

# Análise comparativa de algoritmos clássicos e quânticos para problemas de busca e fatoração

Luis Felipe Lima, Sabrina Rufo, Rosiane de Freitas

**Resumo**—A busca em grandes bases de dados e a fatoração de números inteiros muito grandes são questões centrais na ciência da computação. Enquanto a computação clássica exige  $O(n)$  para a busca não estruturada, e complexidade subexponencial para a fatoração, a computação quântica oferece avanços com os algoritmos de Grover e Shor, que reduzem a busca para  $O(\sqrt{n})$  e a fatoração para complexidade polinomial, respectivamente. Neste trabalho, apresentamos pseudo-códigos de todos os algoritmos, com uma análise crítica da vantagem quântica e os casos de exceção, como o caso da busca em dados estruturados.

**Palavras-Chave**—algoritmo de Grover, algoritmo de Shor, busca binária, busca sequencial, computação quântica, complexidade computacional.

## I. INTRODUÇÃO

A computação quântica representa uma mudança de paradigma na forma como as informações são processadas, oferecendo o potencial para resolver melhor algumas classes de problemas do que em computadores clássicos. Dentre estes problemas, a busca em grandes bases de dados e a fatoração de números inteiros grandes se destacam pelo enorme potencial de aplicações, que vão desde a otimização de sistemas à criptografia de chave pública. A segurança de protocolos como o RSA, por exemplo, baseia-se na dificuldade computacional de fatorar inteiros grandes. Desse modo, neste trabalho é resumida uma análise teórica comparativa entre as abordagens clássica e quântica para estes dois problemas, sob o ponto de vista de complexidade computacional.

## II. ALGORITMOS CLÁSSICOS DE BUSCA E DE FATORAÇÃO

Algoritmos clássicos para o problema da busca e da fatoração são descritos e analisados nesta seção, de modo a embasar a análise comparativa com as versões quânticas dadas mais a frente.

Para o problema de encontrar um elemento dentro de um conjunto ou sequência arbitrária de dados, considera-se dois tipos: dados em ordem arbitrária e ordem ordenados. O algoritmo de **Busca Sequencial**, dado  $n$  elementos em ordem arbitrária e um item a ser procurado, percorre a lista posição a posição, até encontrar o item elemento ou indicar que não está na lista, isto em complexidade polinomial de tempo  $O(n)$ . O algoritmo de **Busca Binária**, dado  $n$  elementos ordenados e

um item a ser buscado, usa a técnica de projeto de divisão-e-conquista, dividindo o espaço de busca pela metade a cada passo, com complexidade polinomial de tempo de  $O(\log n)$ .

Para o problema de fatoração de números inteiros grandes, o algoritmo de melhor desempenho é o **General Number Field Sieve (GNFS)**. Este problema pertence à classe NP com complexidade super-polinomial, o que garante a segurança de sistemas de criptografia, como o RSA (*Rivest-Shamir-Adleman*). No entanto, existe uma versão quântica do algoritmo de Shor, que reduz o problema de fatoração ao de periodização de uma função. Classicamente, essa busca exige um laço de repetição (while) de complexidade exponencial. Este gargalo é o problema que a sub-rotina quântica resolve de modo eficientemente.

## III. ALGORITMOS QUÂNTICOS DE BUSCA E DE FATORAÇÃO

Nesta seção, algoritmos quânticos para o problema da busca e da fatoração são apresentados.

O **Algoritmo de Grover** aborda o problema da busca em uma base de dados não estruturada de  $n$  itens. Diferente de uma busca clássica que requer, em média,  $n/2$  checagens, o algoritmo de Grover encontra o item desejado com alta probabilidade em apenas  $O(\sqrt{n})$  operações.

O **Algoritmo de Shor** é um dos algoritmos quânticos mais importantes devido à sua capacidade de fatorar inteiros em tempo polinomial, com complexidade  $O((\log n)^3)$ , ameaçando criptossistemas como o RSA.

## IV. ANÁLISE COMPARATIVA E DISCUSSÃO

Uma análise detalhada dos pseudocódigos (Figuras 1 e 2) revela que, apesar das diferenças paradigmáticas, os algoritmos clássicos e quânticos partilham de objetivos comuns e, nos casos mais relevantes, de uma interdependência estrutural. Incluímos ainda uma análise de complexidade através da Tabela I que destaca a vantagem quântica, além de um estudo detalhado de cada componente clássica e quântica.

TABELA I: Tabela de Complexidade Computacional

Problema	Abordagem	Algoritmo	Complexidade	
Busca (Ordenada)	Clássica	Binária	$O(\log n)$	
	Busca (Não Ord.)	Clássica	Sequencial	$O(n)$
		Quântica	Grover	$O(\sqrt{n})$
Fatoração	Clássica	GNFS	Super-polinomial	
	Quântica	Shor	$O((\log n)^3)$	

Luis Felipe Lima, Instituto de Computação/Universidade Federal do Amazonas-IComp/UFAM, Manaus-AM, e-mail: luis.lima@icomp.ufam.edu.br ; Sabrina Rufo, Instituto de Computação/Universidade Federal do Amazonas-IComp/UFAM, Manaus-AM, e-mail: sabrinarufo@icomp.ufam.edu.br; Rosiane de Freitas, Instituto de Computação/Universidade Federal do Amazonas-IComp/UFAM, Manaus-AM, e-mail: rosiane@icomp.ufam.edu.br.

Fig. 1: Comparação de paradigmas para o problema de busca.

<p><b>Busca Sequencial</b></p> <pre> function BUSCASEQ(lista, x)   n ← tam(lista)   for i ← 0 até n - 1 do     if lista[i] == x then       return "Achou", i     end if   end for   return Não achou end function </pre>	<p><b>Busca Binária</b></p> <pre> function BUSCABIN(lista, x)   i ← 0; n, f ← tam(lista) - 1   while i ≤ f do     m ← [(i + f) / 2]     if lista[m] == x then       return "Achou", m     else if lista[m] &lt; x then i ←       m + 1     else       f ← m - 1     end if   end while   return Não achou end function </pre>	<p><b>Algoritmo de Grover</b></p> <pre> function GROVER(U<sub>f</sub>, n, A, x)    ψ⟩ ← H<sup>⊗n</sup> 0⟩<sup>⊗n</sup>   k ← ⌊<math>\frac{\pi}{4}\sqrt{n}</math>⌋   for j ← 1 até k do      ψ⟩ ← U<sub>f</sub> ψ⟩      ψ⟩ ← D ψ⟩   end for   i ← Medir  ψ⟩   if A[i] == x then     return "Achou", i   else     return "Não achou"   end if end function </pre>
--	---	---

Fig. 2: Comparação de paradigmas para fatoração.

<p><b>GNFS</b></p> <pre> function GNFS(n)   Escolher f, m t.q. f(m) ≡ 0   (mod n)   Construir bases de fatores   for (a, b) coprimos do     if a - bm e Norma(a - bm)     são suaves then       Guardar relação     end if   end for   Montar matriz M e achar v   t.q. Mv ≡ 0 (mod 2)   Obter x<sup>2</sup> ≡ y<sup>2</sup> (mod n)   g ← MDC(x - y, n)   if 1 &lt; g &lt; n then     return g   else     Repetir   end if end function </pre>	<p><b>Shor Classico</b></p> <pre> function SHORCLASS(n)   Escolher a ∈ {2, ..., n - 1}   if MDC(a, n) &gt; 1 then return   MDC(a, n)   end if   r ← 1 ▷ Gargalo lento   while a<sup>r</sup> (mod n) ≠ 1 do     r ← r + 1   end while   if r é par e a<sup>r/2</sup> ≠ n - 1 then     f ← MDC(a<sup>r/2</sup> - 1, n)     return f, n/f   else     Repetir   end if end function </pre>	<p><b>Shor quântico</b></p> <pre> function ENCONTRARPQ(n, a)   n ← ⌈log<sub>2</sub> n⌉; t ← 2nn   reg1, reg2 ←  0⟩<sup>⊗t</sup>,  0⟩<sup>⊗n</sup>   Aplicar H<sup>⊗t</sup> em reg1   Aplicar U<sub>a,n</sub> (controlado por   reg1)   Aplicar QFT Inversa em reg1   m ← Medir(reg1)   r ← FraçõesContínuas(m/2<sup>t</sup>)   return r end function </pre>
---	--	---

A computação clássica constitui a espinha dorsal de todos os algoritmos. Em etapas pré e pós passos quânticos, a arquitetura clássica se faz necessária, seja para o controle ou no tratamento após a medição. Dessa forma, a computação quântica é empregada em sub-rotinas específicas usando os conceitos de superposição, interferência, oráculos quânticos e mesmo medições para obter acelerações drásticas em relação às suas versões clássicas.

Apesar da superioridade teórica demonstrada, a implementação prática de algoritmos como o de Shor e o de Grover em hardware quântico enfrenta desafios significativos que limitam o seu impacto a curto prazo. A transição da teoria para a realidade é condicionada por obstáculos físicos fundamentais: **decoerência quântica; correção de erros quânticos (QEC); escalabilidade e fidelidade de portas/circuitos quânticos.**

## V. CONSIDERAÇÕES FINAIS

A análise comparativa, destacando aspectos de complexidade computacional, demonstra a superioridade da computação quântica em domínios específicos, com destaque para a aceleração exponencial do algoritmo de Shor para o problema da fatoração de inteiros grandes, que ameaça criptossistemas como o RSA e torna a busca por métodos matemático-computacionais mais robustos para criptografia pós-quântica (PQC) essenciais.

Por outro lado, a análise do algoritmo de Grover para o problema da busca, revela uma conclusão mais sutil. Sua

aceleração quadrática é estritamente contextual à busca em dados não estruturados. Na presença de uma estrutura prévia, como dados ordenados, a vantagem quântica de Grover não apenas desaparece, mas é superada pela eficiência da busca binária em computação clássica. Isto reforça o fato de que a computação quântica não é substituída e sim, complementar.

Portanto, isto reforça o fato de que a computação quântica não substituirá a clássica, mas sim, a complementar. Para a maioria das tarefas, os sistemas clássicos ainda serão mais eficientes, podendo-se aproveitar a supremacia em alguns casos importantes, com o futuro tendendo a ser híbrido, combinando da melhor forma ambos os modelos computacionais.

## REFERÊNCIAS

- [1] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124-134). IEEE.
- [2] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219).
- [3] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press.
- [4] Lenstra, A. K., Lenstra Jr, H. W., Manasse, M. S., & Pollard, J. M. (1990). The number field sieve. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing* (pp. 564-572).
- [5] National Institute of Standards and Technology (NIST). (2022). *Post-Quantum Cryptography*. Acessado em 30 de agosto de 2025. Online: <https://csrc.nist.gov/projects/post-quantum-cryptography>
- [6] Arora, S., & Barak, B. (2009). *Computational complexity: a modern approach*. Cambridge University Press.