

# USO DE UM COMPUTADOR QUÂNTICO PARA REALIZAR UMA TAREFA IMPOSSÍVEL NA COMPUTAÇÃO CLÁSSICA

Luiz Henrique Bailo Netto<sup>1</sup>, Roberto Baginski Batista Santos<sup>2</sup>

<sup>1</sup> ETEC Lauro Gomes

<sup>2</sup> Departamento de Física, Centro Universitário FEI

luiz.netto14@etec.sp.gov.br, rsantos@fei.edu.br

**Resumo:** Estudamos como a computação quântica permite realizar tarefas que seriam impossíveis com computadores clássicos como transmitir uma mensagem de dois bits com a troca de apenas um bit quântico, assim facilitando a troca de informações utilizando a codificação superdensa. Determinamos a probabilidade de sucesso e a eficácia de um computador quântico na execução deste algoritmo e comparamos estes resultados com os que seriam obtidos se o computador quântico produzisse resultados aleatoriamente. A apuração deles mostrou que os computadores quânticos já conseguem realizar algumas tarefas consideradas impossíveis na computação clássica.

## 1. Introdução

A computação quântica promete resolver eficientemente problemas computacionais que desafiam a computação clássica, como a determinação rápida dos fatores primos de número muito grandes, isso se mostra um problema importante para a criptografia de chave pública usada para garantir a segurança em transações realizadas pela internet [1].

Na computação clássica, a informação é representada por bits que podem ter o valor 0 ou 1 e o processamento da informação é feito por portas lógicas como, por exemplo, NOT, AND, OR ou XOR. Na computação quântica os bits são trocados por qubits (bits quânticos) que podem estar no estado [1]

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad (1)$$

que é uma superposição quântica dos estados  $|0\rangle$  e  $|1\rangle$ . Os símbolos  $|0\rangle$  e  $|1\rangle$  são elementos de um espaço vetorial e representam dois estados ortogonais e fisicamente distinguíveis do sistema físico no qual o qubit é implementado. Em uma superposição é como se o qubit estivesse nos dois estados simultaneamente.

O estado mais geral de dois qubits é a superposição

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \quad (2)$$

mas o estado emaranhado de Bell

$$|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \quad (3)$$

é muito importante porque representa uma correlação entre os resultados de duas grandezas que são aleatórias quando medidas individualmente.

O emaranhamento é um recurso que pode ser usado na computação quântica porque armazena informação quântica oculta na correlação.

Na computação quântica, o processamento da informação é realizado pela ação de portas quânticas sobre os qubits. Todas as portas quânticas são reversíveis, ao contrário das portas lógicas clássicas, que podem ser reversíveis, como a porta NOT ou irreversíveis, como as portas AND e OR.

Neste trabalho, mostramos como o computador quântico da IBM (ibmqx2) executa o algoritmo da codificação superdensa, que permite enviar dois bits de informação com a troca de um único qubit [2].

Isso é possível apenas porque as partes compartilham um par de qubits emaranhados e conseguem extrair um bit adicional de informação do emaranhamento.

## 2. Metodologia

A codificação superdensa usa duas portas quânticas que agem sobre um qubit:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (4)$$

e outras duas portas controladas que agem sobre o qubit alvo dependendo do estado do qubit de controle:

$$cX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, cZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (5)$$

O efeito da porta  $X$  é trocar o estado  $|0\rangle$  pelo estado  $|1\rangle$  e vice-versa. A porta  $H$  cria as superposições  $(|0\rangle \pm |1\rangle)/\sqrt{2}$  a partir dos estados  $|0\rangle$  e  $|1\rangle$ . A porta  $cX$  aplica a porta  $X$  ao qubit alvo apenas se o qubit de controle estiver no estado  $|1\rangle$  e a porta  $cZ$  altera o sinal do estado  $|1\rangle$  do qubit alvo sempre que o qubit de controle estiver no estado  $|1\rangle$ .

A figura 1 mostra o circuito quântico usado para a codificação superdensa no caso em que a mensagem a ser transmitida é 11. No computador quântico da IBM, todos os qubits são inicializados em  $|0\rangle$ .

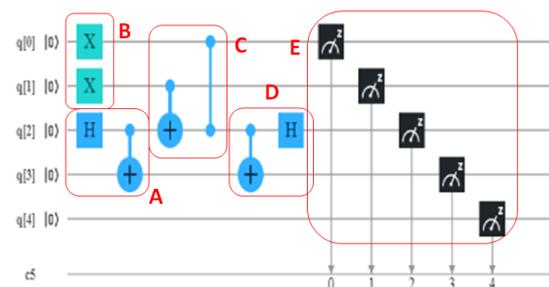


Figura 1. Circuito quântico para a mensagem 11.

O estado emaranhado  $|\beta_{00}\rangle$  é produzido em A usando os qubits  $q_2$  e  $q_3$  enquanto a mensagem 11 é codificada em B nos qubits  $q_1$  e  $q_0$ . O qubit  $q_2$  fica com uma das partes (Alice) e o qubit  $q_3$  fica com a outra parte (Bob). Os qubits  $q_1$  e  $q_0$  que contêm a mensagem ficam com Alice durante todo o processamento.

Na etapa C, as portas controladas  $cX$  e  $cZ$  são usadas por Alice para modificar o qubit  $q_2$  dependendo do estado dos qubits  $q_1$  e  $q_0$  que armazenam a mensagem.

Estas operações não afetam o qubit  $q_3$  que está com Bob. Após a etapa **C**, o qubit  $q_2$  é enviado para Bob.

Na etapa **D**, as portas  $cX$  e  $H$  são usadas para recriar a mensagem original nos qubits  $q_3$  e  $q_2$ . Na etapa **E** Bob mede os qubits para descobrir a mensagem que havia sido codificada anteriormente por Alice nos qubits  $q_1$  e  $q_0$ .

No algoritmo da codificação superdensa, apenas as portas usadas na etapa **B** são variadas dependendo da mensagem que deve ser transmitida. Todas as outras etapas são fixas.

Na codificação superdensa, o único momento em que há troca de informação entre Alice e Bob é entre as etapas **C** e **D**, em que apenas um qubit é enviado de Alice para Bob. Em nenhum momento, Bob tem acesso aos qubits que contêm a mensagem original.

A codificação superdensa mostra que o emaranhamento é recurso que pode ser usado para aumentar a capacidade de comunicação.

Para cada mensagem possível (00, 01, 10 e 11), foram realizadas 1024 execuções do algoritmo no computador quântico ibmqx2 que a IBM disponibiliza em um serviço em nuvem [3].

O computador quântico ibmqx2 é um processador de cinco qubits. Cada qubit é uma junção Josephson supercondutora, em que dois supercondutores são separados por uma camada isolante, ligada a um capacitor para reduzir o ruído de carga elétrica. Os qubits são conectados entre si por guias de micro-ondas.

Foram determinadas as probabilidades de sucesso do computador quântico ao executar o algoritmo para cada uma das mensagens. Para estimar a incerteza nas probabilidades de sucesso, foram realizadas 10 séries de 1024 execuções da porta  $X$  e foi determinado o desvio padrão das probabilidades observadas em cada série.

A fidelidade [1]

$$\mathcal{F} = \sum_i \sqrt{p_i \tilde{p}_i} \quad (6)$$

foi usada como forma de avaliar a eficácia do computador quântico. Na equação (6),  $p_i$  são as probabilidades observadas nos experimentos e  $\tilde{p}_i$  são as probabilidades dos resultados esperados.

A fidelidade mede quanto uma distribuição de probabilidades é semelhante a outra. Assim, uma fidelidade próxima de 1 significa que as probabilidades dos resultados observados são semelhantes às probabilidades esperadas pela análise teórica do algoritmo. Neste caso, o computador quântico executa a codificação superdensa com eficácia.

### 3. Resultados

A tabela 1 mostra as probabilidades de sucesso nas 10 séries de 1024 execuções da porta  $X$ . Em todos os casos, o qubit medido estava inicialmente no estado  $|0\rangle$ .

Tabela 1. Probabilidades de sucesso para a porta  $X$ .

$P_{\text{sucesso}}(\%)$	$P_{\text{sucesso}}(\%)$
97,168	98,340
98,340	97,461
98,047	98,145
98,047	97,266
98,535	97,754

O resultado esperado era que o qubit fosse encontrado no estado  $|1\rangle$  após a aplicação da porta  $X$ . Os resultados obtidos mostram que o desvio padrão da probabilidade é  $\sigma_p = 0,5\%$ .

A tabela 2 mostra as probabilidades de sucesso e a fidelidade para cada uma das quatro mensagens de dois bits na codificação superdensa. A probabilidade de sucesso variou de 59,1% para a mensagem 10 até 85,5% para a mensagem 00. A fidelidade variou entre 0,768 e 0,924, o que está na faixa de intermediária a alta.

Tabela 2. Resultados dos testes da codificação superdensa.

Mensagem inicial ( $q_1 q_0$ )	Resultado esperado ( $q_4 q_3 q_2 q_1 q_0$ )	$P_{\text{sucesso}}(\%)$	Fidelidade $\mathcal{F}$
00	00000	85,5	0,924
10	01010	59,1	0,768
01	00101	63,3	0,814
11	01111	79,6	0,892

Comparamos a distribuição observada de probabilidades com a distribuição que seria gerada por uma decodificação aleatória, no caso em que algum ruído dominasse o processamento.

No caso aleatório, cada um dos quatro resultados possíveis seria obtido com 25% de probabilidade, o que é bem menor do que as probabilidades de sucesso que observamos nos experimentos com o computador quântico. As fidelidades ficariam entre 0,384 no caso 10 e 0,462 no caso 00, o que também está bem abaixo dos valores que observamos nos experimentos com o computador quântico.

## 4. Conclusões

Executamos o algoritmo da codificação superdensa no computador quântico ibmqx2 da IBM. As probabilidades de sucesso e as fidelidades ficaram entre intermediárias e altas, mostrando que o computador quântico não é dominado pelo ruído e apresenta resultados próximos do esperado em uma tarefa impossível de ser realizada com computadores clássicos.

## 5. Referências

- [1] NIELSEN, M.A.; CHUANG, I.L. **Quantum Computation and Quantum Information**. Cambridge: Cambridge University Press, 2000.
- [2] BENNETT, C.H.; WIESNER, S.J. **Physical Review Letters** v. 69, p. 2881, 1992.
- [3] IBM. **IBM Quantum Experience**. Disponível em <<https://quantum-computing.ibm.com>>.

## Agradecimentos

Ao CNPq pela concessão da bolsa de iniciação científica de Ensino Médio, à ETEC Lauro Gomes e ao Centro Universitário FEI pela parceria para realização de iniciação científica e à IBM pelo acesso ao computador quântico.

<sup>1</sup> Aluno de IC do CNPq (PIBIC-Ensino Médio). Projeto com vigência de 08/19 a 07/20.