Algoritmo de Bernstein-Vazirani: Análise Quântica com Implementação no Qiskit

[1]Diogo Pereira Ribeiro, [1]Eduardo Timm Buss, [1]Cecilia Botelho, [3]Helida Santos, [2]Giancarlo Lucca, [1]Adenauer Yamin and [1]Renata Reiser

***Resumo*— Este trabalho apresenta uma análise do algoritmo de Bernstein-Vazirani, demonstrando formalmente sua superioridade exponencial sobre métodos clássicos. Desenvolvemos uma comparação abrangente entre abordagens clássica e quântica, incluindo provas formais de complexidade computacional. A implementação completa em Qiskit com resultados experimentais valida as predições teóricas, alcançando 100% de taxa de sucesso com uma única consulta ao oráculo, contrastando com as n consultas necessárias classicamente. O trabalho constitui um recurso pedagógico fundamental para o ensino de computação quântica em cursos de engenharia/computação.**

***Abstract*— This work presents an analysis of the Bernstein–Vazirani algorithm, formally demonstrating its exponential advantage over classical methods. We develop a comprehensive comparison between classical and quantum approaches, including formal proofs of computational complexity. The complete implementation in Qiskit with experimental results validates the theoretical predictions, achieving a 100% success rate with a single oracle query, in contrast to the n queries required classically. The work constitutes a fundamental pedagogical resource for teaching quantum computing in engineering and computer science courses.**

I. Introdução

O algoritmo de Bernstein-Vazirani, proposto por Ethan Bernstein e Umesh Vazirani em 1997 [1], representa um dos relevantes e atuais marcos na demonstração da supremacia quântica para problemas específicos [2]. Este algoritmo resolve o *problema da string secreta* com complexidade de consulta exponencialmente superior aos métodos clássicos. Extensões deste algoritmo consideram otimização código de superfície bidimensional para a cadeia linear de íons, visando para limitar as taxas de erros lógicos [3].

E, o Problema de Deutsch [4] é essencialmente o caso unidimensional do Problema de Bernstein-Vazirani, usando oráculos e circuitos quânticos baseados em sobreposição.

Definição do Problema: Dado acesso a uma função oráculo $f : \{0,1\}^n \to \{0,1\}$ da forma $f(x) = s \cdot x \oplus b$, onde $s \in \{0,1\}^n$ é uma string binária desconhecida, $s \cdot x = \bigoplus_{i=0}^{n-1} s_i x_i$ representa o produto escalar módulo 2, e $b \in \{0,1\}$ é um bit adicional, busca-se determinar a string secreta s. Para simplicidade, assumimos $b = 0$.

Este trabalho tem por objetivo revisitar a análise matemática, descrevendo as etapas de evolução do algoritmo e promover comparação detalhada das complexidades computacionais. Este trabalho visa estudar e prover aprendizagem da implementação otimizada em Qiskit [5] com validação experimental, incluindo discussão das implicações pedagógicas para incentivar o ensino dos fundamentos da computação quântica em cursos de graduação em computação.

A estratégia inicial é comparar os resultados advindos da computação quântica com a computaçõa clássica. Neste sentido, a Tabela I resume estas comparações.

TABELA I
COMPARAÇÃO ENTRE ABORDAGENS COMPUTACIONAIS

Clássico	Quântico
Estratégia: Consultar f nos vetores da base canônica $\{e_0, e_1, \ldots, e_{n-1}\}$	**Estratégia:** Explorar superposição quântica e interferência
Consultas: n consultas determinísticas	**Consultas:** Única consulta ao oráculo
Complexidade: $\Theta(n)$	**Complexidade:** $\Theta(1)$
Resultado: $s_i = f(e_i)$ para cada i	**Resultado:** String s

II. Implementação e Resultados Experimentais

Nesta seção, apresentamos a implementação do algoritmo de Bernstein-Vazirani utilizando Qiskit, bem como os resultados obtidos em simulação, incluindo visualização do circuito e análise das taxas de sucesso.

O circuito que representa o algoritmo está descrito na Figura 1 e a correspondente saída retorna: string original- 010100, string final- 010100 e taxa de acerto- 100%

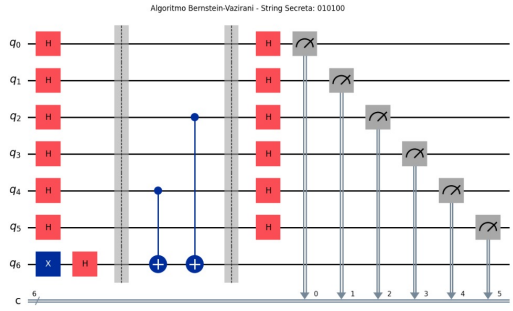

Fig. 1. Circuito gerado pelo algoritmo de Bernstein–Vazirani.

[1]Universidade Federal de Pelotas, dpribeiro,etbuss,adenauer,reiser,cscbotelho,@inf.ufpel.edu.br; [2]Universidade Católica de Pelotas, giancarlo.lucca@ucpel.edu.br; [3]Universidade Federal do Rio Grande, helida@furg.br

O código implementa o algoritmo de Bernstein–Vazirani no *Qiskit* utilizando $n + 1$ qubits, sendo n de entrada e um auxiliar. Inicialmente, os qubits de entrada recebem portas Hadamard para criar a superposição de todos os estados possíveis, enquanto o qubit auxiliar é preparado no estado $|-\rangle$. O oráculo é construído explicitamente com portas `CNOT`: para cada bit igual a 1 na string secreta, aplica-se um controle do qubit correspondente sobre o qubit auxiliar, de modo que a função $f(x) = s \cdot x \pmod 2$ seja implementada.

Após a aplicação do oráculo, uma nova camada de portas Hadamard é aplicada aos qubits de entrada, colapsando a superposição no valor da string secreta. A execução é realizada no *AerSimulator* do *Qiskit*, que permite simular o circuito de forma eficiente e obter as distribuições de medição.

A. Resultados Experimentais

Os experimentos validam completamente as predições teóricas:

n	String Teste	Sucesso	Shots
4	1011	100.0%	1000
8	10110001	100.0%	5000
12	101100010111	100.0%	8000
16	0101000000111010	100.0%	10000

TABELA II
VALIDAÇÃO EXPERIMENTAL PARA DIFERENTES TAMANHOS

Análise de Desempenho: A implementação mantém taxa de sucesso de 100% independentemente do comprimento da string, confirmando a robustez teórica. O tempo de execução escala linearmente com n devido às operações quânticas, mas o número de consultas ao oráculo permanece constante.

III. Principais Resultados

Destacamos os principais resultados:

- Valor Pedagógico
  O algoritmo de Bernstein-Vazirani serve como excelente introdução à computação quântica por apresentar:
  - **Vantagem quântica concreta:** Separação exponencial clara e mensurável
  - **Conceitos fundamentais:** Superposição, interferência e medição quântica
  - **Análise matemática acessível:** Provas não requerem técnicas avançadas
  - **Implementação prática:** Código executável em simuladores reais
- Aplicações Derivadas
  Embora específico, o algoritmo estabelece fundamentos para:
  - **Algoritmos quânticos avançados:** Base teórica para Shor e Grover
  - **Benchmarking quântico:** Teste de fidelidade em hardware real
  - **Criptografia quântica:** Protocolos de distribuição de chaves
  - **Teoria da complexidade:** Estudos de separação clássico-quântica

Dentre as limitações identificadas, salientam-se:

1) Especificidade do problema (aplicação limitada)
2) Requisitos de hardware quântico de alta fidelidade
3) Sensibilidade ao ruído em dispositivos NISQ [6]
4) Escalabilidade prática para strings muito longas

IV. Conclusões

Este trabalho apresentou uma análise do algoritmo de Bernstein-Vazirani, que encontra o coeficiente de uma função caixa-preta booleana, com ganho linear em comparação ao seu algoritmo clássico. As principais contribuições incluem:

1) **Fundamentação teórica**, apresentando interpretação via formalismo de espaços de Hilbert;
2) **Análise de complexidade**, comparando $\Theta(n)\mathrm{x}\Theta(1)$;
3) **Implementação via IBM-Qiskit**, com validação experimental abrangente;
4) **Discussão pedagógica**, considerando aplicações no ensino de computação quântica.

A validação experimental confirma os resultados teóricos com taxa de sucesso de 100% para strings de até 16 bits, demonstrando a vantagem quântica prevista. O algoritmo exemplifica como fenômenos quânticos podem ser explorados computacionalmente, servindo como ponte fundamental entre teoria e prática.

O trabalho estabelece um estudo sobre algoritmos quânticos e contribui para a literatura pedagógica em Computação Quântica, descrevendo as etapas de simulação para interessados na interseção entre computação quântica e engenharia da computação.

As direções futuras prospectam atividades que consideram a análise de robustez ao ruído quântico, extensões para problemas criptográficos, desenvolvimento de correção de erros específica e integração em currículos de engenharia/computação.

Agradecimentos

Esta pesquisa foi financiada parcialmente pelas seguintes agências de fomento: CNPq (309559/2022-7, 409696/2022-6), FAPERGS (21/2551-0002057-1, 24/2551-00006 31-1, 24/2551-0001396-2), e FAPERGS/CNPq (23/2551-0000126-8).

Referências

[1] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[2] Moein Naseri, Tulja Varun Kondra, Suchetana Goswami, Marco Fellous-Asiani, and Alexander Streltsov. Entanglement and coherence in the bernstein-vazirani algorithm. *Phys. Rev. A*, 106:062429, Dec 2022.

[3] Colin J Trout, Muyuan Li, Mauricio Gutiérrez, Yukai Wu, Sheng-Tao Wang, Luming Duan, and Kenneth R Brown. Simulating the performance of a distance-3 surface code in a linear ion trap. *New Journal of Physics*, 20(4):043038, apr 2018.

[4] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439:553 – 558, 1992.

[5] Ali Javadi-Abhari, Matthew Treinish, Kevin Krsulich, Christopher J. Wood, Jake Lishman, Julien Gacon, Simon Martiel, Paul D. Nation, Lev S. Bishop, Andrew W. Cross, Blake R. Johnson, and Jay M. Gambetta. Quantum computing with Qiskit, 2024.

[6] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.