DSC/CEEI/UFCG

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática

DSC
Departamento de Sistemas e Computação

Av. Aprígio Veloso, 882 — Bodocongó
Caixa Postal 10.106
58.109-970 — Campina Grande — PB — Brasil
Fone: 3310-1122 — Fax: 310-1273
e_mail: dsc@dsc.ufcg.edu.br; http://www.dsc.ufcg.edu.br

Relatório Técnico

N° DSC/01/2011

BUSCA QUÂNTICA

Elloá B. Guedes
Francisco M. de Assis
Bernardo Lula Jr.

UFCG/CEEI/DSC/IQuanta
elloa@dsc.ufcg.edu.br

27 páginas

Janeiro de 2011

BUSCA QUÂNTICA

Elloá Barreto Guedes, Francisco Marcos de Assis, Bernardo Lula Jr.

Instituto de Estudos em Computação e Informação Quânticas (IQuanta)

Universidade Federal de Campina Grande

Centro de Engenharia Elétrica e Informática

{elloaguedes, fmarassis, bernardo.lulajr}@gmail.com

RESUMO

Este relatório técnico contempla uma apresentação detalhada do Algoritmo Quântico de Busca, o qual têm por objetivo a busca de determinados elementos em uma base de dados desordenada. Este algoritmo utiliza as leis da Mecânica Quântica e possui desempenho superior à sua contrapartida clássica. Além da descrição deste algoritmo, este relatório contempla uma investigação de recentes resultados e aplicações da busca quântica, incluindo um levantamento sobre implementações físicas do mesmo.

Palavras-Chave: Algoritmo Quântico de Busca, Computação Quântica.

ABSTRACT

This technical report presents a detailed description of the Quantum Search Algorithm. This algorithm aims to search for elements in an unsorted database with better performance than its classical counterpart. Such improvement is due to the use of the Quantum Mechanics laws. Besides the description of this algorithm, this technical report also presents an investigation of recent results and applications of the quantum search, including a survey of its physical implementations.

Keywords: Quantum Search Algorithm, Quantum Computing.

Sumário

1 DESCRIÇÃO

Este relatório técnico detalha o artigo "*A fast quantum mechanical algorithm for database search*" do autor Lov K. Grover [Gro96a] em seis etapas, descritas a seguir:

1. Identificação do problema: consiste na clara descrição do problema de pesquisa tratado pelo artigo. Esta descrição deve contemplar o contexto no qual a pesquisa é realizada, a motivação para a resolução do problema em questão;

2. Formalização do problema como um modelo: nesta etapa, a pergunta ou problema técnico do artigo deve ser expresso utilizando uma linguagem matemática. Normalmente, esta formalização está atrelada a escolha de uma técnica de modelagem para o problema. Esta etapa é dividida em duas sub-etapas:

   (a) Identificação e classificação de variáveis

      - Independentes e dependentes

   (b) Formulação matemática do problema

      - Requer achar relacionamentos entre variáveis
      - Requer desconsiderar certas variáveis
      - Requer fazer suposições simplificadoras

3. Solução do modelo: esta etapa diz respeito a solução do problema original por meio do modelo construído. Normalmente, a solução do modelo é feita de forma analítica, via simulação ou ainda por pesquisa da solução ótima em um espaço de busca;

4. Validação do modelo: nesta etapa verifica-se se o modelo (*i*) endereça o problema original, (*ii*) pode ser usado na prática, (*iii*) faz sentido quando testado com dados reais;

5. Empacotamento do modelo: nesta etapa deve ser verificado se o empacotamento do modelo como uma ferramenta possibilita a compreensão e utilização desta última;

6. Manutenção do modelo: diz respeito à extensões do modelo mediante algumas situações, tais como, modificação do problema original, alteração na importância de fatores, dentre outros.

Este relatório técnico é amplamente baseado no referido artigo de Grover. Portanto, ressaltamos aos leitores dois aspectos importantes: (i) ter o artigo de Grover em mãos auxilia a leitura deste relatório, pois é possível fazer um paralelo entre os elementos identificados e as seções do artigo; e (ii) alguns parágrafos deste relatório apresentam transcrições e traduções livres de trechos do artigo original de Grover. Este último ponto enfatiza novamente a necessidade de ter o artigo original em mãos para que o leitor possa mapear qual a autoria de determinados trechos (quando não referenciados). Reforçamos ainda que este relatório técnico é um *survey* sobre o algoritmo quântico de busca, que compila literatura existente sobre o assunto.

2 IDENTIFICAÇÃO DO PROBLEMA

A busca em uma base desordenada é o problema tratado pelo artigo "*A fast quantum mechanical algorithm for database search*".

Primeiramente, o autor faz uma breve descrição do contexto do problema e pontua como algoritmos clássicos o resolvem. Esta breve descrição baseia-se em um exemplo simples, de um catálogo de telefones que encontra-se desordenado, como mostrado a seguir:

> Suponha um catálogo de telefones contendo N nomes, os quais encontram-se dispostos sem qualquer ordenação. Para encontrar o telefone de alguém, com probabilidade $\frac{1}{2}$, um algoritmo clássico, quer determinístico ou probabilístico, precisa olhar, no mínimo, $\frac{N}{2}$ entradas no catálogo.

Com o exemplo do catálogo de telefones, o leitor é capaz de delinear uma classe de problemas análogos. Segundo Grover, estes problemas são tão típicos que ele próprio os descreve como "problemas mundanos no processamento da informação". A identificação do problema, de uma forma mais específica, é mostrada a seguir:

> O problema é descrito como segue: seja uma base de dados desordenada contendo N ítens, dos quais apenas único satisfaz uma dada condição – este elemento é o que deve ser retornado. Não existe quaisquer ordem ou padrão que possa auxiliar na identificação deste elemento.

O autor vai além da contextualização do problema, reportando problemas de busca na Ciência da Computação teórica. De acordo com o autor, estes problemas teóricos possuem uma pequena diferença em relação ao tipo de problema que é tratado no escopo deste trabalho: há alguma espécie de estrutura que auxilia na velocidade do algoritmo. Apesar desta diferença, há motivação teórico e prática para a resolução do problema, que é endereçado, finalmente, da seguinte forma:

> Quão rápida pode ser a resolução do problema de busca, assumindo a ausência de qualquer estrutura no problema?

Apesar de ser um problema típico, a forma que o autor se propõe a resolvê-lo é inovadora. A idéia de Grover é utilizar Computação Quântica, cujos sistemas podem estar em uma superposição de estados e, em virtude disto, são capazes de examinar múltiplos ítens da base de dados simultaneamente.

A identificação do problema, por fim, pode ser sintetizada em um problema de business e em um problema técnico:

- **Problema de business**: É preciso encontrar um elemento em uma base de dados desordenada. Não há qualquer ordenação ou padrão que possa auxiliar na busca deste elemento.

- **Problema técnico**: Construir um algoritmo quântico capaz de resolver o problema de busca em uma base de dados desordenada. Definir a complexidade de tempo deste algoritmo em função do tamanho da entrada.

3 FORMALIZAÇÃO DO PROBLEMA COMO UM MODELO

O modelo escolhido para a resolução do problema é o modelo de Algoritmos Quânticos. Portanto, o objetivo do trabalho em questão é definir um algoritmo que segue o paradigma computacional da Computação Quântica capaz de resolver o problema proposto.

Nas seções a seguir serão apresentadas a identificação e classificação da variáveis do escopo do problema na Seção 3.1 e a formulação matemática do mesmo na Seção 3.2. A seção 3.3, cujo texto é baseado na Seção 1.2 do artigo de Grover [Gro96a], dá uma visão geral do modelo utilizado pelo autor para resolver o problema em questão.

3.1 Identificação e Classificação das Variáveis

As variáveis do problema e a classificação associada encontram-se dispostos na Tabela 1. O número de variáveis é relativamente pequeno, mas permitem a completa representação dos elementos a serem considerados na definição do algoritmo.

Tabela 1: Variáveis do problema e suas respectivas classificações.

Variáveis	Classificação
$S_1, S_2, \ldots, S_N$ (base de dados)	Independente
N (tamanho da base de dados)	Dependente
S_v (solução do problema)	Dependente

O tamanho da base de dados é uma variável dependente, pois o desempenho do algoritmo em termos da complexidade de tempo é mostrado em função do tamanho da entrada. A solução do problema S_v também é uma variável dependente, pois é ela que é a saída do algoritmo que resolve o problema.

3.2 Formulação Matemática do Problema

A formalização do problema de acordo com o modelo é dada a seguir:

> Seja um sistema quântico com $N = 2^n$ estados, identificados por $S_1, S_2, \ldots, S_N$. Estes 2^n estados são representados como strings de 2^n bits. Seja um único estado, diga-se S_v, que satisfaz a condição $C(S_v) = 1$, e para todos os outros estados S, $C(S) = 0$ (assuma que para qualquer estado S, a condição $C(S)$ pode ser verificada em uma unidade de tempo). O problema é identificar o estado S_v.

Em suma, o objetivo do autor é a definição de um algoritmo quântico com as características mostradas na Tabela 2

Tabela 2: Especificação da entrada e saída do algoritmo que resolve problema.

Entrada:	$S_1, S_2, \ldots, S_N$
Saída:	S_v, tal que $C(S_v) = 1$

3.2.1 Suposições Simplificadoras

As suposições simplificadoras utilizadas pelo autor são resumidas a seguir:

- Há um oráculo C capaz de reconhecer uma solução do problema em uma unidade de tempo;
- Há uma única solução para o problema de busca, S_v tal que $C(S_v) = 1$;
- Não há qualquer ordenação na base de dados que possa auxiliar na resolução do problema;
- O tamanho da entrada é uma potência de 2 ($N = 2^n$);

3.3 Algoritmos Quânticos

Um bom ponto de partida para entender algoritmos quânticos é saber que estes algoritmos também são probabilísticos. Neste último tipo de algoritmos, ao invés do sistema computacional estar em um estado específico, há uma distribuição de vários estados que, com uma certa probabilidade, o sistema pode estar. A cada passo do algoritmo, há uma certa probabilidade de que a transição de um estado para outro ocorra. Conhecendo a distribuição inicial e a matriz de transição de estados, é possível, em princípio, calcular a distribuição de estados que o sistema pode estar em um dado instante de tempo.

Assim como os algoritmos probabilísticos, os algoritmos quânticos lidam com distribuições de probabilidade sobre diversos estados. Porém, diferentemente dos algoritmos probabilísticos, um vetor de probabilidade não descreve completamente o estado do sistema quântico. Em ordem de prover uma descrição completa deste tipo de sistemas, é necessária a noção de amplitude associada a cada estado, que é representada por um número complexo.

A evolução de sistemas quânticos é obtida pela pré-multiplicação do vetor de amplitudes pela matriz de transição, cujas entradas podem compostas de números complexos. As probabilidades associadas a cada estado são dadas pelo quadrado do valor absoluto da amplitude em que o estado se encontra. Para conservar as probabilidades, a matriz de transição de estados deve ser unitária.

O autor apresenta a evolução de sistemas quânticos em termos do produto de matrizes de estados e transições. Atualmente, a notação de Dirac [Dir82] é mais utilizada para esta representação, por acarretar em uma simplificação dos cálculos a serem realizados.

Para que o leitor possa compreender com mais detalhes a solução do modelo, a ser apresentada no próximo capítulo, sugere-se a leitura dos fundamentos da Computação Quântica. Tais conceitos podem ser encontrados no capítulo II da obra de Nielsen e Chuang [NC05], nos capítulos I e II da obra de Guedes e Lula Jr. [GL10], ou no capítulo III da obra de Kaye et al. [KLM07].

4 SOLUÇÃO DO MODELO

Nesta seção será apresentado o algoritmo quântico proposto por Grover capaz de resolver o problema apresentado. A Seção 4.1 ilustra os operadores utilizados; a Seção 4.2 descreve claramente quais os passos utilizados pelo algoritmo e analisa o número de iterações de Grover necessárias; a Seção 4.3 pontua as provas formais efetuadas pelo autor, caracterizando a verificação da corretude do algoritmo; a Seção 4.4 mostra uma interpretação geométrica do modelo proposto por Grover; a Seção 4.5 apresenta considerações do autor a respeito de implementações físicas do algoritmo proposto; a Seção 4.6 ilustra o custo assintótico e discute aspectos da optimalidade em relação aos algoritmos clássicos; e, finalmente, a Seção 4.7 possui um exemplo de busca quântica em uma base de dados desordenada com $N = 8$ elementos.

4.1 Ferramental para o Algoritmo

O ferramental para o algoritmo que resolve o problema proposto é composto por três operadores. O primeiro deles coloca o sistema quântico em uma superposição igualmente distribuída de estados, similar ao lançamento de uma moeda balanceada. Este operador é representado pela matriz M:

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1}$$

Quando aplicado ao estado $|0\rangle$, este operador resulta na superposição $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Quando aplicado ao $|1\rangle$, a magnitude das amplitudes associadas é a mesma, mas a fase do $|1\rangle$ é invertida, ou seja, a aplicação de M ao estado $|1\rangle$ resulta em $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Considerando a dimensão 2^n, cada estado pode ser descrito como uma string de n bits. O resultado de executar a transformação M em cada um destes estados é uma superposição com amplitudes igualmente distribuídas e iguais a $\frac{1}{\sqrt{2^n}}$ para cada um dos 2^n estados, porém alguns destes estados com fase positiva e outros com fase negativa.

A compreensão do sinal atribuído à fase é feita da seguinte forma, a partir da definição da matriz M. A fase muda quando um bit que era previamente 1 continua 1 após a realização da transformação. Se $\bar{i}$ é a string de n bits de entrada que descreve o estado e j é a string de n bits de saída, então o sinal da amplitude de $\bar{j}$ é o resultado da paridade do produto bit a bit de $\bar{i}$ e $\bar{j}$, isto é, $(-1)^{\bar{i}\cdot\bar{j}}$. Esta caracterização define o segundo operador usado no algoritmo, denominado transformação de Walsh-Hadamard. Em síntese, este operador é da forma:

$$W_{ij} = \frac{1}{\sqrt{2}}(-1)^{\bar{i}\cdot\bar{j}} \tag{2}$$

O terceiro operador a ser utilizado é a rotação seletiva da amplitude de determinados estados. A matriz da transformação para um sistema de quatro estados é da forma:

$$R = \begin{bmatrix} e^{i\cdot\phi_1} & 0 & 0 & 0 \\ 0 & e^{i\cdot\phi_2} & 0 & 0 \\ 0 & 0 & e^{i\cdot\phi_3} & 0 \\ 0 & 0 & 0 & e^{i\cdot\phi_4} \end{bmatrix} \tag{3}$$

em que i é a unidade imaginária ($i = \sqrt{-1}$), e ϕ_1, ϕ_2, ϕ_3 e ϕ_4 são números reais arbitrários.

4.2 Descrição do Algoritmo

Os passos do algoritmo que resolvem o problema são:

1. **Inicialização**: Inicializar o sistema com a seguinte distribuição $\left(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \ldots, \frac{1}{\sqrt{N}}\right)$. Isto é, com a mesma amplitude associada a cada estado do sistema;

2. **Iteração de Grover**: Repetir as seguintes operações unitárias $O(\sqrt{N})$ vezes:

   (a) **Inversão de fase**: Suponha que o sistema encontre-se em algum estado S:

   - Se $C(S) = 1$, efetue uma rotação na fase de π radianos;
   - Se $C(S) = 0$, mantenha o estado inalterado.

   (b) **Amplificação de amplitude**: Aplique a transformação de difusão D, cuja matriz é definida como segue:

$$D_{ij} = \frac{2}{N}, i \neq j \tag{4}$$

$$D_{ii} = -1 + \frac{2}{N} \tag{5}$$

3. **Medição**: Efetue uma medição no estado resultante. Se $C(S_v) = 1$, então a probabilidade do estado final estar em S_v é de, pelo menos, $\frac{1}{2}$.

A transformação D pode ser implementada como $D = WRW$, em que R é a matriz de rotação e W é o operador de Walsh-Hadamard apresentado na Seção 4.1. A matriz de R é definida como segue:

$$R_{ij} = \begin{cases} 0 & \text{se } i \neq j \\ 0 & \text{se } i \neq j \text{ e } i = 0 \\ -1 & \text{caso contrário} \end{cases}$$

O operador D pode ser representado como $D \equiv -\mathbb{I} + 2 \cdot P$, em que $\mathbb{I}$ é a matriz identidade e P é um projetor tal que:

$$P_{ij} = \frac{1}{N}, \forall i \ \ \forall j \tag{6}$$

Duas propriedades de P são verificadas: $P^2 = P$, e a atuação de P em um vetor $\bar{v}$ retorna um vetor em que cada componente é a média de todos os componentes.

O operador D pode ser compreendido como uma inversão sobre a média. Considerando a média de todos os componentes do vetor $\bar{v}$ igual a A, quando D atua em um vetor $\bar{v}$ resulta em:

$$\begin{aligned} D\bar{v} &= (-\mathbb{I} + 2 \cdot P)\bar{v} && (7) \\ &= -\bar{v} + 2 \cdot P \cdot \bar{v} && (8) \\ &= -v_i + 2 \cdot A && (9) \\ &= -v_i + A + A && (10) \\ &= (A + (A - v_i)) && (11) \end{aligned}$$

Este resultado é precisamente uma inversão sobre a média.

4.2.1 Número Requerido de Iterações

Na descrição do algoritmo, Grover afirma que o número k de iterações é $O(\sqrt{N})$. Porém, neste caso, um aspecto negativo do uso da notação assintótica é a omissão de uma constante de interesse para a determinação exata do valor de k. O melhor número de iterações de Grover é definido por meio da análise dos operadores como rotações e, como resultado, o valor k do número de iterações é dado por:

$$k = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rceil \tag{12}$$

em que N é o tamanho da base de dados e $\lfloor \cdot \rceil$ denota a função inteiro mais próximo [NC05].

4.3 Verificação do Modelo

A verificação do modelo é feita por meio de provas formais. Tais provas mostram que o algoritmo apresentado é válido, de acordo com o paradigma da Computação Quântica, e que há convergência para o estado desejado com probabilidade $\Omega(1)$. A seguir, as provas apresentadas no artigo de Grover são listadas:

- D é um operador unitário – Prova concluída no Parágrafo 5 da Seção 4;
- D pode ser denotado como $D = WRW$ – Teorema 1 da Seção 5;
- Há a marcação e amplificação da amplitude do elemento procurado – Teorema 2 e Corolários 2.1 e 2.2 da Seção 5;
- São necessárias $O(\sqrt{N})$ iterações para que a amplitude do elemento procurado seja retornada com probabilidade próxima de 1 – Apresentado no Teorema 3 da Seção 4, mas provado na Seção 5.

4.4 Interpretação Geométrica

Em seu artigo, Grover apresenta uma interpretação geométrica para a inversão de fase realizada pelo seu algoritmo. Aqui nesta seção, será apresentada uma interpretação geométrica, baseada na versão apresentada por Grover, porém considerando todos os passos do algoritmo. A interpretação a ser apresentada é baseada na Seção 8.1 da obra de Kaye et al. [KLM07].

Inicialmente, o sistema encontra-se em uma superposição igualmente distribuída de estados, como mostrado na Figura 1. Um destes estados, denotado como $|w\rangle$, é a solução do problema de busca. Há a ênfase na figura que a média das amplitudes é a mesma.

Após a realização da inversão de fase, o único elemento que tem sua fase rotacionada de π radianos é o elemento $|w\rangle$, uma vez que $C(|w\rangle) = 1$, como ilustrado na Figura 2.

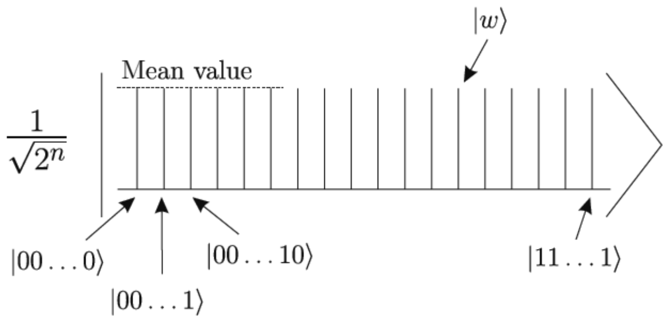

Figura 1: Estado inicial do sistema.

Como a fase de $|w\rangle$ tornou-se negativa, a amplitude dos demais elementos foi aumentada para respeitar a condição de unitariedade.

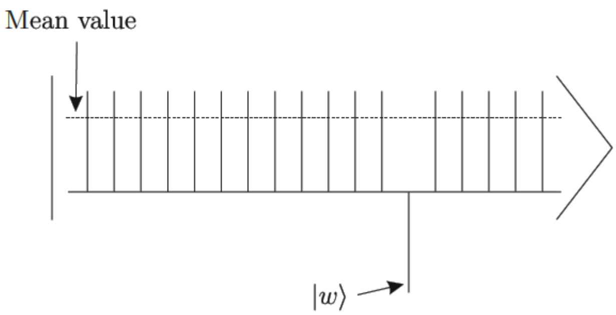

Figura 2: Estado do sistema após a inversão de fase.

Por fim, a amplificação de amplitude é realizada. Nesta etapa, a fase de $|w\rangle$ é re-invertida e a média das amplitudes dos demais elementos é decrescida. Sendo a amplitude inicial de $|w\rangle$ igual a $\frac{1}{\sqrt{N}}$, com esta etapa passa a ser igual a aproximadamente $\frac{2}{\sqrt{N}}$. A amplificação de amplitude é ilustrada na Figura 3.

A interpretação geométrica apresentada ilustra uma única iteração do algoritmo de Grover. Esta interpretação facilita a compreensão do algoritmo, pois introduz recursos visuais que caracterizam as operações realizadas em cada etapa.

4.5 Aspectos de Implementação

O autor pontua que este algoritmo quântico é mais fácil de implementar que outros algoritmos que seguem o mesmo paradigma. Considerações que dão suporte a esta afirmação são:

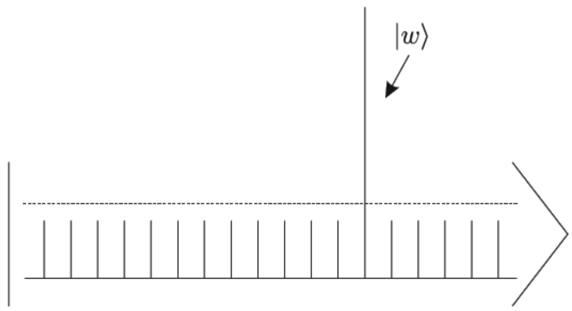

Figura 3: Estado do sistema após a amplificação de amplitude.

1. A transformação de Walsh-Hamamard e o deslocamento condicional de fase são relativamente simples de implementar quando comparadas à outras operações de diversos algoritmos quânticos;

2. Algoritmos que utilizam a transformação de Walsh-Hadamard são mais simples de implementar do que aqueles que utilizam Transformada de Fourier;

3. O deslocamento condicional de fase seria mais fácil de implementar se o algoritmo fosse utilizado de tal modo que a função em cada ponto fosse computada, ao invés de ser recuperada da memória;

4. Se os elementos fossem recuperados de uma tabela, em princípio, seria possível armazená-los em uma memória clássica, mas não descartando o restante do operacional quântico.

4.6 Análise de Complexidade

O melhor algoritmo clássico, seja determinístico ou probabilístico, que efetua a busca em uma base desordenada de dados e retorna o elemento procurado com 100% de certeza possui complexidade $O(N)$, em que N é o tamanho da base de dados. O algoritmo de Grover efetua esta mesma busca com custo $O(\sqrt{N})$. Portanto, comparado ao melhor algoritmo clássico, o algoritmo de Grover possui um ganho quadrático.

Como proposto por Zalka, há uma prova de optimalidade do algoritmo de Grover em relação à todas as soluções clássicas possíveis [Zal99]. Este é um dos casos em que a Computação Quântica é provadamente superior à Computação Clássica. Para outros algoritmos, não é possível fazer tal afirmação, por não se conhecer o melhor algoritmo clássico capaz de resolver o problema, embora a solução quântica para o problema seja eficiente.

4.7 Exemplo

Para ilustrar a execução do algoritmo quântico apresentado, suponha que se deseje procurar um elemento em uma base de dados desordenada contendo 8 ítens. O elemento que se deseja encontrar é $S_4 = 4$. Neste caso, o número de iterações de Grover necessárias é $k = \left\lfloor \frac{\pi}{4}\sqrt{8} \right\rceil = 2$. No exemplo a seguir, será utilizada a notação de Dirac, amplamente aceita por simplificar os cálculos a serem realizados.

Para representar esta base de dados quânticamente, são necessários 3 qubits no primeiro registrador e um qubit auxiliar. Os qubits do primeiro registrador devem ser inicializados com $|0\rangle$:

$$|\varphi_0\rangle = |0\rangle^{\otimes^3} \tag{13}$$

O próximo passo consiste em colocar a entrada em uma superposição igualmente distribuída de estados. Para tanto, será utilizado o operador M:

$$\begin{aligned} |\varphi_1\rangle &= M^{\otimes 3} |0\rangle^{\otimes^3} && (14)\\ &= \left(\frac{1}{\sqrt{8}} \sum_{i=0}^{8-1} |i\rangle \right) && (15)\\ &= \frac{1}{\sqrt{8}} \sum_{i=0}^{8-1} |i\rangle && (16)\\ &= \frac{1}{\sqrt{8}} \sum_{i=0}^{8-1} (|0\rangle + |1\rangle + \ldots + |6\rangle + |7\rangle) && (17) \end{aligned}$$

Para identificar o elemento procurado, é necessário iniciar as iterações de Grover, descritas por:

$$G = (2\,|\varphi_1\rangle \langle\varphi_1| - \mathbb{I}) \otimes U_f \tag{18}$$

em que U_f é o oráculo responsável pela inversão de fase e $2\,|\varphi_1\rangle \langle\varphi_1| - I$ é um operador análogo à transformação de difusão D sugerida pelo autor.

A primeira iteração de Grover, atua da seguinte forma:

$$
\begin{aligned}
|\varphi_2\rangle &= G\,|\varphi_1\rangle && (19)\\
&= [(2\,|\varphi_1\rangle\langle\varphi_1| - \mathbb{I})\otimes U_f]\,|\varphi_1\rangle && (20)\\
&= [(2\,|\varphi_1\rangle\langle\varphi_1| - \mathbb{I})\otimes U_f]\left(\frac{1}{\sqrt{8}}\sum_{i=0}^{8-1}|i\rangle\right) && (21)\\
&= (2\,|\varphi_1\rangle\langle\varphi_1| - \mathbb{I})\left(\frac{1}{\sqrt{8}}\sum_{i=0}^{8-1}U_f\,|i\rangle\right) && (22)\\
&= (2\,|\varphi_1\rangle\langle\varphi_1| - \mathbb{I})\left(\frac{|0\rangle+|1\rangle+|2\rangle+|3\rangle-|4\rangle+|5\rangle+|6\rangle+|7\rangle}{\sqrt{8}}\right) && (23)\\
&= \left[\frac{1}{2\sqrt{8}}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|5\rangle+|6\rangle+|7\rangle\right)\right]+\frac{5}{2\sqrt{8}}\,|4\rangle && (24)
\end{aligned}
$$

Neste ponto, a probabilidade p de encontrar o elemento procurado é $p = \left|\frac{5}{2\sqrt{8}}\right|^2 \cong 78,12\%$, que é um número relativamente alto. Porém, o algoritmo continua com a segunda iteração de Grover:

$$
\begin{aligned}
|\varphi_3\rangle &= G\,|\varphi_2\rangle && (25)\\
&= [(2\,|\varphi_1\rangle\langle\varphi_1| - \mathbb{I})\otimes U_f]\,|\varphi_2\rangle && (26)\\
&= [(2\,|\varphi_1\rangle\langle\varphi_1| - \mathbb{I})\,U_f]\,\cdot && (27)\\
&\cdot \left\{\left[\frac{1}{2\sqrt{8}}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|5\rangle+|6\rangle+|7\rangle\right)\right]+\frac{5}{2\sqrt{8}}\,|4\rangle\right\} && (28)\\
&= [(2\,|\varphi_1\rangle\langle\varphi_1| - \mathbb{I})]\left\{\left[\frac{1}{2\sqrt{8}}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|5\rangle+|6\rangle+|7\rangle\right)\right]-\frac{5}{2\sqrt{8}}\,|4\rangle\right\} && (29)\\
&= \left[\left(-\frac{|0\rangle+|1\rangle+|2\rangle+|3\rangle+|5\rangle+|6\rangle+|7\rangle}{4\sqrt{8}}\right)+\frac{11}{4\sqrt{8}}\,|4\rangle\right] && (30)
\end{aligned}
$$

Após a segunda iteração de Grover, uma medição é realizada. Como resultado da mesma, têm-se que a probabilidade de encontrar $S_4 = |4\rangle$ como resultado é igual a:

$$\left|\frac{11}{4\sqrt{8}}\right|^2 \cong 0,9453 \qquad (31)$$

Com isto, ao verificar o resultado da saída dos medidores ao final do circuito, tem-se o resultado da execução do algoritmo de Grover. É interessante observar que não há ordenação na lista de entrada e que, ainda assim, o algoritmo retorna o elemento procurado com probabilidade próxima de 100%, como esperado.

5 VALIDAÇÃO DO MODELO

Como é característico em trabalhos teóricos, não é apresentada uma seção a respeito da validação do modelo no artigo de Grover. Esta seção é freqüentemente omitida em trabalhos desta natureza, pois o apelo por provas formais é maior, visto que mostram que o trabalho proposto é correto matematicamente.

Nesta seção, a validação do modelo será feita com o auxílio de outras referências na literatura. Tais referências mostram a aplicação do algoritmo de Grover em diversos problemas de busca em domínios distintos. Estes trabalhos reforçam a evidência de que o algoritmo de Grover endereça o problema original. A análise de sensibilidade do algoritmo de Grover será discutida em termos do número de iterações necessárias e será mostrada na seção a seguir.

5.1 Análise de Sensibilidade

A sensibilidade do algoritmo de Grover está intimamente ligada ao número de iterações de Grover necessárias. Em seu artigo, Grover estabelece que este número é limitado por $O(\sqrt{N})$, em que N é a quantidade de elementos na base de dados. Ao utilizar um número de iterações inadequado, a amplitude do elemento marcado não será máxima, ainda que sejam utilizadas mais iterações de Grover que o ideal. Este número de iterações k de Grover a serem utilizadas é apresentado e discutido na Seção 4.2.1.

Para exemplificar o número de iterações adequado, suponha que o algoritmo de Grover deva ser executado em uma base de dados com 8 elementos, em que apenas um deles, diga-se o quarto elemento, satisfaz a $C(S_4) = 1$. A O número de iterações k para este caso é 2. A Figura 4 mostra a amplitude do estado S_4 para diferentes números de iterações. É possível perceber que há maior probabilidade de S_4 ser retornado ao efetuar uma medição quando se realizam 2, 7 e 13 iterações. Porém, considerando os custos de se realizar uma iteração, o melhor destes resultados é o que coincide com k, pois alcança maior probabilidade com menos iterações.

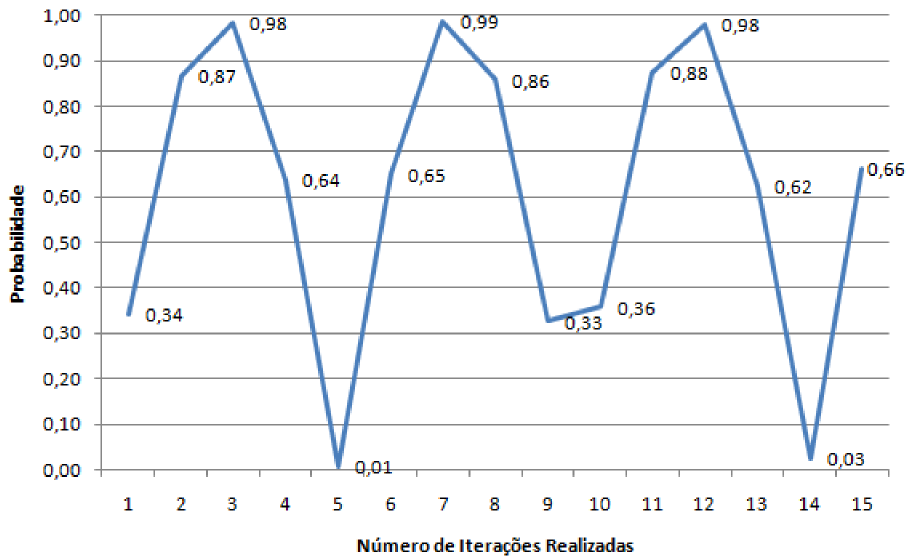

Figura 4: Probabilidade de encontrar a solução de um problema de busca em uma base de dados desordenada com 8 elementos versus número de iterações de Grover utilizadas.

5.2 Aplicações do Algoritmo de Grover

Aplicações do algoritmo de Grover na resolução de diversos problemas reforçam a evidência de que este algoritmo endereça o problema original. Nas subseções a seguir, há a descrição e referências bibliográficas para cinco problemas de áreas distintas em que o algoritmo de Grover é utilizado com sucesso.

5.2.1 Cálculo da Mediana

Problemas de ordem estatística envolvem o processamento de grandes quantidades de dados. O uso de algoritmos quânticos pode tornar este processamento mais rápido. Grover [Gro96b] propôs um algoritmo, baseado no algoritmo de Grover, capaz de retornar a mediana de um conjunto de dados desordenados. Este algoritmo localiza o elemento central da distribuição e amplifica a sua amplitude, iterando este processo um determinado número de vezes. Assim, ao realizar uma medição, há uma alta probabilidade do valor da mediana ser encontrado como resposta. Há uma precisão ε associada ao processo de retornar a mediana.

5.2.2 Algoritmos Genéticos

Algoritmos Genéticos compõem uma técnica amplamente utilizada em problemas de otimização. Um dos procedimentos demandados pela arquitetura de algoritmos genéticos diz respeito à busca pelo melhor elemento, de acordo com dadas condições, dentre a população total de elementos. Udrescu et al. [UPV06] propuseram uma arquitetura de algoritmos genéticos que faz uso de elementos da Computação Quântica. De acordo com esta arquitetura, a busca do melhor elemento é implementada por um oráculo de propósito específico, reduzindo o problema de encontrar o melhor elemento à uma busca com o algoritmo de Grover.

5.2.3 Busca de Menor Caminho em Roteamento

Para encontrar o menor caminho entre dois pontos em uma rede de computadores, diversos algoritmos clássicos vêm sendo utilizados, em especial o algoritmo de Djikstra. O trabalho de Aghaei et al. mostra a utilização de um oráculo quântico em substituição ao algoritmo de Djikstra para obtenção deste menor caminho dada uma árvore de cobertura mínima contendo os nós da rede. Para tanto, os autores propõem um algoritmo híbrido quântico-clássico e utilizam simulações para avaliar o algoritmo proposto. Os resultados mostram que a solução híbrida possui um ganho significativo em relação a sua contrapartida puramente clássica [AZMZ09].

5.2.4 Contagem Quântica

A contagem quântica é um algoritmo para determinar o número de soluções para um problema de busca em uma base desordenada. Este algoritmo foi proposto por Brassard et al. [BHT98], os quais sugerem a utilização da contagem quântica em conjunto com o algoritmo de Grover, pois ao determinar o número de solução presentes na base de dados, é possível determinar com maior precisão o número de iterações de Grover necessárias para realizar a busca na base de dados desordenada com maior probabilidade de sucesso.

5.2.5 Compartilhamento de Segredo

Compartilhamento de segredo é uma técnica para troca segura de informações em que a mensagem secreta é dividida entre diferentes usuários. Apenas quando se junta todas as partes remetidas aos diferentes usuários é que se torna possível a recuperação do segredo original. Chamoli e Bhandari definem um protocolo para compartilhamento de segredo no qual quatro ou mais qubits são enviados a cada participante da comunicação, porém alguns destes qubits possuem a fase invertida, denotando qual a informação de interesse. Ao receberem os qubits, cada participante deve executar uma amplificação de amplitude, para aumentar a probabilidade do segredo ser retornado após uma medição. Estes esquema dá suporte ao compartilhamento de segredo entre três participantes e protege contra alguns tipos de ataque [CB07].

6 EMPACOTAMENTO DO MODELO

Apesar não fazer empacotamento do algoritmo no artigo original, Grover faz considerações sobre aspectos de implementação do mesmo, previamente mencionadas na Seção 4.5. deste trabalho. Apesar desta lacuna no trabalho original, existem diversas formas de fazer empacotamento do algoritmo de Grover.

A primeira maneira, diz respeito ao empacotamento com circuitos quânticos, um modelo de computação provadamente análogo à Máquina de Turing Quântica, porém com uma representação visual que auxilia na compreensão da seqüência de passos do algoritmo. Um circuito quântico que implementa o algoritmo de Grover é mostrado na Figura 5. O detalhamento de uma iteração de Grover é mostrado na Figura 6. A definição detalhada das portas e o acompanhamento do passo-a-passo deste circuito podem ser encontrados no livro de Portugal et al. [PLCM04].

Além desta forma de empacotamento, é possível definir implementações físicas que permitem diversos testes e utilizações práticas deste algoritmo. O empacotamento do algoritmo de Grover segundo diversas tecnologias é sintetizado a seguir:

1. **Óptica Clássica de Fourier**. Bhattacharya et al. mostram que ondas clássicas podem implementar uma busca em uma base de dados desordenada com o

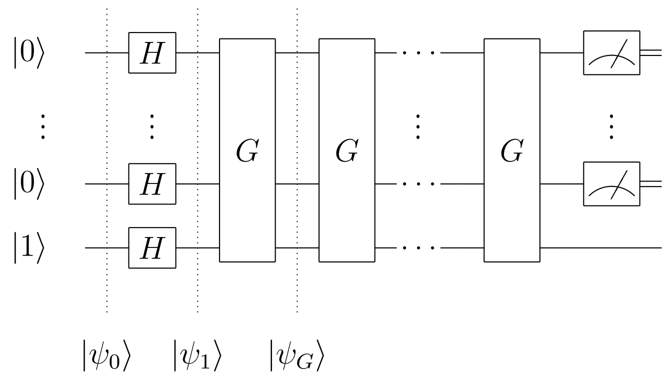

Figura 5: Circuito quântico que implementa o algoritmo de Grover

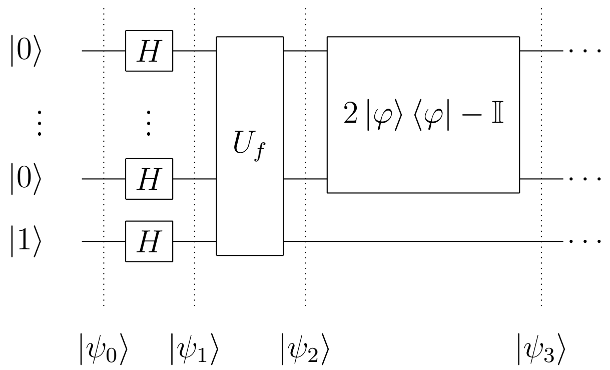

Figura 6: Circuito que ilustra em detalhes as portas que compõem a primeira iteração de Grover.

algoritmo de Grover de forma tão eficiente quanto a Mecânica Quântica. Porém, deixam claro que este tipo de sistema não é capaz de simular um Computador Quântico Universal [BvLvdHS02];

2. **Armadilha de íons**. Brickman et al. mostram uma implementação de um algoritmo quântico em um sistema escalar de armadilha de íons. Os resultados mostram que, para um sistema de dois qubits com uma única iteração de Grover, a probabilidade de sucesso é de 60%, melhor desempenho que o algoritmo clássico equivalente, que tem probabilidade de sucesso de 50% sob iguais condições [BHL+05];

3. **Ressonância Nuclear Magnética**. Dois trabalhos investigados utilizam esta técnica. O primeiro deles utiliza moléculas de clorofórmio para efetuar a busca quântica em um sistema de quatro qubits [CGK98]. O outro artigo mostra experimentos em um sistema de 2-qubits e considera o impacto de algumas alterações

práticas na realização de determinadas operações [LHYT+01].

4. **Spins em semicondutores**. Leuenberger e Loss apresentam uma implementação de Grover que utiliza spins nucleares em semicondutores. Além disto, apresentam um framework para as rotações necessárias e comparam a qualidade na implementação destas rotações com a aproximação para a solução desejada [LL03].

O empacotamento do algoritmo de Grover segundo diversas tecnologias mostra que além de correto, o algoritmo é fisicamente realizável. Atualmente, implementações com um número significativo de qubits ainda são instrumento de estudos experimentais, pois envolve o controle de muitas partículas no nível quântico.

7 MANUTENÇÃO DO MODELO

A manutenção do algoritmo quântico de busca em uma base desordenada é apresentada considerando extensões propostas por Grover e outros autores.

Uma primeira extensão a se considerar diz respeito ao caso de múltiplas soluções. O trabalho de Chen et al. [CFLS75] apresenta uma modificação no algoritmo de Grover tornando-o capaz de marcar e amplificar a amplitude de mais de um elemento da base de dados que satisfaz a condição C.

Uma outra modificação diz respeito à inicialização do algoritmo original, o qual solicita a criação de uma superposição igualmente distribuída de estados. Biham et al. propuseram uma modificação capaz de executar o algoritmo de Grover em qualquer distribuição inicial de amplitudes de estados. Os autores analisam esta modificação e afirmam que a evolução do sistema no tempo pode ser descrita utilizando equações diferenciais lineares de primeira ordem. Os resultados apresentados por estes mostram que o algoritmo de Grover pode tolerar uma certa quantidade de ruído no procedimento de inicialização da amplitude [BBB+99].

Grover propõe uma modificação no algoritmo, tornado a busca adequada para qualquer transformação além da de Walsh-Hadamard. O principal resultado desta modificação é no escopo de implementações do algoritmo, pois, uma vez que qualquer transformação quântica pode ser utilizada, o algoritmo pode se adaptar aos recursos tecnológicos disponíveis [Gro98].

Uma modificação no problema original diz respeito ao conhecimento de uma informação parcial L. Park et al. mostraram que há um ganho de $O(\sqrt{\frac{N}{L}})$ versus $O(\sqrt{N})$, quando esta informação parcial não é utilizada. Os autores utilizaram a transformação de wavelets de Haar no algoritmo de Grover para incorporar a informação parcial à busca quântica [PBK07].

Por fim, para ilustrar outra manutenção possível no modelo original, Rudolph e Grover mostram como utilizar o algoritmo de busca quântica para encontrar determinados elementos em uma base de dados clássica, cujos dados não apresentam propriedades da Mecânica Quântica [RG02].

8 CONSIDERAÇÕES FINAIS

Nas seções anteriores, o artigo de Grover "*A fast quantum mechanical algorithm for database search*" foi re-escrito no formato de seis etapas. Em algumas delas, porém, foram utilizadas outras referências da literatura para complementar as informações requeridas.

Foi visto que este algoritmo, amplamente conhecido como Algoritmo de Grover, é capaz de encontrar um elemento desejado numa base de dados desordenadas com N elementos, com custo menor que o melhor algoritmo clássico equivalente. Diversos aspectos da solução proposta por Grover foram discutidos. O algoritmo quântico de busca proposto é atualmente um dos resultados mais relevantes da Computação Quântica, assim como o algoritmo de Shor [Sho97].

Em relação ao artigo, aspectos que poderiam melhorá-lo consistem na utilização da notação de Dirac, existência de exemplos, e uma interpretação geométrica melhor ilustrada, compreendendo todos os passos do algoritmo e não apenas a amplificação de amplitude. Em relação aos aspectos de formalização, a notação e o modelo utilizados por Grover são adequados e consistentes durante todo o artigo. Não é possível dizer que a notação utilizada é simples, pois contempla diversos elementos necessários para a proposição de um algoritmo quântico e é utilizada ao longo de todas as provas formais efetuadas.

REFERÊNCIAS BIBLIOGRÁFICAS

[AZMZ09] Mohammad Reza Soltan Aghaei, Zuriati Ahmad Zukarnain, Ali Mamat, and Hishamuddin Zainuddin, *A hybrid algorithm for finding shortest path in network routing*, Journal of Theoretical and Applied Information Technology **5** (2009), 360–365.

[BBB+99] Eli Biham, Ofer Biham, David Biron, Markus Grassl, and Daniel A. Lidar, *Grover's quantum search algorithm for an arbitrary initial amplitude distribution*, Physical Review A **60** (1999), no. 4, 2742–2745.

[BHL+05] K.-A. Brickman, P. C. Haljan, P. J. Lee, M. Acton, L. Deslauriers, and C. Monroe, *Implementation of grover's quantum search algorithm in a scalable system*, Physical Review A **050306** (2005), 1–4.

[BHT98] Gilles Brassard, Peter Hoyer, and Alain Tapp., *Quantum counting*, Lecture Notes in Computer Science **1443** (1998), 820–831.

[BvLvdHS02] N. Bhattacharya, H. B. van Linden van den Heuvell, and R. J. C. Spreeuw, *Implementation of quantum search algorithm using classical fourier optics*, Physical Rev Iew Letters **88(13)** (2002), 137901.1–137901.4.

[CB07] Arti Chamoli and C. M. Bhandari, *Grover's algorithm based multi-qubit secret sharing scheme*, 2007, Disponível em http://arxiv.org/abs/0707.1042.

[CFLS75] Goong Chen, Stephen A. Fulling, Hwang Lee, and Marlan O. Scully, *Grover's algorithm for multiobject search in quantum computing*, Lecture Notes in Physics **561/2001** (165-175), 165–175.

[CGK98] Isaac L. Chuang, Neil Gershenfeld, and Mark Kubinec, *Experimental implementation of fast quantum searching*, Physical Review Letters **80** (1998), no. 15, 3408–3411.

[Dir82] Paul Dirac, *The principles of Quantum Mechanics*, 4th ed., Oxford UK, 1982, ISBN 0198520115.

[GL10] Elloá B. Guedes and Bernardo Lula Jr., *Autômatos finitos – com uma introdução aos Autômatos Finitos Quânticos*, Editora da Universidade Federal de Campina Grande, 2010.

[Gro96a] Lov K. Grover, *A fast quantum mechanical algorithm for database search*, 28th annual ACM symposium on Theory of computing, 1996.

[Gro96b] ———, *A fast quantum mechanical algorithm for estimating the median*, Bell Labs Technical Memorandum ITD-96-30115J, Bell Labs, 1996, Disponível em http://arxiv.org/abs/quant-ph/9607024.

[Gro98] ———, *Quantum computers can search rapidly by using almost any transformation*, Physical Review Letters **80** (1998), no. 19, 4329–4332.

[KLM07] Phillp Kaye, Raymond Laflamme, and Michele Mosca, *An introduction to quantum computing*, Oxford University, 2007.

[LHYT+01] L. Long, and Y.S. Li H.Y. Yana, C..C. Tua, J. X. Taoa, H.M. Chena, M.L. Liu, X. Zhange, J. Luoe, L. Xiao, and X.Z. Zenge, *Experimental NMR realization of a generalized quantum search algorithm*, Physics Letters A **286** (2001), 121–126.

[LL03] Michael N. Leuenberger and Daniel Loss, *Grover algorithm for large nuclear spins in semiconductors*, Physical Review B **68** (2003), 165317–1–165317–11.

[NC05] Michael A. Nielsen and Isaac L. Chuang, *Computação quântica e informação quântica*, Bookman, 2005.

[PBK07] Sangwoong Park, Joonwoo Bae, and Younghun Kwon, *Wavelet quantum search algorithm with partial information*, Elsevier – Chaos, Solitons and Fractals **32** (2007), 1371–1374.

[PLCM04] Renato Portugal, Carlile Campos Lavor, Luiz Mariano Carvalho, and Nelson Maculan, *Uma introdução à computação quântica*, Sociedade Brasileira de Matemática Aplicada e Computacional, 2004.

[RG02] Terry Rudolph and Lov K. Grover, *Quantum searching a classical database (or how we learned to stop worrying and love the bomb)*, 2002, Disponível em http://arxiv.org/abs/quant-ph/0206066.

[Sho97] Peter Shor, *Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing **26** (1997), 1484–1509.

[UPV06] Mihai Udrescu, Lucian Prodan, and Mircea Vlăduţiu, *Implementing quantum genetic algorithms: a solution based on grover's algorithm*, CF '06: Proceedings of the 3rd conference on Computing frontiers (New York, NY, USA), ACM, 2006, pp. 71–82.

[Zal99] Christof Zalka, *Grover's quantum searching algorithm is optimal*, Physical Review A **60** (1999), 2746–2751.