



UNIVERSIDADE ESTADUAL DE CAMPINAS  
UNICAMP

DISSERTAÇÃO DE MESTRADO

---

ÁLGEBRA GEOMÉTRICA E O ALGORITMO DE  
GROVER

---

*Autor:*

Rafael Santos de Oliveira  
Alves

*e-mail:*

rsantos@ime.unicamp.br

*Orientador:*

Prof. Dr. Carlile Lavor

*e-mail:*

clavor@ime.unicamp.br

29 de Julho de 2008

# ÁLGEBRA GEOMÉTRICA E O ALGORITMO DE GROVER.

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Rafael Santos de Oliveira Alves** e aprovada pela comissão julgadora.

Campinas, 29 de Julho de 2008.

  
Prof. Dr. Carlile Campos Lavor

Banca Examinadora:

1. Prof. Dr. Carlile Campos Lavor.
2. Prof. Dr. Ricardo Antonio Mosna.
3. Prof. Dr. Reginaldo Palazzo Júnior.
4. Prof. Dr. Nelson Maculan Filho.

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em **Matemática Aplicada**.

**FICHA CATALOGRÁFICA ELABORADA PELA  
BIBLIOTECA DO IMECC DA UNICAMP  
Bibliotecária: Maria Júlia Milani Rodrigues**

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AL87a | <p>Alves, Rafael Santos de Oliveira</p> <p>Álgebra Geométrica e o Algoritmo de Grover / Rafael Santos de Oliveira Alves – Campinas, [S.P.: s.n.], 2008.</p> <p style="text-align: center;">Orientador : Carlile Campos Lavor</p> <p style="text-align: center;">Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.</p> <p style="text-align: center;">1. Álgebra geométrica. 2. Algoritmo de Grover. 3. Computação quântica. 4. Clifford, Álgebra de. I. Lavor, Carlile Campos. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.</p> |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Título em inglês: Geometric Algebra and the Grover's Algorithm.

Palavras-chave em inglês (Keywords): 1. Geometric algebra. 2. Grover's algorithm. 3. Quantum computing. 4. Clifford algebras.

Área de concentração: Computação Quântica/Álgebra Geométrica

Titulação: Mestre em Matemática Aplicada

Banca examinadora:

Prof. Dr. Carlile Campos Lavor (IMECC-UNICAMP)  
Prof. Dr. Ricardo Antonio Mosna (IMECC-UNICAMP)  
Prof. Dr. Reginaldo Palazzo Júnior (FEEC-UNICAMP)  
Prof. Dr. Nelson Maculan Filho (COPPE-UFRJ)

Data da defesa: 29-07-2008

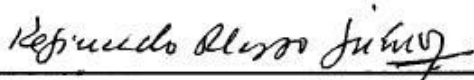
Programa de pós-graduação: Mestrado em Matemática Aplicada

**Dissertação de Mestrado defendida em 29 de julho de 2008 e aprovada**

**Pela Banca Examinadora composta pelos Profs. Drs.**

  
Prof. (a). Dr (a). CARLILE CAMPOS LAVOR

  
Prof. (a). Dr (a). RICARDO ANTONIO MOSNA

  
Prof. (a). Dr (a). REGINALDO PALAZZO JÚNIOR

  
Prof. (a). Dr (a). NELSON MACULAN FILHO

## Dedicatória

*A meus pais.*

*E especialmente a meu  
primo Marcelo (in  
Memorian), que nos  
deixou no último ano, mas  
que sempre fará parte de  
nossas vidas.*

*A meus tios, José  
Fernando e Sueli e a  
minha prima Priscila.*

# Agradecimentos

Agradeço ao Prof. Carlile pela proposta do tema, que me proporcionou estudar sobre duas áreas que eu não conhecia, e por acreditar no trabalho e me incentivar quando mais foi necessário.

Agradeço a meus pais, Rui e Guida, que tornaram possível este trabalho, meu avô Fernando, meus padrinhos, Jaime e Márcia, pelo apoio durante todo o período. E agradeço meus irmãos, Nelson e Eduardo, que, mesmo mais velhos, agora terão que me chamar de Mestre.

Agradeço a todos os meus amigos, pela companhia nos momentos de descontração.

Agradeço especialmente à Mariana Sacrini, por toda dedicação e paciência em todos os momentos, e pelo seu computador, que foi fundamental na edição deste trabalho!

Agradeço também aos funcionários do IMECC, que sempre foram muito eficientes e atenciosos comigo.

Campinas,  
29 de julho de 2008.

Rafael Santos de Oliveira Alves

# Abstract

Grover's algorithm is a quantum algorithm for searching in unstructured databases. Due to the properties of quantum mechanics, it provides a quadratic speedup over their classical counterparts. Using the Geometric Algebra, we present a new way to understand and simplify the operators of Grover's algorithm.

# Resumo

O Algoritmo de Grover é um algoritmo quântico de busca em um conjunto desordenado. Com o uso de propriedades da mecânica quântica, ele apresenta um ganho quadrático em relação a um algoritmo clássico. Neste trabalho, apresentamos uma outra visão deste algoritmo, através da Álgebra Geométrica, motivados pela interpretação geométrica dos operadores, e verificamos que é possível escrevê-lo com uma nova linguagem, e ainda apresentar uma expressão mais simples para o operador de Grover ( $G$ ) além de expressões gerais para estados resultantes de aplicações sucessivas deste operador.



# Sumário

|                                                    |           |
|----------------------------------------------------|-----------|
| Dedicatória                                        | iv        |
| Agradecimentos                                     | v         |
| Abstract                                           | vi        |
| Resumo                                             | vii       |
| <b>1 Introdução</b>                                | <b>1</b>  |
| <b>2 Algoritmo de Grover</b>                       | <b>4</b>  |
| 2.1 Introdução . . . . .                           | 4         |
| 2.2 Operadores do Algoritmo de Grover . . . . .    | 7         |
| 2.3 Complexidade do Algoritmo de Grover . . . . .  | 12        |
| <b>3 Álgebra Geométrica</b>                        | <b>19</b> |
| 3.1 Introdução . . . . .                           | 19        |
| 3.2 Produto de Vetores na AG e o Bivetor . . . . . | 19        |
| 3.2.1 Produto Externo . . . . .                    | 21        |
| 3.2.2 Projeção e Reflexão . . . . .                | 23        |
| <b>4 Reformulação do Algoritmo de Grover</b>       | <b>26</b> |

|          |                                                   |           |
|----------|---------------------------------------------------|-----------|
| 4.1      | Interpretação Geométrica dos Operadores . . . . . | 26        |
| 4.2      | Reescrevendo o Algoritmo de Grover . . . . .      | 29        |
| 4.3      | Exemplos . . . . .                                | 33        |
| 4.3.1    | Exemplo $N = 4$ . . . . .                         | 33        |
| 4.3.2    | Exemplo $N = 8$ . . . . .                         | 34        |
| 4.4      | Forma geral para $G^k$ e $G^k\psi$ . . . . .      | 36        |
| <b>5</b> | <b>Conclusão</b>                                  | <b>40</b> |
|          | <b>Referências Bibliográficas</b>                 | <b>42</b> |

# Capítulo 1

## Introdução

Neste trabalho, apresentamos uma nova visão do Algoritmo de Grover usando a Álgebra Geométrica, com o objetivo de simplificar o operador  $G$  de Grover. Para isso, nos baseamos na interpretação geométrica dos operadores do algoritmo e nas propriedades do produto de Clifford.

No algoritmo de Grover, um algoritmo quântico de busca proposto por Lov K. Grover em 1996 [5], descrito no Capítulo 2, fazemos uso de um operador oráculo. O algoritmo é aplicado a dois registradores, o primeiro com  $n$  q-bits e o segundo com apenas 1 q-bit. Antes da ação do oráculo, utilizamos a porta Hadamard ( $H$ ), descrita mais adiante, para criar uma superposição uniforme, no primeiro registrador, de todos os elementos da base computacional, formada (em sua forma decimal) pelos índices dos elementos da lista. No segundo registrador, a ação de  $H$  retorna um estado que será fundamental para o reconhecimento da solução. Nesse momento, será aplicado o operador  $U_f$  (descrito na Seção 2.2), um operador linear unitário que realiza o papel do oráculo. A solução do problema (consideraremos que o problema contém apenas uma solução) teve o sinal de sua amplitude invertido, dessa forma conseguiremos identificar a solução. Como veremos, a probabilidade de encontrarmos o elemento fazendo uma medida (processo realizado para trazer a informação para o nível clássico) nesse momento é pequena, devido ao módulo dessa amplitude ser “pequeno”, e para aumentá-lo, utilizamos outro operador linear unitário, descrito também na Seção 2.2. A composição dos dois últimos operadores é chamada de operador de *Grover*  $G$ .

## Introdução

---

Na Seção 2.3, demonstramos que o computador quântico, através do algoritmo de Grover, oferece um ganho quadrático em relação ao computador clássico na solução de problemas de busca em listas desordenadas. A complexidade do algoritmo diz respeito ao número de vezes que  $G$  deve ser aplicado, chamamos esse número de  $k$  e mostramos que ele é da ordem de  $\sqrt{N}$ . Mais do que isso, mostramos que a cada aplicação de  $G$ , de fato ficamos mais próximos da solução e ainda, do ponto de vista geométrico, cada aplicação de  $G$  gera uma rotação em direção ao vetor corresponde à solução sempre do mesmo ângulo.

No Capítulo 3, apresentamos alguns conceitos da Álgebra Geométrica ([7], [11]). As considerações são feitas em  $\mathbb{R}^2$  mas podem ser estendidas para dimensões maiores.

Seria útil termos um produto de vetores que satisfizesse os mesmos axiomas da multiplicação de números reais (distributividade, associatividade e comutatividade) e ainda preservasse a norma na multiplicação. Como para  $n \geq 3$  isso é impossível, consideraremos um produto de vetores que não satisfaça a comutatividade. Fazendo exigências sobre esse produto, definiremos uma nova estrutura, chamada de *bivetor*, e esse novo produto entre vetores é representado pela soma de um escalar e um bivetor, e será chamado o Produto de Clifford. Como veremos, esse escalar é o produto interno usual entre os vetores e o bivetor será chamado de produto externo. Como sabemos, para os reais, o produto interno é comutativo, mas o produto externo não tem essa propriedade. Esse fato determina o significado geométrico para a não comutatividade do Produto de Clifford.

Na Seção 3.2.2, discutimos sobre projeção e reflexão de vetores. Na álgebra geométrica, podemos definir o elemento inverso de um vetor  $v$ , como  $v^{-1}$ , tal que  $vv^{-1} = 1$  (esse produto é o produto de Clifford). Esse elemento aparece nas componentes paralela e perpendicular (em relação à projeção) de um vetor  $a$  projetado sobre um vetor  $b$ . Vemos também que podemos definir a reflexão de  $a$  sobre  $b$  de forma simples como  $a' = aba^{-1}$ . Essa operação será fundamental no desenvolvimento do Capítulo 4.

Iniciamos o Capítulo 4 com uma interpretação geométrica dos operadores do algoritmo, e concluímos que a ação de cada operador que compõe  $G$  é dada por uma reflexão, portanto  $G$  é uma composição de reflexões. Na verdade, uma iteração de Grover pode ser interpretada como uma rotação em um espaço bidimensional gerado pelo vetor inicial e pelo vetor que representa a solução do problema. (Uma interpretação geométrica do algoritmo também pode ser encontrada em [9]). Nesse sentido, “substituímos” os operado-

## Introdução

---

res originais do algoritmo de Grover pelas operações de reflexão da Álgebra Geométrica e dessa forma reescrevemos o algoritmo. Por último, apresentamos expressões para os elementos  $G^k$  e  $G^k\psi$ , o estado resultante de  $k$  aplicações de  $G$ .

# Capítulo 2

## Algoritmo de Grover

### 2.1 Introdução

Suponhamos que temos uma lista não ordenada com  $N$  elementos e procuramos por um elemento específico. Classicamente, teríamos que testar elemento a elemento até encontrarmos o elemento procurado, o que, no pior caso, requereria  $O(N)$  testes. Usando propriedades da mecânica quântica, o Algoritmo de Grover (ver, por exemplo, Bennett et al. [3], Boyer et al. [4], Grover [5, 6]) necessita apenas de  $O(\sqrt{N})$  tentativas.

A seguir, descrevemos alguns conceitos básicos da mecânica quântica necessários para a compreensão do algoritmo. A Seção 2.2 apresenta uma revisão do Algoritmo de Grover e, na Seção 2.3, falaremos sobre a complexidade do algoritmo, baseada em conceitos de álgebra linear (mais informações sobre computação quântica assim como outras demonstrações da complexidade do algoritmo de Grover podem ser encontradas em Benenti et al. [2], Hirvensalo [8], Kitaev et al. [10], Nielsen e Chuang [12], Pittenger [14], e Preskill [16]).

Em computadores quânticos, os valores 0 e 1 dos bits são substituídos pelos *bits quânticos* (q-bits)  $|0\rangle$  e  $|1\rangle$  (notação de Dirac). A diferença entre bits e q-bits, é que um q-bit genérico  $|\psi\rangle$  pode ser também uma combinação linear dos q-bits  $|0\rangle$  e  $|1\rangle$ ,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.1)$$

onde  $\alpha$  e  $\beta$  são números complexos.  $|\psi\rangle$  é dita uma *superposição* de  $|0\rangle$  e  $|1\rangle$  com *amplitudes*

$\alpha$  e  $\beta$ . A representação matricial dos q-bits  $|0\rangle$  e  $|1\rangle$  é dada por:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{e} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Dessa forma,  $|\psi\rangle$  é um vetor em um espaço vetorial complexo de duas dimensões, com  $\{|0\rangle, |1\rangle\}$  formando uma base ortonormal, chamada *base computacional*. Em mecânica quântica, vetores são também chamados de *estados*. A interpretação física de  $|\psi\rangle$ , em (2.1), é que ele existe simultaneamente nos estados  $|0\rangle$  e  $|1\rangle$ . O estado  $|\psi\rangle$  pode armazenar uma quantidade infinita de informação em seus coeficientes  $\alpha$  e  $\beta$ , mas esta informação está acessível apenas em nível quântico. Para trazê-la ao nível clássico, precisamos fazer uma medida no q-bit. A mecânica quântica nos diz que o processo de medida altera o estado de um q-bit, fazendo-o colapsar para o estado  $|0\rangle$ , com probabilidade  $|\alpha|^2$ , ou para o estado  $|1\rangle$ , com probabilidade  $|\beta|^2$ . Como a soma das probabilidades deve ser igual a um, temos

$$|\alpha|^2 + |\beta|^2 = 1, \tag{2.2}$$

e usando essa informação, calculamos a norma de  $|\psi\rangle$ :

$$\| |\psi\rangle \| = \sqrt{|\alpha|^2 + |\beta|^2} = 1.$$

Se não for através de uma medida, a evolução de um estado se dá por uma transformação linear unitária, isto é, uma transformação linear com a seguinte propriedade

$$U^\dagger U = U U^\dagger = I,$$

onde  $U^\dagger = (U^*)^T$  ( $*$  indica conjugação complexa e  $T$  indica transposição) e  $I$  é a matriz identidade de ordem 2.

Se quisermos considerar estados com mais de um q-bit, precisaremos empregar o conceito de produto tensorial. Para nossos propósitos, será suficiente a seguinte definição.

Dados os estados  $|v\rangle \in \mathbb{C}^m$  e  $|w\rangle \in \mathbb{C}^n$ , o produto tensorial  $|v\rangle \otimes |w\rangle$  é dado por

$$|v\rangle \otimes |w\rangle = \begin{bmatrix} v_1|w\rangle \\ \vdots \\ v_m|w\rangle \end{bmatrix},$$

onde  $v_1, \dots, v_m$  são as coordenadas do vetor  $|v\rangle$ . Para o produto tensorial, também são usadas as notações  $|v\rangle|w\rangle$  e  $|vw\rangle$ . Por exemplo, se tivermos um computador quântico de 2 q-bits e o primeiro q-bit estiver no estado  $|0\rangle$  enquanto o segundo estiver no estado  $|1\rangle$ , o computador quântico estará no estado  $|0\rangle \otimes |1\rangle$ , dado por

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

Em geral, o estado  $|\psi\rangle$  de um computador quântico de  $n$  q-bits é uma superposição dos  $2^n$  estados  $\{|0\rangle, |1\rangle, \dots, |2^n - 1\rangle\}$ ,

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

com amplitudes  $\alpha_i$  restritas à

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

Como feito antes, uma medida de um estado genérico  $|\psi\rangle$  produz o estado  $|i_0\rangle$  com probabilidade  $|\alpha_{i_0}|^2$ , para  $0 \leq i_0 \leq 2^n$  (a base ortonormal  $\{|0\rangle, \dots, |2^n - 1\rangle\}$  é a base computacional na notação decimal). Geralmente, a medida é realizada q-bit a q-bit produzindo zeros ou uns formando o elemento  $i_0$ .

Finalizando a seção, daremos duas definições que serão usadas à frente. Dados dois vetores  $|\varphi\rangle$  e  $|\psi\rangle$  em um espaço vetorial  $V$ , além do *produto interno* usual, escrito na forma  $\langle\varphi|\psi\rangle$ , também usaremos o *produto externo*  $|\psi\rangle\langle\varphi|$ , definido como o operador linear



sobre  $V$  satisfazendo

$$(|\psi\rangle\langle\varphi|)|v\rangle = \langle\varphi|v\rangle|\psi\rangle, \quad \forall |v\rangle \in V.$$

Assumindo que  $\| |\varphi\rangle \| = \| |\psi\rangle \| = 1$ , o ângulo  $\theta$  entre  $|\psi\rangle$  e  $|\varphi\rangle$  é definido como

$$\theta = \arccos(\langle\varphi|\psi\rangle).$$

Note que se  $\langle\varphi|\psi\rangle \in \mathbb{R}$ , então  $\theta \in [0, \pi]$  (para mais detalhes, ver Apostol [1], p.458). No algoritmo de Grover, todas as amplitudes são números reais. Como veremos, este fato será fundamental para comparar ângulos entre estados.

## 2.2 Operadores do Algoritmo de Grover

O algoritmo de Grover usa  $n$  q-bits no primeiro registrador e 1 q-bit no segundo (Fig. 2.2-1). O primeiro passo é criar uma superposição dos  $2^n$  estados da base computacional  $\{|0\rangle, \dots, |2^n - 1\rangle\}$  do primeiro registrador, realizada da seguinte forma. Inicializamos o primeiro registrador no estado  $|0\rangle \dots |0\rangle$  e aplicamos o operador de *Hadamard*  $H$ ,

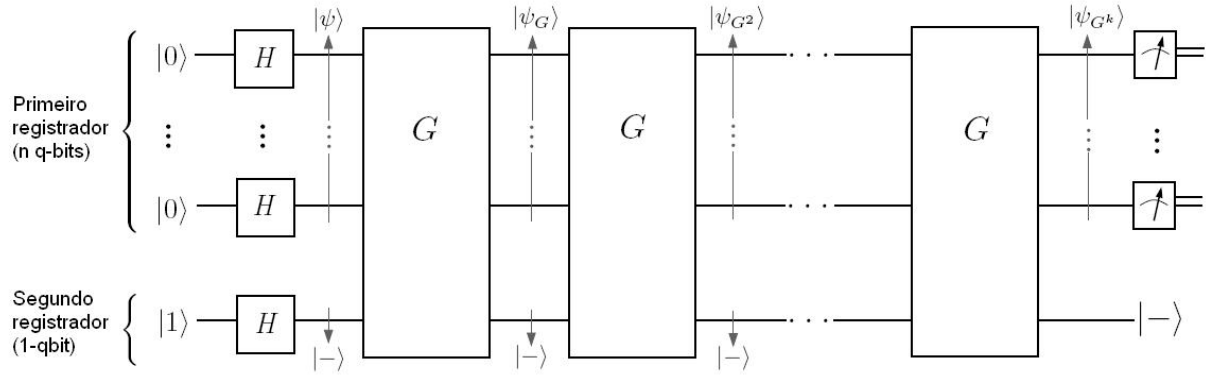
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

em cada q-bit  $|0\rangle$ . Podemos verificar que

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Então, se a entrada for  $|0\rangle$ , o operador de Hadamard cria uma superposição dos estados  $|0\rangle$  e  $|1\rangle$  com mesma amplitude. Generalizando, para um estado de  $n$  q-bits  $|0\rangle \dots |0\rangle$ , o operador de Hadamard produz

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle.$$



**Figura 2.2-1.** Esquema genérico do Algoritmo de Grover. Ao final, cada q-bit do primeiro registrador é medido, produzindo o índice do elemento procurado na notação binária.

Note que  $|\psi\rangle$  é uma superposição de todos os estados da base com amplitudes dadas por  $\frac{1}{\sqrt{2^n}}$ . O segundo registrador (Fig. 2.2-1) é iniciado com  $|1\rangle$  e após a aplicação do operador  $H$ , ele muda para o estado  $|-\rangle$ , dado por

$$|-\rangle = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (2.3)$$

Identificamos os elementos da lista com números inteiros de 0 a  $N - 1$ , e assumimos que  $N = 2^n$  para algum inteiro  $n \geq 2$  (o algoritmo não funciona para  $n = 1$ ).

Seja  $f : \{0, \dots, N - 1\} \rightarrow \{0, 1\}$  a função que reconhece o elemento procurado, dada por:

$$f(i) = \begin{cases} 1, & \text{se } i = i_0 \\ 0, & \text{caso contrário,} \end{cases}$$

onde  $i_0$  é o índice do elemento procurado. Ao invés de usar  $f$ , o algoritmo de Grover usa um operador unitário  $U_f$ , que depende de  $f$ , definido por

$$U_f(|i\rangle |j\rangle) = |i\rangle |j \oplus f(i)\rangle,$$

onde  $|i\rangle$  representa o estado do primeiro registrador ( $i \in \{0, \dots, N - 1\}$ ),  $|j\rangle$  é o estado

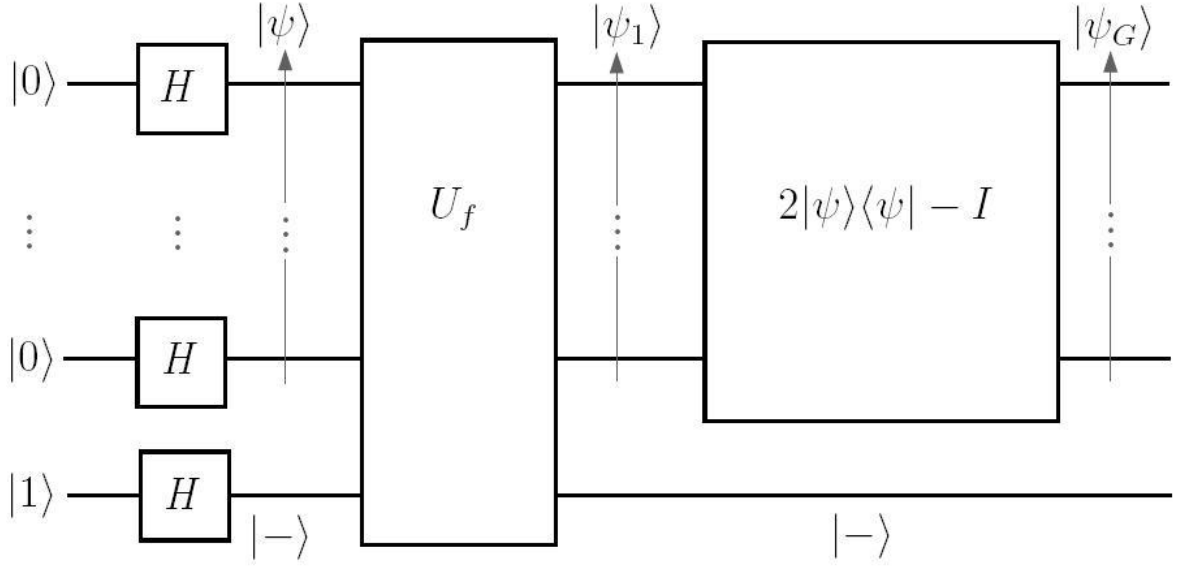


Figura 2.2-2. Uma iteração de Grover.

do segundo registrador ( $j \in \{0, 1\}$ ), e  $\oplus$  é a soma módulo 2. Usando o fato de que

$$1 \oplus f(i) = \begin{cases} 0 & \text{se } i = i_0 \\ 1 & \text{se } i \neq i_0, \end{cases}$$

podemos ver que

$$\begin{aligned} U_f(|i\rangle|-\rangle) &= \frac{U_f(|i\rangle|0\rangle) - U_f(|i\rangle|1\rangle)}{\sqrt{2}} \\ &= \frac{|i\rangle|f(i)\rangle - |i\rangle|1 \oplus f(i)\rangle}{\sqrt{2}} \\ &= (-1)^{f(i)}|i\rangle|-\rangle. \end{aligned} \tag{2.4}$$

Usando esse resultado e aplicando  $U_f$  à superposição gerada no primeiro passo (Fig. 2.2-2), concluímos que podemos manter o segundo registrador constante. Chamaremos de

$|\psi_1\rangle$  o estado resultante do primeiro registrador:

$$\begin{aligned} |\psi_1\rangle |-\rangle &= U_f(|\psi\rangle |-\rangle) \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} U_f(|i\rangle |-\rangle) \\ &= \left( \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i\rangle \right) |-\rangle. \end{aligned} \quad (2.5)$$

$|\psi_1\rangle$  também é uma superposição de todos os elementos da base, mas agora o elemento procurado está marcado por um sinal de menos. Note que a função  $f$  foi aplicada aos  $N$  pontos através de uma única aplicação do operador  $U_f$  (isso é chamado de paralelismo quântico).

No nível quântico, é possível identificar o elemento procurado, pois é o único com amplitude negativa. Entretanto, essa informação não está acessível classicamente. Uma informação clássica de um estado quântico é obtida através de medidas, e, nesse caso, não é interessante medir o estado do primeiro registrador, pois é muito provável que não consigamos identificar o elemento procurado, devido ao módulo de sua amplitude ser pequeno. Antes de realizarmos uma medida, precisamos aumentar a amplitude do elemento procurado enquanto diminuirmos a amplitude dos demais. Isso é feito utilizando-se outro operador unitário, definido por  $(2|\psi\rangle\langle\psi| - I)$  (Fig. 2.2-2).

O estado  $|\psi_1\rangle$ , em (2.5), pode ser escrito como

$$|\psi_1\rangle = |\psi\rangle - \frac{2}{\sqrt{N}} |i_0\rangle, \quad (2.6)$$

onde

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \quad (2.7)$$

e  $i_0$  é o índice do elemento procurado. Vamos calcular o estado  $|\psi_G\rangle$  (Fig. 2.2-2), resultado

da aplicação do operador  $(2|\psi\rangle\langle\psi| - I)$  sobre o estado  $|\psi_1\rangle$ . Usando (2.6), teremos

$$\begin{aligned} |\psi_G\rangle &= (2|\psi\rangle\langle\psi| - I) |\psi_1\rangle \\ &= (2|\psi\rangle\langle\psi| - I) \left( |\psi\rangle - \frac{2}{\sqrt{N}} |i_0\rangle \right) \\ &= (2\langle\psi|\psi\rangle) |\psi\rangle - \left( \frac{4}{\sqrt{N}} \langle\psi|i_0\rangle \right) |\psi\rangle - |\psi\rangle + \frac{2}{\sqrt{N}} |i_0\rangle. \end{aligned} \quad (2.8)$$

De (2.7),

$$\langle\psi|i_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \langle i|i_0\rangle = \frac{1}{\sqrt{N}} \langle i_0|i_0\rangle = \frac{1}{\sqrt{N}}, \quad (2.9)$$

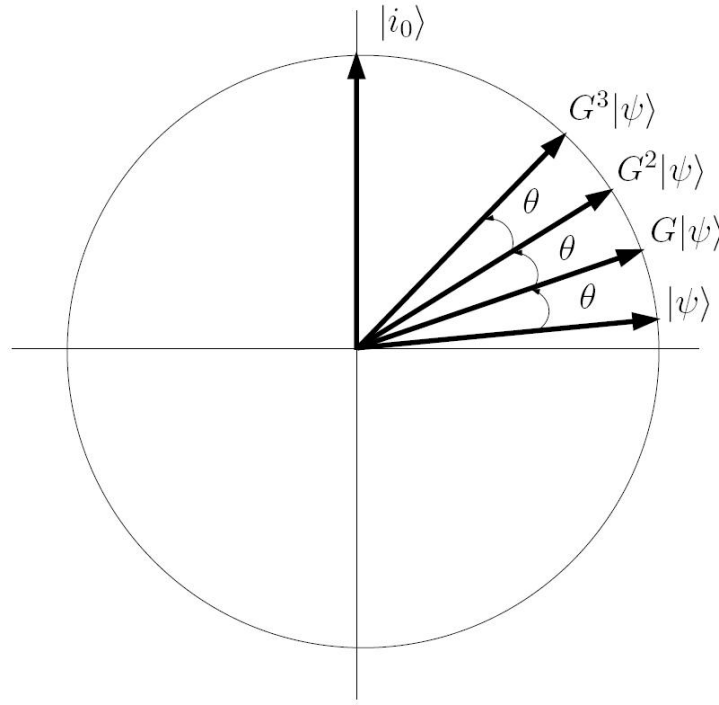
e, substituindo (2.9) em (2.8), obtemos

$$|\psi_G\rangle = \frac{N-4}{N} |\psi\rangle + \frac{2}{\sqrt{N}} |i_0\rangle. \quad (2.10)$$

Os vetores  $|i_0\rangle$  e  $|\psi\rangle$  são mostrados na Fig. 2.2-3. Eles formam um ângulo menor que  $\frac{\pi}{2}$ , já que  $0 < \langle\psi|i_0\rangle < 1$ . Se  $N$  for grande, esse ângulo se aproximará de  $\frac{\pi}{2}$ . Podemos pensar em  $|\psi\rangle$  como o estado inicial do primeiro registrador e nos passos computacionais como as aplicações dos operadores unitários  $U_f$  e  $(2|\psi\rangle\langle\psi| - I)$  (Fig. 2.2-2). Consideraremos apenas a ação da composição desses operadores, chamada de operador de Grover  $G$  (Fig. 2.2-1). De (2.10), podemos ver que a amplitude de  $|i_0\rangle$ , em  $|\psi_G\rangle$ , aumentou enquanto a amplitude de  $|i\rangle$ ,  $i \neq i_0$ , diminuiu em relação aos seus valores iniciais em  $|\psi\rangle$ . Uma medida, nesse ponto, retornará  $|i_0\rangle$  com uma probabilidade maior que antes. Isso nos leva a duas questões:

1. A cada aplicação de  $G$ , o estado resultante está “mais próximo” de  $|i_0\rangle$ ?
2. Nesse caso, quantas aplicações de  $G$  seriam necessárias para “obtermos”  $|i_0\rangle$ ?

Essas questões são tratadas a seguir. O Teorema 1 responde a primeira pergunta enquanto o Teorema 2 responde a segunda.



**Figura 2.2-3.** Efeito de aplicações sucessivas de  $G$ .

## 2.3 Complexidade do Algoritmo de Grover

Inicialmente, veremos que a aplicação de  $G^k$  ( $k \in \mathbb{N}$ ) produz uma rotação de  $|\psi\rangle$  em direção a  $|i_0\rangle$ , de  $k\theta$  graus, no subespaço gerado pelos vetores  $|\psi\rangle$  e  $|i_0\rangle$ , onde  $\theta$  é o ângulo entre  $|\psi\rangle$  e  $G|\psi\rangle$  (Fig. 2.2-3). A demonstração é dividida em quatro lemas. O Lema 1 diz que  $G^k|\psi\rangle$  pertence ao subespaço gerado por  $|\psi\rangle$  e  $|i_0\rangle$ , para todo  $k \in \mathbb{N}$ . O Lema 2 estabelece que o ângulo entre  $G^k|\psi\rangle$  e  $G^{k+1}|\psi\rangle$  também é  $\theta$ , para todo  $k \in \mathbb{N}$ . No Lema 3, é dito que  $G$  rotaciona  $|\psi\rangle$  em direção a  $|i_0\rangle$ . Finalmente, no Lema 4, é provado que o sentido da rotação produzida quando  $G$  é aplicado sobre  $G^k|\psi\rangle$ , para todo  $k \in \mathbb{N}$ , é o mesmo obtido quando  $G$  é aplicado sobre  $|\psi\rangle$ . O subespaço gerado por  $|\psi\rangle$  e  $|i_0\rangle$  será denotado por  $\Omega$  e o estado do primeiro registrador de  $G^k|\psi\rangle$  será denotado por  $|\psi_{G^k}\rangle$ . O estado do segundo registrador ( $|-\rangle$ ) será omitido, pois ele é constante durante todo o processo.

**Lema 1.**  $G^n|\psi\rangle \in \Omega$ , para todo  $n \in \mathbb{N}$ .

*Prova.* A demonstração é por indução. De (2.10), sabemos que

$$G|\psi\rangle = \frac{N-4}{N}|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle. \quad (2.11)$$

Assim, para  $n = 1$  está provado. Agora suponhamos que  $G^k|\psi\rangle \in \Omega$ , para um  $k$  dado. Isto é, existe  $\alpha, \beta \in \mathbb{R}$  tal que

$$G^k|\psi\rangle = \alpha|\psi\rangle + \beta|i_0\rangle.$$

Temos que provar que  $G^{k+1}|\psi\rangle \in \Omega$ . A aplicação do operador  $G$  nos dois lados da expressão acima resulta em

$$G^{k+1}|\psi\rangle = \alpha G|\psi\rangle + \beta G|i_0\rangle. \quad (2.12)$$

Vamos calcular  $G|i_0\rangle$ . Da definição de  $G$ , temos

$$G|i_0\rangle = (2|\psi\rangle\langle\psi| - I)U_f|i_0\rangle. \quad (2.13)$$

De (2.4), obtemos

$$U_f|i_0\rangle = -|i_0\rangle.$$

Substituindo esse valor em (2.13) e usando (2.9), teremos

$$\begin{aligned} G|i_0\rangle &= (2|\psi\rangle\langle\psi| - I)(-|i_0\rangle) \\ &= -2\langle\psi|i_0\rangle|\psi\rangle + |i_0\rangle \\ &= -\frac{2}{\sqrt{N}}|\psi\rangle + |i_0\rangle. \end{aligned} \quad (2.14)$$

Como tanto  $G|\psi\rangle$  quanto  $G|i_0\rangle$  são estados em  $\Omega$ , de (2.12) concluimos que

$$G^n|\psi\rangle \in \Omega, \quad \forall n \in \mathbb{N}.$$

**Lema 2.** *O ângulo entre  $G^k |\psi\rangle$  e  $G^{k+1} |\psi\rangle$  é  $\theta$ , para todo  $k \in \mathbb{N}$ .*

*Prova.* Utilizando a definição de ângulo entre dois vetores dada no final da Seção 1, a afirmação deste lema é equivalente a

$$\langle \psi_{G^k} | \psi_{G^{k+1}} \rangle = \cos \theta, \forall k \in \mathbb{N}.$$

Usando o fato de que

$$(G^k)^\dagger |\psi_{G^k}\rangle = (G^k)^\dagger G^k |\psi\rangle = |\psi\rangle,$$

obtemos (para todo  $k \in \mathbb{N}$ )

$$\begin{aligned} \langle \psi_{G^k} | \psi_{G^{k+1}} \rangle &= \langle \psi_{G^k} | G^k | \psi_G \rangle \\ &= \langle \psi | \psi_G \rangle \\ &= \cos \theta. \end{aligned}$$

**Lema 3.** *O operador  $G$  rotaciona  $|\psi\rangle$  em direção a  $|i_0\rangle$ .*

*Prova.* Como sabemos que  $|\psi_G\rangle \in \Omega$ , para demonstrar este lema é suficiente provar que

$$\arccos(\langle \psi_G | i_0 \rangle) < \arccos(\langle \psi | i_0 \rangle),$$

que é equivalente a

$$\langle \psi_G | i_0 \rangle > \langle \psi | i_0 \rangle.$$



De (2.9) e (2.11), temos

$$\begin{aligned}\langle \psi_G | i_0 \rangle &= \frac{N-4}{N} \langle \psi | i_0 \rangle + \frac{2}{\sqrt{N}} \langle i_0 | i_0 \rangle \\ &= \frac{N-4}{N\sqrt{N}} + \frac{2}{\sqrt{N}} \\ &= \frac{3N-4}{N\sqrt{N}}.\end{aligned}$$

Uma vez que

$$\frac{3N-4}{N\sqrt{N}} > \frac{1}{\sqrt{N}} \quad (\text{for } N > 2),$$

chegamos à conclusão.

**Lema 4.** *A aplicação de  $G$  sobre  $|\psi_{G^n}\rangle$ , para todo  $n \in \mathbb{N}$ , mantém o mesmo sentido de rotação de quando  $G$  é aplicado sobre  $|\psi\rangle$ .*

*Prova.* Usando os Lemas 1, 2, e 3, não é difícil ver que para demonstrar este lema é suficiente provar que

$$G(G^n|\psi\rangle) \neq G^{n-1}|\psi\rangle, \quad \forall n \in \mathbb{N}.$$

A demonstração é por indução. Primeiro, provamos que

$$G(G^1|\psi\rangle) \neq G^0|\psi\rangle,$$

isto é,

$$G|\psi_G\rangle \neq |\psi\rangle.$$

Usando (2.11) e (2.14), podemos calcular  $G|\psi_G\rangle$ :

$$\begin{aligned}
 G|\psi_G\rangle &= G\left(\frac{N-4}{N}|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle\right) \\
 &= \frac{N-4}{N}G|\psi\rangle + \frac{2}{\sqrt{N}}G|i_0\rangle \\
 &= \frac{N-4}{N}\left(\frac{N-4}{N}|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle\right) + \frac{2}{\sqrt{N}}\left(-\frac{2}{\sqrt{N}}|\psi\rangle + |i_0\rangle\right) \\
 &= \left(\frac{N-4}{N}\right)^2|\psi\rangle + \frac{2N-8}{N\sqrt{N}}|i_0\rangle - \frac{4}{N}|\psi\rangle + \frac{2}{\sqrt{N}}|i_0\rangle \\
 &= \left(\left(\frac{N-4}{N}\right)^2 - \frac{4}{N}\right)|\psi\rangle + \frac{4N-8}{N\sqrt{N}}|i_0\rangle.
 \end{aligned}$$

Para  $N \geq 2$ , este estado é diferente de  $|\psi\rangle$ . Agora suponha que, para um  $k$  dado,

$$G(G^k|\psi\rangle) \neq G^{k-1}|\psi\rangle.$$

Já que  $G$  é um operador unitário, podemos aplicá-lo nos dois lados da expressão acima, produzindo

$$G(G^{k+1}|\psi\rangle) \neq G^k|\psi\rangle.$$

Isso conclui a prova.

As demonstrações dos lemas acima podem ser encontradas em [15]. O resultado abaixo segue imediatamente dos Lemas 1, 2, 3, e 4.

**Teorema 1.**  $G^k$  rotaciona  $|\psi\rangle$  em direção a  $|i_0\rangle$  de  $k\theta$  graus, no subespaço gerado por  $|\psi\rangle$  e  $|i_0\rangle$ , para todo  $k \in \mathbb{N}$ .

Agora, consideraremos a complexidade do algoritmo de Grover. Inicialmente, vamos

calcular o ângulo  $\theta$  entre os vetores  $|\psi\rangle$  e  $G|\psi\rangle$ . De (2.9) e (2.10), temos

$$\begin{aligned}\cos \theta &= \langle \psi | \psi_G \rangle \\ &= \frac{N-4}{N} \langle \psi | \psi \rangle + \frac{2}{\sqrt{N}} \langle \psi | i_0 \rangle \\ &= \frac{N-4}{N} + \frac{2}{\sqrt{N}} \left( \frac{1}{\sqrt{N}} \right) \\ &= \frac{N-2}{N},\end{aligned}$$

isto é,

$$\theta = \arccos \left( \frac{N-2}{N} \right). \quad (2.15)$$

Do Teorema 1, sabemos que  $G^k$  rotaciona  $|\psi\rangle$  em direção a  $|i_0\rangle$  de  $k\theta$  graus, no subespaço gerado por  $|\psi\rangle$  e  $|i_0\rangle$ , para todo  $k \in \mathbb{N}$ . Daí, para determinar a complexidade do algoritmo de Grover, temos que calcular o valor de  $k$ , o número de vezes que o operador de Grover  $G$  deve ser aplicado tal que o ângulo entre  $|i_0\rangle$  e  $G^k|\psi\rangle$  se torne zero. Matematicamente, o que queremos é encontrar o valor de  $k$  que satisfaça

$$\arccos(\langle \psi | i_0 \rangle) - k\theta = 0.$$

De (2.9) e (2.15), obtemos

$$\arccos \left( \frac{1}{\sqrt{N}} \right) - k \arccos \left( \frac{N-2}{N} \right) = 0 \Rightarrow k = \frac{\arccos \left( \frac{1}{\sqrt{N}} \right)}{\arccos \left( \frac{N-2}{N} \right)}. \quad (2.16)$$

Comparando  $k$  com  $\sqrt{N}$ , quando  $N$  é grande, deduzimos que

$$\lim_{N \rightarrow \infty} \frac{k}{\sqrt{N}} = \frac{\pi}{4},$$

o que implica que

$$k = O(\sqrt{N}).$$

A discussão acima nos conduz ao seguinte resultado:

**Teorema 2.** *A complexidade do algoritmo de Grover é  $O(\sqrt{N})$ .*

## Capítulo 3

# Álgebra Geométrica

### 3.1 Introdução

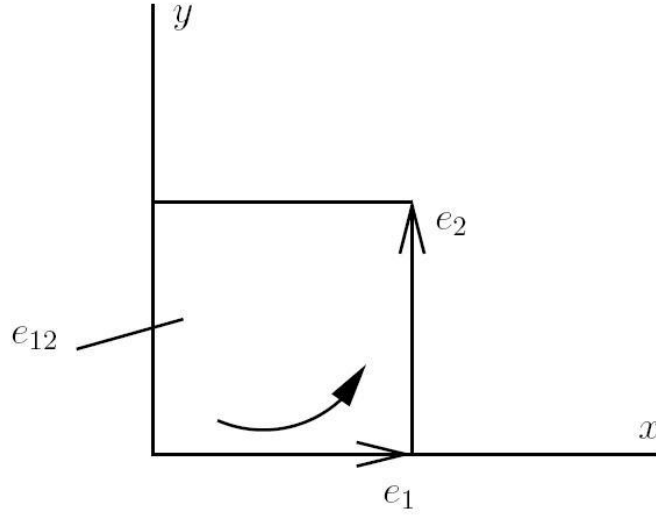
Nesse capítulo são apresentados os conceitos da Álgebra Geométrica (AG) que serão necessários para o desenvolvimento do próximo capítulo, como produto de Clifford, produtos interno e externo, bivectores, projeção e reflexão de vetores, entre outros.

### 3.2 Produto de Vetores na AG e o Bivector

Vamos considerar em  $\mathbb{R}^2$  um produto de vetores que satisfaz a distributividade e a associatividade, mas não satisfaz a comutatividade, e daremos um significado geométrico para a não comutatividade.

Considere os vetores unitários e ortogonais  $e_1 = (1, 0)$  e  $e_2 = (0, 1)$  em  $\mathbb{R}^2$ . O comprimento do vetor  $r = xe_1 + ye_2$  é  $|r| = \sqrt{x^2 + y^2}$ . Se multiplicarmos  $r$  por ele mesmo,  $rr = r^2$ , exigirmos que  $r^2 = |r|^2$  e olharmos para a forma de coordenadas, estaremos introduzindo um produto de vetores tal que

$$(xe_1 + ye_2)^2 = x^2 + y^2. \quad (3.1)$$

Figura 3.2-1. Bivetor  $e_{12}$ .

Usando a distributividade e não assumindo a comutatividade, obtemos

$$x^2 e_1^2 + y^2 e_2^2 + xy(e_1 e_2 + e_2 e_1) = x^2 + y^2. \quad (3.2)$$

Isso é satisfeito no caso de  $e_1$  e  $e_2$  obedecerem as seguintes condições:

$$e_1^2 = e_2^2 = 1 \quad \text{e} \quad e_1 e_2 = -e_2 e_1, \quad (3.3)$$

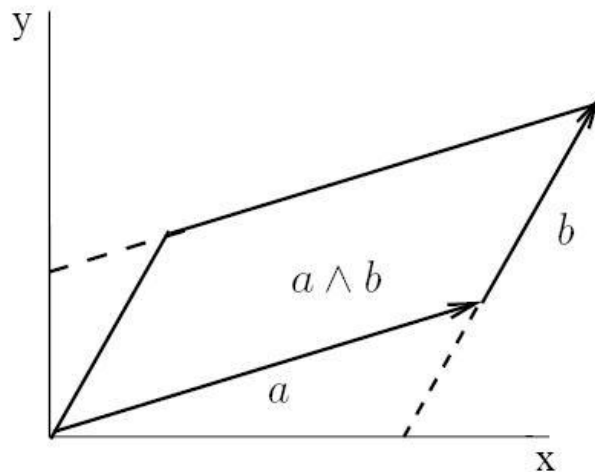
que corresponde a ([11])

$$|e_1| = |e_2| = 1 \quad \text{e} \quad e_1 \perp e_2 \quad (\text{vetores perpendiculares}). \quad (3.4)$$

Isso quer dizer que  $(e_1 e_2)^2 = -e_1^2 e_2^2 = -1$ . Isto é, o **quadrado** desse produto é **negativo**, o que implica que não podemos dizer que  $e_1 e_2$  é um escalar e nem um vetor. Esse produto é um novo tipo de unidade, chamada de **bivetor**. Nesse caso, um bivetor representa um quadrado formado pelos vetores  $e_1$  e  $e_2$ , com uma orientação dada pela "regra da mão direita" (Figura 3.2-1). Usaremos a notação  $e_{12} = e_1 e_2$ .

Definimos então o *Produto de Clifford* de dois vetores  $a = a_1 e_1 + a_2 e_2$  e  $b = b_1 e_1 + b_2 e_2$  como

$$ab = a_1 b_1 + a_2 b_2 + (a_1 b_2 - a_2 b_1) e_{12}, \quad (3.5)$$

Figura 3.2-2. Bivetor  $a \wedge b$ .

dado pela soma de um escalar e um bivetor.

### 3.2.1 Produto Externo

Percebemos que o escalar dentro do produto  $ab$ , dado em (3.5), é exatamente o produto interno usual entre  $a$  e  $b$  no  $\mathbb{R}^2$ , denotado por  $\langle a|b \rangle$ . A outra parte será chamada de **produto externo** entre  $a$  e  $b$ , denotado por  $a \wedge b$ . Logo,

$$ab = \langle a|b \rangle + a \wedge b, \quad (3.6)$$

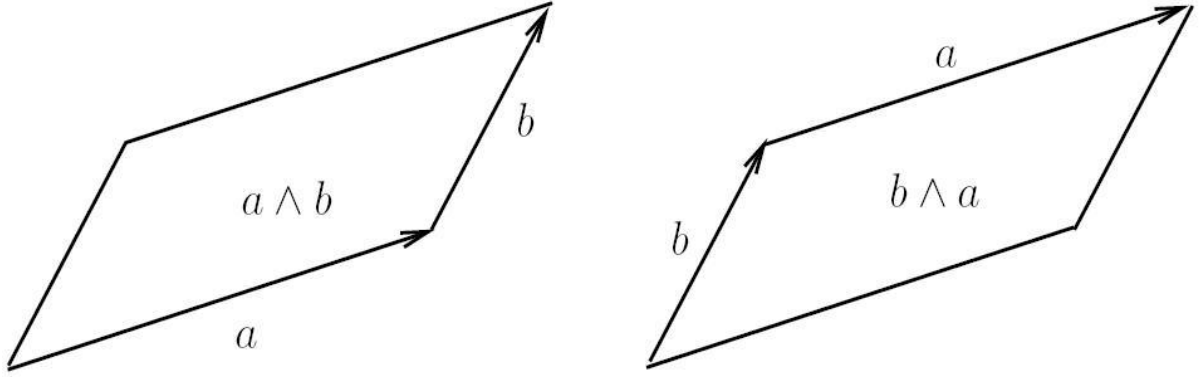
onde

$$\langle a|b \rangle = a_1b_1 + a_2b_2 \quad (3.7)$$

e

$$a \wedge b = (a_1b_2 - a_2b_1)e_{12}. \quad (3.8)$$

O bivetor  $a \wedge b$  representa um paralelogramo definido pelos vetores  $a$  e  $b$  (Figura 3.2-2), também com uma orientação dada pela "regra da mão direita". A área do paralelogramo



**Figura 3.2-3.**  $a \wedge b = -(b \wedge a)$ .

é  $|a_1b_2 - a_2b_1|$  e diremos que essa área é o módulo do bivector, ou seja,

$$|a \wedge b| = |a_1b_2 - a_2b_1|. \quad (3.9)$$

Na Figura 3.2-3, vemos que  $a \wedge b$  e  $b \wedge a$  têm o mesmo módulo, mas sentidos de rotação opostos.

Essa diferença pode ser descrita da seguinte forma:

$$a \wedge b = -(b \wedge a). \quad (3.10)$$

Como  $\langle a|b \rangle = \langle b|a \rangle$ , teremos

$$ba = \langle a|b \rangle - a \wedge b, \quad (3.11)$$

o que implica que

$$ab = ba \iff a \wedge b = 0 \iff ab = \langle a|b \rangle \quad (3.12)$$

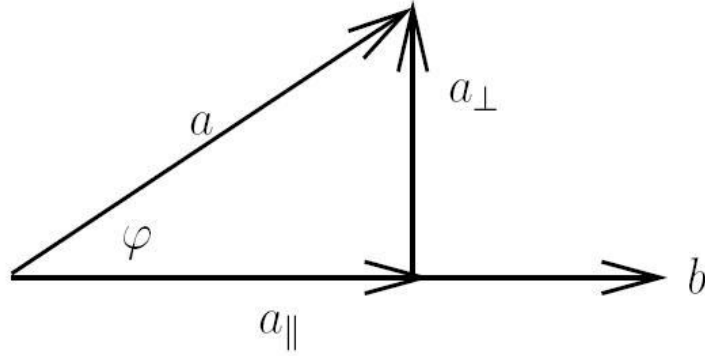
e

$$ab = -ba \iff \langle a|b \rangle = 0 \iff ab = a \wedge b. \quad (3.13)$$

Ou seja,

$$ab = ba \iff a \parallel b \quad (\text{vetores paralelos}) \quad (3.14)$$



Figura 3.2-4. Projeção de  $a$  sobre  $b$ .

e

$$ab = -ba \iff a \perp b \quad (\text{vetores ortogonais}). \quad (3.15)$$

### 3.2.2 Projeção e Reflexão

Consideremos dois vetores em  $\mathbb{R}^2$ ,  $a$  e  $b$ . Vamos calcular as componentes paralela e perpendicular de  $a$ , em relação a  $b$  (Figura 3.2-4).

Sejam  $a_{||}$  a componente de  $a$  paralela a  $b$  e  $a_{\perp}$  a componente de  $a$  perpendicular a  $b$ , onde  $\varphi$  é o ângulo entre  $a$  e  $b$ . Então,

$$a_{||} = |a| \cos \varphi \frac{b}{|b|} = |a||b| \cos \varphi \frac{b}{|b|^2}. \quad (3.16)$$

Como  $|a||b| \cos \varphi = \langle a|b \rangle$  e definindo o inverso de  $b$ ,  $b^{-1}$ , por

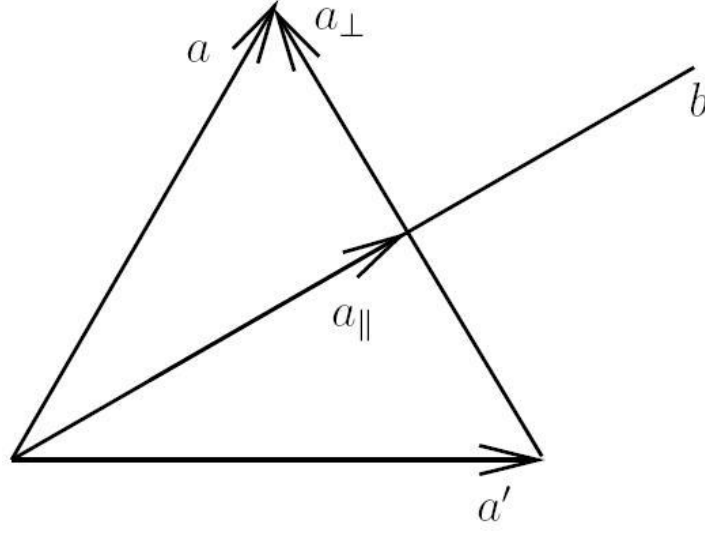
$$b^{-1} = \frac{b}{|b|^2}, \quad (3.17)$$

pois  $bb^{-1} = 1$ , obtemos

$$a_{||} = \langle a|b \rangle b^{-1}. \quad (3.18)$$

Com isso, temos ainda

$$a_{\perp} = a - a_{||} = a - \langle a|b \rangle b^{-1} = (ab - \langle a|b \rangle)b^{-1} = (a \wedge b)b^{-1}. \quad (3.19)$$



**Figura 3.2-5.** Reflexão de  $a$  sobre  $b$ .

Ou seja,

$$a_{\perp} = (a \wedge b)b^{-1}. \quad (3.20)$$

Agora, definindo um vetor  $a'$ , dado pela reflexão de  $a$  sobre  $b$  (Figura 3.2-5), teremos

$$a' = a_{||} - a_{\perp}. \quad (3.21)$$

Usando  $a_{||} = \langle a|b \rangle b^{-1}$  e  $a_{\perp} = (a \wedge b)b^{-1}$ , obtemos:

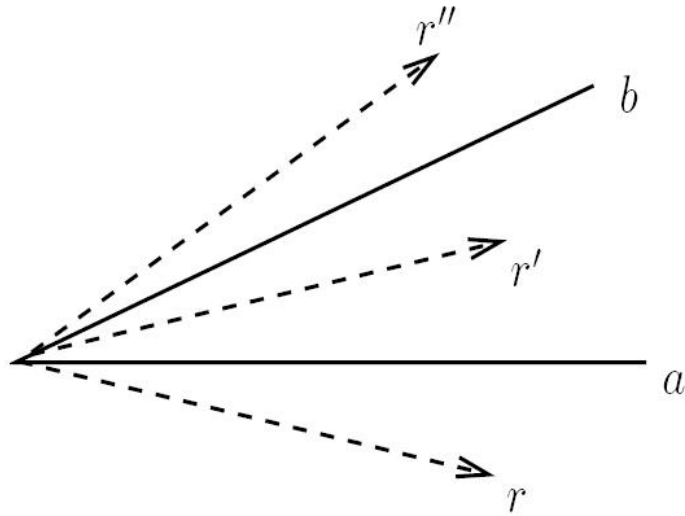
$$a' = \langle a|b \rangle b^{-1} - (a \wedge b)b^{-1} \quad (3.22)$$

$$= (\langle a|b \rangle - a \wedge b)b^{-1} \quad (3.23)$$

$$= (\langle b|a \rangle + b \wedge a)b^{-1} \quad (3.24)$$

$$= bab^{-1}. \quad (3.25)$$

A composição de duas reflexões de um vetor  $r$ , primeiro sobre  $a$  depois sobre  $b$ , é dada



**Figura 3.2-6.** Composição de reflexões.

por (Figura 3.2-6):

$$r \rightarrow r' = ara^{-1} \quad (3.26)$$

$$r' \rightarrow r'' = br'b^{-1}, \quad (3.27)$$

o que implica que

$$r'' = b(ara^{-1})b^{-1} \quad (3.28)$$

$$r'' = (ba)r(ba)^{-1} \quad (3.29)$$

Essa composição gera uma rotação de  $r$  de duas vezes o ângulo entre  $a$  e  $b$  (ver [11] p.13).

## Capítulo 4

# Reformulação do Algoritmo de Grover

### 4.1 Interpretação Geométrica dos Operadores

Para  $|v\rangle = \sum_{\substack{i=0 \\ i \neq i_0}}^{N-1} \alpha_i |i\rangle + \alpha_{i_0} |i_0\rangle$ , um vetor unitário qualquer, gerado pela base

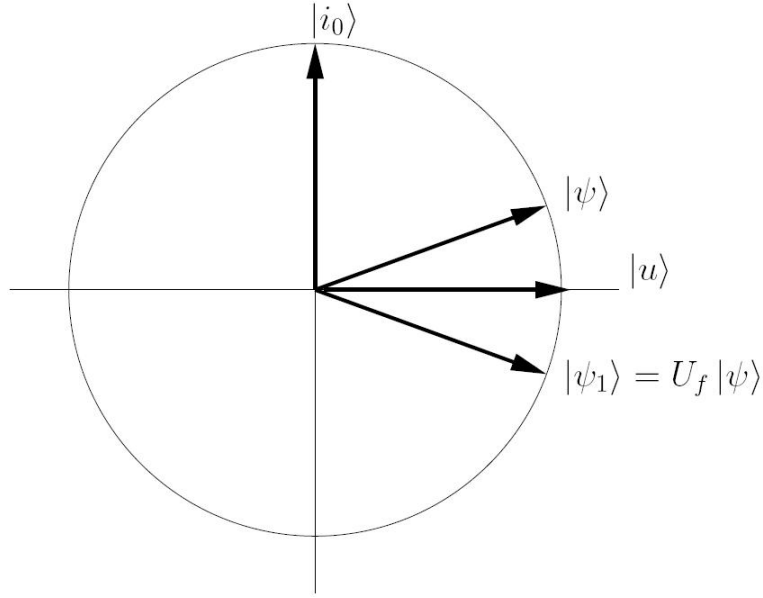
$$\{|0\rangle, \dots, |N-1\rangle\},$$

pode-se mostrar que (Capítulo 2):

$$U_f |v\rangle |-\rangle = \left( \sum_{\substack{i=0 \\ i \neq i_0}}^{N-1} \alpha_i |i\rangle - \alpha_{i_0} |i_0\rangle \right) |-\rangle. \quad (4.1)$$

Analisando bem esse resultado, podemos interpretar geometricamente a ação de  $U_f$  sobre o primeiro registrador. A aplicação de  $U_f$  sobre um vetor unitário qualquer, gerado pelos elementos da base computacional  $\{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$ , resulta numa reflexão desse vetor em relação ao subespaço ortogonal a  $|i_0\rangle$ , gerado por todos os outros elementos da base.

Para visualizar essa reflexão, podemos considerar que ela ocorre em relação à projeção de  $|v\rangle$  sobre o subespaço ortogonal a  $|i_0\rangle$  (Figura 4.1-1). Denotando o vetor unitário dessa



**Figura 4.1-1.** Ação do operador  $U_f$ .

projecção por  $|u\rangle$ , temos:

$$|u\rangle = \frac{1}{\sqrt{N-1}} \sum_{\substack{i=0 \\ i \neq i_0}}^{N-1} |i\rangle. \quad (4.2)$$

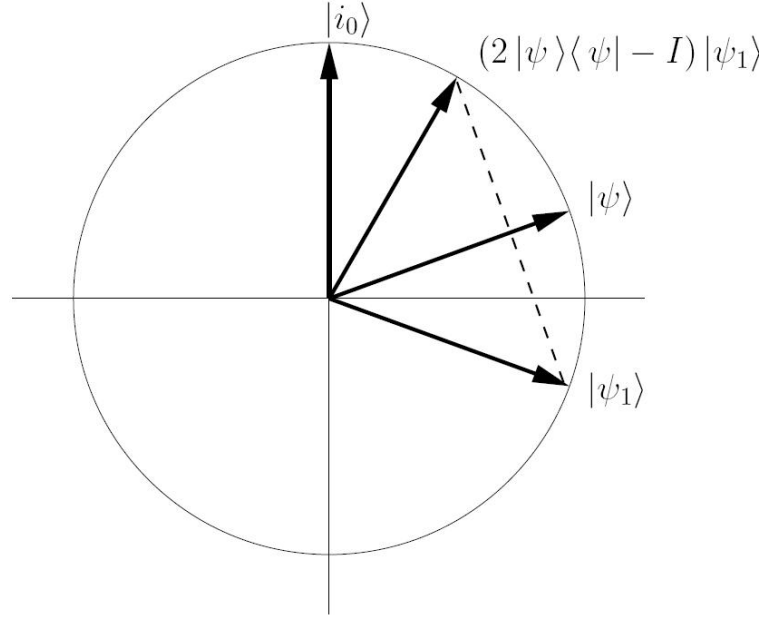
Para completar a visualização geométrica, vamos calcular os produtos internos entre  $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$  e  $|i_0\rangle$  e entre  $|u\rangle$  e  $|i_0\rangle$ :

$$\langle \psi | i_0 \rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \langle i | i_0 \rangle = \frac{1}{\sqrt{N}} \langle i_0 | i_0 \rangle = \frac{1}{\sqrt{N}}, \quad (4.3)$$

e

$$\langle u | i_0 \rangle = \frac{1}{\sqrt{N-1}} \sum_{\substack{i=0 \\ i \neq i_0}}^{N-1} \langle i | i_0 \rangle = 0. \quad (4.4)$$

Ou seja, o ângulo entre  $|\psi\rangle$  e  $|i_0\rangle$  é menor que  $\frac{\pi}{2}$  e o ângulo entre  $|u\rangle$  e  $|i_0\rangle$  é exatamente  $\frac{\pi}{2}$ .



**Figura 4.1-2.** Reflexão de  $|\psi_1\rangle$  em relação a  $|\psi\rangle$ .

Podemos escrever  $|u\rangle$  em função de  $|\psi\rangle$  e  $|i_0\rangle$ , com uma pequena manipulação em (4.2):

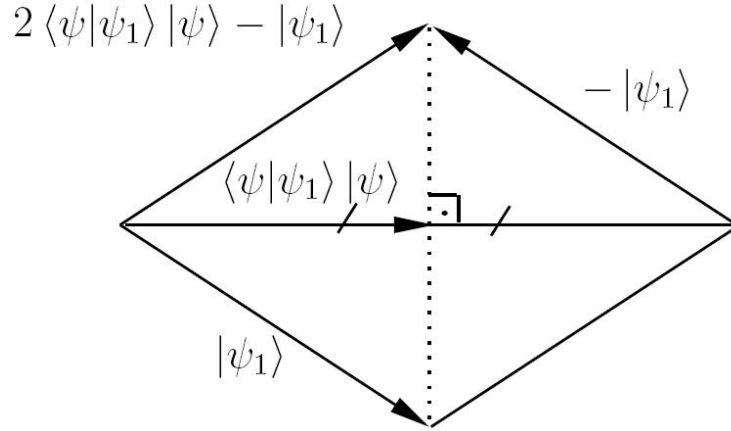
$$\begin{aligned} |u\rangle &= \frac{1}{\sqrt{N-1}} \sum_{\substack{i=0 \\ i \neq i_0}}^{N-1} |i\rangle \\ &= \frac{1}{\sqrt{N-1}} \left( \sum_{i=0}^{N-1} |i\rangle - |i_0\rangle \right) \\ &= \frac{1}{\sqrt{N-1}} \sum_{i=0}^{N-1} |i\rangle - \frac{1}{\sqrt{N-1}} |i_0\rangle. \end{aligned}$$

Ou seja,

$$|u\rangle = \frac{\sqrt{N}}{\sqrt{N-1}} |\psi\rangle - \frac{1}{\sqrt{N-1}} |i_0\rangle. \quad (4.5)$$

Agora, com os resultados de (4.3), (4.4), e (4.5), obtemos uma representação geométrica para a ação de  $U_f$ , através da Figura 4.1-1

Olhando a Figura 4.1-1, percebemos que se refletirmos  $|\psi_1\rangle$  em relação a  $|\psi\rangle$ , teremos um vetor “mais próximo” de  $|i_0\rangle$ , isto é, aumentaríamos a amplitude do elemento procurado  $|i_0\rangle$  em relação à sua amplitude no estado  $|\psi\rangle$  (Figura 4.1-2).



**Figura 4.1-3.** Reflexão de  $|\psi_1\rangle$  em relação a  $|\psi\rangle$ .

A projeção de  $|\psi_1\rangle$  sobre  $|\psi\rangle$  é dada por  $\langle\psi|\psi_1\rangle|\psi\rangle$ . A partir daí e observando a Figura 4.1-2, obteremos o operador que realiza essa reflexão e veremos que o vetor resultante da reflexão de  $|\psi_1\rangle$  em relação a  $|\psi\rangle$  é:

$$(2\langle\psi|\psi_1\rangle|\psi\rangle) - |\psi_1\rangle. \quad (4.6)$$

Usando propriedades dos produtos interno e externo, podemos reescrever a expressão acima:

$$(2\langle\psi|\psi_1\rangle|\psi\rangle) - |\psi_1\rangle = (2|\psi\rangle\langle\psi|)|\psi_1\rangle - |\psi_1\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle. \quad (4.7)$$

Dessa forma, o operador que realiza a ação sobre  $|\psi_1\rangle$  é dado por

$$2|\psi\rangle\langle\psi| - I, \quad (4.8)$$

que é justamente o segundo operador usado no Algoritmo de Grover.

## 4.2 Reescrevendo o Algoritmo de Grover

A partir de agora, não usaremos mais a notação de Dirac, para não causar inconsistências com a Álgebra Geométrica.

Inicialmente, definimos os vetores

$$\psi = \frac{1}{\sqrt{N}} \sum_{j=1}^N e_j \quad (4.9)$$

e

$$u = \frac{1}{\sqrt{N-1}} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j, \quad (4.10)$$

onde  $e_j$ ,  $j = 1, \dots, N$ , são os vetores da base canônica do  $\mathbb{R}^N$  e  $e_{i_0}$  é o vetor associado ao elemento procurado.

Como  $\psi$  e  $u$  são unitários,  $\psi = \psi^{-1}$  e  $u = u^{-1}$ . Usando a operação de reflexão apresentada em (3.25) e a interpretação geométrica dos operadores do algoritmo de Grover, dada na seção anterior, obtemos:

$$\psi_1 = u\psi u$$

e

$$\psi_G = \psi\psi_1\psi = \psi u\psi u\psi,$$

onde  $\psi_1$  e  $\psi_G$  são os vetores associados aos estados  $|\psi_1\rangle$  e  $|\psi_G\rangle$ .

Definindo  $g$  como o produto  $\psi u$ ,

$$g = \psi u, \quad (4.11)$$

e reescrevendo  $\psi_G$ , obtemos:

$$\psi_G = gg\psi = g^2\psi. \quad (4.12)$$

Ou seja, o produto  $gg$  está fazendo o “papel” do operador  $G$ . No lema abaixo, provamos que  $\psi_{G^k} = g^{2k}\psi$ ,  $\forall k \in \mathbb{N}$ , onde  $\psi_{G^k}$  é o vetor associado ao estado  $|\psi_{G^k}\rangle$ .

**Lema 5.**  $\psi_{G^k} = g^{2k}\psi$ ,  $\forall k \in \mathbb{N}$ .

*Prova.* Vamos demonstrar por indução. De (4.12),  $\psi_G = g^2\psi$ , isto é, o resultado é válido para  $k = 1$ . Agora, supomos que o resultado também seja válido para  $k = t$  e verificamos se vale para  $k = t + 1$ .

$$\psi_{G^{t+1}} = G\psi_{G^t} = g^2\psi_{G^t},$$



mas por hipótese,  $\psi_{G^t} = g^{2t}\psi$ . Então

$$\psi_{G^{t+1}} = g^2 g^{2t}\psi = g^{2(t+1)}\psi.$$

■

Obs: Na demonstração acima, note que definimos

$$G = g^2 \tag{4.13}$$

Usando essa definição, vamos obter  $G$  em função de  $N$  e dos elementos  $e_j$ .

De (4.9), (4.10) e (4.11), temos que:

$$\begin{aligned} g = \psi u &= \left( \frac{1}{\sqrt{N}} \sum_{j=1}^N e_j \right) \left( \frac{1}{\sqrt{N-1}} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \right) \\ &= \frac{1}{\sqrt{N}\sqrt{N-1}} (e_1 + \dots + e_{i_0} + \dots + e_N) (e_1 + \dots + e_{i_0-1} + e_{i_0+1} + \dots + e_N) \\ &= \frac{1}{\sqrt{N}\sqrt{N-1}} \left( \sum_{j \neq i_0}^N e_1 e_j + \dots + \sum_{j \neq i_0}^N e_{i_0} e_j + \dots + \sum_{j \neq i_0}^N e_N e_j \right) \\ &= \frac{1}{\sqrt{N}\sqrt{N-1}} \left[ (N-1) + \sum_{\substack{j=1 \\ j \neq i_0}}^N e_{i_0} e_j \right]. \end{aligned}$$

Ou seja,

$$g = \frac{1}{\sqrt{N}\sqrt{N-1}} \left[ (N-1) + e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \right]. \tag{4.14}$$

Calculando agora  $g^2$ , obtemos:

$$\begin{aligned}
g^2 &= \frac{1}{\sqrt{N}\sqrt{N-1}}[(N-1) + e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j] \frac{1}{\sqrt{N}\sqrt{N-1}}[(N-1) + e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j] \\
&= \frac{1}{N(N-1)}[(N-1)^2 + 2(N-1)e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j + \underbrace{(e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j)^2}_{=-(N-1)}] \\
&= \frac{N-1}{N} + \frac{2}{N}e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j - \frac{1}{N} \\
&= \frac{N-2}{N} + \frac{2}{N}e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j.
\end{aligned}$$

Ou seja,

$$\boxed{g^2 = G = \frac{N-2}{N} + \frac{2}{N}e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j} \quad (4.15)$$

$$\begin{aligned}
(*) \quad (e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j)^2 &= e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \\
&= -(e_{i_0})^2 \left( \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \right)^2 \\
&= -1(N-1) = -(N-1) \quad \text{de (3.5) e (3.14)}. \quad (4.16)
\end{aligned}$$

## 4.3 Exemplos

### 4.3.1 Exemplo $N = 4$

Como vimos na página 17, para esse valor de  $N$ , apenas uma aplicação de  $G$  nos retorna o elemento procurado com probabilidade de 100%. Ou seja,

$$k = \frac{\arccos(\frac{1}{\sqrt{4}})}{\arccos(\frac{4-2}{4})} = 1.$$

Para  $N = 4$ , (4.15) nos fornece:

$$G = \left( \frac{1}{2} + \frac{1}{2} e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^4 e_j \right).$$

Desenvolvendo, teremos:

$$\begin{aligned} G\psi &= \frac{1}{2}\psi + \frac{1}{2}e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^4 e_j \left( \sum_{\substack{j=1 \\ j \neq i_0}}^4 e_j + e_{i_0} \right) \frac{1}{\sqrt{4}} \\ &= \frac{1}{2}\psi + \frac{1}{4}e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^4 e_j \sum_{\substack{j=1 \\ j \neq i_0}}^4 e_j + \frac{1}{4} \sum_{\substack{j=1 \\ j \neq i_0}}^4 e_{i_0} e_j e_{i_0} \\ &\quad \underbrace{\hspace{10em}}_{\frac{1}{4}e_{i_0} \cdot 3} \\ &= \frac{1}{2}\psi + \frac{3}{4}e_{i_0} - \frac{1}{4} \sum_{\substack{j=1 \\ j \neq i_0}}^4 \underbrace{e_{i_0} e_{i_0}}_{=1} e_j \\ &= \frac{1}{2}\psi + \frac{3}{4}e_{i_0} - \frac{1}{2} \left( \psi - \frac{1}{2}e_{i_0} \right) \\ &= \frac{4}{4}e_{i_0} = e_{i_0}. \end{aligned}$$

Fazendo uma medida desse estado, obtemos o elemento procurado com probabilidade de 100%.

### 4.3.2 Exemplo $N = 8$

Será utilizado o exemplo da Seção 3.4 de [15], onde

$$|i_0\rangle = |101\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \stackrel{\text{def}}{=} |5\rangle.$$

Como vimos,  $|i_0\rangle$ , nesse caso, será equivalente a  $e_6$ . Para vermos quantas vezes devemos aplicar  $G$ , calculamos  $k$  novamente como em (2.3), ou seja,

$$k = \frac{\arccos(\frac{1}{\sqrt{8}})}{\arccos(\frac{8-2}{8})} \cong 1,67,$$

o que implica que devemos aplicar  $G$  duas vezes. Aplicando  $G$  a primeira vez:

$$G\psi = \psi_G = \left( \frac{N-2}{N} + \frac{2}{N} e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \right) \psi \quad (4.17)$$

$$= \left( \frac{6}{8} + \frac{2}{8} e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^8 e_j \right) \frac{1}{\sqrt{8}} \left( \sum_{\substack{j=1 \\ j \neq i_0}}^8 e_j + e_{i_0} \right) \quad (4.18)$$

$$= \frac{6}{8} \psi + \frac{2}{8\sqrt{8}} e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^8 e_i \sum_{\substack{j=1 \\ j \neq i_0}}^8 e_i + \frac{2}{8\sqrt{8}} \sum_{\substack{j=1 \\ j \neq i_0}}^8 e_{i_0} e_i e_{i_0} \quad (4.19)$$

$$= \frac{6}{8} \psi + \frac{2}{8\sqrt{8}} 7e_{i_0} - \frac{2}{8\sqrt{8}} \sum_{\substack{j=1 \\ j \neq i_0}}^8 e_j \quad (4.20)$$

$$= \frac{4}{8} \psi + \frac{16}{8\sqrt{8}} e_{i_0} \quad (4.21)$$

$$= \frac{\psi}{2} + \frac{2}{\sqrt{8}} e_{i_0}, \quad (4.22)$$

onde a amplitude de  $e_{i_0}$  é  $\frac{5}{2\sqrt{8}}$ , o que nos dá uma probabilidade de aproximadamente 78% de obtermos o elemento procurado. Aplicamos, então,  $G$  pela segunda vez:

$$\begin{aligned}
G\psi_G &= G\left(\frac{1}{2}\psi\right) + G\left(\frac{2}{\sqrt{8}}e_{i_0}\right) \\
&= \frac{1}{2}\psi_G + \frac{2}{\sqrt{8}}Ge_{i_0} \\
&= \frac{1}{2}\psi_G + \frac{2}{\sqrt{8}}\left(\frac{N-2}{N} + \frac{2}{N}e_{i_0}\sum_{\substack{j=1 \\ j \neq i_0}}^N e_j\right)e_{i_0} \\
&= \frac{1}{2}\psi_G + \frac{2}{\sqrt{8}}\left(\frac{6}{8}e_{i_0} + \frac{2}{8}e_{i_0}\sum_{\substack{j=1 \\ j \neq i_0}}^N e_j e_{i_0}\right) \\
&= \frac{1}{2}\psi_G + \frac{2}{\sqrt{8}}\left(\frac{6}{8}e_{i_0} - \frac{2}{8}\sum_{\substack{j=1 \\ j \neq i_0}}^N e_j\right) \\
&= \frac{1}{2}\psi_G + \frac{2}{\sqrt{8}}\left(\frac{6}{8}e_{i_0} - \frac{2}{8}\left(\sum_{j=1}^N e_j - e_{i_0}\right)\right) \\
&= \frac{1}{4}\psi + \frac{1}{\sqrt{8}}e_{i_0} - \frac{4}{8}\psi + \left(\frac{12}{8\sqrt{8}} + \frac{4}{8\sqrt{8}}\right)e_{i_0} \\
&= \frac{-1}{4}\psi + \frac{3}{\sqrt{8}}e_{i_0}.
\end{aligned}$$

Logo,

$$\psi_{G^2} = \frac{-1}{4}\psi + \frac{3}{\sqrt{8}}e_{i_0}. \quad (4.23)$$

Esse resultado mostra que a amplitude de  $e_{i_0}$  agora é  $\frac{-1}{4\sqrt{8}} + \frac{3}{\sqrt{8}} = \frac{11}{4\sqrt{8}}$ , e a probabilidade de termos encontrado o elemento passa a ser  $\left|\frac{11}{4\sqrt{8}}\right|^2 = 94,53\%$ , o mesmo resultado que aparece em [15].

#### 4.4 Forma geral para $G^k$ e $G^k\psi$

Nesta seção, encontramos uma expressão geral para  $G^k$ , onde  $k$  é o número de iterações que o algoritmo deve realizar. O operador  $G$ , como vimos, é definido como

$$G = \frac{N-2}{N} + \frac{2}{N}e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j. \quad (4.24)$$

Para simplificar o desenvolvimento, faremos a seguinte identificação:

$$\frac{N-2}{N} = A, \quad \frac{2}{N} = B, \quad e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j = X.$$

Os elementos  $A$  e  $B$  são números reais, a dificuldade está no elemento  $X$ . Vamos ver o que acontece quando mudamos a potência de  $X$ :

$$\begin{aligned} X^2 &= (e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j)^2 = -(N-1) = 1-N \quad \text{de (4.16)} \\ X^3 &= (1-N)X, \\ X^4 &= (1-N)^2, \\ X^5 &= (1-N)^2X, \end{aligned}$$

e assim sucessivamente. Portanto, temos

**Lema 6.** *Para todo  $i \in \mathbb{N}$ , temos*

$$X^{2i} = (1-N)^i \quad (4.25)$$

$e$

$$X^{2i+1} = (1 - N)^i X \quad (4.26)$$

$$= (1 - N)^i e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j. \quad (4.27)$$

*Prova.* A demonstração de (4.25) é por indução. Para  $i = 1$ , como já vimos, temos  $X^2 = 1 - N$ . Suponhamos que seja válido para  $i = k$ , e provamos que é válido para  $i = k + 1$ .

$$\begin{aligned} X^{2(k+1)} &= X^{2k} X^2 \\ X^{2(k+1)} &= (1 - N)^k (1 - N) \quad (\text{pela hipótese de indução}) \\ X^{2(k+1)} &= (1 - N)^{k+1}. \end{aligned} \quad (4.28)$$

Portanto a equação (4.25) é válida e (4.26) segue imediatamente desse resultado.  $\blacksquare$

Considerando  $G = A + BX$ ,  $G^k$  é dado por:

$$G^k = (A + BX)^k = \sum_{r=0}^k \binom{k}{r} A^{k-r} B^r X^r. \quad (4.29)$$

Obtemos então

$$G^k = \sum_{r=0}^{\lfloor \frac{k}{2} \rfloor} \left[ \binom{k}{2r} A^{k-2r} B^{2r} (1 - N)^r + \binom{k}{2r+1} A^{k-(2r+1)} B^{2r+1} (1 - N)^r X \right], \quad (4.30)$$

onde  $\lfloor x \rfloor$  representa a função “maior inteiro menor ou igual a  $x$ ”.

Substituindo os valores de  $A$ ,  $B$  e  $X$ , obtemos finalmente:

$$G^k = \sum_{r=0}^{\lfloor \frac{k}{2} \rfloor} \left[ \binom{k}{2r} \left( \frac{N-2}{N} \right)^{k-2r} \left( \frac{2}{N} \right)^{2r} (1-N)^r + \binom{k}{2r+1} \left( \frac{N-2}{N} \right)^{k-(2r+1)} \left( \frac{2}{N} \right)^{2r+1} (1-N)^r e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \right]. \quad (4.31)$$

Agora, vamos encontrar o estado resultante de  $k$  aplicações de  $G$ ,  $G^k\psi$

$$G^k\psi = \sum_{r=0}^{\lfloor \frac{k}{2} \rfloor} \left[ \binom{k}{2r} \left( \frac{N-2}{N} \right)^{k-2r} \left( \frac{2}{N} \right)^{2r} (1-N)^r + \binom{k}{2r+1} \left( \frac{N-2}{N} \right)^{k-(2r+1)} \left( \frac{2}{N} \right)^{2r+1} (1-N)^r e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \right] \psi. \quad (4.32)$$

Para  $\psi = \frac{1}{\sqrt{N}} \sum_{j=1}^N e_j$ , teremos

$$G^k\psi = \sum_{r=0}^{\lfloor \frac{k}{2} \rfloor} \left[ \binom{k}{2r} \left( \frac{N-2}{N} \right)^{k-2r} \left( \frac{2}{N} \right)^{2r} (1-N)^r \frac{1}{\sqrt{N}} \sum_{j=1}^N e_j + \binom{k}{2r+1} \left( \frac{N-2}{N} \right)^{k-(2r+1)} \left( \frac{2}{N} \right)^{2r+1} (1-N)^r \frac{1}{\sqrt{N}} e_{i_0} \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \sum_{l=1}^N e_l \right]. \quad (4.33)$$



Logo,

$$G^k\psi = \sum_{r=0}^{\lfloor \frac{k}{2} \rfloor} \left[ \binom{k}{2r} \left( \frac{N-2}{N} \right)^{k-2r} \left( \frac{2}{N} \right)^{2r} (1-N)^r \frac{1}{\sqrt{N}} \sum_{j=1}^N e_j \right. \\ \left. + \binom{k}{2r+1} \left( \frac{N-2}{N} \right)^{k-(2r+1)} \left( \frac{2}{N} \right)^{2r+1} (1-N)^r \frac{1}{\sqrt{N}} \left( (N-1)e_{i_0} - \sum_{\substack{j=1 \\ j \neq i_0}}^N e_j \right) \right]. \quad (4.34)$$

Essa expressão ainda pode ser escrita como

$$G^k\psi = \sum_{r=0}^{\lfloor \frac{k}{2} \rfloor} \left[ \binom{k}{2r} \left( \frac{N-2}{N} \right)^{k-2r} \left( \frac{2}{N} \right)^{2r} (1-N)^r \psi \right. \\ \left. + \binom{k}{2r+1} \left( \frac{N-2}{N} \right)^{k-(2r+1)} \left( \frac{2}{N} \right)^{2r+1} (1-N)^r \left( \frac{N}{\sqrt{N}} e_{i_0} - \psi \right) \right]. \quad (4.35)$$

Refazendo o exemplo  $N = 8$  usando (4.35), teremos

$$G^2\psi = \binom{2}{0} \left( \frac{6}{8} \right)^2 \psi + \binom{2}{1} \left( \frac{6}{8} \right) \left( \frac{2}{8} \right) \left( \frac{8}{\sqrt{8}} e_{i_0} - \psi \right) + \binom{2}{2} \left( \frac{2}{8} \right)^2 (-7)\psi \\ = \left( \frac{36}{64} - \frac{24}{64} - \frac{28}{64} \right) \psi + \frac{24}{8\sqrt{8}} e_{i_0} \\ = -\frac{1}{4} \psi + \frac{3}{\sqrt{8}} e_{i_0},$$

o mesmo resultado obtido em (4.23).

# Capítulo 5

## Conclusão

Neste trabalho apresentamos uma nova alternativa de leitura do Algoritmo de Grover, através de conceitos da Álgebra Geométrica, motivados pela interpretação geométrica de cada operador envolvido.

Os principais resultados da dissertação são descritos no Capítulo 4, onde reescrevemos o algoritmo, usando uma linguagem e uma notação alternativas ao uso da notação de Dirac e da linguagem da mecânica quântica. Descrevemos as operações do algoritmo, essencialmente através de operações de reflexão da Álgebra Geométrica, operações representadas de forma simples por produtos de vetores. Com a notação da mecânica quântica, a expressão para o operador de Grover  $G$  é

$$G = (2|\psi\rangle\langle\psi| - I) \otimes I)U_f,$$

onde  $|\psi\rangle$  é a superposição inicial dos estados da base. Com a notação da Álgebra Geométrica essa expressão pode se reduzir a

$$G = (\psi u)^2,$$

onde  $\psi$  representa o estado inicial do primeiro registrador e  $u$  o vetor unitário da projeção de  $\psi$  sobre o subespaço ortogonal a  $e_{i_0}$ , vetor que representa a solução do problema de busca. Na Seção 4.2 essa expressão foi escrita em função de  $N$  (o tamanho da lista) e dos elementos da base, e é representada pela soma de escalar e um bivector.

## Conclusão

---

Outros resultados importantes apresentados nesta dissertação são as expressões gerais para os elementos  $G^k$  e  $G^k\psi$ . O objetivo era reduzir o trabalho de aplicar sucessivamente o operador  $G$ , e já ter uma expressão pronta para o estado resultante de  $k$  iterações do algoritmo. As deduções dessas expressões foram detalhadas na Seção 4.4 e elas são escritas em função apenas do tamanho da lista ( $N$ ), do números de vezes que  $G$  é aplicado ( $k$ , que depende de  $N$ ) e dos vetores da base. Através dessas expressões, foi possível resolver novamente o problema para  $N = 8$  (resolvido na seção 4.3) de forma mais rápida e direta.

# Referências Bibliográficas

- [1] T.M. Apostol, *Calculus*, volume I, John Wiley & Sons (1967).
- [2] G. Benenti, G. Casati, e G. Strini, *Principles of Quantum Computation and Information*, volume I, World Scientific (2004).
- [3] C.H. Bennett, E. Bernstein, G. Brassard, e U. Vazirani, Strengths and weaknesses of quantum computing, *SIAM Journal on Computing*, **26** (1997), 1510–1523.
- [4] M. Boyer, G. Brassard, P. Hoyer, e A. Tapp, Tight bounds on quantum searching, *Fortschritte der Physik*, **46** (1998), 493–505.
- [5] L.K. Grover, A fast quantum mechanical algorithm for database search, em *Proc. 28th Annual ACM Symposium on the Theory of Computing* (1996), 212–219.
- [6] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Physical Review Letters*, **79** (1997), 325–328.
- [7] D. Hestenes e G. Sobczyk, *Clifford Algebra to Geometric Calculus: A Unified Language for Mathematics and Physics*, D. Reidel Pub. Co., Dordrecht (1987).
- [8] M. Hirvensalo, *Quantum Computing*, Springer, New York (2001).
- [9] R. Josza, *Searching in Grover's Algorithm*, quant-ph/9901021, (1999).
- [10] A.Y. Kitaev, A. Shen, e M. Vyalyi, *Classical and Quantum Computing*, American Mathematical Society (2002).
- [11] P. Lounesto, *Clifford Algebras and Spinors*, Cambridge University Press, Cambridge, 1997.

- [12] M.A. Nielsen e I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (2000).
- [13] C. H. Papadimitriou, *Complexity Theory*, Addison Wesley Pub. Co., Massachusetts (1994).
- [14] A.O. Pittenger, *An Introduction to Quantum Computing Algorithms*, Birkhäuser, Boston (1999).
- [15] R. Portugal, C. Lavor, L.M. Carvalho, e N. Maculan, *Uma Introdução à Computação Quântica*, 2ªEd., Notas em Matemática Aplicada 8, SBMAC (2005).
- [16] J. Preskill, *Quantum information and computation*, Lecture Notes, California Institute of Technology (1998).