forma transversal, o que o torna o código ideal para realizar os experimentos deste trabalho. Além disso, ele é um código $[[7, 1, 3]]$, o que significa que codifica 1 qubit lógico em 7 qubits físicos e tem distância 3, ou seja, pode corrigir erros arbitrários em até 1 qubit. O conjunto usado para descrevê-lo é composto pelos operadores

$$\begin{matrix} \texttt{IIIXXXX} \\ \texttt{IXXIIXX} \\ \texttt{XIXIXIX} \\ \texttt{IIIZZZZ} \\ \texttt{IZZIIZZ} \\ \texttt{ZIZIZIZ} \end{matrix}.$$

Os estados $|0_L\rangle$ e $|1_L\rangle$ lógicos são dados por

$$|0_L\rangle = \frac{1}{\sqrt{8}}[|00000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle] \quad (2.52)$$

e

$$|1_L\rangle = \frac{1}{\sqrt{8}}[|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle]. \quad (2.53)$$

A tabela 2.2 mostra as principais portas do grupo de Clifford codificadas no código de Steane. Observe que apenas as versões codificadas das portas Y e S não correspondem ao produto tensorial da versão original. No caso da porta Y_L, o comportamento esperado é $Y_L\,|0_L\rangle = i\,|1_L\rangle$ e $Y_L\,|1_L\rangle = -i\,|0_L\rangle$, mas note que $Y^{\otimes 7}\,|0_L\rangle = -i\,|1_L\rangle$ e $Y^{\otimes}\,|1_L\rangle = i\,|0_L\rangle$, ou seja, $Y^{\otimes 7}$ gera resultados com o sinal oposto ao esperado para Y_L. Para corrigir isso, aplicamos $Z^{\otimes 7}$ antes de $Y^{\otimes 7}$ para inverter o sinal ao aplicar Y_L em $|1_L\rangle$ e depois para inverter o sinal ao aplicar em $|0_L\rangle$. No caso da porta S_L, o comportamento esperado é $S_L\,|0_L\rangle = |0_L\rangle$ e $S_L\,|1_L\rangle = i\,|1_L\rangle$, note que, aplicada

ao estado $|0_L\rangle$, $S^{\otimes 7}$ gera o resultado esperado para S_L, mas $S^{\otimes 7}|1_L\rangle = -i|1_L\rangle$, ou seja, resultado com sinal oposto ao esperado. Para corrigir isso, aplicamos $Z^{\otimes}$ antes para inverter o sinal ao aplicar S_L ao estado $|1_L\rangle$.

Tabela 2.2: Principais portas do grupo de Clifford codificadas no código de Steane

Porta	Versão codificada
X	$X_L = X^{\otimes 7}$
Z	$Z_L = Z^{\otimes 7}$
Y	$Y_L = (ZYZ)^{\otimes 7}$
H	$H_L = H^{\otimes 7}$
S	$S_L = (ZS)^{\otimes 7}$

2.7 Randomized benchmarking

O Randomized Benchmarking (RB) é um protocolo que permite caracterizar parcialmente a qualidade da implementação de um conjunto de portas quânticas ao fornecer uma estimativa da fidelidade entre o canal identidade e o ruído médio $\mathcal{E}$ neste conjunto, que é dada por

$$F(\mathcal{E}) = \int \mathrm{d}\psi \, \langle\psi| \, \mathcal{E}(|\psi\rangle \langle\psi|) \, |\psi\rangle \, . \tag{2.54}$$

Este protocolo foi proposto em [9] e expandido em [8] considerando que o ruído depende da porta e do tempo em que ele atua. É apresentado também, no entanto, um modelo que considera que o ruído é independente de porta e tempo, sendo este o que será utilizado neste trabalho. O RB é executado com o seguinte protocolo:

1. Escolher um tamanho de sequência m e preparar um estado ρ;

2. Escolher aleatoriamente uma sequência de m portas de Clifford, aplicá-la ao circuito e, em seguida, aplicar uma porta de inversão, que, em uma situação ideal, inverte toda a sequência e deixa o circuito equivalente à identidade. Cada operação $\mathcal{C}_j$, está sujeita a um erro Λ, assim, cada sequência por ser representada pela operação

$$\mathcal{S} = \bigcirc_{j=1}^{m+1} (\Lambda \circ \mathcal{C}_j), \tag{2.55}$$

   onde $\mathcal{C}_j$ é a operação que representa a porta aplicada no instante j.

3. Realizar a medição para determinar se voltou ao estado inicial.

Os passos acima devem ser repetidos para estimar a probabilidade de sobrevivência, isto é, a probabilidade de voltar ao estado inicial, para cada tamanho de sequência, que é dada por $\mathrm{Tr}[E_\psi \mathcal{S}(\rho_\psi)]$ para a sequência $\mathcal{S}$. Considerando que são escolhidas K_m sequências de m portas, a fidelidade da sequência média é dada por

$$F_{seq}(m, \psi) = \mathrm{Tr}[E_\psi \mathcal{S}_{K_m}(\rho_\psi)], \tag{2.56}$$

onde

$$\mathcal{S}_{K_m} = \frac{1}{N} \sum_{i=1}^{N} \mathcal{S}_i \tag{2.57}$$

é a operação que representa a sequência média.

A curva da probabilidade de sobrevivência em função do número de portas, chamada de *curva de decaimento de fidelidade*, pode ser ajustada ao modelo

$$\mathcal{F}_g(m, |\psi\rangle) = Ap^m + B, \tag{2.58}$$

onde

$$A = \mathrm{Tr}\left[E_\psi \Lambda \left(\rho_\psi - \frac{I}{d}\right)\right], \tag{2.59}$$

$$B = \mathrm{Tr}\left[E_\psi \Lambda \left(\frac{I}{d}\right)\right], \tag{2.60}$$

e

$$p = \frac{dF(\Lambda) - 1}{d - 1}. \tag{2.61}$$

Nas equações acima, ρ_ψ é um estado que leva em conta erros na preparação de $\rho = |\psi\rangle\langle\psi|$ e E_ψ é o operador POVM que leva em consideração erros de medição. No caso ideal, $\rho_\psi = E_\psi = |\psi\rangle\langle\psi|$.

No limite de $K_m \to \infty$, $F_{seq}(m, \psi)$ converge para a fidelidade da média exata sobre todas as sequências possíveis de m portas de Clifford, dada por

$$\mathcal{F}_g(m, \psi) = \mathrm{Tr}[E_\psi \mathcal{S}_m(\rho_\psi)], \tag{2.62}$$

onde

$$\mathcal{S}_m = \frac{1}{|\mathrm{Clif}_n|^m} \sum_{(i_1,\ldots,i_m)} \Lambda \circ \mathcal{C}_{i_{m+1}} \circ \cdots \circ \Lambda \circ \mathcal{C}_{i_1} \tag{2.63}$$

é a média de todas as sequências possíveis. Logo, o modelo $F(m)$ será derivado em termos de $\mathcal{F}_g(m, \psi)$. Considere a seguinte mudança de variáveis:

1. $\mathcal{D}_{i_1} = \mathcal{C}_{i_1}$

2. Para $j \in 2, \ldots, m$, $\mathcal{D}_{i_{j+1}}$ é definido unicamente por

$$\mathcal{D}_{i_{j+1}} = \mathcal{C}_{i_{j+1}} \circ \cdots \circ \mathcal{C}_{i_1} = \bigcirc_{s=1}^{j+1} \mathcal{C}_{i_s} \tag{2.64}$$

Como $\mathcal{C}_{i_j}$ e $\mathcal{C}_{i_k}$ são independentes se $j \neq k$, $\mathcal{D}_{i_j}$ é independente de $\mathcal{D}_{i_{j-1}}$. Assim, obtemos uma nova sequência $(\mathcal{D}_{i_1}, \ldots, \mathcal{D}_{i_m})$ a partir de $(\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_m})$ e temos que

$$\begin{aligned} \mathcal{S}_{i_m} &= \Lambda \circ \mathcal{C}_{i_{m+1}} \circ \Lambda \circ \mathcal{C}_{i_m} \circ \cdots \circ \Lambda \circ \mathcal{C}_{i_1} \\ &= \Lambda \circ \mathcal{D}_{i_{m+1}} \circ \mathcal{D}_{i_m}^\dagger \circ \Lambda \circ \mathcal{D}_{i_m} \circ \cdots \circ \mathcal{D}_{i_1}^\dagger \circ \Lambda \circ \mathcal{D}_{i_1}. \end{aligned} \tag{2.65}$$

Como $\mathcal{C}_{i_{m+1}} = \mathcal{C}_{i_1}^\dagger \circ \cdots \circ \mathcal{C}_{i_m}^\dagger$ e $\mathcal{D}_{i_{m+1}} = \mathcal{C}_{i_{m+1}} \circ \cdots \circ \mathcal{C}_{i_1}$,

$$\mathcal{D}_{i_{m+1}} = I, \tag{2.66}$$

logo,

$$\begin{aligned} \mathcal{S}_{i_m} &= \Lambda \circ \mathcal{C}_{i_{m+1}} \circ \Lambda \circ \mathcal{C}_{i_m} \circ \cdots \circ \Lambda \circ \mathcal{C}_{i_1} \\ &= \Lambda \circ \mathcal{D}_{i_m}^\dagger \circ \Lambda \circ \mathcal{D}_{i_m} \circ \cdots \circ \mathcal{D}_{i_1}^\dagger \circ \Lambda \circ \mathcal{D}_{i_1}. \end{aligned} \tag{2.67}$$

Como mostrado em [34], existe p tal que, para todo ρ,

$$\int U\Lambda(U^\dagger \rho U)U^\dagger dU = p\rho + (1-p)\frac{I}{d}. \tag{2.68}$$

Como o grupo de Clifford é um 2-design unitário, temos que

$$\frac{1}{|\mathrm{Clif}_n|} \sum_{j=1}^{|\mathrm{Clif}_n|} C_j \Lambda(C_j^\dagger \rho C_j) C_j^\dagger = \int U\Lambda(U^\dagger \rho U)U^\dagger dU = p\rho + (1-p)\frac{I}{d}. \tag{2.69}$$

Portanto, podemos escrever $\mathcal{S}_m$ como

$$\mathcal{S}_m = \Lambda \circ \Lambda_d \circ \cdots \circ \Lambda_d = \Lambda \circ (\bigcirc_{j=1}^m \Lambda_d), \tag{2.70}$$

onde Λ_d é o canal despolarizador. Assim,

$$\begin{aligned} \mathcal{F}_g(m, |\psi\rangle) &= \mathrm{tr}(\mathcal{S}_m(\rho_\psi)E_\psi) \\ &= \mathrm{tr}(\Lambda(\rho_\psi)E_\psi)p^m + \mathrm{tr}\left(\Lambda\left(\frac{I}{d}\right)E_\psi\right)(1-p^m) \\ &= Ap^m + B. \end{aligned} \tag{2.71}$$

Esta técnica pode ser usada para comparar a fidelidade dos qubits físicos com a de qubits lógicos codificados com códigos de detecção e correção de erros. Em

uma situação em que o ruído pode ser controlado usando um único parâmetro, essa comparação pode ser feita buscando um limiar. Neste trabalho, o termo *limiar* significa o valor de parâmetro em que as curvas de decaimento de fidelidade de experimentos codificados e não codificados são aproximadamente iguais. Desta forma, se o valor do parâmetro for maior que o limiar, circuitos não codificados vão gerar melhores resultados, se o valor for menor, circuitos codificados terão o melhor desempenho. Para o caso não codificado, utilizamos o protocolo apresentado acima, para o codificado, utilizamos aquele que será apresentado na Seção 2.7.1.

2.7.1 Randomized benchmarking lógico

Como mencionado no Capítulo 1, Combes *et al.* apresentaram um protocolo RB lógico, baseado naquele proposto por Magesan *et al.* [8, 9], que é adequado para avaliar a implementação de um código quântico de correção de erros no nível lógico. Para estimar a fidelidade média do conjunto de portas de Clifford de um código, os seguintes passos devem ser executados para vários tamanhos de sequência m e várias vezes para cada m:

1. Escolher um estado inicial ρ e um tamanho de sequência m.
2. Escolher aleatoriamente uma sequência de m portas de Clifford $s_m = \{U_1, U_2, \ldots, U_m\}$
3. Fazer o seguinte T vezes.
   (a) Codificar o estado ρ usando o código de Steane.
   (b) Para cada $U \in \{U_1, U_2, \ldots, U_m\}$:
      i. Aplicar a versão codificada da porta U.
      ii. Aplicar o procedimento de correção de erro.
   (c) Aplicar a porta $U^{-1} = \prod_{U \in S_m} U^\dagger$ codificada.
   (d) Aplicar o procedimento de correção.
   (e) Aplicar a decodificação.
   (f) Medir ρ com um operador POVM E.
4. Calcular o percentual F_m de execuções que voltou ao estado inicial para m portas.

O protocolo acima permite estimar a probabilidade de sobrevivência para vários tamanho de sequência, dando origem a uma curva que pode ser ajustada ao modelo da equação 3.2. Com uma estimativa para o parâmetro p, é possível também estimar $F(\mathcal{E})$.

A Figura 2.2 mostra um exemplo de circuito para uma sequência de tamanho m. A primeira linha corresponde ao espaço do código e as demais correspondem ao espaço da síndrome. O estado $|\psi_z\rangle$ é igual a $|\psi\rangle \otimes |0\rangle^{\otimes n-1}$ onde $|\psi\rangle$ é o estado a ser codificado e n é o número de qubits do bloco do código. $\mathcal{E}$ representa a codificação, $\mathcal{D}$ a decodificação, $\mathcal{R}$ o procedimento de recuperação, os canais $\mathcal{U}_i$, para $0 \leq i \leq m$, representam as portas da sequência e $\mathcal{U}^{-1}$ representa a porta que inverte a sequência. O operador POVM E representa a situação em que o qubit volta ao estado inicial e $I - E$ a situação oposta.

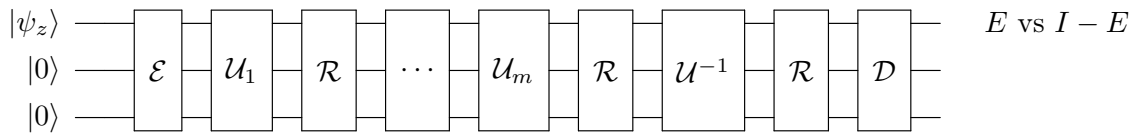


Figura 2.2: Exemplo de circuito para uma sequência de tamanho m

2.8 Canais quânticos

Para entender o conceito de canais quânticos, é preciso primeiro entender o formalismo de operação quântica, que é usado para descrever a evolução de sistemas quânticos em uma variedade de situações [20]. Uma operação quântica é uma mapa linear que atua sobre operadores densidade, que escrevemos como

$$\rho' = \mathcal{E}(\rho) \tag{2.72}$$

e é completamente positivo e mantém ou diminui o traço. Um canal quântico é uma operação quântica que preserva o traço [35].

2.8.1 Canal despolarizador

O canal despolarizador representa um tipo importante de ruído quântico [20]. Quando submetido a esse canal, um estado quântico é, com probabilidade p, despolarizado, o que significa ser substituído pelo estado completamente misturado, $I/2$. Com probabilidade $1 - p$, o estado permanece inalterado. Esse comportamento é descrito por

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1 - p)\rho. \tag{2.73}$$

Uma maneira alternativa de descrever o canal despolarizador é a representação em operador soma:

$$\mathcal{E}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z). \tag{2.74}$$

Através desta expressão, vemos que os operadores do canal despolarizador são $\sqrt{(}1-3p/4)I$, $\sqrt{p}X/2$, $\sqrt{p}Y/2$ e $\sqrt{p}Z/2$.

A figura 2.3 mostra o efeito do canal despolarizador na esfera de Bloch. Note como a esfera diminui em direção ao centro, que corresponde ao estado completamente misturado $I/2$.

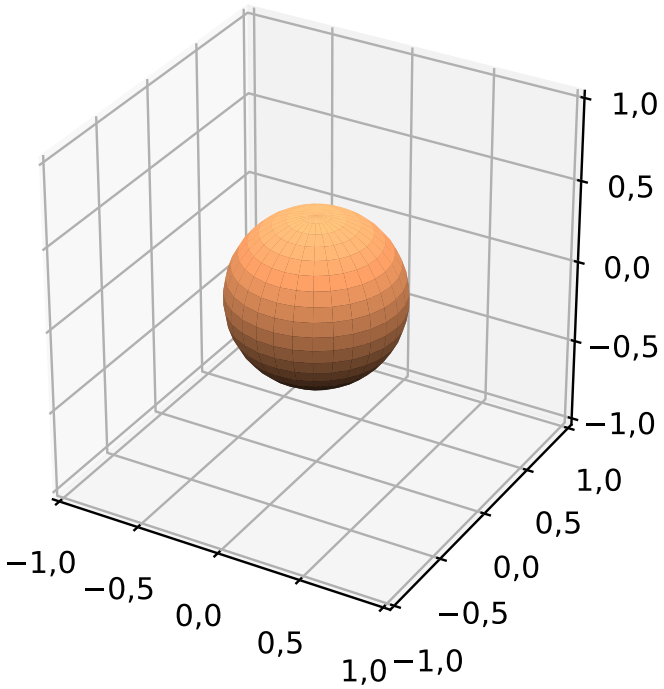


Figura 2.3: Efeito do canal despolarizador na esfera de Bloch para $p = 0{,}5$

O canal despolarizador pode ser generalizado para um sistema quântico de dimensão d. Neste caso, o estado é substituído pelo estado completamente misturado I/d com probabilidade p e permanece inalterado com probabilidade $1 - p$. Esse comportamento é descrito por

$$\mathcal{E}(\rho) = \frac{pI}{d} + (1-p)\rho. \tag{2.75}$$

2.8.2 Atenuação de amplitude

O canal de atenuação de amplitude de 1 qubit é definido por

$$\mathcal{E}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger, \tag{2.76}$$

onde

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} \tag{2.77}$$

e

$$E_1 = \begin{bmatrix} 0 & \sqrt{\lambda} \\ 0 & 0 \end{bmatrix}. \tag{2.78}$$

A Figura 2.4 mostra o efeito da atenuação de amplitude na esfera de Bloch. Note como a esfera diminui em direção ao estado $|0\rangle$. Isso acontece porque o operador E_0 deixa $|0\rangle$ inalterado e diminui a amplitude de $|1\rangle$ e o operador E_1 transforma o estado $|1\rangle$ em um $|0\rangle$.

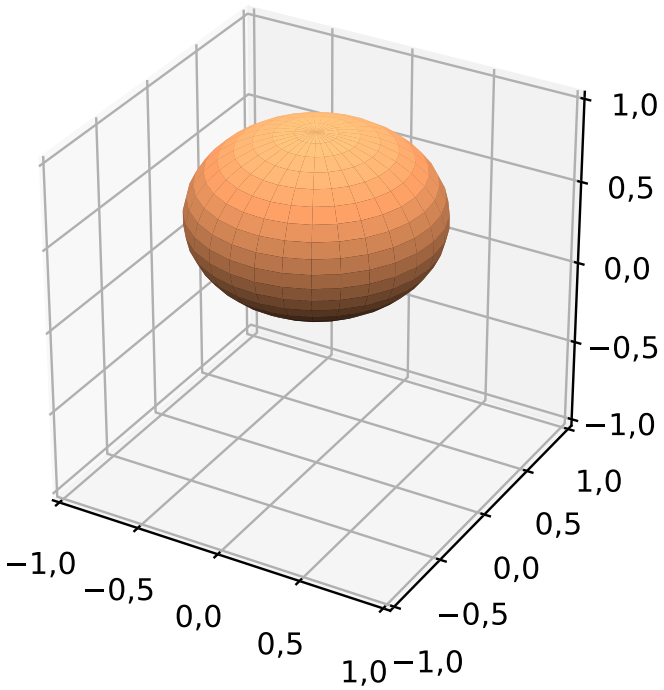


Figura 2.4: Efeito da atenuação de amplitude na esfera de Bloch para $\lambda = 0{,}5$

Os operadores da atenuação de amplitude de dois qubits [36] são obtidos por meio de

$$E_{ij} = E_i \otimes E_j, (i, j = 0, 1), \tag{2.79}$$

logo, os operados são os seguintes:

$$E_{00} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-\lambda} & 0 & 0 \\ 0 & 0 & \sqrt{1-\lambda}0 & \\ 0 & 0 & 0 & 1-\lambda \end{bmatrix}, \tag{2.80}$$

$$E_{01} = \begin{bmatrix} 0 & \sqrt{\lambda} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{\lambda(1-\lambda)} \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{2.81}$$

$$E_{10} = \begin{bmatrix} 0 & 0 & \sqrt{\lambda} & 0 \\ 0 & 0 & 0 & \sqrt{\lambda(1-\lambda)} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{2.82}$$

e

$$E_{11} = \begin{bmatrix} 0 & 0 & 0 & \lambda \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{2.83}$$

2.8.3 Atenuação de fase

O canal de atenuação de fase de 1 qubit é definido por

$$\mathcal{E}(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger, \tag{2.84}$$

onde E_0 é o mesmo da atenuação de amplitude e

$$E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}. \tag{2.85}$$

Também é possível representar este canal através de outro conjunto de elementos de operação, são eles

$$\tilde{E}_0 = \sqrt{\alpha} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.86}$$

e

$$\tilde{E}_1 = \sqrt{1-\alpha} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2.87}$$

onde

$$\alpha = \frac{1 + \sqrt{1 - \lambda}}{2}. \tag{2.88}$$

Ou seja, na atenuação de fase, com probabilidade α, o estado permanece inalterado e com probabilidade $1 - \alpha$ ele é submetido a uma porta Z.

A Figura 2.5 mostra o efeito da atenuação de fase na esfera de Bloch. Note como a esfera diminui em direção ao eixo Z.

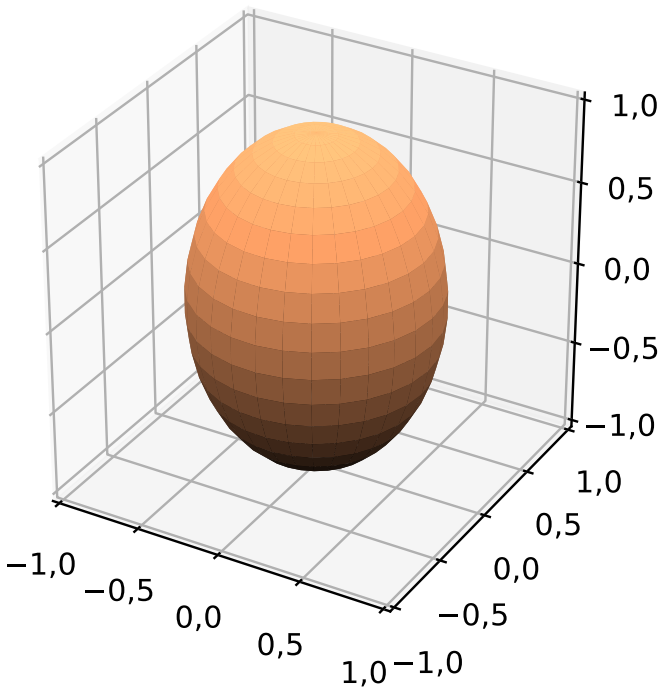


Figura 2.5: Efeito da atenuação de fase na esfera de Bloch para $\lambda = 0{,}5$

Os operadores da atenuação de fase de dois qubits são obtidos da mesma forma que na atenuação de amplitude, logo, o operador E_{00} é igual ao da equação 2.80 e os demais são

$$E_{01} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \sqrt{\lambda} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{\lambda(1-\lambda)} \end{bmatrix}, \tag{2.89}$$

$$E_{10} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\lambda} & 0 \\ 0 & 0 & 0 & \sqrt{\lambda(1-\lambda)} \end{bmatrix} \tag{2.90}$$

e

$$E_{11} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix}. \tag{2.91}$$

Capítulo 3

Metodologia

Para o desenvolvimento deste trabalho, foram utilizados o IBM Quantum [14] e o Qiskit [15]. O IBM Quantum é uma plataforma online permite acesso a vários dispositivos quânticos e simuladores da IBM, muitos de forma gratuita, e o Qiskit é um kit de desenvolvimento de software para trabalhar com computadores quânticos que permite criar circuitos e acessar os dispositivos do IBM Quantum usando a linguagem de programação Python.

Neste trabalho foram utilizados dois simuladores quânticos, o *qasm_simulator*, que está disponível diretamente no Qiskit e pode ser executado localmente, e o *ibmq_qasm_simulator*, que é um dos dispositivos disponíveis no IBM Quantum. Os experimentos mais simples, com menor número de portas, especialmente aqueles com circuitos não codificados, foram executados no primeiro, já os maiores, por demandarem mais recursos computacionais, foram executados no IBM Quantum.

Optamos por utilizar simuladores porque instruções importantes como retornar um qubit ao estado zero (`reset`), medições intermediárias e aplicações de portas condicionadas ao valor no registrador clássico (`if`), não estavam disponíveis nos dispositivos reais no início do trabalho. Embora as duas primeiras tenha ficado disponíveis posteriormente, o `if` continua indisponível. Essas instruções são indispensáveis para a correta aplicação do código de Steane.

Foram realizados experimentos com ruídos em diferentes números de qubits. O objetivo foi determinar o limiar aproximado em que os circuitos codificados e não codificados tem o mesmo desempenho, isto é, curvas de fidelidade próximas. Assim, é possível determinar um valor tal que, se utilizado um modelo de ruído com parâmetro inferior a ele, um circuito codificado terá um desempenho melhor que um não codificado. Foram utilizados modelos de ruído baseados nos canais quânticos apresentados na Seção 2.8, que são alguns dos mais relevantes.

3.1 Modelos de ruído

Foi construído um modelo de ruído para cada um dos canais quânticos apresentados na seção 2.8. A cada modelo, foram adicionados erros de 1 e 2 qubits dos respectivos canais. Os modelos foram criados através do Qiskit, o que permite que sejam aplicados ao executar algum experimento em um dos simuladores acessíveis. Em um modelo de ruído do Qiskit, é possível adicionar erros associados às instruções de porta, medição e `reset`.

Em cada modelo, erros de 1 qubit foram associados às portas $U1$, $U2$, $U3$ e I e erros de 2 qubits associados à porta $CNOT$. Esses erros são aplicados após a instrução de cada porta. Não foram adicionados erros às instruções de medição e `reset`. Para cada canal, foram construídos modelos de 7 tipos. Um modelo do tipo i possui ruído nos i primeiros qubits do bloco do código, partindo do menos significativo para o mais significativo. Desta forma, um modelo é caracterizado pelo tipo, pelo canal e pelo parâmetro do canal.

É importante dizer que o conjunto de portas $\{U1, U2, U3, I, CNOT\}$ foi escolhido para a construção dos modelos de ruído pois, no início deste trabalho, ele representava as portas base dos dispositivos quânticos da IBM, o que significa que circuitos construídos a partir de outras portas, para serem executados nestes dispositivos, seriam convertidos em um circuito equivalente usando apenas as portas do conjunto. O objetivo foi obter no simulador um processo parecido com a execução em um dispositivo real. Posteriormente, as portas base dos computadores quânticos da IBM foram alteradas, mas optamos por continuar com este conjunto para manter o que estava sendo desenvolvido.

Para exemplificar o uso e o funcionamento de um modelo de ruído do Qiskit, a Figura 3.1 apresenta um modelo simples criado com base no canal despolarizador. Na linha 3 é criado um erro despolarizador com parâmetro $p = 0{,}1$ atuando em 1 qubit e na linha 5 ele é adicionado a um modelo de ruído, atuando sobre a porta de Hadamard no qubit 1. Na parte inferior, podemos observar um dicionário Python que descreve o modelo criado. Ele é representado usando as portas I, X, Y, e Z, de acordo com o modelo da Equação 2.74. Note que a probabilidade de aplicar cada uma das instruções `x`, `y`, e `z` é $\frac{p}{4} = 0{,}025$ e a da instrução `id` é $1 - \frac{3p}{4} = 0{,}925$.

Da mesma forma, a Figura 3.2 apresenta um modelo criado com base na atenuação de amplitude. O erro é criado na linha 3 com parâmetro $\lambda = 0{,}5$ e adicionado ao modelo na linha 5, vinculado à porta de Hadamard e ao qubit 1. Neste caso, o canal é representado por uma instrução que utiliza os operadores de Kraus. Note que os parâmetros desta instrução são exatamente os operadores das Equações 2.77 e 2.78 para o parâmetro utilizado.

Por fim, a Figura 3.3 apresenta um modelo criado com base na atenuação de fase.

```
[1]:
1 from qiskit.providers.aer.noise import NoiseModel, depolarizing_error
2 from pprint import pprint
3 de=depolarizing_error(0.1,1)
4 nm=NoiseModel()
5 nm.add_quantum_error(de,'h',[1])
6 pprint(nm.to_dict())

{'errors': [{'gate_qubits': [[1]],
             'instructions': [[{'name': 'x', 'qubits': [0]}],
                              [{'name': 'y', 'qubits': [0]}],
                              [{'name': 'z', 'qubits': [0]}],
                              [{'name': 'id', 'qubits': [0]}]],
             'operations': ['h'],
             'probabilities': [0.025, 0.025, 0.025, 0.925],
             'type': 'qerror'}]}
```

Figura 3.1: Exemplo de modelo de ruído com erro despolarizador

```
[1]:
1 from qiskit.providers.aer.noise import NoiseModel, amplitude_damping_error
2 from pprint import pprint
3 ade=amplitude_damping_error(0.5)
4 nm=NoiseModel()
5 nm.add_quantum_error(ade,'h',[1])
6 pprint(nm.to_dict())

{'errors': [{'gate_qubits': [[1]],
             'instructions': [[{'name': 'kraus',
                                'params': [array([[-1.        +0.j,  0.        +0.j],
       [ 0.        +0.j, -0.70710678+0.j]]),
                                           array([[0.        +0.j, 0.70710678+0.j],
       [0.        +0.j, 0.        +0.j]])],
                                'qubits': [0]}]],
             'operations': ['h'],
             'probabilities': [1.0],
             'type': 'qerror'}]}
```

Figura 3.2: Exemplo de modelo de ruído com erro atenuação de amplitude

Da mesma forma que os erros anteriores, na linha 3 é criado um erro com parâmetro $\lambda = 0{,}5$ e adicionado ao modelo na linha 5 para atuar em portas Hadamard no qubit 1. Observe que o erro é representado pela probabilidade de aplicar a identidade, ou seja, de manter o estado inalterado, e pela probabilidade de aplicar a porta Z. Essa é exatamente a descrição dada pelos elementos de operação das Equações 2.86 e 2.87. Perceba que $\alpha = (1 + \sqrt{1-\lambda})/2 = 0{,}856$, como na figura.

3.2 Método experimental

Nesta seção, descreveremos em detalhes como os experimentos foram feitos. Primeiro explicaremos como foi feita a implementação do código de Steane, descrevendo as etapas de codificação, recuperação e decodificação, e em seguida como os circuitos foram construídos.

```
[1]: from qiskit.providers.aer.noise import NoiseModel, phase_damping_error
     from pprint import pprint
     pde=phase_damping_error(0.5)
     nm=NoiseModel()
     nm.add_quantum_error(pde,'h',[1])
     pprint(nm.to_dict())

     {'errors': [{'gate_qubits': [[1]],
                  'instructions': [[{'name': 'z', 'qubits': [0]}],
                                   [{'name': 'id', 'qubits': [0]}]],
                  'operations': ['h'],
                  'probabilities': [0.14644660940672632, 0.8535533905932738],
                  'type': 'qerror'}]}
```

Figura 3.3: Exemplo de modelo de ruído com erro atenuação de fase

3.2.1 Implementação do código de Steane

Para utilizar 1 qubit lógico codificado no código de Steane, são necessários 13 qubits físicos, sendo 7 qubits do código e 6 qubits auxiliares, que são utilizados para medir os geradores do código e obter as síndromes de erro. A codificação de um qubit físico é feita utilizando o circuito da figura 3.4 [37]. A decodificação é feita com o circuito inverso.

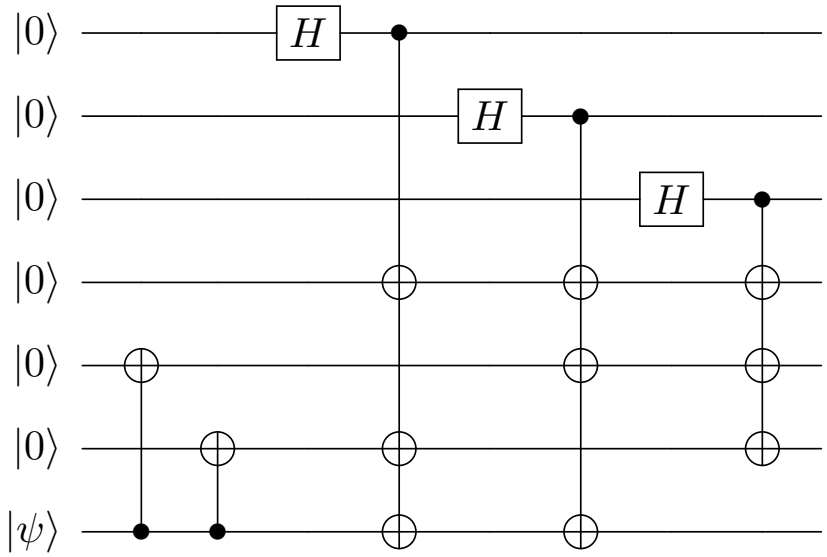


Figura 3.4: Circuito utilizado na codificação no código de Steane

O procedimento de correção de erros pode ser dividido em duas etapas, a medição das síndromes e a recuperação da síndrome. A medição das síndromes é feita medindo os geradores do código. Para isso, cada qubit auxiliar é usado para medir um gerador, como ilustrado pela figura 3.5. Seja β_i o resultado da medição do gerador i e $\{E_j\}$ um conjunto de erros corrigíveis do código de Steane. A recuperação é feita aplicando E_j tal que $E_j g_i E_j^\dagger = \beta_i g_i$ para todo i. A tabela 3.1 mostra o erro E_j utilizado para cada síndrome.

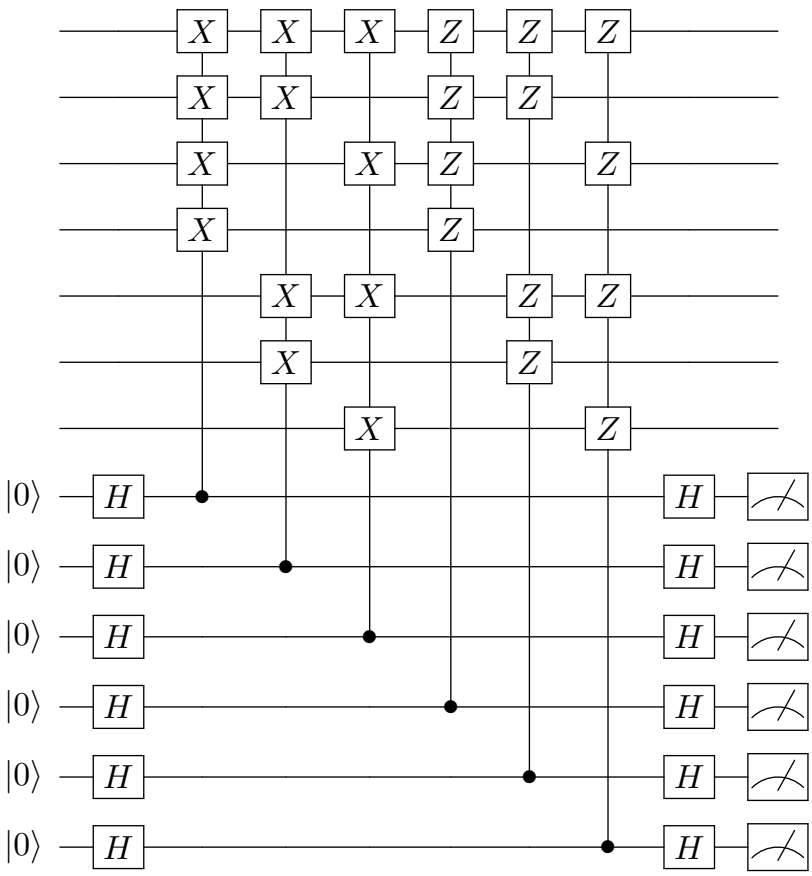


Figura 3.5: Circuito para medição dos geradores do código de Steane

3.2.2 Experimentos com qubits auxiliares livres de ruído

Os experimentos realizados utilizaram modelos de erro em que os qubits auxiliares não estão sujeitos a ruídos. Foram construídos circuitos com 1 qubit lógico codificado no código de Steane de acordo com o algoritmo apresentado na Seção 2.7.1. Cada circuito foi executado 1024 vezes para se obter a probabilidade aproximada de voltar ao estado inicial. Além disso, foram utilizados os estado iniciais $|0\rangle$ e $|1\rangle$ e 30 valores diferentes para m. Os resultados obtidos foram usados para construir gráficos da probabilidade de sobrevivência em função do número de portas m e as curvas obtidas foram ajustadas à função da equação 2.58.

A seleção de portas do grupo de Clifford foi feita através de uma função disponível no Qiskit, que utiliza o método de [38]. Os circuitos são montados inicialmente com as portas X, Y, Z, H, S, $S^\dagger$ e $CNOT$, além de instruções de medição e `reset`. Estas últimas são utilizadas em todos os qubits auxiliares após cada procedimento de recuperação para deixá-los prontos para o próximo. Antes da execução no simulador, no entanto, as portas de 1 qubit são convertidas nas portas $U1$, $U2$ e $U3$, pois os modelos de ruído foram construídos com base nelas.

Ao final do circuito, todos os qubits do bloco do código são medidos e armazena-

Tabela 3.1: Conjunto de erros corrigíveis utilizado

Síndrome	Erro	Síndrome	Erro
000000	IIIIIII	100000	IIIZIII
000001	XIIIIII	100001	XIIZIII
000010	IXIIIII	100010	IXIZIII
000011	IIXIIII	100011	IIXZIII
000100	IIIXIII	100100	IIIYIII
000101	IIIIXII	100101	XIIYIII
000110	IIIIIXI	100110	IXIYIII
000111	IIIIIIX	100111	IIXYIII
001000	ZIIIIII	101000	IIIIZII
001001	YIIIIII	101001	YIIZIII
001010	ZXIIIII	101010	IXIIZII
001011	YXIIIII	101011	IIXIZII
001100	ZIIXIII	101100	ZIIYIII
001101	YIIXIII	101101	IIIIYII
001110	ZIIIIXI	101110	IIXIYII
001111	YIIIIXI	101111	IXIIYII
010000	IZIIIII	110000	IIIIIZI
010001	XZIIIII	110001	XIIIIZI
010010	IYIIIII	110010	IYIZIII
010011	XYIIIII	110011	IIYIZII
010100	IZIXIII	110100	IZIYIII
010101	IZIIXII	110101	IIZIYII
010110	IYIXIII	110110	IIIIIYI
010111	IYIIXII	110111	XIIIIYI
011000	IIZIIII	111000	IIIIIIZ
011001	YZIIIII	111001	YIIIIZI
011010	ZYIIIII	111010	IYIIZII
011011	IIYIIII	111011	IIYZIII
011100	IIZXIII	111100	IIZYIII
011101	IIZIXII	111101	IZIIYII
011110	IIYIXII	111110	ZIIIIYI
011111	IIYXIII	111111	IIIIIIY

dos em um registrador clássico de 7 qubits. Como pode ser observado na Figura 3.4, o qubit codificado é sétimo, logo, ao verificar se houve ou não retorno ao estado inicial ao fim circuito, apenas o bit correspondente do registrador clássico é considerado. Embora seja esperado que os demais qubits do bloco do código também retornem aos seus estados iniciais, isto é, ao estado $|0\rangle$, pode acontecer de o sétimo qubit retornar ao estado inicial e alguns dos demais não, mas nesse caso consideramos que o estado de interesse foi obtido de volta.

Capítulo 4

Resultados

Os experimentos foram realizados com modelos de erro atuando em diferentes número de qubits para determinar o limiar em cada caso. Foram criados 7 tipos de modelo, um com ruído atuando apenas no primeiro qubit do bloco do código, outro atuando nos dois primeiros e assim por diante, até o modelo atuando nos 7 qubits do bloco. Não foram utilizados modelos atuando nos qubits auxiliares devido ao alto número de portas necessário para encontrar os limiares neste caso, que exigiria uma quantidade enorme de memória e tempo para a execução dos experimentos. É importante dizer que foram feitos experimentos com ruído em apenas 1 qubit para mostrar que obtemos sempre uma curva quase constante próxima de 1,0 de sobrevivência, o que é explicado pelo fato de o código de Steane possuir distância 3. Devido a isso, buscamos os limiares apenas para 2 a 7 qubits ruidosos.

As três primeiras seções deste capítulo apresentam, respectivamente, os resultados obtidos com os experimentos com modelos de ruído baseados no canal despolarizador, atenuação de amplitude e atenuação de fase. Na Seção 4.4, comparamos os resultados obtidos com cada canal quântico, apresentando curvas do limiar em função do número de qubits com ruído e as fidelidades encontradas para alguns dos modelos.

4.1 Canal despolarizador

A Figura 4.1 mostra as curvas obtidas com os experimentos dos modelos de ruído do canal despolarizador. Ela é composta de 6 gráficos, cada um representando o limiar para um número de qubits com ruído, de 2 a 7. Em cada gráfico, o eixo x representa o número de portas codificadas no código de Steane utilizadas nos circuitos correspondentes, sem contar a porta de inversão, e o eixo y representa a probabilidade de sobrevivência, ou seja, o percentual de experimentos em que o estado após a medição é igual ao inicial. Além disso, cada gráfico apresenta 8 curvas, 7 representando resultados de experimentos com circuitos codificados com ruído em diferentes

números de qubits, de 1 a 7, para mostrar a relação entre esses modelos, e uma representando resultados com circuitos físicos, ou seja, não codificados, para mostrar que é aproximadamente a mesma curva que aquela obtida para o tipo de modelo ao qual corresponde o limiar. Cada uma delas é identificada pela legenda do gráfico. O valor de p utilizado em todos os modelos representados em um determinado gráfico da Figura 4.1 é apresentado em seu título.

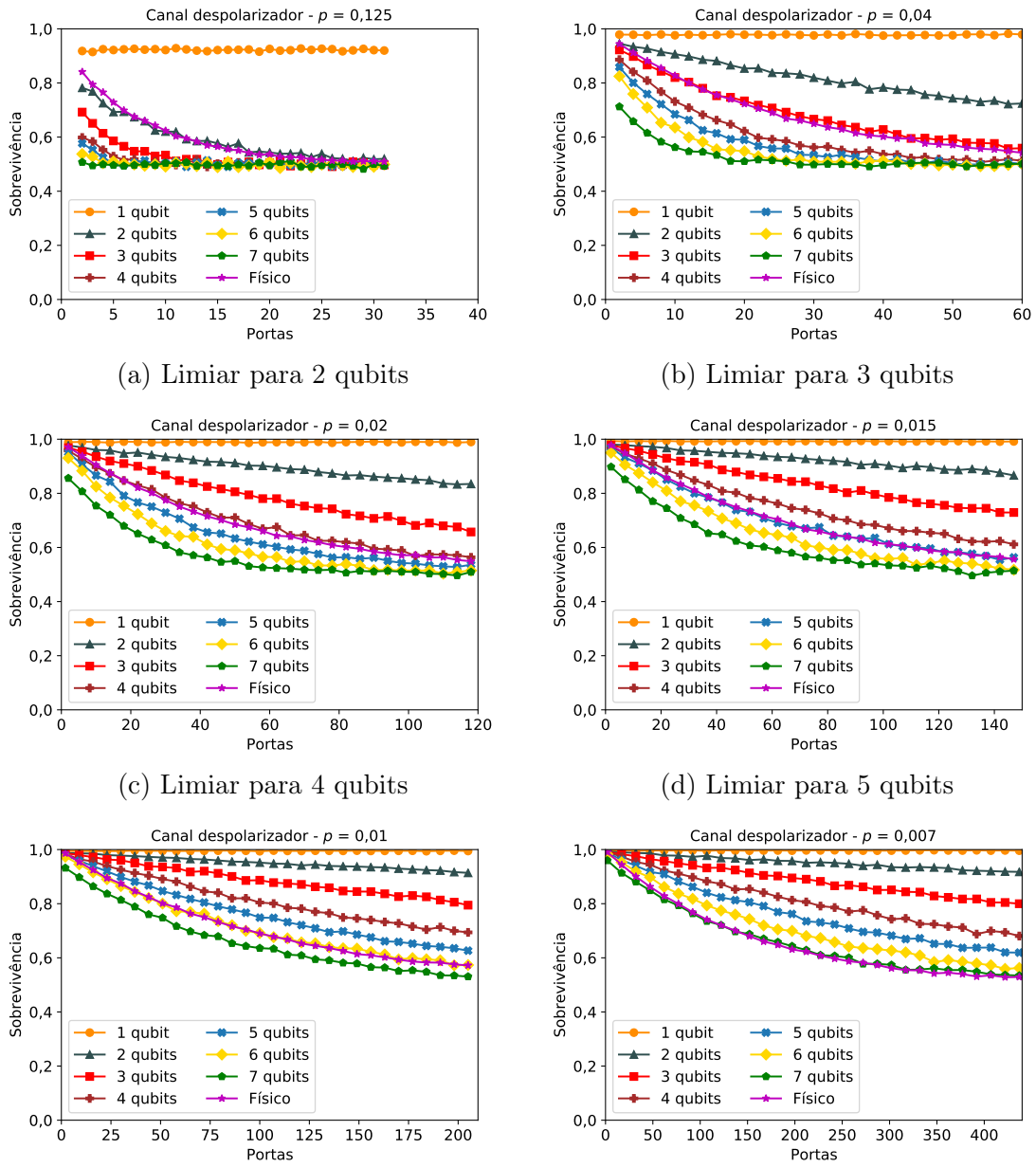
Este canal quântico foi aquele que apresentou os limiares mais baixos, o que significa que ele causa mais erros que os demais modelos para um mesmo valor de parâmetro. Perceba que, com um número de portas grande o bastante, todas as curvas tendem à probabilidade 0,5, o que significa que toda a informação foi perdida em função da atuação do ruído. O limiar mais alto obtido, para o modelo com ruído em apenas 2 qubits, foi 0,125 e o mais baixo, para ruído em 7 qubits, foi 0,007. Podemos observar que a curva dos experimentos não codificados coincide com a dos codificados correspondente ao limiar em quase todos os gráficos, com exceção do gráfico do limiar para 2 qubits, em que há uma pequena diferença entre as curvas no início.

É interessante analisar o porquê de existir um limiar. No caso do canal despolarizador com parâmetro p, um erro acontece durante a execução de um circuito não codificado com probabilidade p. Por outro lado, no caso de um circuito codificado a probabilidade de erro é da ordem de p^2, pois é necessário ocorrer erros em pelo menos dois qubits físicos para que o procedimento de correção não funcione perfeitamente. Assim, para valores altos de p, o grande número de portas utilizado no procedimento de correção faz com que execuções de circuitos codificados gerem curvas de decaimento de fidelidade com valores mais altos. No entanto, para uma função da ordem de p^2, existe um valor abaixo do qual o valor de p será maior, o que garante a existência do limiar.

4.2 Atenuação de amplitude

A Figura 4.2 mostra as curvas obtidas com os experimentos dos modelos de ruído da atenuação de amplitude e foi construída da mesma forma que a Figura 4.1. Os limiares obtidos com este canal são mais altos que aqueles obtidos com o canal despolarizador, no entanto, a diferença é pequena. O limiar mais alto obtido foi 0,15 e o mais baixo foi 0,01, para ruídos em 2 e 7 qubits, respectivamente. A curva dos experimentos com ruído em apenas 1 qubit fica, como esperado, sempre próxima de 1, pois é um erro que o código de Steane consegue corrigir.

É importante enfatizar que, conforme explicado no Capítulo 3, foram feitos experimentos com estados iniciais $|0\rangle$ e $|1\rangle$ e as curvas apresentadas na Figura 4.2 são as médias obtidas a partir desses dois tipos de experimento. No caso específico de



(a) Limiar para 2 qubits

(b) Limiar para 3 qubits

(c) Limiar para 4 qubits

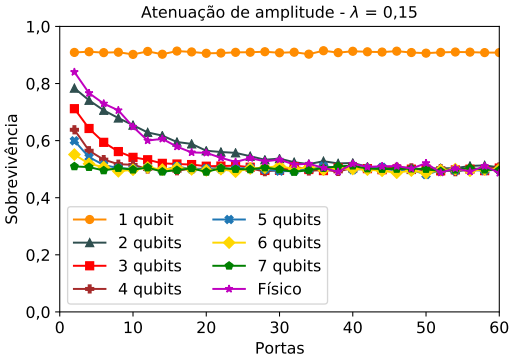
(d) Limiar para 5 qubits

(e) Limiar para 6 qubits

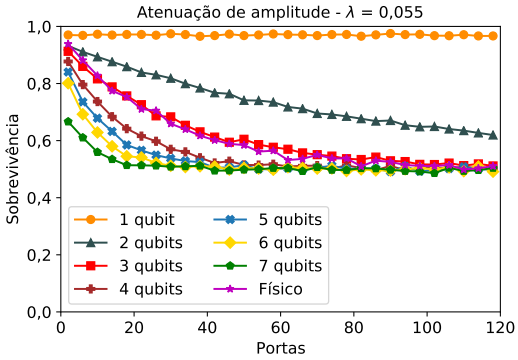
(f) Limiar para 7 qubits

Figura 4.1: Gráficos com os resultados dos experimentos com modelos de ruído do canal despolarizador. Em cada gráfico, o eixo x é o número de portas e o eixo y é a probabilidade de sobrevivência. Além disso, cada gráfico apresenta 8 curvas, 7 delas representando experimentos com ruído em diferentes números de qubits e 1 representando experimentos físicos, como indicado nas legendas. O valor de p utilizado em cada um é indicado no título.

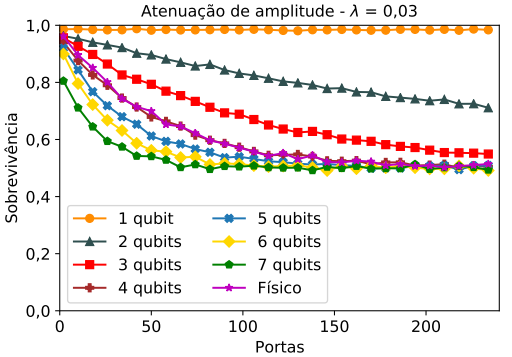
modelos de ruído baseados na atenuação de amplitude, esse fato é especialmente relevante, pois este é um canal que trata os estados $|0\rangle$ e $|1\rangle$ de maneira desigual. Quando analisamos os dados obtidos com o modelo com ruído em 7 qubits para esses dois estados iniciais de forma separada, encontramos anomalias. Com estado inicial $|0\rangle$, a curva obtida fica acima das demais, praticamente constante em 0,7,



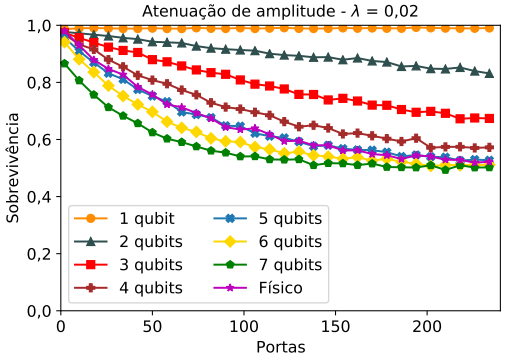
(a) Limiar para 2 qubits



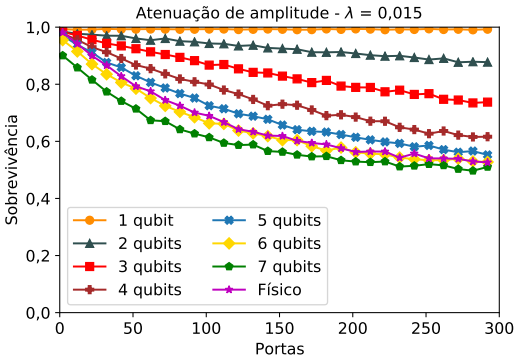
(b) Limiar para 3 qubits



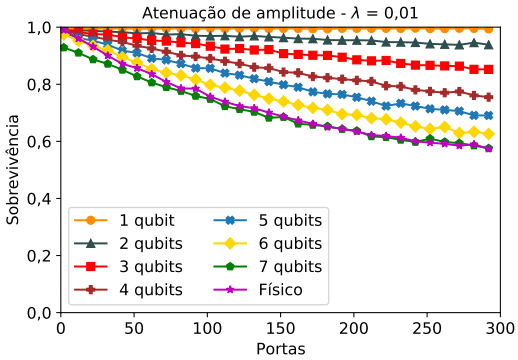
(c) Limiar para 4 qubits



(d) Limiar para 5 qubits



(e) Limiar para 6 qubits



(f) Limiar para 7 qubits

Figura 4.2: Gráficos com os resultados dos experimentos com modelos de ruído da atenuação de amplitude. Em cada gráfico, o eixo x é o número de portas e o eixo y é a probabilidade de sobrevivência. Além disso, cada gráfico apresenta 8 curvas, 7 delas representando experimentos com ruído em diferentes números de qubits e 1 representando experimentos físicos, como indicado nas legendas. O valor de λ utilizado em cada um é indicado no título.

diferente do esperado, pois é a curva obtida de experimentos com mais ruído. Por outro lado, com estado inicial $|1\rangle$, a curva fica praticamente constante em 0,3, abaixo das demais, que possuem seus mínimos em aproximadamente 0,5.

Essa anomalia ocorre apenas quando modelos com ruído em 7 qubits são usados porque eles são os únicos que atuam no qubit 7, que é aquele que se encontra no

estado a ser codificado e onde o estado resultante do experimento é decodificado. Como a atenuação de amplitude privilegia o estado $|0\rangle$, os dados obtidos de experimentos com este estado inicial acabam sendo muito melhores do que o esperado e, consequentemente, quando o estado inicial é $|1\rangle$, ocorre o oposto, gerando resultados piores do que aqueles obtidos quando toda a informação é perdida, que é a sobrevivência de 50%. Com esses comportamentos opostos, após a média, a anomalia de uma curva anula a da outra e obtemos curvas com comportamento parecido ao das demais. Desta forma, vemos o quão importante é fazer a média dos experimentos iniciados em $|0\rangle$ e $|1\rangle$ para obtermos os resultados esperados e que representam o que um usuário deve encontrar no uso real de um sistema cujo ruído possa ser modelado pela atenuação de amplitude.

4.3 Atenuação de fase

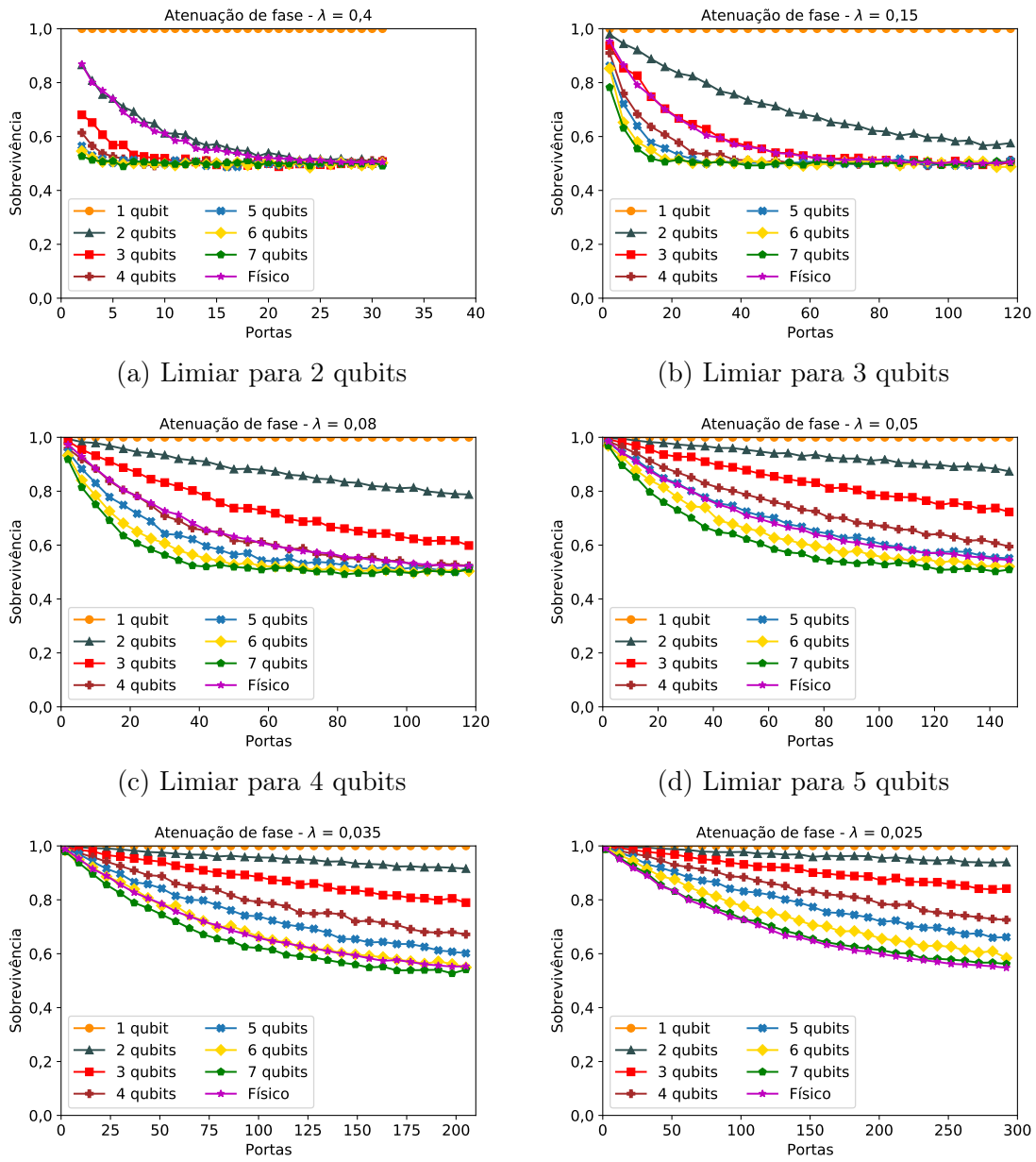
A Figura 4.3 mostra as curvas obtidas com os experimentos dos modelos de ruído da atenuação de fase e foi construída da mesma forma que a Figura 4.1. Os limiares obtidos com este canal são significativamente maiores do que aqueles obtidos com os outros dois. O limiar mais alto obtido foi 0,4 e o mais baixo foi 0,025, para ruídos em 2 e 7 qubits, respectivamente, mostrando que este canal não causa uma perda de informação tão grande quanto os outros dois para o mesmo parâmetro.

Como pode ser observado na Figura 2.5, o efeito da atenuação de fase na esfera de Bloch é uma redução no sentido do eixo x, mantendo os polos inalterados. Além disso, através da representação alternativa deste canal apresentada na Seção 2.8.3, podemos ver que a atuação do erro consiste da aplicação da porta Z com certa probabilidade, que depende de λ. Assim, podemos entender porque este canal causa uma perda de informação menor que os demais, já que ele apenas causa uma redução na fase do estado $|1\rangle$.

Embora este canal tenha uma representação muito parecida com a da atenuação de amplitude, tendo até mesmo um elemento de operação em comum, ele não atua de maneira desigual no $|0\rangle$ e no $|1\rangle$ e, por isso, os gráficos da Figura 4.3 não apresentam a mesma anomalia.

4.4 Discussão comparativa

A partir dos gráficos, podemos concluir que o limiar depende do número de qubits com erro. Quanto maior esse número, menor o limiar. Embora os experimentos tenham sido feitos com ruído apenas nos qubits do código, os resultados indicam que seria possível encontrar um limiar ao considerar ruído em todos os qubits, logo,



(a) Limiar para 2 qubits

(b) Limiar para 3 qubits

(c) Limiar para 4 qubits

(d) Limiar para 5 qubits

(e) Limiar para 6 qubits

(f) Limiar para 7 qubits

Figura 4.3: Gráficos com os resultados dos experimentos com modelos de ruído da atenuação de fase. Em cada gráfico, o eixo x é o número de portas e o eixo y é a probabilidade de sobrevivência. Além disso, cada gráfico apresenta 8 curvas, 7 delas representando experimentos com ruído em diferentes números de qubits e 1 representando experimentos físicos, como indicado nas legendas. O valor de λ utilizado em cada um é indicado no título.

com um parâmetro suficientemente pequeno, o uso do código de Steane pode ser vantajoso.

A Figura 4.4 mostra um gráfico em escala logarítmica do limiar em função número de qubits com ruído para cada modelo utilizado, que é um resumo dos resultados obtidos. Podemos observar que as curvas induzidas pelos pontos de cada canal são

quase retas. Considerando que o limiar é apenas uma aproximação e que alguns valores próximos a este também poderiam ser considerados limiares, podemos dizer que, nesta escala, obtemos retas. Obter algo próximo de uma reta nesta escala significa que uma função na forma $f(x) = ax^b$ pode ser ajustada aos pontos. Este ajuste foi feito para os pontos da Figura 4.4 e os resultados estão na Tabela 4.1.

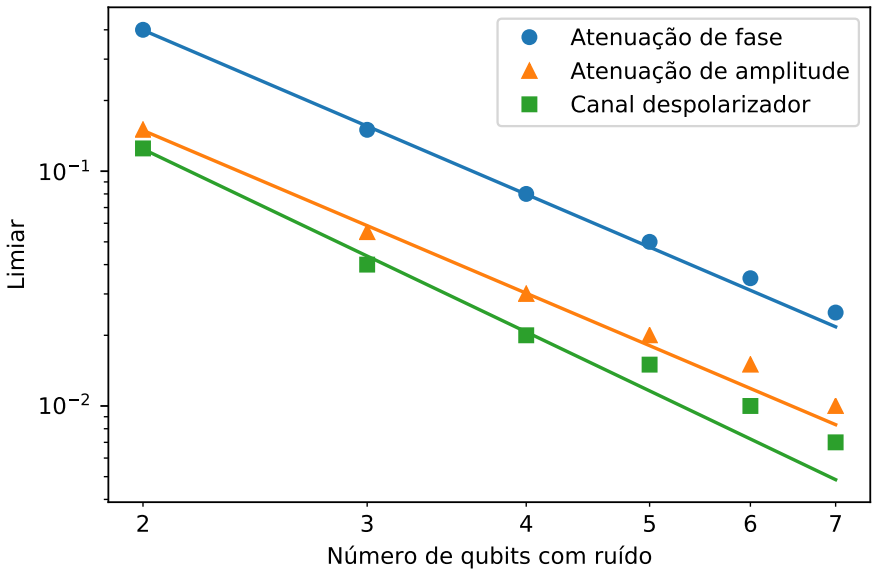


Figura 4.4: Limiar em função do número de qubits com ruído para cada canal. O eixo x representa o número de qubits com ruído e o eixo y representa o parâmetro dos modelos, sendo o p para a curva do canal despolarizador e λ para as curvas das atenuações de amplitude e de fase.

Tabela 4.1: Funções ajustadas aos pontos da Figura 4.4

Canal	Função ajustada
Atenuação de fase	$f(x) = 1{,}99x^{-2{,}32}$
Atenuação de amplitude	$f(x) = 0{,}73x^{-2{,}30}$
Canal despolarizador	$f(x) = 0{,}75x^{-2{,}59}$

Vale ressaltar que o comportamento dessas curvas provavelmente é diferente ao considerar os qubits auxiliares, pois a quantidade e o tipo das portas atuando nesses qubits é diferente. Há, por exemplo, uma série de CNOTs com controle nos qubits auxiliares e alvo nos qubits do código.

A tabela 4.2 mostra as fidelidades médias encontradas para experimentos com parâmetros iguais ao limiar para 7 qubits com ruído para cada canal. A algumas curvas de decaimento de fidelidade não foi possível realizar o ajuste da função da equação 2.58 por elas terem um formato próximo de uma reta, o que levaria a um

Tabela 4.2: Fidelidades médias encontradas. A coluna Configuração indica se é a fidelidade resultante de experimentos não codificados ou o número de qubits com ruído caso o código de Steane tenha sido usado.

Canal	Parâmetro	Configuração	Fidelidade média
Canal depolarizador	$p = 0{,}007$	5 qubits	0,9983
		6 qubits	0,9977
		7 qubits	0,9969
		Não codificado	0,9967
Atenuação de amplitude	$\lambda = 0{,}01$	5 qubits	0,9985
		6 qubits	0,9977
		7 qubits	0,9971
		Não codificado	0,9968
Atenuação de fase	$\lambda = 0{,}025$	5 qubits	0,9981
		6 qubits	0,9971
		7 qubits	0,9961
		Não codificado	0,9960

ajuste impreciso que daria um valor de fidelidade incorreto. Isso acontece especialmente com as curvas que já iniciam com uma probabilidade de sobrevivência próxima de 0,5 e com aquelas referentes a experimentos com erros em apenas 1 qubit, que apresentam alta sobrevivência, mas são praticamente constantes. Devido a isso, optamos por apresentar apenas as fidelidades para experimentos no limiar de 7 qubits e com ruído em pelo menos 5 qubits ou não codificados.

Na tabela 4.2 vemos que as fidelidades médias dos experimentos com 7 qubits e não codificados são muito próximas, com diferença de no máximo 3×10^{-4}, indicando que as respectivas curvas são realmente parecidas. Note que as fidelidades considerando ruído em 5 e 6 qubits já são um pouco maiores do que aquela para um qubit não codificado. Isso significa que, com esses modelos, já obteríamos melhores resultados ao utilizar o código de Steane do que ao não utilizar nenhum CQCE. Além disso, como a fidelidade com 7 qubits ruidosos e praticamente igual àquela dos experimentos não codificados, podemos concluir que parâmetros mais baixos, experimentos mais baixos resultariam em fidelidades maiores, ou seja, nessas condições também obteríamos menos erros ao utilizar o código de Steane.

Capítulo 5

Conclusões

Neste trabalho buscamos analisar, usando a medida de fidelidade, como o uso de um código quântico de correção de erros influencia a qualidade da computação de circuitos quânticos. Escolhemos para a análise o código de Steane $[[7, 1, 3]]$, que codifica 1 qubit lógico em 7 qubits físicos, devido às suas boas características, que facilitam a implementação, como o fato de ser um código CSS, permitindo que todas as portas de Clifford possam ser implementadas de forma transversal. Para isso, utilizamos o protocolo randomized benchmarking lógico descrito por Combes et al. [10], que é uma versão modificada do RB físico descrito por Magesan *et al.* [8, 9]. Utilizamos a plataforma IBM Quantum e o kit de desenvolvimento de software Qiskit para executar os experimentos.

Devido a algumas limitações dos recursos utilizados para realizar os experimentos, foram aplicadas algumas restrições a eles. Uma das restrições aplicadas foi o uso de simuladores quânticos ao invés de dispositivos reais. Isto foi necessário porque algumas instruções importantes para a aplicação do código de Steane (medições intermediárias, `reset` e `if`) não estavam disponíveis nos computadores quânticos do IBM Quantum no início deste trabalho. Com isso, optamos por simular ruído criando modelos baseados, separadamente, no canal despolarizador, na atenuação de amplitude e na atenuação de fase, alguns dos mais importantes canais quânticos. Outra restrição foi a criação de modelos com ruído em apenas parte dos qubits. Isto foi necessário porque, para encontrar parâmetros para os modelos tais que o desempenho dos circuitos codificados fosse melhor que o daqueles não codificados, estimamos que seria necessária uma quantidade de portas da ordem de dezenas de milhares, o que exigiria uma quantidade de memória da ordem de dezenas de *gigabytes*, muito acima dos 8 GB disponíveis na plataforma. Assim, decidimos analisar o desempenho dos circuitos com ruído em diferentes números de qubits, mas considerando apenas os qubits do bloco do código, deixando os qubits auxiliares livres de ruído.

Para todos os três canais quânticos utilizados, conseguimos encontrar o limiar

para os 6 diferentes tipos de modelos de ruído. Assim, concluímos que, em um cenário sem ruído nos qubits auxiliares e ruído suficientemente baixo nos qubits do bloco do código, é vantajoso o uso do código de Steane o conjunto de portas de Clifford. Os modelos baseados no canal despolarizador foram aqueles que levaram a limiares mais baixos, seguido da atenuação de amplitude. Para a atenuação de fase, obtivemos os limiares mais altos. Com isso, podemos concluir que o canal despolarizador é o que causa mais danos à informação comparado com os outros dois com o mesmo valor de parâmetro. É importante destacar, no entanto, que os parâmetros tem diferentes interpretações em cada canal. Como esperado, conforme o número de qubits com ruído aumenta, o limiar diminui, e mostramos que existe uma função que pode ser usada para prever o valor do limiar. Embora a função não se ajuste perfeitamente às curvas de limiar em função do número de qubits com ruído, vale notar que mesmo com pequenas alterações nos valores dos parâmetros, a curva de fidelidade média obtida ainda pode ser considerada aproximadamente igual àquela obtida antes da alteração, isso significa que o limiar pode ser levemente alterado e continuar válido. Com essas pequenas alterações, é possível fazer com que as curvas da Figura 4.4 se ajustem às funções encontradas.

Embora seja esperado um comportamento diferente ao buscar limiares com modelos com ruído nos qubits auxiliares, devido à estrutura diferente desta parte do circuito, podemos concluir, a partir dos resultados encontrados, que com parâmetros suficientemente pequenos, é possível ter um desempenho melhor com circuitos codificados no código de Steane do que com não codificados. A maior contribuição deste trabalho foi mostrar que vale a pena usar o código de Steane no cenário apresentado no parágrafo anterior. Além disso, mostramos que, para os três canais, quando o parâmetro é igual ao limiar para 7 qubits ruidosos, experimentos com ruído nos 6 primeiros qubits do bloco do código já resultam em uma fidelidade média maior do que no caso não codificado.

5.1 Trabalhos futuros

Embora tenhamos obtido resultados positivos no que tange ao uso de código de Steane para obter melhores resultados na execução de circuitos quânticos, nossos experimentos foram realizados sob certas restrições, como a falta de ruídos nos qubits auxiliares e o uso de modelos de ruído que não tentam imitar exatamente o comportamento de um dispositivo real e a codificação de apenas 1 qubit. Desta forma, um possível trabalho futuro é a realização deste estudo com menos restrições. É possível criar modelos de erro mais complexos, que tentem imitar o que ocorre em um computador quântico como, por exemplo, os modelos disponíveis no Qiskit, que buscam simular o ruído dos dispositivos da IBM e são uma combinação do canal

despolarizador e da relaxação termal. Além disso, com mais recursos computacionais disponíveis, é possível encontrar os limiares para modelos com ruído também nos qubits auxiliares e realizar experimentos com dois ou mais qubits lógicos.

Uma outra possível continuação deste trabalho é a utilização do RB lógico para avaliar o desempenho de outro CQCE e comparar os resultados. Dependendo das características do código utilizado, pode ser possível executar os experimentos diretamente em dispositivos reais, gerando resultados ainda mais valiosos. Após o início deste trabalho, as medições intermediárias e a instrução `reset` se tornaram disponíveis nos computadores quânticos da IBM. Isso é um indicativo de que talvez a instrução `if` se torne disponível também, o que finalmente permitiria a execução do código de Steane e de outros códigos que dependem dessas instruções.

Referências Bibliográficas

[1] SHOR, P. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994. doi: 10.1109/SFCS.1994.365700.

[2] HARROW, A. W., HASSIDIM, A., LLOYD, S. "Quantum algorithm for linear systems of equations", *Physical Review Letters*, v. 103, n. 15, pp. 150502, 2009.

[3] FEYNMAN, R. P. "Simulating physics with computers". In: *Feynman and computation*, CRC Press, pp. 133–153, 2018.

[4] LLOYD, S. "Universal quantum simulators", *Science*, pp. 1073–1078, 1996.

[5] GERJUOY, E. "Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers", *American Journal of Physics*, v. 73, n. 6, pp. 521–540, 2005.

[6] PRESKILL, J. "Quantum computing in the NISQ era and beyond", *Quantum*, v. 2, pp. 79, 2018.

[7] GILL, S. S., KUMAR, A., SINGH, H., et al. "Quantum computing: A taxonomy, systematic review and future directions", *Software: Practice and Experience*, v. 52, n. 1, pp. 66–114, 2022.

[8] MAGESAN, E., GAMBETTA, J. M., EMERSON, J. "Characterizing quantum gates via randomized benchmarking", *Physical Review A*, v. 85, n. 4, pp. 042311, 2012.

[9] MAGESAN, E., GAMBETTA, J. M., EMERSON, J. "Scalable and robust randomized benchmarking of quantum processes", *Physical Review Letters*, v. 106, n. 18, pp. 180504, 2011.

[10] COMBES, J., GRANADE, C., FERRIE, C., et al. "Logical randomized benchmarking", *arXiv preprint arXiv:1702.03688*, 2017.

[11] HARPER, R., FLAMMIA, S. T. "Fault-tolerant logical gates in the ibm quantum experience", *Physical Review Letters*, v. 122, n. 8, pp. 080504, 2019.

[12] HASHAGEN, A., FLAMMIA, S., GROSS, D., et al. "Real randomized benchmarking", *Quantum*, v. 2, pp. 85, 2018.

[13] STEANE, A. M. "Error correcting codes in quantum theory", *Physical Review Letters*, v. 77, n. 5, pp. 793, 1996.

[14] "IBM Quantum". `https://quantum-computing.ibm.com/`, 2021.

[15] ANIS, M. S., ABRAHAM, H., ADUOFFEI, et al. "Qiskit: An Open-source Framework for Quantum Computing". 2021.

[16] MORVAN, A., RAMASESH, V., BLOK, M., et al. "Qutrit randomized benchmarking", *Physical Review Letters*, v. 126, n. 21, pp. 210504, 2021.

[17] BROWN, W. G., EASTIN, B. "Randomized benchmarking with restricted gate sets", *Physical Review A*, v. 97, n. 6, pp. 062323, 2018.

[18] MAGESAN, E., GAMBETTA, J. M., JOHNSON, B. R., et al. "Efficient measurement of quantum gate error by interleaved randomized benchmarking", *Physical Review Letters*, v. 109, n. 8, pp. 080505, 2012.

[19] PROCTOR, T. J., CARIGNAN-DUGAS, A., RUDINGER, K., et al. "Direct randomized benchmarking for multiqubit devices", *Physical Review Letters*, v. 123, n. 3, pp. 030503, 2019.

[20] NIELSEN, M. A., CHUANG, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge, Cambridge University Press, 2010. doi: 10.1017/CBO9780511976667.

[21] KAYE, P., LAFLAMME, R., MOSCA, M. *An introduction to quantum computing.* OUP Oxford, 2006.

[22] GROSS, D., AUDENAERT, K., EISERT, J. "Evenly distributed unitaries: On the structure of unitary designs", *Journal of Mathematical Physics*, v. 48, n. 5, pp. 052104, 2007.

[23] HAAR, A. "Der Massbegriff in der Theorie der kontinuierlichen Gruppen", *Annals of Mathematics*, pp. 147–169, 1933.

[24] EMERSON, J., ALICKI, R., ŻYCZKOWSKI, K. "Scalable noise estimation with random unitary operators", *Journal of Optics B: Quantum and Semiclassical Optics*, v. 7, n. 10, pp. S347, 2005.

[25] MATTEO, O. D. "A short introduction to unitary 2-designs". https://glassnotes.github.io/OliviaDiMatteo_Unitary2Designs.pdf, 2014. "Acessado em 26/01/2022".

[26] BETTEN, A., BRAUN, M., FRIPERTINGER, H., et al. *Error-correcting linear codes: Classification by isometry and applications*, v. 18. Springer Science & Business Media, 2006.

[27] CALDERBANK, A. R., SHOR, P. W. "Good quantum error-correcting codes exist", *Physical Review A*, v. 54, n. 2, pp. 1098, 1996.

[28] STEANE, A. "Multiple-particle interference and quantum error correction", *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, v. 452, n. 1954, pp. 2551–2577, 1996.

[29] GAITAN, F. *Quantum error correction and fault tolerant quantum computing*, v. 6000. CRC Press Boca Raton, FL, 2008.

[30] BENNETT, C. H., DIVINCENZO, D. P., SMOLIN, J. A., et al. "Mixed-state entanglement and quantum error correction", *Physical Review A*, v. 54, n. 5, pp. 3824, 1996.

[31] LAFLAMME, R., MIQUEL, C., PAZ, J. P., et al. "Perfect quantum error correcting code", *Physical Review Letters*, v. 77, n. 1, pp. 198, 1996.

[32] SHOR, P. W. "Scheme for reducing decoherence in quantum computer memory", *Physical Review A*, v. 52, n. 4, pp. R2493, 1995.

[33] POULIN, D. "Stabilizer formalism for operator quantum error correction", *Physical Review Letters*, v. 95, n. 23, pp. 230504, 2005.

[34] NIELSEN, M. A. "A simple formula for the average gate fidelity of a quantum dynamical operation", *Physics Letters A*, v. 303, n. 4, pp. 249–252, 2002.

[35] WEEDBROOK, C., PIRANDOLA, S., GARCÍA-PATRÓN, R., et al. "Gaussian quantum information", *Reviews of Modern Physics*, v. 84, n. 2, pp. 621, 2012.

[36] GUO, Y.-N., TIAN, Q.-L., ZENG, K., et al. "Quantum coherence of two-qubit over quantum channels with memory", *Quantum Information Processing*, v. 16, n. 12, pp. 1–18, 2017.

[37] CHANDAK, S., MARDIA, J., TOLUNAY, M. "Implementation and analysis of stabilizer codes in pyQuil". https://cs269q.stanford.

edu/projects2019/stabilizer_code_report_Y.pdf. "Acessado em 26/01/2022".

[38] BRAVYI, S., MASLOV, D. “Hadamard-free circuits expose the structure of the Clifford group”, *IEEE Transactions on Information Theory*, v. 67, n. 7, pp. 4546–4563, 2021.

Índice Remissivo

computação clássica, 5
- algoritmos clássicos, 1
- códigos lineares clássicos, 16
- portas lógicas, 5

computação quântica, 5
- algoritmos quânticos, 1
- atenuação de amplitude, 26
- atenuação de fase, 28
- canais quânticos, 25
- canal despolarizador, 25
- esfera de Bloch, 7
- estado puro, 12
- estados misturados, 12
- fidelidade, 21
- operador densidade, 12
- operação quântica, 25
- qubits, 5
- superposição, 5

correção de erros quânticos, 16
- codificação, 25
- código de Steane, 20
- código dual, 17
- códigos CSS, 17
- códigos estabilizadores, 19
- decodificação, 25
- distância, 16
- distância de Hamming, 16
- espaço da síndrome, 25
- espaço de código, 19
- estabilizador, 18
- formalismo estabilizador, 18
- matriz de verificação de paridade, 16
- matriz geradora, 16
- palavra-código base, 17
- palavras-código, 17
- qubit físico, 18
- qubit lógico, 18
- recuperação, 25

designs unitários, 14

fase global, 18

grupos, 13
- associatividade, 13
- coclasse à direita, 14
- coclasse à esquerda, 14
- fechamento, 13
- gerador, 14
- grupo de Clifford, 15
- grupo de Pauli, 18
- grupo finito, 13
- grupo unitário, 13
- identidade, 13
- inversos, 13
- operação binária, 13
- subgrupo, 13
- teoria dos grupos, 13

IBM Quantum, 31

mecânica quântica, 8
- evolução, 10

formalismo POVM, 11
medição na base computacional, 11
medição projetiva, 10
medição quântica, 10
sistemas compostos, 12
modelo de ruído, 32

portas quânticas, 6
porta $\pi/8$, 6
porta $CNOT$, 6
porta de fase, 6
porta de Hadamard, 6
portas de Pauli, 6
produto tensorial, 12

Qiskit, 31

randomized benchmarking, 21
curva de decaimento de fidelidade, 22
limiar, 24
probabilidade de sobrevivência, 22
randomized benchmarking lógico, 24
sequência, 21
sequência média, 22

simuladores quânticos, 31