Portas quânticas e o Código de Shor

Analisse Magalhães Alves, Raíssa Karoliny da Silva Rodrigues e Clarice Dias de Albuquerque

***Resumo*— A Informação e a Computação Quântica são estudos do processamento de informação que pode ser efetuado usando propriedades de mecânica quântica. Este trabalho busca introduzir os conceitos básicos da computação quântica, como bit quântico e portas quânticas, bem como os conceitos iniciais da teoria de códigos corretores de erros quântico. Por fim, apresenta-se o Código de Shor, um análogo quântico para o código de repetição clássico.**

***Palavras-Chave*— Computação quântica, Qubit, Código corretor de erro quântico.**

***Abstract*— Quantum Computing and Information are studies of information processing that can be performed using properties of quantum mechanics. This work aims to introduce the basic concepts of quantum computing, such as quantum bits and quantum gates, as well as the initial concepts of quantum error-correcting codes theory. Finally, the Shor Code, a quantum analogue of the classical repetition code, is presented.**

***Keywords*— Quantum Computing, Qubit, Quantum Error-Correcting Code.**

I. Introdução

Pode-se entender a Informação Quântica e Computação Quântica como o estudo do processamento de informações que pode ser efetuado usando mecânica quântica, Nielsen e Chuang (2005). A computação quântica busca simular e aperfeiçoar os processamentos da computação clássica, oferecendo uma vantagem significativa de tempo de processamento sobre essa.

Na computação clássica a unidade básica da informação é o bit, que pode ser representado pelos estados 0 e 1. A computação quântica apresenta como unidade básica o bit quântico ou qubit, que além de poder assumir os estados zero $|0\rangle$ e um $|1\rangle$, que formam a base computacional, também pode estar em uma combinação linear desses estados conhecida como superposição:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

desde que satisfeita a condição $|\alpha|^2 + |\beta|^2 = 1$.

Outra representação para esses estados é a seguinte:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Analogamente à computação clássica em que os circuitos são formados por portas lógicas, na computação quântica existem as portas quânticas. Destacam-se quatro portas que são fundamentais para o processamento de informação quântica, conhecidas como portas ou matrizes de Pauli, representadas por:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

A matriz identidade I não altera o qubit, a porta X troca o estado da base computacional (bit flip), a porta Y realiza uma rotação no eixo e a porta Z troca a fase do qubit (phase shift):

$$I\,|0\rangle = |0\rangle \quad I\,|1\rangle = |1\rangle$$

$$X\,|0\rangle = |1\rangle \quad X\,|1\rangle = |0\rangle$$

$$Y\,|0\rangle = i|1\rangle \quad Y\,|1\rangle = -i|0\rangle$$

$$Z\,|0\rangle = |0\rangle \quad Z\,|1\rangle = -|1\rangle$$

Além disso, outra importante porta de um qubit é a porta de Hadamard, cuja representação matricial é dada por:

$$H = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Essa porta é responsável por transformar o estado $|0\rangle$ no estado $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e o estado $|1\rangle$ no estado $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

A teoria de códigos corretores de erros quânticos se baseia em diversos aspectos à teoria dos códigos clássicos de correção de erros, mas apresenta diferenças importantes devido às particularidades da física quântica. Ressalta-se que os erros provocados por ruídos ou imperfeições nas portas estão ainda mais presentes na computação quântica, que necessita fortemente de correção de erros. Dessa forma, a necessidade de adição de redundância à informação para que a mensagem original seja recuperada após sofrer alguma interferência se torna essencial para o funcionamento da computação.

Embora existam similaridades no princípio do estudo da teoria de códigos quânticos e clássicos, existem impossibilidades físicas que impedem que os procedimentos realizados na codificação clássica sejam reproduzidos na quântica. A de maior relevância é a impossibilidade de copiar ou clonar estados quânticos arbitrários, ferramenta muito utilizada na codificação clássica. Contudo, é possível contornar esse problema e desenvolver alternativas no processo de correção de erros.

O código de Shor, um análogo quântico para o código de repetição, é um código quântico capaz de proteger contra um erro arbitrário de inversão de bit (bit flip) ou inversão de fase (phase shift) em um único qubit. Esse código é a concatenação do código bit flip, que protege contra erros de inversão de bit,

Analisse Magalhães Alves, Centro de Ciência e Tecnologia, Universidade Federal do Cariri, Juazeiro do Norte-CE, e-mail: analisse.magalhaes@aluno.ufca.edu.br; Raíssa Karoliny da Silva Rodrigues, Centro de Ciência e Tecnologia, Universidade Federal do Cariri, Juazeiro do Norte-CE, e-mail: raissa.karoliny@aluno.ufca.edu.br; Clarice Dias de Albuquerque, Centro de Ciência e Tecnologia, Universidade Federal do Cariri, Juazeiro do Norte-CE, e-mail: clarice.albuquerque@ufca.edu.br. Este trabalho foi parcialmente financiado pela Funcap (31052.001951/2025-81).

e do código phase shift, que protege contra erros de inversão de fase.

Os estados lógicos do código bit flip podem ser representados por:

$$|0\rangle \rightarrow |0_L\rangle \equiv |000\rangle$$
$$|1\rangle \rightarrow |1_L\rangle \equiv |111\rangle$$

Os estados lógicos de código phase shift são dados por:

$$|0_L\rangle \equiv |+++\rangle$$
$$|1_L\rangle \equiv |---\rangle$$

Onde $\{|+\rangle, |-\rangle\}$ é conhecido como base conjugada.

O resultado será um código de nove qubits, com estados lógicos dados por:

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)$$

Os parâmetros do código de Shor são $[[9, 1, 3]]$, pois codifica 1 qubit em 9 qubits, pode corrigir até 1 erro arbitrário em um qubit e é formado por uma combinação de códigos de 3 qubits.

II. Conclusões

A Computação Quântica apresenta semelhanças conceituais com a Computação Clássica. No entanto, os mecanismos e conceitos apresentados demonstram que a utilização de física quântica modifica a forma como o processamento de informações ocorre. Como consequência, há uma significativa economia de tempo de processamento, quando comparada à clássica. Entretanto, a teoria de códigos corretores de erros se torna ainda mais necessária para proteger a informação da adição de ruídos. O código de Shor foi o primeiro código criado para correção de erros quânticos. Entender esse código permite realizar o processamento de informações quânticas de maneira eficiente.

Agradecimentos

Agradecemos à Universidade Federal do Cariri pelo suporte institucional e pela infraestrutura disponibilizada, bem como ao CNPq pela concessão da bolsa de Iniciação Científica, fundamentais para a realização deste projeto de pesquisa.

Referências

[1] C. D. de Albuquerque. "Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais". Tese de doutorado. FEEC UNICAMP, 2009.

[2] M. A. Nielsem e I. L. Chuang, **Computação Quântica e Informação Quântica**.Cambridge University Press, 2000. isbn = 978-1-107-00217-3.

[3] R. Portugal, "Códigos Quânticos". Em: **1º Encontro de Teoria dos Códigos e Criptografia**. 2010.