XXIX Congresso de Iniciação Científica UNICAMP 2021

Não-localidade de Bell e o princípio da causalidade da informação

Aluno: Gabriel Hideki Fucuda Nascimento
Orientador: Profº Dr. Rafael Luiz da Silva Rabelo

Palavras-chave: códigos de acesso aleatório, emaranhamento, não-localidade, causalidade da informação, circuito quântico.

1 Introdução

Este projeto de iniciação científica possui como finalidade o estudo sobre a teoria quântica da informação e os fundamentos da mecânica quântica. A proposta inicial do projeto era voltado para não-localidade e o princípio da causalidade da informação, todavia, conforme o andamento do projeto, o novo enfoque foi voltado para não-localidade e também os *códigos de acesso aleatório clássicos* (RAC)[1] e *quânticos* (QRACs)[2], por ser um assunto de extremo interesse e fundamentais para se estudar o princípio da causalidade da informação.

O desenvolvimento do projeto se deu através do estudo dos primeiros capítulos de (1). Este material apresenta os conceitos básicos da teoria quântica da informação e uma revisão sobre álgebra linear e os postulados da mecânica quântica em seus dois primeiros capítulos. Posteriormente, iniciou-se a leitura dos artigos [(2), (3), (4)], onde são expostos a definição de RACs e QRACs e suas estratégias. Para o aprendizado sobre não-localidade e emaranhamento, foi utilizada a referência (5). Por fim, houve o estudo do quarto capítulo de (1) sobre circuitos quânticos, com o intuito de reproduzir os resultados de QRACs para evidenciar as vantagens quânticas presentes.

[1] Sigla do inglês *random access code*
[2] Sigla do inglês *quantum random access code*

2 Métodos

Considere a seguinte situação entre duas partes denominadas Alice e Bob. Alice possui m bits e Bob deseja saber o valor de algum destes bits, escolhido uniformemente por ele. Os *códigos de acesso aleatório* consistem em estratégias de codificação-decodificação com a finalidade de maximizar a probabilidade de Bob acertar o bit desejado.

Os RACs são caracterizados pelo símbolo $m \overset{p}{\mapsto} n$ significando que m bits são codificados em n bits, e qualquer bit inicial pode ser recuperado com a probabilidade de pelo menos p. No caso quântico (QRAC), os m bits serão codificados em n qubits para Bob, o qual realizará uma medição para obter o bit inicial desejado. Para determinar a qualidade de uma estratégia, são analisadas duas medidas: a probabilidade de sucesso do pior caso e a probabilidade média de sucesso. Essas probabilidades devem ser calculadas de acordo com todas as possibilidades dos pares (x, i) onde $x \in \{0,1\}^n$ é o bit de entrada e $i \in 1, ..., n$ é o bit solicitado.

Subsequentemente, foi estudado o conceito de não-localidade. Este conceito parte de correlações descritas por probabilidades e desigualdades. Imagine a seguinte situação: uma fonte F prepara duas partículas, A e B, cada uma das quais será enviada para dois laboratórios, pertencentes à Alice e Bob. Alice decide realizar a medição x e Bob decide pela medição y. Os resultados de Alice e Bob são a e b, respectivamente.

A descrição deste cenário é tomada como as probabilidades conjuntas de se obter cada par de resultados a e b, quando Alice e Bob realizam as medições x e y, respectivamente. Esta probabilidade é expressa como $p_{a,b|x,y}$. Emprega-se uma condição denominada *não-sinalização*, que exige que não troquem qualquer sinal de comunicação. Todavia, a condição de não-sinalização não garante que os resultados das medições sejam independentes. Caso não sejam, então apresentam alguma correlação que faz com que a probabilidade conjunta não seja igual ao produto das respectivas probabilidades marginais, onde estas representam a descrição individual de cada parte supondo que não haja comunicação entre os mesmos. Ademais, esta correlação deverá ter sido criada de um passado comum de ambos os eventos de medição. Assim é denominada a hipótese de *causalidade local*.

A formalização desta hipótese se dá pela suposição de uma teoria onde uma coleção de variáveis λ possa descrever todas as possíveis causas locais de dois eventos de medição $\mathcal{M}_A$ e $\mathcal{M}_B$ espacialmente separados. Se esta teoria assumir também a hipótese de causalidade local então, fixadas λ, nenhum outro fator é capaz de correlacionar os eventos, ou seja:

$$p_{a,b|x,y,\lambda} = p_{a|x,\lambda} p_{b|y,\lambda}. \tag{1}$$

Na falta de conhecimento sobre a variável λ, pode-se pensar nesta como "variáveis ocultas" e, sem perda de generalidade, assumir que é uma variável única e contínua. Dito isto, a melhor maneira de descrever o experimento é tomando a média sobre todos os valores possíveis:

$$p_{a,b|x,y} = \int_\Lambda q_\lambda p_{a|x,\lambda} p_{b|y,\lambda} d\lambda, \tag{2}$$

onde q_λ é uma distribuição de probabilidades da variável λ de um conjunto Λ. Todas as correlações cujas probabilidades podem ser escritas da forma (2), serão ditas *correlações locais*. Caso não haja um conjunto de variáveis λ tais que as correlações dos eventos não possam ser escritos da forma (2), então serão ditas *correlações não-locais*.

Em seguida, foi estudado o emaranhamento quântico. Um sistema quântico composto é dito emaranhado se o estado global do sistema não puder ser descrito como uma mistura de produtos de estados individuais. Em outras palavras, só é possível descrever o sistema como um todo, independentemente da separação espacial dos subsistemas.

O próximo tema foi causalidade da informação. Esta representa um princípio físico proposto para a explicação dos limites da não-localidade quântica. Ela enuncia que uma transmissão de m bits clássicos pode-se obter, no máximo, um ganho de informação de m bits. Considere um RAC $N \mapsto q$, onde Alice possui N bits e pode, apenas, enviar q bits clássicos para Bob. Ele recebe uma variável aleatória $i \in \{0, 1, ..., N-1\}$ e Alice envia apenas um vetor dado por $\vec{x} = \{x_0, x_1, ..., x_{q-1}\}$. Denote o valor de Bob por β para o bit. Define-se a quantificação da eficiência da estratégia adotada por Alice e Bob como $\mathcal{I} = \sum_{K=0}^{N-1} I(x_K : \beta | i = K)$, onde $I(x_k : \beta | i = K)$ é a *informação mútua* entre x_K e β, vinculada ao recebimento da variável $i = K$ por Bob e é definida como $I(x : y) = \sum_x \sum_y p_{x,y} \log\left(\frac{p_{x,y}}{p_x p_y}\right)$. Diz-se que a causalidade da informação não é violada sempre que $\mathcal{I} \leq m$.

Por fim, os circuitos quânticos. Estes possuem a mesma essência dos circuitos clássicos. São compostos por fios e portas lógicas. Os primeiros apenas transportam a informação (qubit) enquanto que os segundos modificam a informação. As portas quânticas agem como operadores sobre o qubit e alterar o seu estado, mantendo a normalização do mesmo. Também existem portas lógicas quânticas para mais de um qubit, entre elas uma família particularmente importante, a família de portas U-controladas. Elas possuem um qubit de controle e os qubits alvo. Caso o qubit de controle tenha o valor 1, a porta lógica U é operada nos qubits alvo, do contrário não.

3 Resultados e discussão

Segundo o artigo (2), existe um teorema que enuncia que um RAC puramente clássico $n \mapsto 1$ com função de decodificação identidade e funções de codificação majoritária é um ótimo RAC, onde a função de codificação majoritária significa que a saída é qual bit mais se repetiu na string de entrada enquanto que a função de decodificação identidade retorna o mesmo bit que recebeu. Este teorema nos proporciona, para o caso $2 \mapsto 1$, uma probabilidade p no valor de 0.75.

Ainda no mesmo artigo, são apresentados os QRACs $2 \mapsto 1$, $3 \mapsto 1$ e uma breve explicação da impossibilidade do caso $4 \mapsto 1$. A ideia dessas estratégias, de acordo com (2; 3; 4), consiste em pegar n pares mutuamente ortogonais de vetores antipodais de Bloch como as bases de medição para Bob. Em seguida, dividir a esfera de Bloch em 2^n partes com n planos e tomar

os pontos mais distantes possíveis destes planos que cortam a esfera. A razão pela qual não é possível o caso $4 \mapsto 1$ parte da impossibilidade de se cortar a esfera de Bloch em 16 partes utilizando 4 planos, o número máximo de partes chega a 14. Utilizando-se dessa estratégia para o caso $2 \mapsto 1$, foi possível encontrar uma probabilidade de sucesso p no valor de 0.85, evidenciando assim a vantagem quântica sobre os RACs clássicos $2 \mapsto 1$.

Posteriormente, com o intuito de reproduzir os resultados encontrados por (3), foi construído uma simulação do QRAC $2 \mapsto 1$ com probabilidade de 85% através de circuitos quânticos pela IBM Quantum(6).

A estratégia utilizada por Ambainis et al. (3) foi: dependendo dos seus dois bits b_0b_1 iniciais, Alice preparar o seu qubit no estado $|\phi_{b_0b_1}\rangle$. Os quatro estados foram escolhidos para se localizar no equador da esfera de Bloch, separados por ângulos de $\pi/2$ radianos, onde a parametrização é dada por: $|\psi(\theta,\phi)\rangle = cos(\frac{\theta}{2})|0\rangle + e^{i\phi}sen(\frac{\theta}{2})|1\rangle$. Isto posto, os estados de decodificação são:$|\psi_{00}\rangle = |\psi(\pi/2,\pi/4)\rangle$, $|\psi_{01}\rangle = |\psi(\pi/2,7\pi/4)\rangle$, $|\psi_{10}\rangle = |\psi(\pi/2,3\pi/4)\rangle$, $|\psi_{11}\rangle = |\psi(\pi/2,5\pi/4)\rangle$.

Caso Bob queira recuperar o bit b_0, a medição necessária será a projeção sobre o eixo x e, para recuperar b_1, a medição é a projeção sobre o eixo y. Associa-se o resultado 0, caso o resultado da medição seja positiva e 1, do contrário.

Para todos os casos separados da simulação, foi alcançado com sucesso o valor de 85% de sucesso. Para o caso geral, implementou-se o circuito da Figura 1 e foram realizadas 2048 tentativas nos computadores quânticos da IBM. A estatística das tentativas pode ser vista na Figura 2. A média de sucesso obtida foi de 54%, onde a média de cada caso variou entre 70% e 42%.

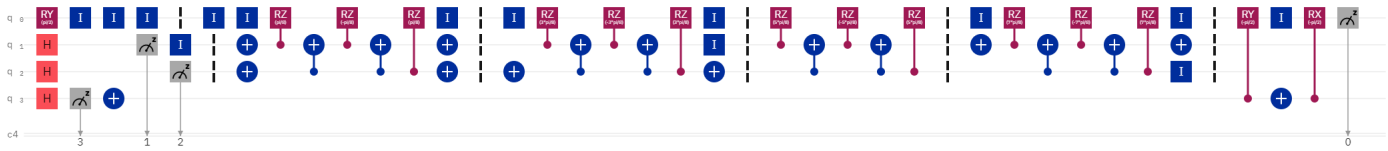

Figura 1: Circuito do caso geral do QRAC $2 \mapsto 1$.

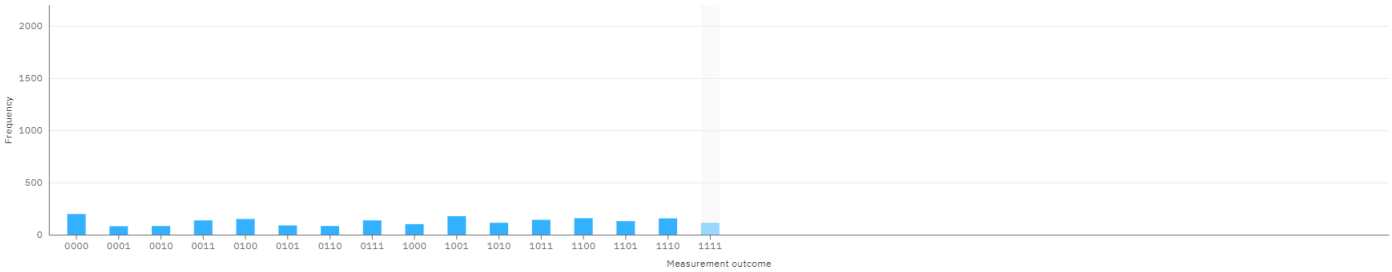

Figura 2: Estatística das tentativas da simulação do QRAC $2 \mapsto 1$.

O resultado obtido não foi o esperado. A diferença ocorre devido a alguns fatores. Na simulação, operação é feita simulando um dispositivo quântico ideal enquanto que, na IBM,

a operação é realizada em dispositivos reais que são suscetíveis a pequenos erros. Por consequência, quanto mais operações num circuito, maior a propagação de erro e, como visto, o circuito apresentado é relativamente grande. Ademais, o número de tentativas é relativamente baixo, caso se estendesse para milhares, as estatísticas seriam melhores.

4 Considerações finais

Neste trabalho há o conteúdo estudado durante um ano de iniciação científica. Resumidamente há a definição de códigos de acesso aleatório, o conceito de não-localidade, emaranhamento quântico e circuitos quânticos. Por fim, é apresentado a simulação do QRAC $2 \mapsto 1$ através dos circuitos quânticos pelo software de computadores quânticos da IBM, evidenciando a vantagem obtida pela teoria quântica nas tarefas de processamento de informação.

Referências

[1] NIELSEN, M.; CHUANG, I. *"Quantum Computation and Quantum Information"*. [S.l.]: Cambridge University Press, 2000.

[2] AMBAINIS, A. et al. Quantum random access codes with shared randomness. 2009. Disponível em: <https://arxiv.org/abs/0810.2937v3>.

[3] AMBAINIS, A. et al. Dense quantum coding and a lower bound for 1-way quantum automata. *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, p. 376–383, 1999.

[4] AMBAINIS, A. et al. Dense quantum coding and quantum finite automata. *Journal of the ACM*, v. 49, n. 4, p. 496–511, 2002.

[5] RABELO, R. L. da S. *Não-localidade quântica: matemática e fundamentos*. Dissertação (Mestrado) — Universidade Federal de Minas Gerais, 2010.

[6] IBM. Disponível em: <https://quantum-computing.ibm.com>.