Solução Quântica para 3-SAT com Grover: Uma abordagem prática e amigável

Ricardo G. M. S. Ruiz[1], **Gabriel A. R. Gomes**[1], **Calebe P. Bianchini**[1]

[1]Faculdade de Computação e Informática
Universidade Presbiteriana Mackenzie
São Paulo – SP – Brasil

{10389321,10389313}@mackenzista.com.br, calebe.bianchini@mackenzie.br

Abstract. *This meta-article aims to explore a quantum circuit approach to solving the classic and costly satisfiability problem, using the infamous Grover's algorithm as the main resolution algorithm. In conjunction with the use of the Qiskit library, the article discusses a practical and theoretical approach that implements the solution to the problem.*

Resumo. *Este meta-artigo visa explorar uma abordagem de circuitos quânticos para a resolução do clássico e custoso problema da satisfabilidade, utilizando como principal algoritmo de resolução o famigerado algoritmo de Grover. Em conjunto com a utilização da biblioteca Qiskit, o artigo discorre sobre uma abordagem prática e teórica que implementa a solução para o problema.*

1. Introdução

O constante avanço da computação e a crescente demanda por soluções mais eficientes têm conduzido a um cenário de busca contínua por algoritmos que otimizem a resolução de problemas complexos. Tanto na ciência e na produção de hardware quanto no mercado de trabalho, algoritmos clássicos têm sido pilares fundamentais para uma ampla gama de aplicações. No entanto, o advento da computação quântica promete revolucionar a forma como abordamos essas questões, oferecendo um novo paradigma de processamento que pode superar as limitações dos algoritmos clássicos em determinados contextos e superar o limite físico apresentado nos computadores atuais. Enquanto a computação clássica utiliza bits que podem estar em estados 0 ou 1, a computação quântica utiliza qubits que podem existir em estados de sobreposição, representando simultaneamente 0 e 1. Essa capacidade de processamento paralelo quântico é o que confere à computação quântica sua notável vantagem em certos tipos de cálculos. 3-SAT é um desafio importante na ciência da computação que é difícil de resolver, mas a computação quântica, especialmente o algoritmo de Grover, pode oferecer uma solução mais eficiente. Portanto, esses se tornaram os tópicos centrais de nosso estudo.

2. Referencial Teórico

Antes de entrar em nosso estudo, é necessário entendermos alguns conceitos como Máquina de Turing, problema NP, K-SAT, Grover e Hadamard.

[Sipser 2007] A Máquina de Turing é um modelo abstrato de computação que utiliza uma fita infinita dividida em células discretas para manipular símbolos com base

em regras definidas. Apesar de sua simplicidade, esse modelo é capaz de executar qualquer algoritmo computacional. A máquina consiste em uma cabeça que percorre a fita, podendo ler e escrever símbolos em cada célula. Cada célula contém um símbolo retirado de um conjunto finito de símbolos. Além disso, a máquina opera em um conjunto finito de estados. No início, a fita contém apenas a sequência de entrada e está vazia em todos os outros lugares. Caso a máquina precise armazenar informações, ela pode escrevê-las na fita. Para ler as informações escritas, a máquina pode mover sua cabeça de volta sobre elas. A computação continua até que a máquina decida produzir uma saída. As saídas "aceitar"e "rejeitar"são determinadas ao entrar em estados especificamente designados para tal. Caso não entre em nenhum estado de aceitação ou rejeição, a máquina continuará indefinidamente, sem parar.

Os problemas NP são aqueles para os quais, dada uma solução, é possível verificar, no pior caso, utilizando uma Máquina de Turing não determinística, em tempo limitado polinomial. Acontece que, para determinados problemas, ao executar esse mesmo problema só que em uma máquina de turing determinística, obtemos um tempo limitado não polinomialmente. Por conta disso, os problemas NP são considerados os mais custosos de serem resolvidos computacionalmente no pior caso, e apresentam uma grande importância na teoria da computação.

[Varmantchaonala et al. 2022] O problema SAT é um dilema combinatório de grande relevância teórica e prática. Assim como outros problemas combinatórios, a busca por uma solução consome tempo, e esse tempo aumenta de maneira exponencial conforme o tamanho das entradas. Esse problema foi um dos primeiros a ser reconhecido como NP-Completo, possuindo uma complexidade de $O(2^n)$. Seja $x_1, \ldots, x_n$ variáveis booleanas, um literal pode ser uma variável booleana x_1 ou sua negação $\neg x_i$. Uma fórmula k-FNC (forma normal conjuntiva) é uma conjunção de cláusulas, onde cada cláusula é uma disjunção de exatamente k literais. O problema k-SAT é dado um k-FNC, decidir se é satisfazível ou não.

[Qiu et al. 2022] O algoritmo de Grover é um método quântico para buscar um elemento alvo em um banco de dados não ordenado, e é significativamente mais rápido do que qualquer algoritmo clássico para o mesmo problema. O artigo discute uma versão distribuída do algoritmo de Grover, que permite computar uma função Booleana com menos consultas e um número menor de bits de entrada. A ideia central é decompor a função em subfunções, cada uma com menos bits de entrada, e então calcular essas subfunções para encontrar o objetivo com menos consultas.

[Silva 2018] O termo Hadamard se refere à geração de bits aleatórios. O Hadamard, neste contexto, está relacionado à Transformada de Hadamard, que é uma operação linear fundamental em computação quântica. Ela é usada para criar superposições de estados quânticos, permitindo que um qubit esteja em uma combinação de estados 0 e 1 simultaneamente. Isso é crucial para algoritmos quânticos, como a geração de números aleatórios, pois permite explorar o paralelismo quântico e realizar cálculos em muitos estados possíveis ao mesmo tempo. A Transformada de Hadamard é representada por uma matriz específica que, quando aplicada a um vetor de estado de um qubit, resulta na superposição desejada de estados.

3. Trabalhos Relacionados

[Portilheiro 2018]

Neste artigo, a introdução destaca o potencial da computação quântica para acelerar soluções para problemas conhecidos, como demonstrado pelos algoritmos de Shor e Grover. O foco é explorar a aplicação do algoritmo de Grover ao problema Unique-k-SAT, que é NP-completo. O autor apresenta uma solução competitiva para tal problema usando o algoritmo de Grover, alcançando um tempo assintótico de execução de $O(2^{n/2})$, superando os melhores tempos de execução clássicos conhecidos para casos específicos do problema. O artigo pressupõe conhecimento básico em complexidade computacional e computação quântica, particularmente o modelo de circuito quântico e os portões de Hadamard e CNOT.

Na parte seguinte sobre Unique-k-SAT, o artigo discute o problema de encontrar a única atribuição satisfatória para uma fórmula em forma normal conjuntiva (FNC), onde cada cláusula contém no máximo k variáveis booleanas. O autor menciona que a solução ingênua seria iterar por todas as possíveis atribuições de variáveis, o que levaria um tempo $O(2^n)$. No entanto, soluções mais avançadas oferecem um tempo de execução determinístico para a solução Unique-3-SAT de $O(1.307^n)$, e uma solução probabilística para o 4-SAT de $O(1.46981^n)$.

o Algoritmo de Grover é apresentado como uma técnica de busca quântica que pode ser aplicada para resolver o problema da satisfabilidade booleana única (Unique-k-SAT), que é um desafio computacional clássico. Embora frequentemente descrito como uma busca em banco de dados quântico, o Algoritmo de Grover é mais precisamente um método para encontrar entradas que produzam um valor de saída específico em uma função avaliável em um computador quântico. A implementação prática do algoritmo envolve a construção de um oráculo quântico, que é uma porta de controle que permite a avaliação da função f em uma entrada x utilizando um bit ancilla (um qubit "extra").

A próxima seção aborda a construção do oráculo U_f. O autor enfatiza que, se fosse difícil construir o oráculo, o algoritmo de Grover não ofereceria vantagens práticas. No entanto, o artigo explica que existem técnicas para implementar oráculos a partir de circuitos clássicos, o que é aplicado na construção do oráculo para o problema proposto.

O processo de construção do oráculo U_f para o algoritmo de Grover aplicado ao problema Unique-k-SAT. O oráculo é essencial para que o algoritmo funcione corretamente, pois ele permite a avaliação da função f em um computador quântico. A construção do oráculo envolve a utilização de portas NOT e CNOT para configurar qubits auxiliares que representam as cláusulas da fórmula em forma normal conjuntiva (FNC). Esses qubits auxiliares são ajustados para refletir a satisfação de suas respectivas cláusulas com base nos valores de entrada. Após a configuração dos qubits das cláusulas, um qubit de saída é usado para representar a satisfação da fórmula CNF completa. O autor também destaca a necessidade de "desfazer" os cálculos dos qubits das cláusulas para implementar o oráculo de maneira reversível. O autor mostra um exemplo da criação do circuito utilizando a seguinte fórmula: $f = (x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2) \wedge (x_1 \vee \neg x_3)$. O autor também cita o teorema de De Morgan, a fim de facilitar a construção do circuito, que passa a possuir a seguinte fórmula: $f = \neg(\neg x_2 \wedge \neg x_3) \wedge \neg(x_1 \wedge x_2) \wedge \neg(\neg x_1 \wedge x_3)$.

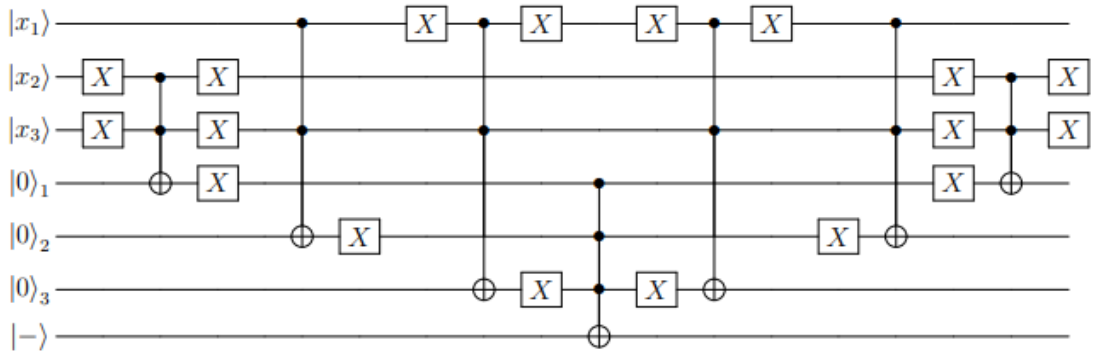

Figura 1. Exemplo do circuito quântico do artigo.

O circuito é simétrico após a aplicação do CNOT no qubit de saída. Os portões antes deste ponto de simetria são explicados com base nas cláusulas da fórmula: para a primeira cláusula, $x2$ e $x3$ são negados antes do CNOT e o bit de cláusula é negado após o CNOT, para a segunda cláusula, como $x1$ e $x2$ são negados, suas linhas de qubit não precisam ser negadas, e o resultado no qubit da cláusula 2 é negado após o CNOT, para a cláusula 3, apenas a linha de qubit para $x1$ precisa ser negada, pois $x3$ já está negado na cláusula. O texto também menciona que a construção de um portão k-controlled-NOT é possível com apenas $k1$ ancilla adicionais, permitindo a construção do oráculo U_f para uma fórmula f de m cláusulas usando apenas $m + k - 1$ ancilla adicionais. Isso torna a aplicação do algoritmo de Grover eficiente tanto em tempo de execução quanto em espaço.

[Gamberi and Bianchini 2022]

Este artigo apresenta um estudo sobre algoritmos quânticos e suas implementações, com foco no algoritmo de busca de Grover. A computação quântica é destacada como um campo de pesquisa essencial, com avanços tecnológicos permitindo superar desafios práticos na fabricação de computadores quânticos. O conceito de qubits é introduzido, explicando sua capacidade de assumir superposições e a necessidade de medição para determinar seu estado, o que resulta na perda do estado anterior do qubit. A esfera de Bloch é usada para representar a superposição de um qubit, com ênfase no eixo z, onde são calculadas as probabilidades durante a medição.

O artigo prossegue com uma discussão sobre oráculos em algoritmos quânticos. A biblioteca Qiskit é introduzida como uma ferramenta para implementar algoritmos quânticos, permitindo a criação e execução de circuitos quânticos por meio de simulação ou processadores quânticos em nuvem. O Quantum Algorithm Zoo é explorado como um repositório de algoritmos quânticos, categorizados em quatro tipos: algébricos e número teóricos, oraculares, aproximação e simulação, e otimização, numéricos e aprendizado de máquina.

O algoritmo de fatoração de Shor é examinado por sua capacidade de quebrar a criptografia RSA, e o cálculo do logaritmo discreto é analisado por sua eficiência em quebrar criptografias baseadas em curvas elípticas. O problema da soma dos subconjuntos é mencionado como tendo uma solução quântica não tão vantajosa em comparação com a clássica. O algoritmo de busca de Grover é destacado por reduzir significativa-

mente o número de consultas necessárias para encontrar um item em um conjunto, e sua generalização, a estimação de amplitude, é reconhecida como um conceito importante para algoritmos quânticos.

O artigo detalha a implementação do algoritmo de Grover, utilizando a biblioteca Qiskit e um notebook Python. O processo começa com a aplicação de um oráculo em um sistema uniformemente superposto, seguido por rotações específicas e a aplicação da matriz de difusão. O algoritmo é testado com um oráculo simples e depois com um exemplo mais prático, demonstrando a capacidade do algoritmo de Grover de identificar estados específicos com alta probabilidade.

Duas alternativas ao algoritmo de Grover são propostas: o algoritmo de busca quântico por probabilidade (ABQP) e o algoritmo de busca quântico por rotação (ABQR). O ABQP codifica números em um vetor de estados e utiliza um portão lógico para subtrair cada estado pelo estado buscado, enquanto o ABQR codifica números ao longo do perímetro do eixo y de um qubit e aplica rotações para identificar o número buscado. Ambos os métodos são explorados, com o ABQR mostrando um desempenho superior.

O artigo [Portilheiro 2018] desempenhou um papel crucial neste estudo devido à sua abordagem semelhante na aplicação de uma solução quântica para um problema de satisfatbilidade, utilizando o algoritmo de Grover. Além disso, o método empregado para a criação do oráculo, conforme descrito no artigo, serviu como base para o desenvolvimento do nosso próprio oráculo, ilustrado na Figura 2. O artigo [Gamberi and Bianchini 2022] teve uma contribuição fundamental no desenvolvimento do nosso trabalho. Ele não apenas enriqueceu nosso entendimento sobre computação quântica, mas também nos apresentou à biblioteca Qiskit, que incorporamos em nosso projeto. Importante ressaltar que nós adotamos diretamente em nosso projeto a implementação do Algoritmo de Grover descrita no artigo.

4. Metodologia

Para adentrar na abordagem prática para a resolução do problema, foi feito um breve estudo sobre como utilizar a biblioteca Qiskit, ferramenta altamente utilizada para desenvolvimento e execução de circuitos quânticos. Em consonância com o conteúdo exposto no livro [Silva 2018], foi empreendido um estudo aprofundado sobre circuitos quânticos. Tal investigação permitiu não apenas a compreensão das complexidades teóricas, mas também a aplicação prática dos conceitos abordados. Adicionalmente, foi conduzida uma análise rigorosa sobre a implementação do algoritmo de Grover, conforme delineado no trabalho de [Gamberi and Bianchini 2022]. Essa investigação possibilitou a atualização do procedimento para a versão mais recente do Qiskit, considerando que este empregava uma versão anterior da biblioteca em questão.

Na sequência do estudo, procedeu-se à análise do trabalho de [Portilheiro 2018], que estabelece a viabilidade de implementar um oráculo representando uma expressão lógica, seguido pela aplicação do operador de Grover. Esta etapa foi crucial para a compreensão teórica e prática das possibilidades oferecidas pela computação quântica e na resolução do problema do k-SAT e sua fusão com o operador de Grover. Posteriormente, realizou-se a integração desta abordagem com as contribuições de [Gamberi and Bianchini 2022], atualizadas conforme citado anteriormente. A fusão resultou na adaptação do oráculo existente, que, a fim de obter uma prova de conceito, a

implementação de um oráculo previamente definido por uma abstração da biblioteca Qiskit. Nesta abstração, uma expressão na Forma Normal Conjuntiva (FNC) é fornecida, e a própria biblioteca se encarrega de construir o oráculo necessário.

Prosseguindo com a investigação, e no intuito de substituir a abstração do oráculo proposta pelo Qiskit, aprofundou-se no estudo do método proposto por [Portilheiro 2018] para a criação do circuito referente a uma expressão lógica. A implementação dessa técnica foi um passo crucial, culminando na obtenção de resultados parciais que são explorados neste documento.

5. Resultados Parciais

Com base nos estudos citados acima, foi implementado um oráculo que representa a expressão lógica, em combinação com o operador de Grover, representado pela seguinte forma geral:

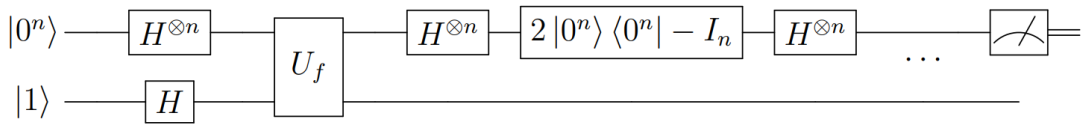

Figura 2. Forma geral do circuito para resolução de problemas de satisfabilidade com operador de grover [Portilheiro 2018]

Onde foi escolhido a seguinte fórmula lógica em FNC para ser utilizada como entrada para o oráculo:

$$(\neg A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (A \vee B \vee \neg C)$$

Dito isso, em conjunto com o estudo explicado em [Portilheiro 2018], foi criado um circuito quântico que representa tal expressão lógica, onde a quantidade de Qubits é obtida pela seguinte fórmula:

$$\text{Qubits} = \text{QtdTermos} + \text{QtdClausulas} + 1$$

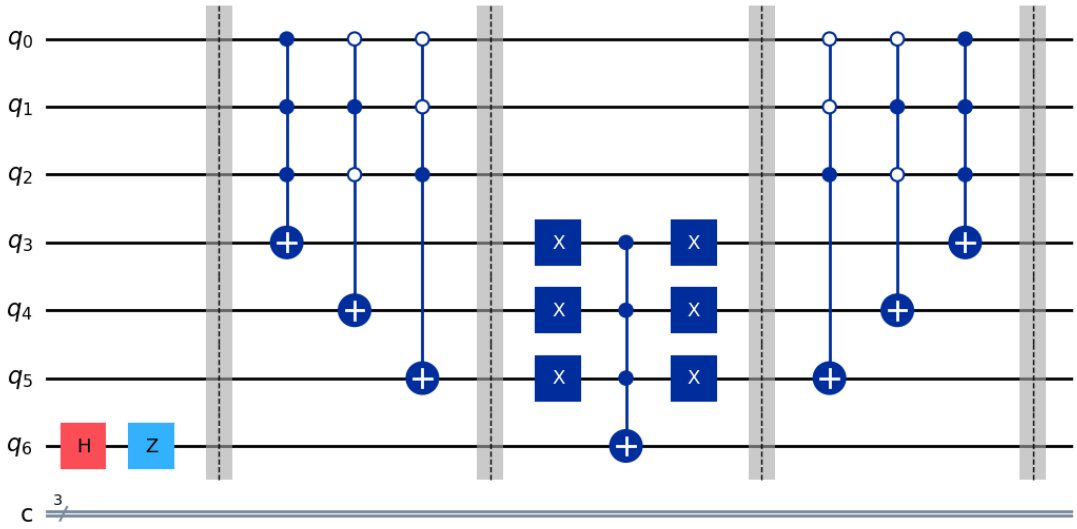

Figura 3. Oráculo que representa a fórmula da expressão lógica, onde as cláusulas são representadas nos três primeiros qubits, e são passados para o qubit ancilla. Após isso, é feito o espelhamento para retornar os estados

Após a criação do oráculo, o passo consecutivo foi a implementação e a adição do circuito de Grover munido pelo trabalho de [Gamberi and Bianchini 2022], e aplicando hadamart antes do oráculo:

Listing 1. Adição do operador de Grover ao oráculo

```
def ApplyGrover(oracle):
  num_qubits = 7
  qr = QuantumRegister(num_qubits)
  qc = QuantumCircuit(qr, name)
  qubits = [0,1,2,3,4,5,6]
  qc.compose(oracle, qubits, inplace=True)

  # Aplica Hadamart Para cada qubit queremos medir
  qc.h(0)
  qc.h(1)
  qc.h(2)

  #Aplica a diagonal para os 3 qubits que desejamos medir
  qc.compose(
      GetDiagonal(oracle),qubits=[0,1,2], inplace=True
  )
  # Aplica Hadamart Para cada qubit que queremos medir
  qc.h(0)
  qc.h(1)
  qc.h(2)
```

```
    return qc
```

Obtendo então o circuito final:

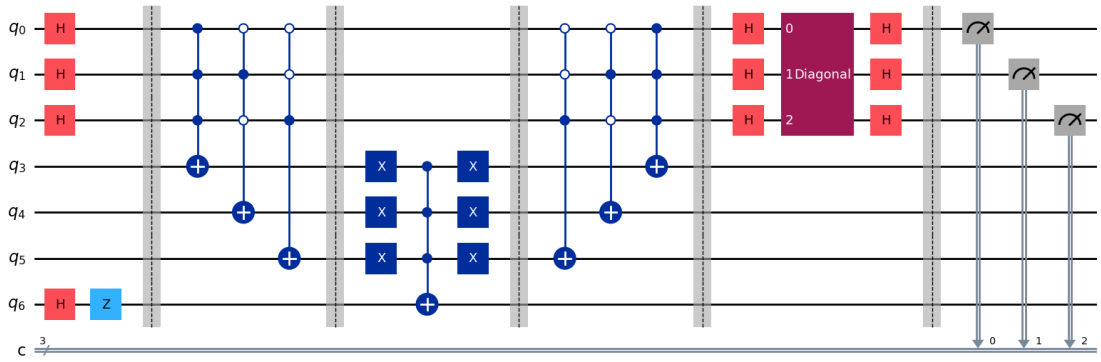

Figura 4. Circuito final após aplicar Grover e Hadamard

Executando o circuito obtido, conseguimos obter a probabilidade dos valores de entrada de C,B,A, respectivamente que resultam nas entradas que resultam na não satisfabilidade do circuito, e, portanto, as demais probabilidades de menor valor, resultam nos valores que representam a satisfabilidade do circuito:

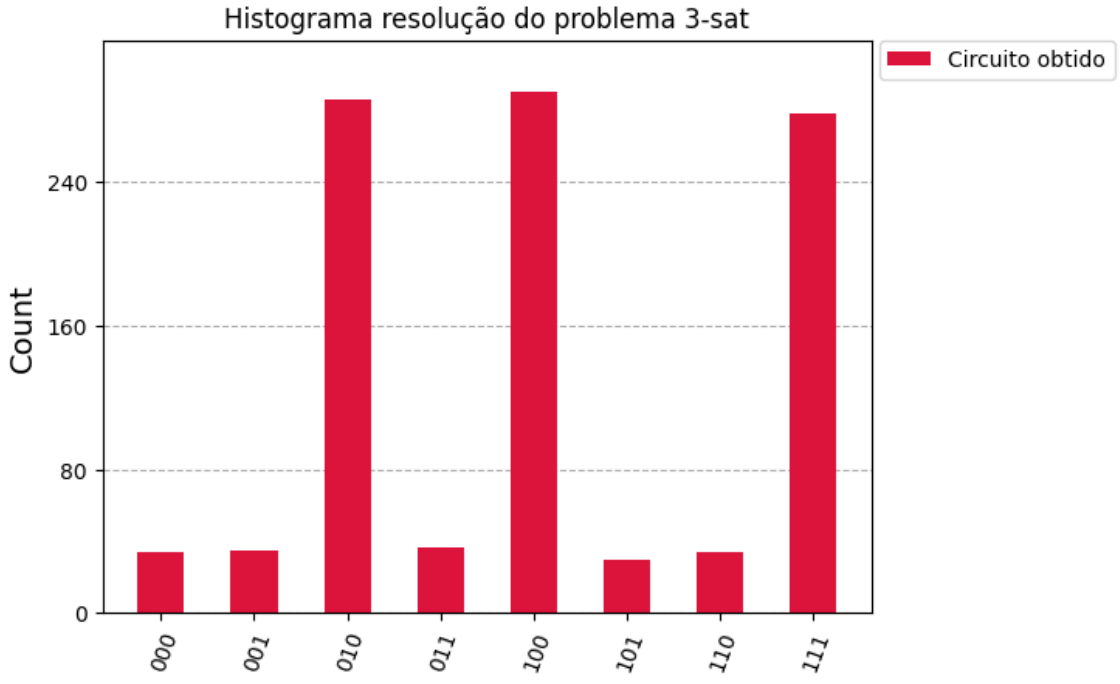

Figura 5. Histograma obtido para a resolução do problema 3-SAT em questão, onde 000, 001, 011, 101, 110 representam as atribuições de C,B,A, respectivamente para a obtenção da satisfabilidade

Em conjunto com isso, foi utilizado uma implementação automática da biblioteca Qiskit como gabarito para o histograma obtido:

Figura 6. Histograma obtido utilizando abstrações da biblioteca Qiskit para a resolução do problema 3-SAT em questão, onde 000, 001, 011, 101, 110 representam as atribuições de C,B,A, respectivamente para a obtenção da satisfabilidade

Listing 2. Criação do circuito utilizando as abstrações da biblioteca Qiskit

```
qiskit_oracle = PhaseOracle(EXPRESSION)

sampler = Sampler()

qiskit_problem = AmplificationProblem(qiskit_oracle)
qiskit_grover = Grover(sampler = sampler, iterations=1)
qiskit_result = qiskit_grover.amplify(qiskit_problem)
```

Os resultados parciais obtidos acima encaixam perfeitamente nos valores de atribuição para C, B, A a fim de obter a satisfabilidade da equação, como comprovado na tabela verdade abaixo:

	A	B	C	Result
0	False	False	False	True
1	False	False	True	False
2	False	True	False	False
3	False	True	True	True
4	True	False	False	True
5	True	False	True	True
6	True	True	False	True
7	True	True	True	False

Figura 7. Tabela verdade para a expressão escolhida

O código fonte para visualização da criação de tal circuito e resultados está disponível para visualização pública, e pode ser obtido no final deste artigo.

6. Cronograma

Tabela 1. Cronograma para o Desenvolvimento do TCC

ATIVIDADE	SEMANA											
	1	2	3	4	5	6	7	8	9	10	11	12
Refinar resultados parciais												
Obter speedup quântico da solução												
Comparação com a computação clássica												
Estudar possibilidades de aumentar os termos (4-sat, 5-sat)												
Comparação dos resultados com trabalhos relacionados												
Revisão e escrita do artigo												

O cronograma acima foi elaborado para garantir um desenvolvimento contínuo e estruturado do Trabalho de Conclusão de Curso. Cada atividade está distribuída ao longo de doze meses, permitindo tempo suficiente para pesquisa, coleta e análise de dados, bem como para a redação e revisão do trabalho. A organização das atividades por mês facilita o acompanhamento do progresso e ajuda a garantir que todas as etapas sejam concluídas dentro do prazo estabelecido.

7. Considerações/Conclusões

Em conclusão, os resultados obtidos até agora reforçam o papel promissor da computação quântica na resolução de problemas clássicos da computação. A característica não determinística da computação quântica nos permite obter resultados de várias maneiras. Especificamente, o algoritmo de Grover provou ser uma ferramenta versátil para lidar com o

problema 3-SAT. Este trabalho apresentou uma abordagem prática para a implementação do algoritmo de Grover, demonstrando sua aplicabilidade e eficácia.

Referências

Gamberi, G. P. and Bianchini, C. D. P. (2022). Estudo de algoritmos quânticos e suas implementações. https://dspace.mackenzie.br/items/071a8df2-1a8f-45c2-ab22-49749d06479b.

Portilheiro, V. (2018). Applying grover's algorithm to unique-k-sat. https://vportilheiro.github.io/assets/writeups/quantum-sat.pdf.

Qiu, D., Luo, L., and Xiao, L. (2022). Distributed grover's algorithm. https://arxiv.org/abs/2204.10487.

Silva, V. (2018). *Practical Quantum Computing for Developers*. Apress L. P., 1st edition.

Sipser, M. (2007). *Introdução Á Teoria da Computação*. Thomson, 2nd edition.

Varmantchaonala, C. M., Fendji, J. L. K. E., Njafa, J. P. T., and Atemkeng, M. (2022). Quantum hybrid algorithm for solving sat problem. https://www.sciencedirect.com/science/article/abs/pii/S0952197623002427?via%3Dihub.

* Código fonte com a implementação do circuito, disponível para consumo público: https://github.com/gabrielms201/Quantum-Implementation-For-SAT-Problem-Solving