"Planeta Água: a cultura oceânica para enfrentar as mudanças climáticas no meu território"
SECT - ICE
XII Semana de Ciência e Tecnologia SECT ICE
20 a 23 de Outubro de 2025
Realização:
INSTITUTO DE CIÊNCIAS EXATA

Eficiência Computacional em Busca e Fatoração: um Estudo Comparativo entre Algoritmos Clássicos e Quânticos

Luis Felipe dos Santos Lima[1*], Sabrina Rufo[2*], Rosiane Freitas[2*]

[1]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.

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 [5]. 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 [1], 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.

Algoritmos Clássicos de Busca e 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 itemelemento 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)**[3]. 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*)[1]. 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.

Algoritmos Quânticos de Busca e 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 $O(\sqrt{n})$ [2] 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[6].

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 1 que destaca a vantagem quântica,

Tabela 1: 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	$O((\log n)^3)$

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**[5].

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

Busca Sequencial

```
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
```

Busca Binária

```
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] < x then i ← m + 1
        else
            f ← m − 1
        end if
    end while
    return Não achou
end function
```

Algoritmo de Grover

```
function GROVER(U_f, n, A, x)
    |ψ⟩ ← H^⊗n |0⟩^⊗n
    k ← ⌊(π/4)√n⌋
    for j ← 1 até k do
        |ψ⟩ ← U_f |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
```

Figura 2: Comparação de paradigmas para fatoração.

GNFS

```
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 − bθ) são suaves then
            Guardar relação
        end if
    end for
    Montar matriz M e achar v
      t.q. Mv ≡ 0 (mod 2)
    Obter x² ≡ y² (mod n)
    g ← MDC(x − y, n)
    if 1 < g < n then
        return g
    else
        Repetir
    end if
end function
```

Shor Classico

```
function SHORCLASS(n)
    Escolher a ∈ {2, .., n − 1}
    if MDC(a, n) > 1 then return MDC(a, n)
    end if
    r ← 1                    ▷ Gargalo lento
    while a^r (mod n) ≠ 1 do
        r ← r + 1
    end while
    if r é par e a^(r/2) ≠ n − 1 then
        f ← MDC(a^(r/2) − 1, n)
        return f, n/f
    else
        Repetir
    end if
end function
```

Shor quântico

```
function ENCONTRARPQ(n, a)
    n ← ⌈log₂ n⌉; t ← 2nn
    reg1, reg2 ← |0⟩^⊗t, |0⟩^⊗n
    Aplicar H^⊗t em reg1
    Aplicar U_{a,n} (controlado por reg1)
    Aplicar QFT Inversa em reg1
    m ← Medir(reg1)
    r ← FraçõesContínuas(m/2^t)
    return r
end function
```

Conclusões

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 matemáticos-computacionais mais robustos para criptografia pós-quântica (PQC)[6;4] 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[2]. 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 substituta e sim, complementar.

Portanto, isto reforça o fato de que a computação quântica não substituirá a clássica, mas sim, a complementará[5]. 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.

Agradecimentos

Os autores fazem parte do grupo de Computação Quântica - Algoritmos, Otimização e Complexidade (ALGOX) do Programa de Pós-Graduação em Informática da UFAM e do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), com pesquisa realizada com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES-PROEX) - Código de Financiamento 001, bem como parcialmente financiado pela Fundação de Amparo à Pesquisa do Estado do Amazonas – FAPEAM – por meio do projeto POSGRAD 2024/2025.

Referências

Arora, S., & Barak, B. (2009). *Computational complexity: a modern approach*. Cambridge University Press.

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).

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).

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

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press.

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.