Projecto de Licenciatura do 5º Ano

Departamento de Engenharia Informática

Instituto Superior de Engenharia do Porto

Projecto realizado pelo Aluno:

980340 Mário Sousa

Turma 5CD

Computação Quântica

Índice

Índice Tabelas

Índice Figuras

Prefácio

A dissipação de calor dos processadores está relacionada com a perda de informação, que ocorre durante os processos computacionais.
A termodinâmica da computação explica o porquê desta dissipação.
Segue-se o trabalho de investigação, que explica os fundamentos físicos para o aparecimento da *computação quântica*, e a sua aplicação prática.

Capítulo I – Introdução

A palavra "Informática", foi criada em 1962 pelo francês Philippe Dreifus, e advém da conjugação de duas palavras: "**Infor**mação" e "Auto**mática**".
A informática é o conjunto de conhecimentos e técnicas ligadas ao processamento automático da informação.
Na base de todas as áreas que permitem o processamento automático da informação, está a *Computação*.

É sobre esta área que vou falar nos próximos capítulos, e que sem esta nada do que é feito através de computadores, seria possível.

Capítulo II – Teoria da Informação

Em 1948 *Claude Shannon*[1] publicou o trabalho: "A Mathematical Theory of Comunication", no qual se destaca a ***Teoria da Informação***.
Esta teoria revolucionou o mundo das telecomunicações.

[1] Claude Shannon[1916-2001] – Matemático americano, que publica um trabalho em 1948 sobre comunicação de informação, que revolucionou o mundo das telecomunicações – "A Mathematical Theory of Comunication".

Princípios da Teoria da Informação

A informação, é algo que pode ser expresso de várias formas.

As frases "o objectivo deste projecto é compreender a computação quântica" e "the objective of this project is to understand quantum computation", têm algo em comum.
Ambas dizem exactamente o mesmo, contudo as regras gramaticais da língua em que foram escritas são totalmente distintas.

Elas partilham algo, que é chamado de **conteúdo da informação**.

Num computador, a informação é guardada e processada através de números, nomeadamente através do código ASCII[2].
O código ASCII standard, atribui a cada número[3] um determinado caracter.

Através do código ASCII, a frase "o objectivo deste projecto é compreender a computação quântica", assume a seguinte forma:

ASCII	111	111	98	106	101	99	116	105	118	112	...
Caracter	o	o	b	j	e	c	t	i	v	o	...

Os números por sua vez, são representados através de uma sequência de dígitos binários[4], ou seja através de uma sequência de *0's* ou *1's*.

Seja qual for a forma de representação da informação, todas têm algo em comum.

---

[2] ASCII - American Standard Code Information Interchange. Pode consultar o Anexo IV, para verificar a atribuição dada para os caracteres alfanuméricos.

[3] Entre 0 e 127.

[4] Em inglês: *binary digit*, mais conhecido como **bit**. Pode consultar o Anexo IV, para verificar a sequência de bits utilizada para representar uma sequência numérica de 0 a 20.

Todas utilizam processos físicos para o fazerem.
As palavras quando ditas, são possíveis devido à variação da pressão atmosférica. Quando escritas são possíveis devido ao contacto das moléculas de tinta, com o papel. Quando pensadas são possíveis devido á interacção dos nossos neurónios.

Processo transmissão

O processo de transmissão de informação requer três fases:

1ª Fase

É conhecida como p*reparação*, na qual é identificado o contexto da comunicação, e o que significa cada sequência de bits.
O significado da sequência de bits é conhecida como "*código*".

2ª Fase

Envolve a *comunicação*. Fase em que a sequência de bits é enviada para o receptor.
A sequência de bits, é conhecida como "*dados"*.

3ª Fase

Envolve a *recepção* dos *dados*, e a *descodificação* da sequência de bits, para obter o conteúdo da informação.

Aspectos mais importantes a reter sobre a teoria da informação:

- Independentemente do processo físico que representa a informação, o bit é o nível de abstracção ideal para a representar;
- Após a *descodificação* bit(s)-significado, obtém-se o *conteúdo da informação*;

- A quantidade de informação necessária para transmitir essa mesma informação, é obtida por $\log_2 n = x$, uma vez que $2^x = n$, ou seja $\log_2 n$ **bits**[1];
- Tal como qualquer processo de comunicação, a transmissão de informação está sujeita a erros(que podem ser minimizados):
  - durante a codificação;
  - durante a transmissão;
  - durante a recepção.
- A Informação pode ser transmitida de um local para outro;
- A Informação pode ser guardada e lida/obtida mais tarde;

Capítulo III – Computação Clássica

Recorda-se neste capítulo, os princípios básicos da computação dos computadores actuais.

A Máquina de Turing

A Máquina de Turing(MT), foi inventada por *Alan Turing*[5] em 1936 numa tentativa de criar um calculador universal.

O princípio de funcionamento desta máquina é a base para a forma como os processadores actuais processam a informação.

Uma MT, é conhecida como uma máquina finita de estados(MFE).

Elementos

- Conjunto finito de estados $S = \{s_1, s_2, s_3, ..., s_s; s_{s+1} = s_{parar}\}$;
- Alfabeto finito $A = \{a_1, a_2, a_3, ..., a_s; a_{s+1} = vazio\}$;
- Conjunto finito de instruções $I = \{i_1, i_2, i_3, ..., i_i\}$.

---

[5] Alan Turing[1912-1954]–Matemático inglês que com a criação da Máquina de Turing, criou a base para o processamento de informação dos computadores actuais.

O estado si , corresponde a um determinado estado funcional da máquina. A MT está apenas num destes estados, num determinado instante temporal.

Existe um estado em que nenhuma instrução é executada. Esse estado é o estado *parar(* S_{parar} *)*.

Os símbolos do alfabeto, servem para codificar a informação que é processada pela máquina:

- Dados de input;
- Resultados de operações intermédias;
- Dados de output

O símbolo *vazio*, é utilizado para separar strings de dados, do resto dos símbolos do alfabeto.

As instruções são associadas aos estados de S . Estas identificam a acção que a MT vai efectuar se estiver num determinado estado, e qual o estado em que a MT vai estar após terminar a sua execução.

Componentes

A MT é constituída por três componentes, que utiliza os três elementos descritos da seguinte forma:

- Uma fita infinita externa à máquina, que pode ser trabalhada em ambos os lados, e que está dividida em células. Cada célula contém apenas um símbolo $ai \in A$;
- Uma cabeça de leitura/escrita que pode ler ou escrever um símbolo $ai \in A$, em cada célula da fita;
- Uma unidade de controlo que controla a leitura/escrita da cabeça, baseado no estado actual da máquina, e no conteúdo da célula que está a ser lida pela cabeça. O controlo é feito através do par (si, ai);

A cabeça é capaz efectuar uma das seguintes acções:

- Escrever ou apagar na célula que está a ser *trabalhada*.
- Mudar o estado interno da máquina.
- Mover a cabeça para a esquerda ou direita. Crie-se a notação $y \in \{E, D\}$, para descrever o movimento da cabeça.

O comportamento da MT, é condicionado pelo conjunto de instruções. As instruções descrevem a transição de um estado inicial (si, ai), para um estado final (sf, af), acrescido de um movimento da cabeça.

Cada instrução $i \in I$, é representada pelo tuplo $[(si, ai), (sf, af; y)]$, que por sua vez representa a seguinte transição:

$$I \ni i : (si, ai) \text{®} (sf, af; y)$$

Utilização de uma MT

Considere-se o funcionamento da MT, através de um processamento que "parece" imediato quando executado pelos computadores actuais:

A Soma de duas variáveis: $n1 + n2$**.**

Preparação:

Para representar a variável $n1$ e $n2$ na fita da MT, atribui-se uma string de 1's para representar o valor numérico de $n1$, seguido de um 0, seguido de uma string de 1's para representar o valor numérico da variável $n2$.

Se $n1 = 2$ e $n2 = 2$, então a fita de input teria o seguinte aspecto: 00000110110000

Sequência Operações:

1. Retira-se o 1 que está mais á esquerda da fita;
2. Move-se a cabeça para a direita até encontrar o primeiro 0(que funciona aqui como o símbolo *vazio*)
3. Substitui-se o 0 por 1.
4. Para-se a execução da máquina.

Aplicando este algoritmo, teríamos a seguinte fita de output: 00000011110000, que representa 4 ($4*1=4$).

A figura seguinte, mostra a relação entre estado-símbolo, e os movimentos da MT, durante o algoritmo anterior:

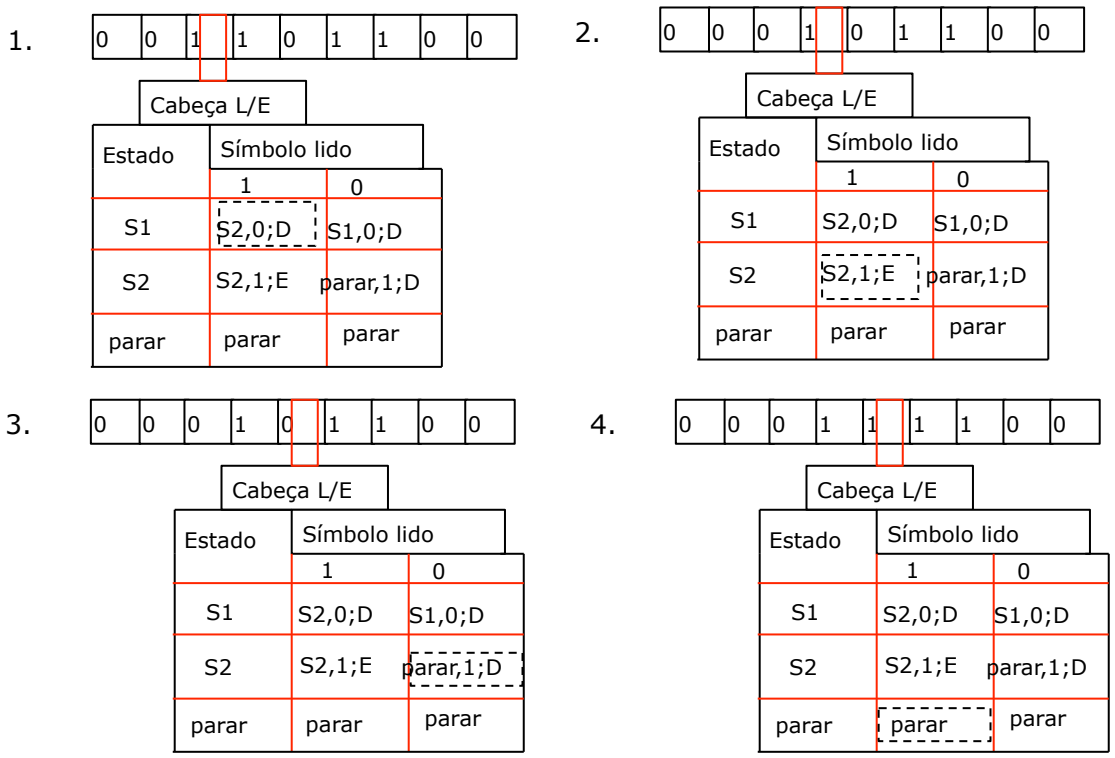


Figura 1 – Relação estado-símbolo da MT

A MT apesar de ser uma máquina teórica extremamente funcional, não é de todo prática, para efectuar o processamento de informação nos computadores actuais. Quer pelo seu tamanho, quer pela demora na produção de resultados.

O princípio funcional de uma MT(máquina de estados, para processar informação), é implementado actualmente através de circuitos electrónicos, que produzem o mesmo resultado[6], a uma velocidade superior, e ocupam muito menos espaço.

O Bit Matemático

O Bit, como já pôde verificar é muito simples. Tem apenas dois valores possíveis.
A matemática que é utilizada para manipular bits é conhecida como *Álgebra de Boole*, criada pelo matemático *George Boole*[7].
A álgebra é um ramo da matemática, que trabalha com variáveis que podem assumir um determinado conjunto de valores.
No caso da álgebra de boole, os valores possíveis são apenas dois: 0 e 1.

Existem quatro funções booleanas[8] para processar um valor booleano:

1. *IDENTITY*, que retorna o valor que foi enviado para a função;
2. *NOT*, que nega o valor enviado para a função;
3. *ZERO*, que devolve sempre 0;
4. *ONE*, que devolve sempre 1;

As cinco funções booleanas mais conhecidas, e as mais utilizadas no mundo da computação, recebem como argumento dois valores booleanos:

x	$f(x)$				
Argumento	AND	NAND	OR	NOR	XOR
00	0	1	0	1	0

[6] Esta equivalência foi demonstrada pelo teorema: "Máquinas de Turing e famílias de circuitos uniformes", ao longo de vários anos, por vários matemáticos.

[7] George Boole[1815-1864] – Matemático inglês que durante os seus estudos sobre lógica, introduz a álgebra de boole.

[8] As funções booleanas, quando aplicadas na informática para o processamento dos bits, são conhecidas como **operadores lógicos**, ou para utilizar a nomenclatura inglesa: **Boolean Gates**.

01	0	1	1	0	1
10	0	1	1	0	1
11	1	0	1	0	0

Tabela 1- Funções Booleanas sobre 2 bits

O funcionamento destes operadores lógicos é importante para compreender uma das razões para o aparecimento da computação quântica, que por motivos de disposição estrutural está descrito no Anexo I.

O Bit Físico/Clássico

Para que a informação possa ser processada, esta tem que ter uma forma física.

Nos computadores actuais, são utilizados *transístores*[9].

À organização destes transístores, dá-se o nome de ***chip de silício*** ou ***circuitos integrados***, e além de persistirem o valor do bit, permitem também a implementação física dos operadores lógicos[8].

Rapidez no Processamento

A rapidez de processamento de um computador, tem vindo a duplicar em cada 2 anos[10]. Esta rapidez deve-se à diminuição do tamanho dos transístores.

Com a diminuição de tamanho, o tempo de comunicação entre transístores diminui, e aumenta o número de operações lógicas que um processador consegue executar em cada instante temporal.

---

[9] Os transístores, são feitos a partir de semicondutores. O semicondutor é um material que não é um bom condutor de electricidade, nem um bom isolador. Actualmente o mais comum é o silicone. Este material, é manipulado, para permitir a ausência/presença de electrões para guardar os dois valores possíveis do bit – 0 ou 1.

[10] Este valor está relacionado com a célebre "Lei de Moore".

Segundo Gordon Moore[11], o Homem, vai chegar aos limites da miniaturização dos chips de silício através da *física macroscópica*[12] em 2017.
Vamos ver o porquê desta afirmação.

Capítulo IV –Porquê Computação Quântica?

Com a diminuição do tamanho dos componentes que constituem os chips, deparamo-nos com dois problemas que têm que ser contornados para que a capacidade de processamento dos processadores continue a crescer:

1. O Homem vai necessitar de manipular estruturas atómicas, para construir os circuitos integrados. Para isso tem que recorrer a outro conjunto de leis. Essas leis são definidas pela *física quântica*.
2. A densidade de calor que é dissipada pelos chips, aumenta com a diminuição do tamanho dos componentes. Esta dissipação influencia a transmissão de corrente eléctrica, e deteriora os materiais que constituem os chips.

O problema mais preocupante é o 2º.

Nos próximos capítulos, explica-se a razão principal dessa dissipação, e a melhor forma de minimizar os danos causados pela mesma.

Reversibilidade, Termodinâmica, Entropia, Energia Dissipada, Processamento de Informação

[11] Gordon Moore[1929-], presidente da Intel Corporation, afirmou em 1965, altura em que foram descobertos os circuitos integrados, que o crescimento do número de transístores num circuito integrado seria exponencial de 2 em 2 anos.

[12] A utilização do termo *física macroscópica*, serve para realçar o facto de estarem a ser utilizados materiais constituídos por átomos na construção dos circuitos integrados.

O conceito de reversibilidade é importante para perceber a relação entre a dissipação de calor e o processamento de informação.
Distinga-se o conceito de reversibilidade entre dois tipos de processos, que estão envolvidos no processamento de informação:

1. Processos Lógicos
   - Todos os processos matemáticos que permitem o processamento de informação.
2. Processos Físicos
   - Todos os processos físicos que permitem implementar os processos lógicos.

Reversibilidade de Processos Lógicos

Um processo lógico reversível, é aquele que a partir do estado final é possível determinar o seu estado inicial.
No caso da computação, existem operadores lógicos irreversíveis. A irreversibilidade lógica, leva à perda de bits durante o seu funcionamento[13].

Reversibilidade Processos Físicos

O conceito de reversibilidade de processos físicos, e a relação entre a física e a informática, levou-me a estudar a área da termodinâmica. Para perceber a sua definição de reversibilidade, é necessário explicar mais alguns conceitos.

Termodinâmica

A termodinâmica é uma área da física que estuda o comportamento da energia em sistemas fechados[14].

[13] Para verificar esta irreversibilidade, consulte o Anexo I.

[14] Entenda-se sistema fechado, como um sistema sem qualquer acção do exterior.

O alvo do estudo da termodinâmica são: moléculas de gases ou átomos de uma substância, e relaciona as interacções entre cada elemento do sistema, como por exemplo: volume, pressão, temperatura, entre outros.

Destes estudos resultam três leis, que no âmbito deste projecto apenas interessa explicar duas.

1ª Lei da Termodinâmica:

Princípio da 1ª lei da termodinâmica:
Princípio da Conservação de Energia.

Este princípio refere o seguinte:
A energia de um sistema fechado não pode aumentar nem diminuir. Esta é transferida de um sistema para o outro.

[Para processos irreversíveis: $dE = dQ - dW$ *]*

[Para processos reversíveis: $dE = TdS - PdV$ *]*

2ª Lei da Termodinâmica:

Princípio da 2ª lei da termodinâmica:
A ***entropia*** *de um sistema fechado nunca pode diminuir ao longo do tempo. (O nome da variável, que representa a variação da entropia no sistema ao longo do tempo é:* dS *)*

Para perceber porque é que a *entropia* nunca pode diminuir ao longo do tempo, temos que compreender o que é *entropia*.

Caixa no Vácuo

Considere-se o seguinte cenário, que vai introduzir o conceito de reversibilidade e entropia:

Uma caixa isolada no vácuo, que contém moléculas de um gás ideal[15].
Na parte superior da caixa existe um êmbolo que se pode movimentar na direcção vertical.
Por cima do êmbolo, existe um bloco que no estado inicial está preso por um fio, sem exercer qualquer pressão sobre o êmbolo.

Nesta fase (I) o sistema, está em equilíbrio.

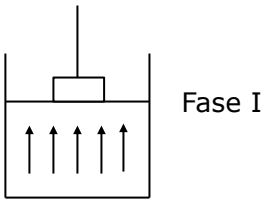


Figura 2 – 1º Estado de equilíbrio

Quando se corta o fio, o bloco começa a exercer pressão sobre o êmbolo, e este desce até atingir um novo estado de equilíbrio(II).

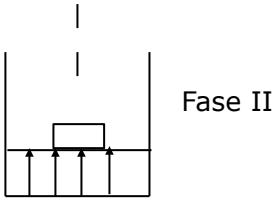


Figura 3 – 2º Estado de equilíbrio

A consequência imediata deste movimento é o choque entre as moléculas do gás. O choque aumenta a energia cinética de cada molécula, e aumenta a temperatura do sistema.

O conceito de reversibilidade de processos físicos é introduzido quando se coloca a seguinte pergunta:

Podemos a partir do novo estado de equilíbrio(II), voltar ao estado de equilíbrio inicial(I)?

A resposta a esta pergunta, é dada pela resposta a outra pergunta:

---

[15] Um gás ideal, é aquele em que as colisões entre átomos ou moléculas são perfeitamente elásticas e onde não existe qualquer força intermolecular atractiva.

Se retirarmos o bloco que está em cima do êmbolo na fase II, o êmbolo volta ao estado inicial(I)?.

A resposta a esta pergunta é *não*.

Isto acontece, porque a *entropia* que foi induzida no sistema para este atingir o novo estado de equilíbrio, é superior à *entropia* do sistema no estado inicial.

Entropia

Mas afinal, o que é ***entropia*****?**
Reveja-se alguns conceitos sobre energia.

A energia existe no universo sob duas formas: Cinética(EC)[16] e Potencial(EP)[17].

De acordo com a 1ª lei da termodinâmica, a energia que estava no sistema foi transferida.
Interessa descobrir como ocorreu a transferência energética.
A primeira energia em equação, talvez por ser a mais lógica, é a energia cinética(EC), uma vez que ao aumentar a pressão da caixa, as moléculas entram em contacto entre si, e aumentam a sua EC.

A segunda só pode ser energia potencial.

Pergunta
Qual?
Resposta com uma pergunta

---

[16] A EC refere-se à energia associada ao movimento de uma partícula, ou um corpo e pode ser obtida através da equação: $E = \frac{1}{2} mv^2$.

[17] A energia potencial(EP), refere-se à energia em potência (ou em condições de ser aproveitada).

O que fez com que o êmbolo se move-se no sentido descendente?
A resposta é: A força gravítica.

Deduz-se então que a energia potencial em causa, é a energia potencial gravítica[18](EPG).

Retire-se da equação $dE = TdS - PdV$, as energias em causa:

Primeiro, a mais lógica devido ao movimento descendente do êmbolo é a EPG.

Dado $Ep = mgh$, deduz-se que a EPG é directamente proporcional à distância entre o solo e o corpo.

A EPG além de diminuir, toma um valor negativo, uma vez que desde a fase I até à fase II, a distância do solo até ao êmbolo diminui.

Deduz-se então que $-PdV$, refere-se à EPG, e que TdS refere-se à EC do sistema.

No início do capítulo referi que dS , se refere à variação de entropia ao longo do tempo. Deduz-se então o seguinte:

- Após TdS , obtém-se a unidade de energia: Joule[19].
- A unidade fundamental de dS é Joule por Kelvin[20].
- Se a unidade fundamental de dS , é Joule por Kelvin, então S relaciona a energia e a temperatura de algo.

---

[18] Energia potencial gravítica de um corpo é vulgarmente dada pela equação: $E = mgh$

[19] Joule, é a unidade fundamental da energia. 1J=1 kg m^2 s^{-2}=1/4.184 de uma caloria.

[20] Isto acontece, porque Kelvin, é a unidade utilizada no Sistema Internacional para representar a temperatura.

A entropia (S), relaciona a energia cinética de cada uma das moléculas, que constituem o gás ideal por cada Kelvin, com a quantidade de estados possíveis do sistema em causa.

Esta é obtida através da seguinte fórmula: $S = k_b \ln N$ [21].

Para que se perceba claramente o que significa entropia, é necessário falar sobre a *desordem* ou *desorganização* de um sistema.

Organização Vs. Desorganização

Relembre-se pela última vez o cenário anterior para explicar o significado de entropia:

As moléculas do gás, estão organizadas de uma determinada forma para manter o sistema em equilíbrio(Figura 2 – 1º Estado de equilíbrio).
Esta organização, não deixa que o êmbolo se mova no sentido descendente.

Quando se corta o fio, introduz-se energia no sistema. Esta energia é transferida para o sistema sob a forma de *desordem* das moléculas, e aumenta a *desorganização* do sistema, retirando-o do equilíbrio.

Ao retirar o bloco, as moléculas reorganizam-se para colocar o sistema num novo estado de equilíbrio(Figura 3 – 2º Estado de equilíbrio).

Relembre-se então, uma questão colocada anteriormente:

---

[21] $S = k_b \ln N$, onde k_b é a Constante de Boltzmann e N é a quantidade de estados possíveis do Sistema. Um estado, é entendido como uma determinada disposição espacial de todas as moléculas do gás.
Foi Ludwig Boltzmann[1844-1906], físico austríaco que estudou o comportamento dos gases, que criou a célebre Constante de Boltzmann. Esta relaciona a quantidade de energia cinética de uma molécula de um gás ideal por cada Kelvin. $k_b \approx 1.3807 \text{ x } 10^{-23}$ Joules/Kelvin.

"Se retirarmos o bloco que está em cima do êmbolo na fase II, o êmbolo volta ao estado inicial(I)?".

A resposta a esta questão foi:
"Não"

E a explicação foi:
"...porque a *entropia* que foi induzida no sistema para este atingir o novo estado de equilíbrio, é superior à *entropia* do sistema no estado inicial."

Trocando a palavra *entropia* por *desordem* a explicação é:

"...porque a *desordem* que foi induzida no sistema para este atingir o novo estado de equilíbrio, é superior à *desordem* do sistema no estado inicial."

A reversibilidade do processo, só acontece quando o êmbolo volta ao estado de equilíbrio inicial.

Pergunta

O que impede o êmbolo de voltar ao estado inicial?

Resposta

A *desordem* do sistema.

Explicação

A desordem induzida no sistema, quando o bloco começa a fazer pressão sobre o êmbolo, é superior à desordem do sistema na Fase I.

Quando o êmbolo chega ao estado inicial, as moléculas ainda estão desorganizadas. Para se reorganizarem, elas continuam a empurrar o êmbolo afim de compensarem a desorganização induzida no sistema, no momento em que o bloco começou a exercer pressão sobre o êmbolo.

A organização das moléculas, coloca o êmbolo sempre acima da posição inicial, quando este atinge o 3º estado de equilíbrio(III).

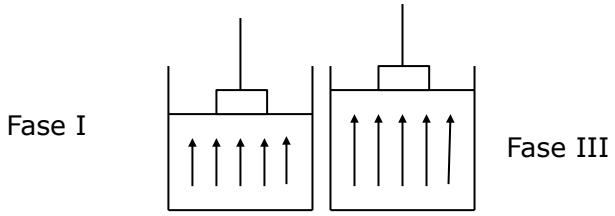


Figura 4 – Comparação entre o 1º e o 3º estado de equilíbrio

Será a reversibilidade de processos físicos possível?

A reversibilidade só é possível quando existem alterações infinitesimais entre dois estados de equilíbrio. Isto sucede apenas quando a *desorganização* das moléculas dentro da caixa é infinitesimal, permitindo ao êmbolo voltar ao estado inicial.

A reversibilidade física garante que não existe variação de entropia durante o processo termodinâmico.[2]

Explica-se de seguida, a razão principal para a dissipação de calor nos processadores.

Energia Dissipada, Processamento de Informação

A relação entre Temperatura, Energia, e Entropia é dada pela seguinte equação matemática: $T = {dE}/{dS}$ [22], a partir da qual se deduz: $dE = TdS$.

Associe-se o que foi explicado, para perceber a razão principal para a dissipação do calor nos processadores:

---

[22] Desta relação podemos deduzir que 1 Kelvin de Temperatura é gerado sempre que é utilizado $\approx 1{,}38 \times 10^{-23}\, Joule$ de Energia, para gerar 1 Joule/Kelvin de Entropia.

Imagine-se o funcionamento de um operador lógico num computador, que após processar dois bits, perde irreversivelmente um bit:

- No estado inicial, o sistema pode estar num de 4 estados possíveis.
- No estado final, o sistema pode estar num de 2 estados possíveis.
- Calculando a variação da entropia, entre os dois estados: $dS = k_b \ln 2 - k_b \ln 4 \cong -k_b \ln 2 \approx -0{,}6931 k_b$.

Após o cálculo, verifica-se que a entropia diminuiu. Isto acontece porque não estamos a tratar o computador como um sistema fechado, mas apenas os operadores lógicos como o sistema.
Considerando o sistema fechado, a entropia do sistema não diminui.

A entropia gerada pelos operadores, é transferida para o ambiente sob a forma de energia(energia dissipada), quando os transístores são limpos para a próxima computação[23][3].

Foi o físico Rolf Landauer[24], que em 1961 chegou a esta conclusão[25], após analisar o funcionamento dos processadores, e levou a criação de um princípio que é conhecido como o Princípio de Landauer:

A perda irreversível de 1 bit requer a dissipação mínima de $k_b T \ln 2$ *de energia.*

---

[23] A operação que prepara o transístor, é conhecida como RESTORE TO ONE, e coloca o estado do transístor a 1, após uma computação. É esta operação que requer a dissipação mínima de $k_b T \ln 2$ Joules de Energia.

[24] Rolf Landauer[1927-1995], físico alemão que trabalhou como investigador na IBM, explicou que a dissipação de energia de um computador, deve-se a perda irreversível de bits durante a computação.

[25] Landauer, chegou à conclusão que a perda de bits durante o processo computacional, acontece devido á operação RESTORE TO ONE, após uma computação.

Estudos actuais, revelam que a tecnologia utilizada para desenvolver os processadores, vai chegar ao limite da dissipação de $k_b T \ln 2$ Joule de energia em 2035, criando um processador que será 1 milhão de vezes mais rápido que um processador de 1GHz.

Relembre-se os pontos fundamentais, para conseguir ultrapassar este limite:

- A reversibilidade do processo físico, garante que não existe dissipação de energia, uma vez que $dE = T0$.
- A dissipação de energia, resulta da reprodução da irreversibilidade lógica, dos operadores físicos[25].
- É necessário tornar os operadores lógicos reversíveis, para garantir que não existe perda de bits, após o seu funcionamento.
- É necessário tornar toda a arquitectura física reversível, para diminuir ao máximo a dissipação de energia.[4]
- É necessário criar o bit quântico.

É sobre estas, e outras questões que vou falar nos próximos capítulos.

Capítulo V- Máquina de Turing Reversível

A solução para obter a reversibilidade dos operadores lógicos, está numa MT reversível[5].

Soluções possíveis para a reversibilidade da computação

1ª solução:

- Adicionar uma fita à MT, que guarda todos os estados das operações a serem executadas, para que se possa saber todos os estados da computação, tornado a computação reversível.

A 1ª solução, apenas adia o problema da perca de bits, uma vez que a fita tem que ser limpa, para que a próxima computação possa ser executada.

2ª solução:

- Adicionar uma fita à MT, que guarda todos os estados das operações a serem executadas, para que no final se possa reverter a computação.

Esta solução traz a desvantagem, de nunca se saber qual o estado final da computação, porque de seguida esta é revertida, e volta ao estado inicial.

3ª solução:

- Adicionar uma fita à MT, que guarda todos os estados das operações a serem executadas.
- Antes de reverter a computação, o resultado é copiado.
- Após reverter a computação, o sistema tem o input da computação, e uma cópia do output. O output original é "apagado", quando a computação é revertida.

A 3ª solução, é a mais indicada para criar uma MT reversível[6].
No entanto, existe uma característica que é comum às três soluções, que se torna uma desvantagem para a implementação prática de uma MT reversível:

- É necessário uma grande quantidade de fita(memória), para guardar todos os estados da computação.

Altere-se então a MT descrita no capítulo II, para que esta se torne uma MT reversível.

Elementos adicionais

- Conjunto finito de instruções que vão reverter a computação $I' = \{i'_1, i'_2, i'_3, ..., i'_i\}$.

Cada instrução $i' \in I'$, é representada pelo tuplo $\left[(sf, af), (si, ai; y)\right]$, que por sua vez representa a seguinte transição:

$$I' \ni i' : (sf, af) \rightarrow (si, ai; y)$$

Componentes adicionais e alterações

- Uma fita infinita externa à máquina, que pode ser trabalhada em ambos os lados, que está dividida em células, e guarda o histórico de cada computação;
- Uma unidade de controlo que controla a leitura/escrita da cabeça, baseado no estado actual da máquina, e no conteúdo da célula que está a ser lida pela cabeça. O controlo é feito através do par (sf, af), se reverte a computação.
- Uma unidade de controlo, responsável por criar a cópia do output da computação, antes de a reverter.

As instruções que revertem a computação, descrevem transição de um estado final (sf, af) , para um estado inicial (si, ai) , seguido de um movimento da cabeça.

Reversibilidade Computacional Física

Só quando o processo físico que implementa a lógica computacional é reversível, se atinge a dissipação mínima de energia, ou seja 0 Joule.
Comprovou-se neste trabalho que a reversibilidade física só é possível quando existem variações infinitesimais em todo o processo.
No caso da computação, a variação infinitesimal traduz-se em pequenos processos computacionais.

É necessário recorrer à física quântica para alcançar a reversibilidade física, sem que se diminua a rapidez de processamento dos processadores.

Capítulo VI- Física Quântica

O conceito *quântico* foi criado por Max Planck[26] em 1900, quando este introduziu a ideia, que a energia existe em pequenas unidades individuais. Na altura chamou-lhes ***quanta***.

Ao longo dos 30 anos seguintes, vários cientistas desenvolveram aquilo a que se chama: ***Teoria Quântica***.

Elementos essenciais da Teoria Quântica:

- A energia, como por exemplo matéria, consiste em unidades discretas.
- O movimento de partículas elementares de matéria, apresentam um movimento aleatório, e por isso imprevisível.
- A leitura simultânea de dois valores complementares, de uma partícula, como posição e momento é incerto. Quanto maior é a precisão da medida de um valor, mais incerta é a medida do valor complementar.

Desenvolvimentos futuros da Teoria Quântica:

Niels Bohr[27], propôs uma interpretação acerca da teoria quântica, na qual refere o seguinte:

Uma partícula é aquilo para que é medida. Não se pode assumir que esta tenha propriedades específicas, ou que exista, até que seja medida.

Esta ideia introduziu o princípio da *sobreposição*, que mais tarde explica-se em pormenor:

---

[26] Max Planck[1858-1947], físico alemão que em 1918, recebe o prémio Nobel da física pela sua teoria quântica.

[27] Niels Bohr[1885-1962], físico dinamarquês que em 1922, recebe o prémio Nobel da física pelo seu estudo, e descrição da estrutura do átomo.

Enquanto uma partícula não for medida, não é possível saber o estado em que esta está. Esta está em todos os estados simultaneamente, enquanto não for medida.

O alvo de estudo da física quântica, é também conhecido como atómico, e estuda o comportamento de partículas em sistemas de pequena dimensão, como por exemplo: átomos, electrões ou fotões.

Mecânica Quântica

A mecânica quântica, é a área da física quântica que explica estes comportamentos.

Ondas e Partículas

A nível macroscópico existem dois tipos de fenómenos físicos[28]: Ondas e Partículas.

- Fenómenos de partículas, envolvem transporte de massa e energia.
- Fenómenos ondulatórios, apenas envolvem transporte de energia.

Um exemplo concreto:

Os objectos físicos que manuseamos no dia a dia, são fenómenos de partículas, enquanto a propagação de ondas num lago são fenómenos ondulatórios.

A distinção entre estes fenómenos, sob as leis da mecânica quântica não é tão simples, porque

- entidades que assumem um papel de partícula, como por exemplo: um electrão, podem sob determinadas circunstâncias, apresentar características ondulatórias;

[28] Este fenómenos são regidos pela física clássica. Física onde as propriedades do mundo atómico são ignoradas.

- e entidades que assumem um papel ondulatório, como por exemplo: luz, podem sob determinadas circunstâncias, apresentar características de uma partícula.

Esta ideia é conhecida como o **Princípio da Dualidade Onda – Partícula**[29].

O comportamento ondulatório de uma partícula num sistema quântico ao longo do tempo, é descrito através da equação de Schrödinger[30]. Esta equação é conhecida como *wavefunction* ou função ondulatória.

Escreve-se de seguida os princípios mais importantes sobre a medição destas partículas a nível quântico:

- Existem várias funções ondulatórias que medem sempre o mesmo estado da partícula, em diferentes alturas. Esta situação é conhecida como *sobreposição de funções ondulatórias*. Isto significa que só no momento da leitura da situação, se conhece qual o estado da partícula no sistema.
- No momento da leitura, a partícula salta da *sobreposição*, para o estado medido. Esta situação é conhecida como *colapso da sobreposição*.
- Ao medir, de seguida o valor complementar da posição: momento, a partícula passa para uma sobreposição de funções de momento, e escolhe uma das funções ondulatórias para definir o seu estado.
- Ao medir novamente a posição da partícula, a partícula deixa o estado de colapso de *sobreposição de momento*, para uma *sobreposição de posição*, colapsando de seguida para o estado que define a posição da partícula. No entanto, este valor pode não ser o

---

[29] Prince Louis de Broglie[1892-1987], físico francês, que em 1929 recebe o prémio Nobel da física por ter comprovado este princípio, através do comportamento ondulatório do electrão, que até então era apenas considerado como uma partícula.

[30] Erwin Schrödinger[1887-1961], físico austríaco, que em 1933 recebe o prémio Nobel da física, pela criação da equação que define o comportamento ondulatório de uma partícula num sistema quântico.

mesmo que o primeiro, porque ao medir o momento da partícula pode-se ter alterado o sistema. O mesmo se aplica ao valor do momento, que pode não corresponder ao momento da partícula na primeira posição.

Estes princípios são importantes, para compreender uma das dificuldades da implementação física da computação quântica.

Maior Dificuldade

É necessário criar um sistema quântico, que corrija as variações induzidas no sistema no momento da leitura, para saber num determinado instante qual é o estado do bit quântico[31], sem influenciar o estado dos outros qubits.

Segue-se a experiência, que comprova o princípio da *sobreposição*.

Polarização de um Fotão

Elementos

- Emissor de uma fonte de luz, que emite a mesma quantidade fotões com polarização horizontal e vertical;
- Três filtros:
- Filtro A - Filtrar Fotões com 100% de polarização horizontal;
- Filtro B - Filtrar Fotões com 50% de polarização horizontal e 50% de polarização vertical.;
- Filtro C - Filtrar Fotões com 100 % de polarização vertical.

Os filtros desempenham um papel fundamental na experiência. O objectivo é deixar passar os fotões com a mesma polarização do filtro.

---

[31] Em inglês o bit quântico é conhecido como qubit - *Qu*antum *B*ynary Dig*it*. O qubit, é entendido como um sistema físico.

Passos

Passo 0: Emissão de luz.

Passo 1: Inserção do filtro A

Após a inserção do filtro, a luz que o filtro deixa passar, tem apenas metade da intensidsade inicial, uma vez que filtra apenas os fotões com polarização vertical.

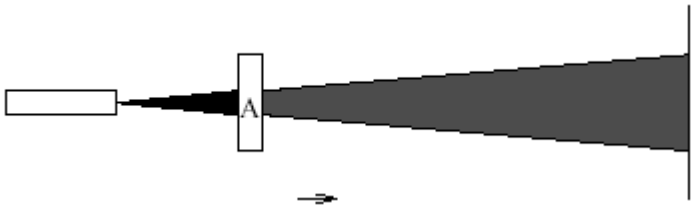


Figura 5- Inserção Filtro A

Passo 2: Inserção do filtro C depois do Filtro A

Ao colocar o filtro C, a intensidade de luz que é filtrada é de 100%.

O filtro C não deixa passar qualquer fotão, uma vez que não existe qualquer fotão com 100% de polarização vertical, a partir do momento em que se coloca o filtro A.

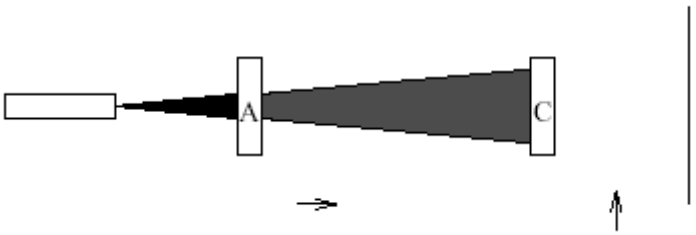


Figura 6- Inserção Filtro C

Passo 3: Inserção do filtro B entre o filtro A e o filtro C

A intensidade que agora é filtrada pelo filtro C é de 50%.

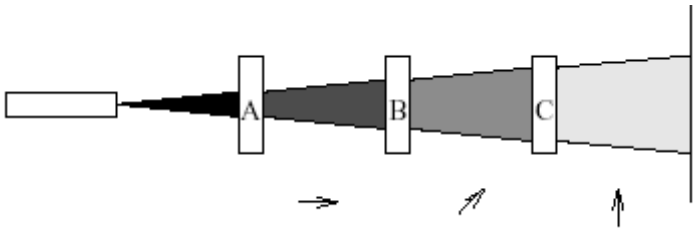


Figura 7- Inserção Filtro B

Segue-se a explicação:

Ao colocar o filtro B entre o filtro A e C, verifica-se o fenómeno de *sobreposição*.

O facto de o filtro C filtrar 50% de fotões só é possível, porque os fotões estão em duas polarizações ao mesmo tempo.

Ao colocar o filtro B, os fotões que estavam numa sobreposição de polarização horizontal e vertical, colapsam para a polarização medida pelo filtro, ou seja 50% de polarização horizontal e 50% de polarização vertical.

Conclusão da experiência:

Com esta experiência comprova-se o princípio da sobreposição, e mostra-se que através da manipulação da polarização de um fotão, é possível criar o *qubit*.

Capítulo VI - Computação Quântica

O termo computação quântica, foi introduzido pela primeira vez por Richard Feynman[32], em 1982 onde refere num dos seus livros que os fenómenos quânticos nunca poderiam ser simulados num computador clássico, mas sim num *computador quântico*.[7]

A computação quântica, rege-se pelos princípios da mecânica quântica.

[32] Richard Feynman[1918-1988], físico americano que em 1965 recebe o prémio Nobel da física, pelo seu estudo sobre electrodinâmica quântica.

Nomenclatura matemática

Segue-se uma introdução à nomenclatura matemática utilizada para descrever a computação quântica:

A mecânica quântica é linear

O estado de um sistema quântico pode ser representado por uma representação linear, como por exemplo:

$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$.

O estado de sobreposição de um fotão, pode ser representado da seguinte forma:

$|\psi\rangle = {}^{1}\!/\!_{\sqrt{2}}|\text{®}\rangle + {}^{1}\!/\!_{\sqrt{2}}|\uparrow\rangle$

Os coeficientes α_i são números complexos[33] normalizados

A seguinte equação tem que se verificar: $\sum_i |\alpha_i|^2 = 1$, para que $|\alpha_i|^2$, represente a probabilidade de o sistema se encontrar no estado ψ_i, após ter sido medido o sistema.

Leitura de um estado

Se a função ondulatória que define um sistema quântico for: $|\psi\rangle = \sum_i \alpha_i|\psi_i\rangle$,

e se após a leitura do sistema, este se encontra no estado ψ_i , então a função ondulatória que define o sistema quântico passa a ser: $|\psi\rangle = |\psi_i\rangle$.

[33] A revisão no Anexo II, sobre números complexos é essencial para a compreensão das explicações que se seguem.

Matrizes Unitárias

Estado do Sistema

Qualquer estado quântico, é representado por uma matriz unitária[34] de números complexos com tamanho $n*1$, onde n representa os graus de liberdade do sistema.

Representação genérica

$$V = \begin{pmatrix} V_1 \\ V_2 \\ \dots \\ V_n \end{pmatrix}, \text{ tal que } V^{\dagger}V = I$$

Transformação reversível de um sistema

O sistema quântico evolui ao longo do tempo, através de uma transformação.
Esta transformação é representada por uma matriz unitária de números complexos de tamanho $n*n$.

Representação genérica

$W = UV$, tal que $U^{\dagger}U = I$, onde W representa o novo estado do sistema e U , representa a transformação aplicada a V .

Qualquer transformação aplicada ao sistema é reversível, uma vez que $V = WU^{\dagger}$ *.*

---

[34] Diz-se que M é uma matriz unitária, quando $M^{\dagger}M = I$. Para rever alguns conceitos sobre matrizes, consulte o Anexo III "Revisões sobre Matrizes".

Qubit – Sistema Quântico

O *qubit*, é um sistema físico que contém o menor número de estados possíveis num sistema quântico.[8]

Interpretação gráfica de um qubit

Um qubit representa qualquer ponto na superfície de uma esfera de Bloch[35], onde o pólo norte representa o estado $|0\rangle$, e o pólo sul representa o estado $|1\rangle$ **[36]**.

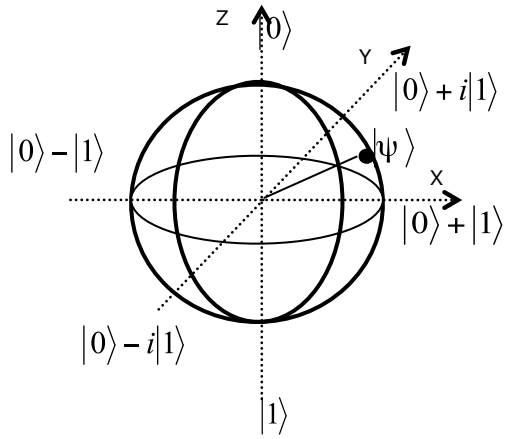


Figura 8 - Parametrização de um estado de 1 qubit numa esfera de bloch

Ao contrário de um bit clássico, o qubit não assume só um valor. Este pode estar num sobreposição de valores, e assumir qualquer ponto na esfera de bloch.

Este facto leva à criação do princípio: *computação quântica paralela*.

Princípio funcional de uma computação quântica

---

[35] A esfera de Bloch, é o local tridimensional onde se pode representar graficamente um qubit.

[36] Lembre-se que a projecção do qubit no plano XOY, é obtida através de: $\cos\theta + i\sin\theta \cong e^{\theta i}$

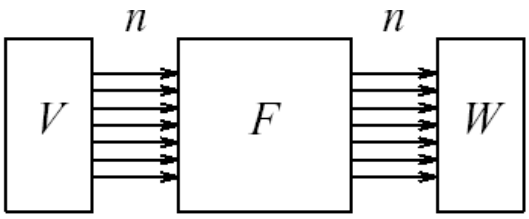


Figura 9 - Computação quântica genérica

Na Figura 9:

- V representa um registo onde são enviados n qubits;
- W representa um registo onde são colocados n qubits, após a computação F.

Considere-se a sobreposição dos n qubits no registo V:

$$V = \sum_{0}^{2^n} {}^{1}\!/\!_{\sqrt{2}} \left(|0_i\rangle + |1_i\rangle \right)$$

Ao computar a função F, o computador quântico aplica a função aos 2^n números em simultâneo, criando a computação em paralelo.

O registo W, após a computação F, seria o seguinte:

$$W = \sum_{0}^{2^n} {}^{1}\!/\!_{\sqrt{2}} \left(|F(0_i)\rangle + |F(1_i)\rangle \right)$$

Este poder computacional nos computadores clássicos, só é alcançado após 2^n computações ou quando se utilizam n registos em simultâneo.

O poder computacional de um computador quântico é de: 2^n, ao contrário de um computador clássico cujo poder computacional é de $2n$.

Operadores lógicos quânticos

Tal como num computador clássico, um computador quântico requer operadores lógicos[8], para efectuar o processamento de informação. Este operadores são conhecidos como *operadores quânticos*[37].

A aplicação de cada operador lógico, corresponde a uma ou várias rotações do qubit na esfera de bloch.

Genericamente, um operador lógico pode ter como input vários qubits.

Apresenta-se de seguida, os operadores mais importantes que recebem como input, um número pequeno de qubits.

1 qubit

Operador Rotação

O Operador de Rotação genérico permite efectuar uma rotação do qubit na esfera de Bloch[38]. Este operador é a base para todos os operadores de 1 qubit.

O operador unitário é representado pela matriz:

$$U_{ROT} = \begin{pmatrix} \cos(\alpha) & \sin(\alpha)e^{i\phi} \\ -\sin(\alpha)e^{-i\phi} & \cos(\alpha) \end{pmatrix}$$

Operador NOT

O operador quântico NOT, recebe como input 1 qubit, e o seu funcionamento lógico, é em tudo semelhante ao seu homónimo clássico.
O operador unitário é representado pela matriz:

---

[37] Em inglês são conhecidos como *quantum gates*.

[38] Lembre-se novamente, que a projecção do qubit no plano XOY, é obtida através de: $\cos\theta + i\sin\theta \cong e^{\theta i}$

$$U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Aplique-se o operador U_{NOT} aos qubits:

$|\psi_1\rangle = 1|0\rangle + 0|1\rangle = |0\rangle$ e $|\psi_2\rangle = 0|0\rangle + 1|1\rangle = |1\rangle$, representados pelas matrizes

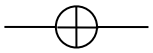
$V_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $V_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ respectivamente.

Aplicando o operador U_{NOT}, temos:

$$W_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad W_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Desta aplicação resulta a negação do qubit:

$U_{NOT}|\psi_1\rangle = 0|0\rangle + 1|1\rangle = |1\rangle$ e $U_{NOT}|\psi_2\rangle = 1|0\rangle + 0|1\rangle = |0\rangle$

Esquematicamente, temos: 

Operador Hadamard

O operador Hadamard(U_H), é responsável por criar a sobreposição do qubit, e é representado pela matriz:

$$U_H = 1/\sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Aplique-se o operador U_H aos qubits:

$|\psi_1\rangle = 1|0\rangle + 0|1\rangle = |0\rangle$ e $|\psi_2\rangle = 0|0\rangle + 1|1\rangle = |1\rangle$, representados pelas matrizes

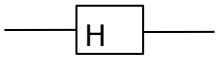
$V_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $V_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ respectivamente

Aplicando o operador U_H, temos:

$$W_0 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad W_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Desta aplicação resulta a seguinte sobreposição do qubit:

$$U_H|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \text{ e } U_H|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Esquematicamente, temos: 

2 qubits

Operador CNOT

O operador CNOT(U_{CNOT}), é responsável por negar o segundo qubit, no caso de o 1º qubit ser igual a 1:

$$U_{CNOT} = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}$$

Aplique-se o operador U_{CNOT} ao qubit:

$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, representado pela matriz:

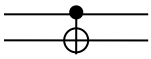
$$V = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

Aplicando o operador U_H, temos:

$$W = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}$$

Desta aplicação resulta o qubit:

$$|\psi\rangle = a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$$

Esquematicamente, temos: 

3 qubits

Operador CCNOT

O operador CCNOT(U_{CCNOT}), que também é conhecido como operador de Toffoli[39], é responsável por negar o terceiro qubit, no caso de o 1º e o 2º qubit serem igual a 1:

[39] Tommaso Toffoli, Professor do Departamento de Engenharia Electrónica e Computação da Universidade de Boston.

$$U_{CCNOT} = \begin{pmatrix} 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000001 \\ 00000010 \end{pmatrix}$$

Aplique-se o operador U_{CCNOT} ao qubit:

$$|\psi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|010\rangle + e|011\rangle + f|100\rangle + g|101\rangle + h|110\rangle + i|111\rangle \quad ,$$

representado pela matriz:

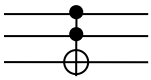
$$V = \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \\ i \end{pmatrix}$$

Aplicando o operador U_H, temos:

$$W = \begin{pmatrix} 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000001 \\ 00000010 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \\ i \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \\ e \\ f \\ g \\ i \\ h \end{pmatrix}$$

Desta aplicação resulta o qubit:

$$|\psi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|010\rangle + e|011\rangle + f|100\rangle + g|101\rangle + i|110\rangle + h|111\rangle$$

Esquematicamente, temos: 

Redes quânticas

A combinação dos operadores mais elementares, têm o nome de *rede quântica*, e permite criar computações mais complexas.
Vejam-se os seguintes exemplos:

Exemplo 1

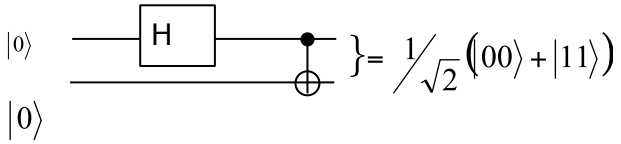


Figura 10 – Exemplo de um circuito quântico

O funcionamento do circuito é lido da seguinte forma:

O estado de input do circuito é: $|0\rangle|0\rangle = |00\rangle$

É aplicado o operador Hadamard ao 1º qubit, colocando o circuito no seguinte estado: $1/\sqrt{2}\left(|0\rangle + |1\rangle\right)|0\rangle = 1/\sqrt{2}\left(|00\rangle + |10\rangle\right)$

Aplicando o operador CNOT, a rede quântica produz o seguinte output: $1/\sqrt{2}\left(|00\rangle + |11\rangle\right)$.

Exemplo 2

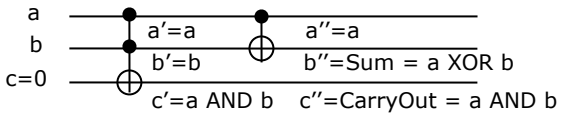


Figura 11 – Adição de dois bits a partir de operadores quânticos

A rede quântica de adição de dois bits, consiste num operador de Toffoli, seguido de um operador CNOT.

Os dois bits de input de controlo do operador de Toffoli, são *a* e *b*. O bit de output é $c' = c \oplus (aANDb) = (aANDb)$, é utilizado como o bit de CarryOut.

O valor de *a* e *b* propagam-se para o input do operador CNOT sem serem alterados, produzindo $b'' = aXORb$, como o resultado da adição dos dois bits.

Exemplo 3

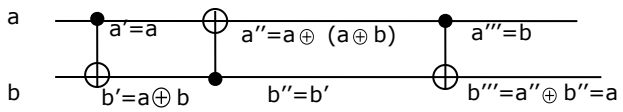


Figura 12 – Troca de 2 bits, através do três operadores CNOT[40]

Como *a* e *b* são variáveis booleanas, verificam-se as seguintes equações:

$a \oplus (a \oplus b) = (a \oplus a) \oplus b = b$;

$b \oplus (a \oplus b) = (b \oplus b) \oplus a = a$, onde $(a \oplus a) = 0,0 \oplus b = b$, resultando na troca dos 2 bits de input.

Operadores quânticos universais

Um operador quântico, é universal quando a partir deste é possível criar com algum grau de semelhança qualquer um dos outros operadores lógicos.

Mostra-se a título de exemplo, que o operador CCNOT, é um operador quântico universal de qualquer operador quântico de 1 qubit:

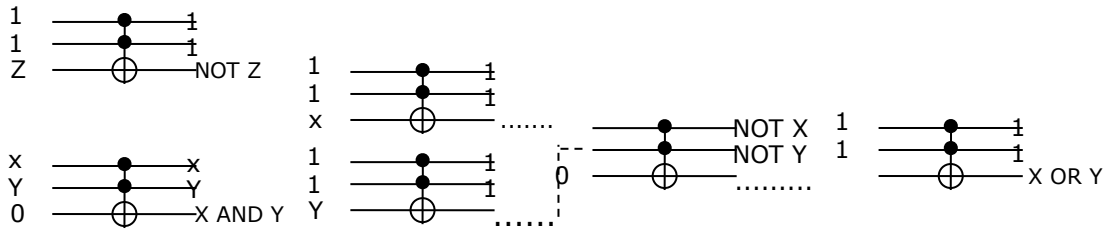


Figura 13 – Operador CCNOT Universal

Capítulo VII- Desafios e Aplicações práticas

Correcção de erro quântico

[40] Em inglês, este operador é conhecido como o operador SWAP.

Qualquer medida ao estado de um qubit(sistema quântico), pode provocar uma variação do seu estado, comprometendo assim todas as vantagens computacionais, que foram referidas ao longo deste trabalho.
É necessário detectar e corrigir qualquer variação que possa ocorrer durante a fase de medição.
O primeiro algoritmo de correcção de erros quântico, foi criado primeira vez por Peter Shor[41].

Negação do bit

Considere-se o seguinte circuito quântico[42]:

$|0\rangle$ ® $|000\rangle$
$|1\rangle$ ® $|111\rangle$

Após a aplicação do circuito quântico, imagine-se que o resultado seria:

$|0\rangle$ ® $|100\rangle$
$|1\rangle$ ® $|011\rangle$

O algoritmo que Peter Shor implementou, baseia-se num cálculo aritmético, que devolve a posição(1,2,3) do qubit que foi modificado em formato binário:

$|xyz\rangle$ ® $(y \oplus z, x \oplus z)$

Se nenhum dos qubits foi alterado durante o processo de codificação, o resultado de $\oplus$, será sempre 0. Caso contrário, pelo menos um dos cálculos será 1.

No exemplo dado, o resultado seria:

$|100\rangle$ ® $(0 \oplus 0{,}1 \oplus 0)$® $(0{,}1)$

---

[41] Peter Shor, investigador dos laboratórios AT&T, na área de computação quântica.

[42] Repetição do qubit, por forma a minimizar o erro de codificação. Este circuito é homólogo ao método de codificação/transmissão de um bit clássico: 0->000; 1->111

$|011\rangle \to (1 \oplus 1, 0 \oplus 1) \to (0,1)$, o que indica que o qubit modificado está na posição 1.

Alteração da fase do qubit

Quando se dá a alteração da fase do qubit $a|0\rangle + b|1\rangle \to a|0\rangle - b|1\rangle$, o algoritmo anterior não funciona.

Considere-se o circuito quântico:

$$|0\rangle \to \frac{1}{2^{3/2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \to \frac{1}{2^{3/2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

Após a aplicação do circuito quântico, imagine-se que o resultado seria:

$$|0\rangle \to \frac{1}{2^{3/2}}(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle \to \frac{1}{2^{3/2}}(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

Verifica-se que a fase do primeiro cluster difere dos restantes.

Da mesma forma, que a correcção da negação do bit, não foi baseada na leitura do bit a analisar, a correcção da fase do qubit, não é baseada na leitura da fase de cada cluster, mas sim na comparação de pares de fases dos três clusters.
Comparando clusters que têm fases diferentes a fase resultante será sempre negativa.
Comparando os três clusters dois a dois, descobre-se qual dos clusters têm a fase modificada, conseguindo corrigir o erro de codificação.

Princípio fundamental da correcção de erros quânticos

Medir o erro, sem perturbar(alterar) o sistema quântico.[9]

Factorização de números primos

A factorização de números primos é a técnica mais utilizada na área da criptografia.
O algoritmo RSA[43], é o algoritmo de encriptação mais utilizado no mundo, nomeadamente no mundo da internet.
O algoritmo é utilizado para encriptar dados importantes, que são transmitidos via internet, como por exemplo: número de cartões de crédito.
O algoritmo RSA é seguro, se o processo de factorização de um número primo N (com um grande número de dígitos), requerer uma quantidade de tempo exponencial, para encontrar p,q, tal que $p*q=N$.

Escreve-se de seguida um algoritmo[44] que permite factorizar um número primo:

- Seja N, o número primo que pretendemos factorizar.
- Seja x, um número aleatório.
- Seja a, um número entre 0 e $q-1$, onde q, é uma potência de dois tal que $n^2 \leq q \geq 2n^2$, então a sequência númerica produzida por $x^a \pmod N$, possui um determinado período.
- Seja r o período de $x^a \pmod N$, então um dos factores de N, é obtido através do cálculo do maior divisor comum(MDC) entre $x^{r/2}-1$ e N.

Factorize-se o número 33, para comprovar a funcionalidade do algoritmo anterior:

---

[43] RSA- Significa: Rivest, Shamir and Adleman, o nome de três criptologistas que inventaram o primeiro algoritmo criptográfico comercial.

[44] Algoritmo criado por Peter Shor em 1998.

- Seja 5, o número aleatório.
- A tabela seguinte mostra o resultado após 14 iterações para calcular o período de $5^a \pmod{33}$:

a	x^a	$x^a \pmod n$
0	1	1
1	5	5
2	25	25
3	125	26
4	625	31
5	3125	23
6	7825	16
7	390625	4
9	1953125	20
10	9765625	1
11	48828125	5
13	244120625	25
14	1220703125	26

Tabela 2- Cálculo do período

A partir da tabela, lê-se que a sequência numérica $x^a \pmod N$, repete-se após 10 iterações, pelo que o cálculo do MDC, é feito entre $5^5 - 1$ e 33.

O MDC($5^5 - 1$, 33)=11, é um factor de 33, e um número primo.

A execução do melhor algoritmo de factorização, demora cerca de $O\left(\exp\left[\left(64/9\right)^{1/3}(\ln N)^{1/3}(\ln N)^{2/3}\right]\right)$.[10]

O tempo de execução do algoritmo anterior, num computador convencional aumenta exponencialmente, com o número de dígitos do número a factorizar. [10]

Em 1994, um número primo de 129 dígitos, foi factorizado utilizando o algoritmo anterior, em cerca de 1600 PC por todo mundo. O processo de factorização demorou oito meses.[10]
Usando este factor, prevê-se que com o mesmo poder computacional, a factorização de um número de 250 dígitos, demore 800,000 anos.[10]

Factorização Quântica

O tempo de execução do algoritmo de factorização, é essencial para garantir que informação importante esteja segura.

Um computador quântico, utiliza a sobreposição para calcular em paralelo a factorização de um número.

O processo de factorização, envolve a utilização de dois registos para guardar os valores que permitem descobrir um dos factores do número que se pretende factorizar[11]:

Registo 1
No registo 1, encontram-se os bits que representam o número a.

Coloca-se o registo 1, num estado de sobreposição: $1/\sqrt{q}\sum_{a=0}^{q-1}|a\rangle|0\rangle$. Esta sobreposição coloca cada bit no registo no estado: $1/\sqrt{2}\left(|0\rangle+|1\rangle\right)$.

Registo 2

No registo 2, efectua-se o cálculo $x^a \pmod N$, com o valor de a, no registo 1.

O registo 2, após o cálculo, encontra-se no estado: $1/\sqrt{q}\sum_{a=0}^{q-1}|a\rangle|x^a \pmod N\rangle$.

O tempo de execução do algoritmo explicado, num computador quântico diminui para cerca de $O\left((\ln N)^3\right)$.[10].

Esta rapidez de cálculo computacional, obriga a que os algoritmos de factorização sejam rescritos, para tornar o processo de encriptação de dados, ainda mais seguro.

Procura de dados em estruturas desordenadas

O tempo de execução do algoritmo que procura dados em estruturas desordenadas, num computador clássico requer no máximo $O(N)$, em que N, representa a quantidade de dados na estrutura desordenada.

Apresenta-se de seguida, uma explicação sucinta do algoritmo quântico, que reduz o tempo de procura para $O(\sqrt{N})$:

Seja $x_1, x_2, ..., x_n$, os estados do sistema, tal que $2^n \geq N$

Seja x_0, um estado que satisfaça a seguinte condição P, tal que:

$P(x_0) = 1$
$P(x) = 0$, encontre-se o valor de x_0

Resolução:

1. Prepara-se um registo com uma sobreposição de todos os valores de: $x_i \in \{0,1,...2^n - 1\}$
2. Aplica-se o operador U_P, à sobreposição anterior, em $U_P|x,0\rangle \text{ ® } |x,P(x)\rangle$.
3. A aplicação deste operador, leva à sobreposição: $1/\sqrt{2} \sum_{x=0}^{N-1} |x,P(x)\rangle$
4. Após aplicar o operador U_P, dos 2^n estados possíveis, apenas um estado terá o valor 1.

Para procurar o estado em causa, é necessário aumentar a amplitude do estado, cujo valor é 1, para que a probabilidade seja 100%.
O processo que procura o estado que possui o valor 1, reduz o tempo de procura para $O\left(\sqrt{N}\right)$[45][12].

Conclusão

Pretendeu-se, através deste trabalho mostrar uma área de investigação, que irá revolucionar a forma como os processadores actuais processam informação – Computação Quântica -.

Para isso:

- Mostrou-se que a dissipação de calor nos processadores, está relacionada com a diminuição do tamanho dos componentes que os constituem, e com a perda de bits que ocorrem durante os processos computacionais.
- Explicou-se, que em teoria é possível criar o processo computacional sem qualquer dissipação de calor. Para isso, é necessário que a computação seja lógica e fisicamente reversível.
- Mostrou-se que a reversibilidade física é atingível, apenas quando se recorre às leis da física quântica.
- Introduziu-se, a nomenclatura matemática, e gráfica que descreve os processos físico-quânticos.
- Mostrou-se, que é possível criar uma unidade quântica que permita manipular informação, o *qubit*.
- Explicou-se o funcionamento dos principais operadores quânticos, através de exemplos concretos.
- Mostrou-se que é possível ultrapassar a maior dificuldade para a criação de um computador quântico – *alteração do estado do qubit*, através de dois exemplos concretos.

---

[45] A explicação completa do algoritmo de aumento de amplitude, pode ser encontrado em "A fast quantum mechanical algorithm for database search.", desenvolvido por Lov Grover.

- Mostrou-se, como os avanços computacionais quânticos reduzem o tempo de execução de algoritmos complexos, como algoritmos criptográficos e algoritmos de procura em estruturas desordenadas.

Agradecimentos

Quero agradecer ao meu orientador Eng.º Paulo Ferreira, ao Eng.º Armando Vieira, Eng.º Rodrigo de Abreu, pelas suas opiniões e incentivos.

Aos colegas Hélder Parracho, Hugo Branco e Nuno Ferreira, obrigado pelo vosso interesse, e paciência durante as várias horas que me ouviram falar sobre este assunto.

Dedico este trabalho aos meus Pais e ao meu Irmão.

Anexos

Anexo I – Funcionamento operadores lógicos clássicos

Apresenta-se de seguida o funcionamento dos principais operadores lógicos com dois bits de input.

Operador AND

Input		Output
A	B	A B
0	0	0
0	1	0
1	0	0
1	1	1

Tabela 3 – Input Vs. Output do operador AND

Operador OR

Input		Output
A	B	A + B
0	0	0
0	1	1
1	0	1
1	1	1

Tabela 4 – Input Vs. Output do operador OR

Operador NAND

Input		Output
A	B	A B
0	0	1
0	1	1
1	0	1
1	1	0

Tabela 5 – Input Vs. Output do operador NAND

Operador NOR

Input		Output
A	B	A + B
0	0	1
0	1	0
1	0	0
1	1	0

Tabela 6 – Input Vs. Output do operador NOR

Operador XOR

Input		Output
A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

Tabela 7 – Input Vs. Output do operador XOR

Operador XNOR

Input		Output
A	B	$A \oplus B$
0	0	1
0	1	0
1	0	0
1	1	1

Tabela 8 – Input Vs. Output do operador XNOR

Seja qual for o operador lógico utilizado, concluí-se que os operadores não são reversíveis, e que após o seu funcionamento perde-se um bit de informação.

Anexo II - Números Complexos

Um número C diz-se complexo, quando é composto por uma parte *real* e uma parte *imaginária*(i).

C, passa então a ser definido pela seguinte equação: $C = a + bi$, em que a, representa a parte real e bi, representa a parte imaginária.

Um número complexo, pode ser representado também através do par (a,b).

Represente-se o número C, num eixo cartesiano:

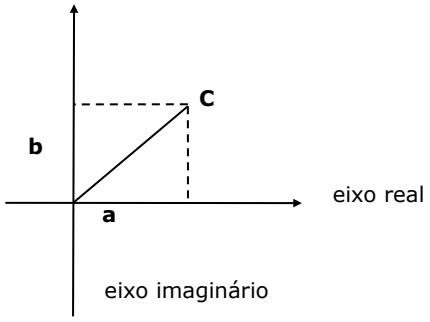


Figura 14 – Representação de C num eixo cartesiano

Conjugação de C

Conjugue-se C: $C^* = (a+bi)^* = (a-bi)$

Represente-se o número C^*, num eixo cartesiano:

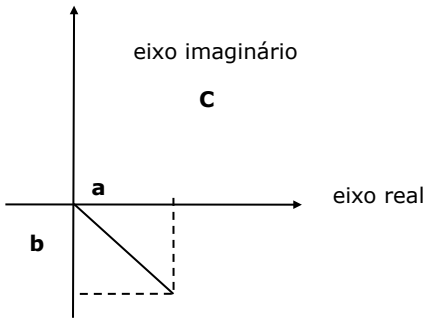


Figura 15 – Representação de C* num eixo cartesiano

Exponenciação:

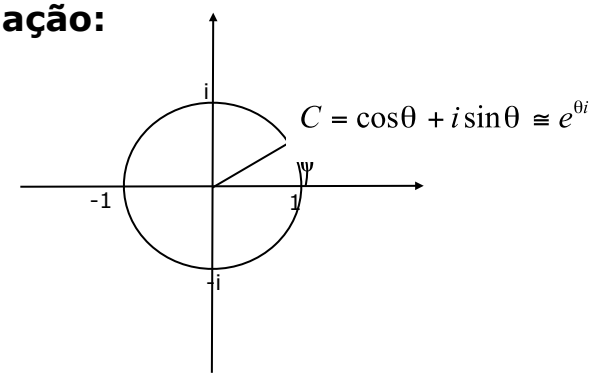


Figura 16 – Cálculo genérico de C

Adição:

$C_1 = a_1 + b_1 i$, $C_2 = a_2 + b_2 i$

$C_1 + C_2 = (a_1 + a_2) + (b_1 + b_2)i \cong (a_1 + a_2, b_1 + b_2)$

Multiplicação:

$C_1 = a_1 + b_1 i$, $C_2 = a_2 + b_2 i$

$$C_1 \times C_2 = ((a_1 \times a_2) - (b_1 \times b_2)) + ((a_1 \times a_2) + (b_1 \times b_2))i \cong (((a_1 \times a_2) - (b_1 \times b_2)), (a_1 \times a_2) + (b_1 \times b_2))$$

Anexo III- Revisão sobre Matrizes

Dá-se o nome matriz $m \times n$, quando a matriz em causa, possui m linhas horizontais e n colunas.

A operação que troca linhas por colunas, de uma matriz é designada de *transposta*:

Seja $M = \begin{pmatrix} 100 \\ 101 \end{pmatrix}$, a matriz a transpôr, então $M^t = \begin{pmatrix} 11 \\ 00 \\ 01 \end{pmatrix}$, é a matriz transposta.

Adição:

Seja $A = \begin{pmatrix} A_{11} A_{12} \\ A_{21} A_{22} \end{pmatrix}$, e $B = \begin{pmatrix} B_{11} B_{12} \\ B_{21} B_{22} \end{pmatrix}$, então $A + B = \begin{pmatrix} A_{11} + B_{11} A_{12} + B_{12} \\ A_{21} + B_{21} A_{22} + B_{22} \end{pmatrix}$

Multiplicação:

Seja $A = \begin{pmatrix} A_{11} A_{12} \\ A_{21} A_{22} \end{pmatrix}$, e $B = \begin{pmatrix} B_{11} B_{12} \\ B_{21} B_{22} \end{pmatrix}$, então

$$A * B = \begin{pmatrix} (A_{11} \times B_{11} + A_{12} \times B_{21})(A_{11} \times B_{12} + A_{12} \times B_{22}) \\ (A_{21} \times B_{11} + A_{22} \times B_{21})(A_{21} \times B_{12} + A_{22} \times B_{22}) \end{pmatrix}$$

Matrizes Números Complexos

A operação †, consiste em transpor uma matriz de números complexos, e de seguida conjugar todos números complexos que esta contém.

Para simplificar $A^{\dagger}{}_{ij} = A_{ji}{}^{*}$.

Propriedades mais importantes

Seja A , uma matriz $n \times 1$ de números complexos, então:

$$|A_{11}|^2 + |A_{21}|^2 + \ldots + |A_{n1}|^2 = 1$$

Anexo IV – Código ASCII /Sequência Binária

Apresenta-se de seguida, uma tabela que mostra a atribuição número-caractér, para caracteres alfanuméricos :

ASCII	Caracter	ASCII	Caracter
65	A	97	a
66	B	98	b
67	C	99	c
68	D	100	d
69	E	101	e
70	F	102	f
71	G	103	g
72	H	104	h
73	I	105	i
74	J	106	j
75	K	107	k
76	L	108	l
77	M	109	m
78	N	110	n
79	O	111	o
80	P	112	p
81	Q	113	q
82	R	114	r
83	S	115	s
84	T	116	t
85	U	117	u
86	V	118	v
87	W	119	w
88	X	120	x
89	Y	121	y
90	Z	122	z

Tabela 9 - Código ASCII- Caracteres Alfanuméricos

Formato Decimal	Formato Binário
0	0

1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011
20	10100

Tabela 10 - Formato Decimal Vs. Formato Binário

Referências

[1] Shannon, C. E., "A Mathematical Theory of Communication", Pág. 1.

[2] Abreu, R., "The Energy-Entropy Principle", Pág. 5.

[3] Landauer, R., "Irreversibility and Heat Generation in the Computing Process", Págs. 183-191.

[4] Carlin J.V., "Reversible Computer Engineering and Architecture", Pág. 23.

[5] Bennett, C. "Logical Reversiblility of Computation" Pág. 526.

[6] Bennett, C. "Logical Reversiblility of Computation" Pág. 527.

[7] Feynman, R.P., "Simulating Physics with Computers", Págs. 466-468.

[8] Deutsch, D. "Lectures on Quantum Computation", Vídeo I.

[9] Preskill, J., "Quantum information and quantum computation", Pág. 26.

[10] Braunstein S.L, "Quantum Computation", Pág.9.

[11] Shor, P.W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", Pág. 10.

[12] Grover, L.K, 1996, "A fast quantum mechanical algorithm for database search", Pág. 4.

Bibliografia

Abreu, R., "The Energy-Entropy Principle", http://arxiv.org/abs/physics/0207022

Aharonov, D., "Quantum computation", http://arXiv.org/abs/quant-phys/9812037

Barenco, A., 1995, "A universal two-bit gate for quantum computation", Proc. R. Soc. London http://arXiv.org/abs/quant-ph/9505016

Bennett, C.H, Landauer Ralf, 1985, "The fundamental physical limits of computation",http://www.aeiveos.com/~bradbury/Authors/Computing/Bennett-CH/TFPLoC.html

Bennett, C.H., 1982, "The Thermodynamics of Computation", http://www.research.ibm.com/people/b/bennetc/bennettc1982666c3d53.pdf

Bennett, C.H., 1995, "Quantum information and computation", Physics Today, Outobro.

Bennett, C.H., 1973 "Logical Reversibility of Computation", IBM Journal, http://www.research.ibm.com/people/b/bennetc/bennettc19734c533842.pdf

Braunstein S.L, "Quantum Computation", http://www-users.cs.york.ac.uk/~schmuel/comp/comp_best.pdf

Carlin J.V., 1999, "Reversible Computer Engineering and Architecture", Massachusetts Institute of Technology, http://www.ai.mit.edu/people/cvieri/main.ps

Deutsch, D. "Lectures on Quantum Computation", Video I. http://www.quiprocone.org/Protected/David_Deutsch_1.wmv

Deutsch, D., A. Barenco, A. Ekert, 1995, "Universality in quantum computation", Soc. London, http://arXiv.org/abs/quant-ph/9508012

DiVincenzo, D., 1994, "Two-bit gates are universal for quantum computation", http://arXiv.org/abs/cond-mat/9407022

Ekert, A., C. Macchiavello, 1996, "Quantum error correction for communication", http://arXiv.org/abs/quant-phys/9602022.

Ekert, A., P. Hayden, H. Inamori, 2000, "Basic concepts in quantum computation", http://arXiv.org/abs/quant-ph/0011013

Feynman, R.P., 1996, "Feynman lectures on computation", Editora Addison-Wesley.

Feynman, R.P., 1982. "Simulating Physics with Computers", International Journal of Physics.

Galindo, A., M. A. Martin-Delgado, 2000, "A family of Grover's quantum searching algorithms", http://arXiv.org/abs/quant-ph/0009086

Grover, L.K, 1996, "A fast quantum mechanical algorithm for database search", http://arxiv.org/abs/quant-ph/9605043

Landauer, R., 1961, "Irreversibility and heat generation in the computing process",http://www.aeiveos.com/~bradbury/Authors/Computing/Landauer-R/IaHGitCP.html

Landauer, R., 1991, "Information is physical", Physics Today, Vol. 44

Landauer, R., 1996, "The physical nature of information", Phys. Lett. A 217

Preskill, J., 1997, "Quantum information and quantum computation", www.theory.caltech.edu/~preskill

Riffel, E., W. Polack, 1998, "An introduction to quantum computing for non-physicists", http://arXiv.org/abs/quant-ph/9809016.

Shannon, C. E., "A Mathematical Theory of Communication", Bell Systems Technical Journal, http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

Shor, P.W., 1994, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", http://arXiv.org/abs/quant-ph/9508027.