COERÊNCIA EM CÓDIGOS QUÂNTICOS DE CORREÇÃO DE ERROS

Orientador: Prof. Dr. Marcos Cesar de Oliveira
Aluno bolsista: Pedro Henrique Pereira de Carvalho Alvarez/ RA: 185729
Vigência: Janeiro a Setembro de 2020

1. Introdução

Com o crescimento de pesquisa e investimento para desenvolvimento de computadores quânticos com alta contagem de qubits, a demanda para o desenvolvimento de protocolos de segurança para evitar falhas se torna cada vez maior. O presente trabalho busca a análise de códigos quânticos através de uma lente de teoria de recursos. O foco foi a coerência, um recurso puramente quântico que mede a quantidade de emaranhamento no sistema, onde buscou-se entender seu papel como ferramenta para o estudo e desenvolvimento de novos códigos quânticos de correção de erros.

No total foram estudados 5 códigos de correção de erros pertencentes a diferentes classes, entre estes códigos dois faziam o uso de um ebit (um par emaranhado de qubits) buscando aumentar a eficiência em comparação com códigos sem ebits. Tais códigos pertencem a classe de códigos assistidos por emaranhamento. Estes códigos com emaranhamento também foram estudados na presença de decoerência usando os estados de Werner para o ebit, assim simulando um emaranhamento instável.

2. Coerência

Coerência é um recurso novo em teoria da informação quântica e ainda é discutido uma forma de medi-la. Ela é armazenada nos termos fora da diagonal principal do operador densidade e depende da base em que a matriz é definida. Para este trabalho foi escolhida a entropia relativa de Von Neumann junto de bases mutuamente imparciais para realizar esta medida.

$$C(\rho) = S(\rho_{diag}) - S(\rho)$$

Onde ρ é a matriz densidade, ρ_{diag} é a matriz com apenas a diagonal principal da matriz densidade e $S(\rho)$ é a entropia de Von Neumann dessa matriz densidade. A matriz densidade representa o operador densidade em uma base. As bases usadas foram a base computacional para qubits ($|0\rangle$ e $|1\rangle$) e sua base mutuamente imparcial, a base $\pm($ $|+\rangle$ e $|-\rangle$). Foi usada a base mutuamente imparcial, pois esta maximiza a coerência [7].

3. Códigos estudados

Foram escolhidos 5 códigos já estabelecidos na literatura para realizar esta pesquisa. Logo abaixo tem-se uma breve descrição de cada código e como é construído.

a. Código de Shor

É o código mais simples deste estudo, e um dos primeiros a ser introduzidos a novos estudantes de teoria quântica de correção de erros. O código de Shor é capaz de corrigir erros generalizados em canais quânticos, aplicando dois códigos simples de repetição um seguido do outro. Primeiro, o qubit da mensagem é codificado usando o código de phase-flip, que protege o qubit contra o erro que troca o sinal da fase deste qubit, aplicando uma transformação da Hadamard e então repetindo o qubit 3 vezes, alterando o qubit da seguinte forma:

$$|0\rangle \rightarrow |+++\rangle, \quad |1\rangle \rightarrow |---\rangle$$

Então o qubit é codificado novamente usando o código de bit-flip, que apenas repete cada qubit 3 vezes, levando aos estados finais:

$$|0\rangle \rightarrow |0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}},$$

$$|1\rangle \rightarrow |1_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}.$$

Assim uma mensagem $|0\rangle$ é codificada no $|0_L\rangle$ ou "zero lógico", que é a representação da mensagem após a codificação. Note que o código de Shor utiliza 9 qubits para codificar 1 qubit de informação, então tem uma taxa de transferência de 1/9, sendo o maior código e o menos eficiente dentre os estudados.

b. Código de Steane

O código de Steane de 7 qubits[6] é o mais famoso e mais usado pela sua simplicidade. As palavras código são geradas a partir da matriz de geradores, que define as transformações que aplicadas não alteram o estado das palavras códigos, então são estabilizadores deste estados. O formalismo de matriz geradora pode ser usado para todos os códigos neste estudo e foi usado para facilitar a análise na parte final do trabalho. A matriz geradora do código de Steane é:

$$\left[\begin{array}{ccccccc|ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]$$

Onde cada linha representa um gerador g, cada 1 a esquerda da linha separadora representa um operador Pauli-X, a direita representa um Pauli-Z e quando há 1 dos dois lados representa Pauli-Y. Se há apenas 0, representa a identidade, por exemplo, o gerador da primeira linha $g_1 = IIIXXXX$ onde cada operador afeta seu respectivo qubit.

c. Código de 5 qubits

Pelo limite de Hamming quântico[4], este é o código mais eficiente possível usando apenas qubits para a codificação, apesar disso não é tão utilizado quanto o código de Steane pela sua complexidade.

d. Código de Shaw e Código de Wilde

Código de Shaw[5] e o código de Wilde[8] são os dois códigos que utilizam pares emaranhados (ebits) para codificar a mensagem[1]. Um dos qubits do par emaranhado fica com Bob enquanto Alice envia seu qubit codificado. Isso aumenta a taxa de transmissão do código em troca do uso do ebit, além disso, o qubit que está com Bob é imune a erros causados durante qualquer computação feita usando a mensagem codificada, diminuindo a possibilidade de erros durante uma computação tolerante a erros.

Quando ambos os códigos foram construídos usando um par emaranhado nos estados de Werner[3], para simular decoerência, pode-se notar que há diminuição da coerência nos códigos com a perda do emaranhamento. Isto é esperado em uma construção de emaranhamento instável.

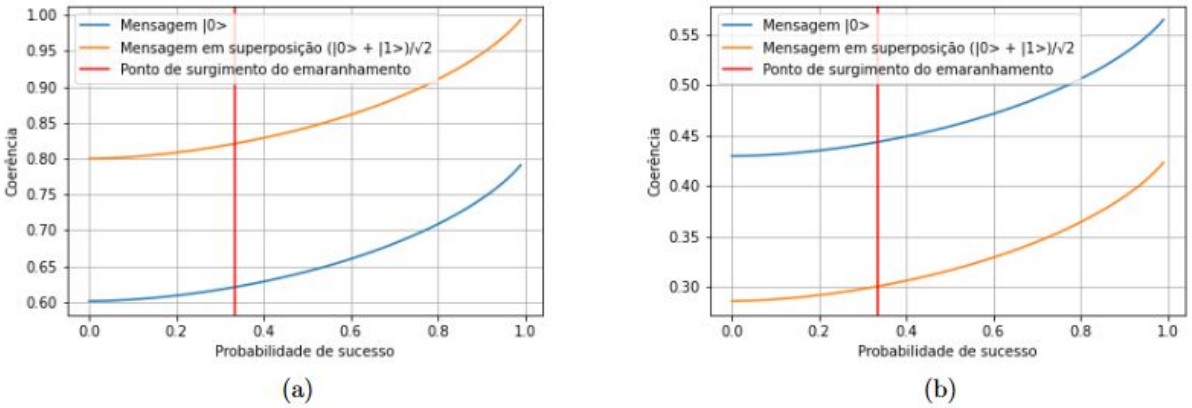

Figura 1: a) Crescimento da coerência com a probabilidade de sucesso na formação do emaranhamento no código de Wilde e (b) Crescimento da coerência com a probabilidade de sucesso na formação do emaranhamento no código de Shaw.

4. Coerência em canais ruidosos

Alguns dos tipos mais comuns de canais ruidosos são os de despolarização (onde a informação dos qubits é perdida devido ao estado ser trocado por um estado completamente misto I/2, onde I é a identidade), relaxação de amplitude (que modela o processo de emissão de fótons, levando os qubits a um estado de menor energia até o estado não-excitado), e de amortecimento de fase (que modela o espalhamento dos qubits, assim perdendo a informação da fase relativa entre os autoestados do qubit e zerando os termos fora da diagonal do operador densidade). É simples ver como estes canais diminuem a coerência do estado da mensagem, zerando os termos fora da diagonal. Este efeito também pode ser visto no canal bit-phase flip, o último canal ruidoso analisado, como pode ser visto nas figuras 2 e 3. Isto mostra uma relação entre a coerência e os efeitos do canal ruidoso sobre a mensagem codificada.

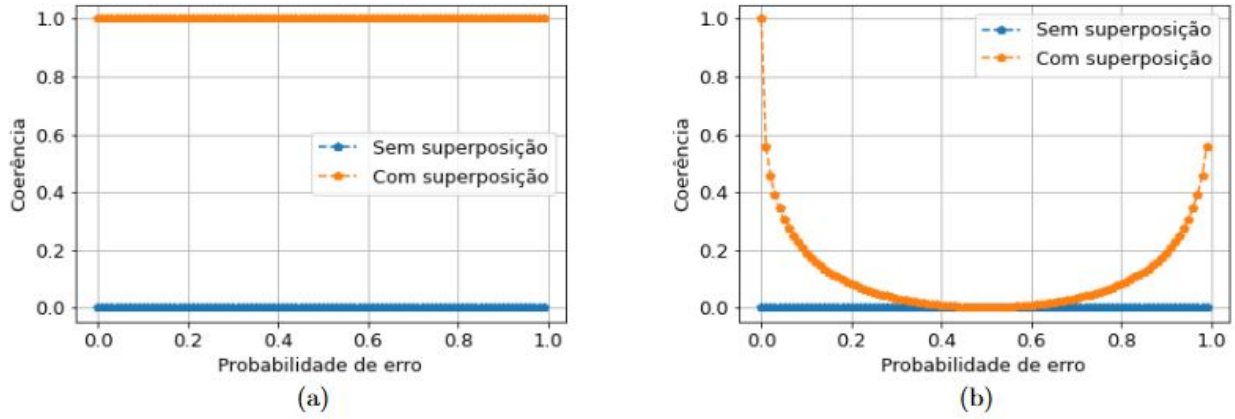

Figura 2: (a) Coerência contra probabilidade de erro no canal de bit flip para um qubit e (b) Coerência contra probabilidade de erro no canal de phase flip para um qubit

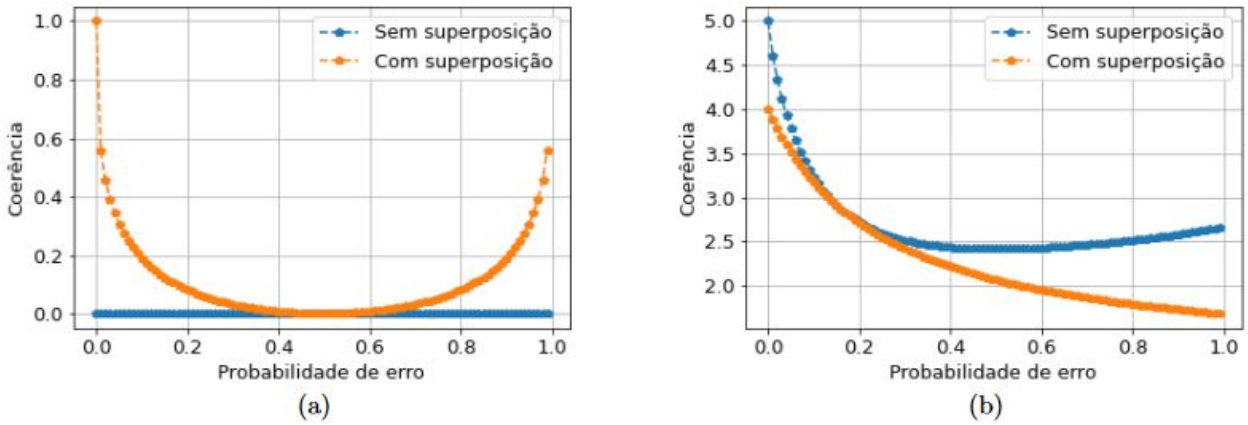

Figura 3: (a) Coerência contra probabilidade de erro no canal de bit-phase flip para um qubit e (b) Coerência medida na base $|\pm\rangle$ contra probabilidade de erro no canal de bit-phase-flip para um qubit codificado no código de 5 qubits.

5. Coerência nos códigos

Computando as coerência dos códigos nas duas bases estudadas e com mensagens sem superposição ($|0\rangle$) e com superposição (($|0\rangle + |1\rangle$)/$\sqrt{2}$), se percebe algumas relações entre a coerência e os códigos. A coerência está ligada ao número de palavras código do estado do código, ou número de autoestados pelos quais o estado do código está espalhado. O código de Steane e de Shaw tem apenas 8 palavras código e tem coerência igual e menor que os códigos de Wilde e 5 qubits que possuem 16 palavras código. A coerência não está ligada a usabilidade do código, pois o código mais útil e simples (Steane) não possui a maior coerência.

A coerência do código de Shor tem este comportamento inesperado devido a forma como é codificado. Como é primeiro aplicado portas Hadamard no sistema, então os qubits são mais espalhados pelo espaço da base $|\pm\rangle$ e são pouco espalhados na base computacional. Isso não ocorre nos outros códigos por serem construídos de forma mais generalizada, independente da base de construção, dependendo apenas dos estabilizadores dos estados do código.

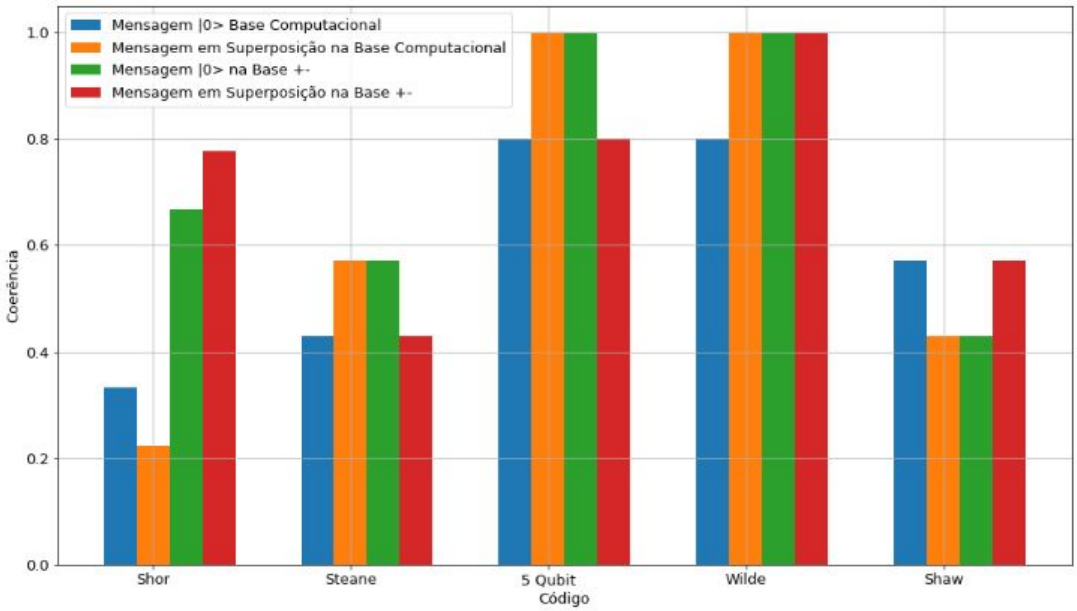

Figura 4: Coerência normalizada medida nas bases computacionais e mais-menos para mensagens com superposição e sem superposição.

6. Erro no Bloco e Taxa de Transmissão

Inspirado por conceito de probabilidade de erro no bloco em teoria da correção de erros clássica, onde é medida a probabilidade de ocorrer um erro ou mais no código e normaliza pela quantidade de bits, foi feita uma comparação semelhante entre os códigos quânticos usando a análise para computação tolerante a erros de Gottesman[2].

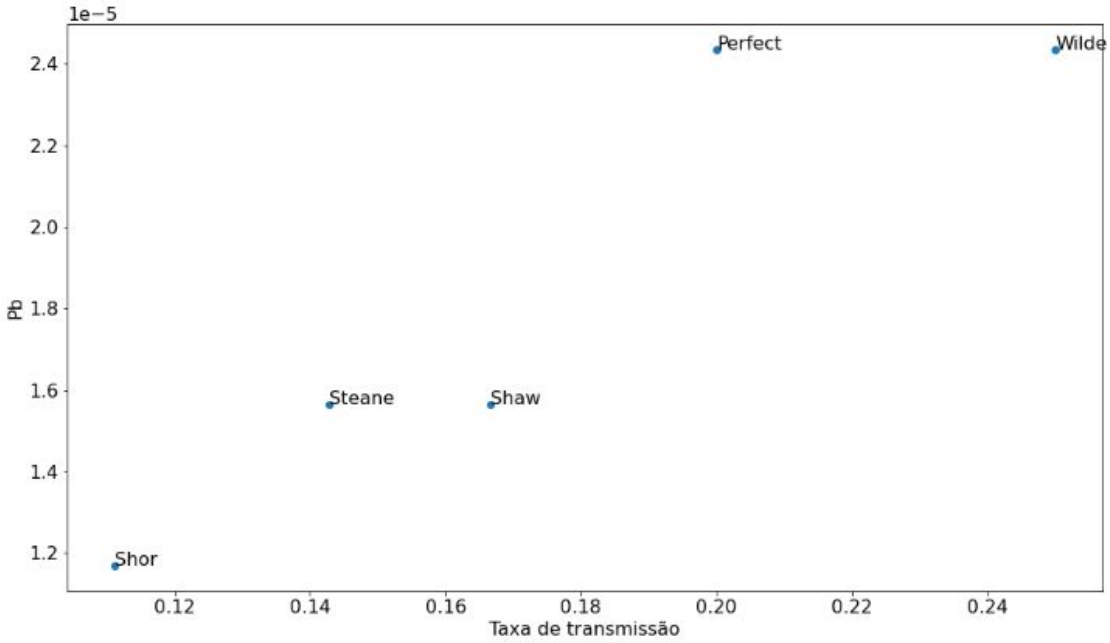

Figura 7: Taxa de transmissão versus a probabilidade de erro no bloco para os códigos quânticos analisados, dado uma probabilidade de erro de 0,1.

Isso demonstra a vantagem dos códigos com emaranhamento, mantendo a mesma probabilidade de erro mas aumentando a taxa de transmissão, onde a única limitação é a estabilidade dos ebits.

7. Referências

[1]Todd Brun, Igor Devetak, and Min-Hsiu Hsieh. Correcting quantum errors with entanglement.Science,314(5798):436–439, 2006.

[2] Daniel Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation,2009.

[3] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement.Rev. Mod. Phys., 81:865–942, Jun 2009.

[4] Michael A. Nielsen and Isaac L. Chuang.Quantum Computation and Quantum Information: 10th Anni-versary Edition. Cambridge University Press, 2010.

[5] Bilal Shaw, Mark M. Wilde, Ognyan Oreshkov, Isaac Kremsky, and Daniel A. Lidar. Encoding one logical qubit into six physical qubits.Phys. Rev. A, 78:012337, Jul 2008.

[6] Andrew Steane. Multiple-particle interference and quantum error correction.Proceedings of the RoyalSociety, 452:2551–2577, Nov 1996.

[7] Alexander Streltsov, Hermann Kampermann, Sabine Wölk, Manuel Gessner, and Dagmar Bruß. Maximal Coherence and the resource theory of purity.New Journal of Physics, 20(5):053058, may 2018.

[8] Mark M. Wilde. Quantum coding with entanglement, 2008