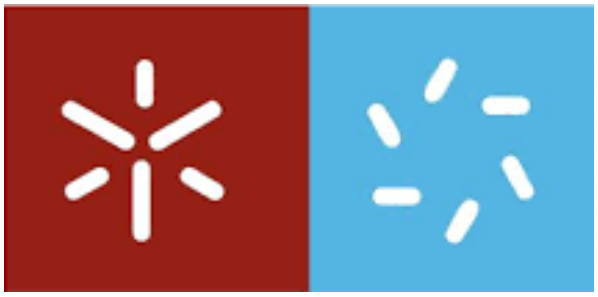

Computação Quântica
Projeto Final
LCC - 3º Ano - 2º Semestre

Nuno Machado - A68702

Diogo Aires - A91685

27 de março de 2023

Conteúdo

1 Introdução

No âmbito da unidade curricular de IC foi-nos proposto como trabalho prático o o estudo sobre o problema da satisfazibilidade utilizando o algoritmo de Grover. Iremos resolver 4 tarefas tendo em principal foco o problema 3-SAT. As 4 tarefas incidem sobre a resolução de um problema 3-SAT através de uma fórmula booleana satisfazível, a aplicação do Algortimo de Grover para a resolução desse problema e estudar a complexidade do algoritmo internamente ligado com o seu numero de iterações. Iremos abordar em cada capitulo cada tarefa resolvida.

2 Enuciado

2.1 Algoritmo de Grover

- Algoritmo quântico de pesquisa não estruturada que encontra com alta probabilidade a entrada exclusiva para uma função de caixa preta que produz um valor de saída específico. A aplicação canónica do algorítmo é o problema de pesquisa/procura num array.
- Para um array com N elementos, o algorítmo de Grover tem complexidade de $\mathcal{O}(\sqrt{N})$

2.2 Algoritmo de Grover - Oráculo

- Caixa negra, também considerada como função
- Pode encontrar variados inputs de uma função que produz um output particular. Se a caixa negra tiver r inputs, que produz um determinado output, a complexidade deste algoritmo é de $\mathcal{O}(\sqrt{N/r})$

2.3 Problema de Satisfação Booleana

- Um problema de satisfação booleana determina se uma fórmula booleana é satisfeita, ou seja, avalia-se como TRUE (Verdadeiro) dada uma atribuição específica das suas variáveis - se tal ocorrer, denomina-se a fórmula como satisfazível
- Se nenhuma atribuição desse tipo ocorrer, a função expressa pela fórmula é FALSE (Falsa) para todas as variações possíveis das variáveis, e, a fórmula diz-se insatisfazível.

3 Resumo

Temos como principal objetivo resolver o problema da satisfazibilidade. O problema consiste então em encontrar uma atribuição satisfazível para uma determinada fórmula booleana em FNC, onde cada clausula tem no máximo 3 váriáveis. São utilizados algoritmos pouco eficientes para resolvê-lo. Vamos utilizar o Algoritmo de Grover que atinge metade da eficiência sendo que os restantes têm valores mais baixos.

4 Fórmula Booleana 3-SAT

4.1 Exemplo dado

f(v1,v2,v3) = $(\neg v1 \vee v2 \vee v3) \wedge (v1 \vee v2 \vee v3) \wedge (v1 \vee v2 \vee v3) \wedge (v1 \vee v2 \vee v3) \wedge (v1 \vee v2 \vee v3)$

Aqui pode-se verificar que a formúla boleana apresentada pelo professor é uma FNC (Forma Normal Conjuntiva) pelo que podemos criar uma tabela de verdade de forma a encontrar os valores de verdade (0-Falso, 1-Verdadeiro) correspondentes v1,v2,v3 de forma a verificar se existe combinação com satisfaça a condição.
Tabela de verdade:

v1	v2	v3	$(\neg v1 \vee \neg v2 \vee \neg v3)$	$(v1 \vee \neg v2 \vee v3)$	$(v1 \vee v2 \vee \neg v3)$	$(v1 \vee \neg v2 \vee \neg v3)$	$(\neg v1 \vee v2 \vee v3)$	f
0	0	0	1	1	1	1	1	1
0	0	1	1	1	0	1	1	0
0	1	0	1	0	1	1	1	0
0	1	1	1	1	1	0	1	0
1	0	0	1	1	1	1	0	0
1	0	1	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1
1	1	1	0	1	1	1	1	0

Tabela 1: Tabela de verdade

Aqui se infere que temos 3 possiveis combinações como solução para a função booleana ser satisfazível tais como:

1. v1=0; v2=0; v3=0;
2. v1=1; v2=0; v3=1;
3. v1=1; v2=1; v3=0;

Daqui rapidamente se conclui que nessas combinações f é satisfazível.

5 Algoritmo de Grover

O algoritmo de Grover é um algoritmo de pesquisa quântica e pode ser utilizado para encontrar soluções para um problema de 3-SAT como falado acima.

5.1 Funcionamento do Algoritmo

5.1.1 Preparação do estado inicial

O algoritmo de Grover começa com um estado inicial composto por uma superposição uniforme de todos os estados possíveis. Para preparar esse estado, criamos um registo quântico com n qubits. Em seguida, aplicamos uma série de portas Hadamard a cada qubit, o que coloca todos os estados de igual probabilidade de ser encontrado como solução.

5.1.2 Oráculo

O oráculo identifica o estado que representa a solução procurada. O oráculo aplica uma marcação ao estado de solução, enquanto deixa os outros estados inalterados. Essa marcação é feita pela multiplicação por (-1) de forma a garantir a inversão do sinal desse estado.

5.1.3 Difusor

Depois de aplicar o oráculo, o algoritmo de Grover precisa aumentar a amplitude do estado de solução em relação aos outros estados, para que seja mais provável que a solução seja medida na saída do algoritmo. Isso é feito pelo difusor, que amplia a amplitude do estado de solução e reduz a amplitude dos outros estados. O difusor é construído a partir de duas etapas: primeiro, aplicamos novamente as portas Hadamard a cada qubit. De seguida, aplicamos o difusor, porque ela difunde as amplitudes dos estados, aumentando a amplitude do estado de solução em relação aos outros estados que a cada iteração do algoritmo a amplitude da solução vai aumentando em detrimento da amplitude dos demais estados encontrando assim a solução atribuindo uma maior probabilidade que aos outros.

5.2 Qualidade da Solução Obtida pelo Algoritmo de Grover

A qualidade da solução obtida pelo algoritmo de Grover depende do número de iterações e do número de cláusulas na fórmula. À medida que o número de cláusulas aumenta, a dificuldade de encontrar uma condição que satisfaça a equação booleana diminui sendo por vezes necessário aumentar o nº de iterações para que tal acontença. A probabilidade de sucesso do algoritmo de Grover é dada pela equação:

$P = sen^2((2k + 1)\theta/2)$, onde:

k = iterações;
θ = ângulo entreo estado inicial e o estado final da solução (amplitude);

Para um problema 3-SAT com n variáveis e m cláusulas, a probabilidade de sucesso

é proporcional a $\sqrt{m}$ e o número ideal de iterações é aproximadamente $\sqrt{m}/2$. Portanto, em um problema 3-SAT, a qualidade da solução obtida pelo algoritmo de Grover depende do número de cláusulas e do número de iterações utilizadas. No entanto, a probabilidade do Algoritmo de Grover encontrar uma solução ronda os 50 por cento, pelo que não é garantido que encontre solução, pelo menos nos casos mais complicados (com mais claúsulas). Ainda assim, o Algoritmo de Grover é o que oferece maior probabilidade face a outros algoritmos.

5.3 Complexidade do Algoritmo

O número ideal de iterações de Grover necessárias para chegar a uma solução para um problema 3-SAT com n variáveis e m cláusulas pode ser estimado usando a equação:

$\mathrm{k} = (\pi/4 * \sqrt{(}m/2^n))$,

como se pode verificar na implementação do algoritmo
Essa equação assume que o estado inicial é uma superposição uniforme de todas as possíveis atribuições de valores booleanos às variáveis, o que é obtido aplicando o portão de Hadamard a cada qubit. A complexidade do algoritmo de Grover para o problema 3-SAT é, portanto, proporcional ao número de iterações necessárias, que é aproximadamente $\sqrt{m}$. Como o número de cláusulas m cresce exponencialmente com o número de variáveis n, a complexidade do algoritmo é exponencial no pior caso. No entanto, na prática, o número ideal de iterações é geralmente muito menor do que a estimativa de pior caso, e o algoritmo pode encontrar uma atribuição satisfatória com alta probabilidade num pequeno número de iterações como se pode ver pela equação de iterações descrita acima. Em suma, o Algoritmo de Grover é bastante superior em termos de eficiência em comparação com outros algoritmos, como indicado acima, para o problema 3-SAT, mas o seu desempenho depende do nº de iterações que por consequência depende do nº de cláusulas aplicadas ao problema.

6 Dificuldades do Grupo

Tivemos alguma dificuldade em interpretar o que era pretendido com este trabalho. Em relação à 1ª tarefa não sabíamos se tínhamos de encontrar uma função booleana 3-SAT satisfazível e estudar sobre ela ou se tínhamos de testar a função fornecida em enunciado. Optamos por incidir sobre a fórmula dada. Aprendemos e estudamos o Algoritmo de Grover nas aulas tendo estas um enorme peso na implementação do algoritmo pedido.

7 Conclusão

O grupo espera ter cumprido com os requisitos necessários para ter uma boa aprovação pela equipa docente. Fomos capazes de trabalhar sobre as 4 tarefas ao longo dos capítulos deste relatório e, em suma, foi um projeto com grande aproveitamento para a aprendizagem do modelo quântico estudado nas aulas, com principal apreciação sobre o Algoritmo de Grover.