



UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM BIOMETRIA E ESTATÍSTICA
APLICADA

CARLA PATRÍCIA DE CARVALHO OLIVEIRA

MEMÓRIA QUÂNTICA PROBABILÍSTICA
PARAMETRIZADA

RECIFE – PE

2018

CARLA PATRÍCIA DE CARVALHO OLIVEIRA

**MEMÓRIA QUÂNTICA PROBABILÍSTICA
PARAMETRIZADA**

Dissertação apresentada ao Programa de
Pós-Graduação em Biometria e Estatística
Aplicada como exigência parcial à obtenção
do título de Mestre.

ORIENTADOR: Prof. Dr. Adenilton José da Silva

RECIFE – PE

2018

CARLA PATRÍCIA DE CARVALHO OLIVEIRA

MEMÓRIA QUÂNTICA PROBABILÍSTICA
PARAMETRIZADA

BANCA EXAMINADORA

Prof. Dr. Adenilton José da Silva (Orientador)
Universidade Federal Rural de Pernambuco
DC/DEInfo/UFRPE

Prof. Dr. Wilson Rosa de Oliveira Junior
Universidade Federal Rural de Pernambuco
DC/DEInfo/UFRPE

Prof. Dr. Valmir Macário Filho
Universidade Federal Rural de Pernambuco
DC/UFRPE

Dedico esse trabalho com todo amor a Deus,
à minha família, meus amigos e professores.

“ Aos outros, dou o direito de ser como são.
A mim, dou o dever de ser cada dia melhor.”

(Chico Xavier)

Resumo

A computação quântica é um modelo de computação que exhibe todas as suas potencialidades por meio dos seus fenômenos quânticos, e, para isso, na execução de tarefas computacionais com mais eficiência tanto no processamento de dados quanto na transmissão de dados e de informações, permitindo solucionar problemas na otimização do desempenho de algoritmos de aprendizagem de máquinas, problemas estes, acarretados principalmente, pelo crescente número de dados (big data) que diariamente são gerados e a necessidade de encontrar abordagens tecnológicas inovadoras para o tratamento e a análise desse fluxo de dados. Exemplificando o que se afirma acima, tem-se a Memória Quântica Probabilística (MQP) proposta por Trugenberger em que um novo padrão de entrada deverá ser reconhecido, quando apresentam distâncias de Hamming próximas, acarretando o reconhecimento do novo padrão estabelecido na entrada. Nesse sentido, este trabalho faz a inclusão de um parâmetro a esta memória, permitindo que as memórias armazenadas reconheçam o novo padrão inserido com uma elevada probabilidade. Como demonstrado neste trabalho, realiza-se um ajuste à memória com a inclusão de um parâmetro a n (tamanho da memória), denominada de Memória Quântica Probabilística Parametrizada (MQPP) possibilitando uma melhor funcionalidade da memória, ao conseguir separar de forma eficiente, o novo padrão. A proposta e a implementação dessa alteração é embasada em resultados alcançados utilizando dados artificiais, através da comparação dos resultados usando a MQP e a MQPP, percebe-se os resultados satisfatórios provenientes da modificação sugerida à memória. Nesse contexto, conforme a alteração feita ao algoritmo de recuperação de informação, mostramos que o padrão de entrada será classificado, apenas pela memória que retorna com uma alta probabilidade. Assim, este trabalho valida a proposta de melhoramento da limitação existente na MQP de forma simples e eficaz.

Palavras-chave: Computação Quântica, Aprendizado de Máquina, Memória Quântica Probabilística, Memória Quântica Probabilística Parametrizada.

Abstract

Quantum computing is a model of computation that exhibits all its potentialities through its quantum phenomena, and, for this, in the execution of computational tasks more efficiently in data processing as well as in the transmission of data and information, allowing to solve problems in the optimization of the performance of machine learning algorithms. These problems are caused mainly by the increasing number of daily data generated and the need to find innovative technological approaches to the treatment and analysis of this data flow. For example, we have the Probability Quantum Memory (MQP) proposed by Trugenberger in which a new input pattern should be recognized, when they present close Hamming distances, leading to the recognition of the new standard established at the input. In this sense, this work adds a parameter to this memory, allowing the stored memories to recognize the new pattern inserted with a high probability. As shown in this work, a memory fit is performed with the inclusion of a parameter to n (memory size), called Parameterized Probabilistic Quantum Memory (MQPP), allowing better memory functionality, by efficiently separating , the new standard. The proposal and implementation of this change is based on results obtained using artificial data, by comparing the results using the MQP and the MQPP, we can see the satisfactory results from the suggested modification to memory. In this context, according to the change made to the information retrieval algorithm, we show that the input pattern will be classified, only by the memory that returns with a high probability. Thus, this work validates the proposal to improve the existing limitation in the MQP in a simple and effective way.

Keywords: Quantum Computation, Machine Learning, Probabilistic Quantum Memory, Parametrized Probabilistic Quantum Memory.

Lista de Figuras

Figura 1 – Mapa de Pesquisa das atividades em ordem cronológica	15
Figura 2 – Porta quântica (CNOT)	21
Figura 3 – Outra representação da porta quântica (CNOT)	21
Figura 4 – Porta de Toffoli	22
Figura 5 – Porta de Toffoli	22
Figura 6 – Porta U-controlada	23
Figura 7 – Circuito de uma porta Hadamard	23
Figura 8 – Representação gráfica da iteração de Grover	27
Figura 9 – Circuito quântico que implementa o algoritmo de Grover	28
Figura 10 – Probabilidade de reconhecimento do padrão $ i\rangle$ para $n = 26$ em uma Memória Quântica Probabilística	40
Figura 11 – Circuito recuperação memória quântica probabilística parametrizada	46
Figura 12 – Probabilidade de reconhecimento do padrão $ i\rangle$ para $a = 5$ em uma Memória Quântica Probabilística Parametrizada.	50
Figura 13 – Ilustração do comportamento da distância de Hamming $d(i, p^k)$ e suas probabilidades (y) em uma Memória Quântica Probabilística Parametrizada.	51

Lista de Siglas

AM	<i>Aprendizagem de Máquina</i>
IA	<i>Inteligência Artificial</i>
IQ	<i>Informação Quântica</i>
CQ	<i>Computação Quântica</i>
AR	<i>Aprendizagem por Reforço</i>
AMQ	<i>Aprendizagem de Máquina Quântica</i>
RNA	<i>Redes Neurais Artificiais</i>
MQP	<i>Memória Quântica Probabilística</i>
MQPP	<i>Memória Quântica Probabilística Parametrizada</i>
MAQ	<i>Memória Associativa Quântica</i>

Sumário

1	Introdução	11
1.1	Motivação	11
1.2	Problema de Pesquisa	13
1.3	Objetivos	14
1.3.1	Geral	14
1.3.2	Específicos	14
1.4	Mapa de pesquisa	14
1.5	Organização da dissertação	14
2	Computação Quântica	16
2.1	Introdução	16
2.2	Postulados da Mecânica Quântica	17
2.3	Qubits	18
2.4	Produto Tensorial	19
2.5	Emaranhamento Quântico	19
2.6	Operações sobre um qubit	20
2.6.1	A porta de Toffoli	21
2.6.2	A porta U-controlada	22
2.7	Circuitos quânticos e portas quânticas	22
2.8	Superposição quântica	23
2.9	Paralelismo quântico	24
2.10	Não Clonagem	24
2.11	Algoritmos Quânticos	25
2.11.1	Algoritmo de Grover	25
3	Memória Quântica Probabilística	29
3.1	Introdução	29
3.2	O algoritmo de armazenamento de padrões quânticos	30
3.3	O algoritmo de recuperação de padrões quânticos	32
3.4	Sumário do capítulo	40
4	Memória Quântica Probabilística Parametrizada	42
4.1	Introdução	42

4.2	Limitação da Memória Quântica Probabilística	42
4.3	Memória Quântica Probabilística Parametrizada	43
4.3.1	Escolha do Parâmetro	44
4.4	Sumário do Capítulo	51
5	Conclusão	53
5.1	Considerações finais	53
5.2	Contribuições deste trabalho	53
5.3	Trabalhos Futuros	54
	Referências	55

1 Introdução

Neste capítulo é apresentado a motivação para o trabalho, o estudo e uma modificação a memória quântica probabilística. A Seção 1.1 apresenta um breve histórico sobre a memória quântica probabilística, citando inclusive alguns dos problemas de uma memória quântica probabilística. Na Seção 1.2 são descritos os objetivos desta dissertação. Na Seção 1.3 são descritos os capítulos desta dissertação.

1.1 Motivação

A aprendizagem de máquina (AM) refere-se a um campo da ciência da computação em que os algoritmos “aprendem” com a experiência em relação a alguma tarefa, em que o algoritmo interpreta os dados e busca a melhor maneira de resolver este problema (MITCHELL et al., 1997; MAGLOGIANNIS, 2007). A AM é aplicada, por exemplo, para o reconhecimento de imagem e fala, identificação de padrões, filtragem de spams no e-mail, detecção de invasão na rede, detecção de fraudes, carros autônomos, otimização de estratégias, avaliação do comportamento do consumidor, desenvolvimento de estratégias para jogos de computador (DUNJKO; BRIEGEL, 2017), entre outras.

As aplicações atuais da AM requerem um grande volume de dados o que aumenta o custo computacional dos algoritmos de aprendizagem comprometendo o desempenho da AM clássica (BIAMONTE et al., 2017). Necessita-se de uma estratégia para reduzir o custo computacional dos algoritmos de aprendizado, permitindo que o desenvolvimento de aplicações com grandes volumes de dados de forma mais eficiente. Com a Computação Quântica (CQ) (NILSSON, 1996; WIEBE et al., 2012; REBENTROST et al., 2014; WIEBE et al., 2014) em concomitância com a Aprendizagem de Máquina (AM) (RUSSELL; NORVIG, 2016; ROSENBLATT, 1958; SASAKI et al., 2001; SASAKI; CARLINI, 2002) e a Inteligência Artificial (IA) (RUSSELL; NORVIG, 2016; HARROW et al., 2009; CLADER et al., 2013; WIEBE et al., 2012; WIEBE et al., 2014; REBENTROST et al., 2014; LLOYD et al., 2014) podem ser propostos algoritmos para aprendizado de máquina que possuam vantagens em relação aos algoritmos clássicos.

A computação quântica (CQ) (MANIN, 1999; NIELSEN; CHUANG, 2010;

FEYNMAN, 1982; BARENDS et al., 2014; DIVINCENZO et al., 2000) surgiu devido aos diferentes comportamentos que apresentam um estado da matéria em escala subatômica. Foi observado que o custo computacional da simulação de um sistema quântico por um computador clássico utilizando o melhor algoritmo conhecido é exponencialmente maior do que a simulação em um computador quântico, utilizando os algoritmos atuais. Um computador quântico utiliza recursos inerentemente quânticos, como, por exemplo, a superposição quântica (SILVA et al., 2012; HIRVENSALO, 2013), o emaranhamento quântico (ÖMER, 1998; HIRVENSALO, 2013), o paralelismo quântico (SILVA et al., 2012; HIRVENSALO, 2013), a interferência quântica (JOSÉ et al., 2013; HIRVENSALO, 2013) entre outros. A computação quântica tem sido utilizada para desenvolver algoritmos mais eficientes do que os algoritmos clássicos conhecidos (HARROW et al., 2009; CHILDS et al., 2015; REBENTROST et al., 2018; WIEBE et al., 2012; LLOYD et al., 2013; REBENTROST et al., 2014; WIEBE et al., 2014; LLOYD et al., 2014; DEUTSCH, 1985; SHOR, 1999; SIMON, 1997; GROVER, 1997).

O campo da Aprendizagem de Máquina Quântica (AMQ) oferece um grande potencial de aprimorar a AM clássica (SCHULD et al., 2015; BIAMONTE et al., 2017). Diversos algoritmos de AMQ já foram propostos (HARROW et al., 2009; CLADER et al., 2013; REBENTROST et al., 2014; WIEBE et al., 2014; LLOYD et al., 2014; RIGATOS; TZAFESTAS, 2007; KAK, 1995) utilizando redes neurais artificiais (RNA) (SILVA et al., 2016a; SILVA et al., 2016b; SILVA et al., 2012), reconhecimento de padrões (TRUGENBERGER, 2002; VENTURA; MARTINEZ, 2000; SCHÜTZHOLD, 2003; DUNJKO et al., 2016; CHIAPPETTA et al., 1994) no ganho na velocidade computacional para a execução de sub-rotinas de algoritmos clássicos de aprendizagem de máquina em um computador quântico (LLOYD et al., 2013; REBENTROST et al., 2014; WIEBE et al., 2014), no aperfeiçoamento da linguagem nos sistemas quânticos abertos, na aprendizagem quântica de máquina adiabática em algumas classes de otimização (NEVEN et al., 2009; PUDENZ; LIDAR, 2013; NEIGOVZEN et al., 2009), entre outros.

1.2 Problema de Pesquisa

Uma memória quântica probabilística (VENTURA; MARTINEZ, 2000; TRUGENBERGER, 2001) possibilita o aumento exponencial na capacidade de armazenamento de informações pela memória. Diversos estudos mostraram limitações da memória probabilística quântica (BRUN et al., 2003; SCHULD et al., 2014a; SCHULD et al., 2014b; DUNJKO; BRIEGEL, 2017). Em (DUNJKO; BRIEGEL, 2017) é afirmado que a memória quântica probabilística não é um modelo completo, pois, ao recuperar uma informação ocorre o colapso da memória, assim, o simples fato de observar o sistema pode alterá-lo. Constata-se uma segunda limitação deste modelo, em que ao ser utilizado como classificador não consegue classificar padrões de entrada muito próximos. Neste trabalho, mostrou-se uma variação a esta memória através de uma alteração ao modelo em que n (tamanho da memória) é substituído por um parâmetro denominado de ϕ , separando com mais eficácia o padrão de entrada em relação às memórias armazenadas, com isso, aumenta a probabilidade de classificação dos padrões. Conforme já abordado anteriormente, a modificação feita estabelece um ajuste a memória e o novo padrão de entrada deverá ser classificado com uma alta probabilidade, portanto, conseguindo separar este novo padrão de entrada.

O problema de pesquisa desta dissertação é uma área da computação quântica em bastante expansão, destacam-se trabalhos como (NJAJA et al., 2013; SCHULD et al., 2014a; SINGH et al., 2017) que utilizam o algoritmo para o reconhecimento de padrões quânticos para características binárias, processo baseado na memória quântica probabilística (MQP) (TRUGENBERGER, 2001). Segundo o modelo, a memória retorna com uma alta probabilidade em torno dos padrões que apresentam a menor distância de Hamming para os padrões de entrada. Ressalta-se o trabalho (DUNJKO; BRIEGEL, 2017), mencionando que o modelo sofre de falta de escalabilidade, isto é, se houver muitos padrões para inicializarem a memória, o custo computacional ficará elevado. Conforme (BRUN et al., 2003; SCHULD et al., 2014b) a desvantagem do modelo é apresentada na fase de recuperação da informação, pois, a memória colapsa e precisa ser novamente, reiniciada. Porém, em (TRUGENBERGER, 2003) afirma que o seu modelo deve apresentar um número de entrada polinomial. Em (SCHULD et al., 2014a) apresenta-se uma abordagem utilizando o modelo para o reconhecimento de padrões.

1.3 Objetivos

1.3.1 Geral

Aprimorar a Memória Quântica Probabilística, contribuindo para uma melhor adequação aos dados, através da inclusão de um parâmetro que permite um ajuste no cálculo da distância entre os padrões.

1.3.2 Específicos

1. Definir um modelo de Memória Quântica Probabilística Parametrizada que ao incluir um parâmetro ajustável, possibilite uma melhor adaptação e ajuste dos dados, aprimorando o desempenho na correta classificação dos padrões.
2. Definir um modelo de Memória Quântica Probabilística Parametrizada que possua ganho exponencial em relação à memória clássica no tamanho da memória. Utilizando como base, a definição de uma memória quântica probabilística.
3. Avaliar a Memória Quântica Probabilística Parametrizada utilizando dados artificiais.

1.4 Mapa de pesquisa

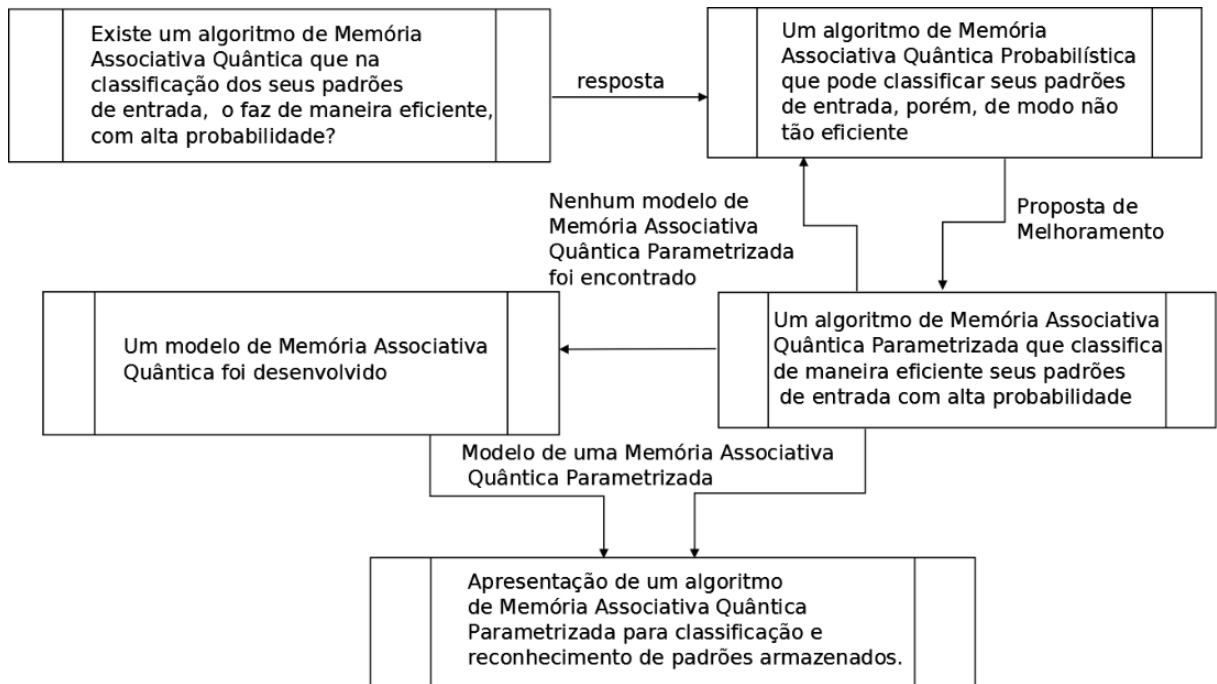
O mapa na Fig. 1 apresenta de forma geral a estrutura lógica das etapas executadas nesta pesquisa.

1.5 Organização da dissertação

O restante deste trabalho está dividido em 4 capítulos. No capítulo 2 são descritos conceitos, processos e estruturas da computação quântica tais como: conceito de qubit; produto tensorial; operações sobre dois qubits; circuitos quânticos; portas quânticas; superposição quântica; emaranhamento quântico; teorema da não-clonagem. É também apresentado no capítulo 2, o algoritmo de Grover. No capítulo 3 é descrita a memória quântica probabilística com capacidade exponencial de armazenar 2^n padrões de n qubits utilizando n bits quânticos. No capítulo 4 é apresentado a modificação proposta ao modelo da memória quântica probabilística, definida como memória quântica probabilística

parametrizada através da inclusão de um parâmetro ajustável ϕ . Neste capítulo são apresentados os resultados deste trabalho. No capítulo 5 são apresentadas a conclusão da dissertação, as considerações finais e sugestões para trabalhos futuros.

Figura 1 – Mapa de Pesquisa das atividades em ordem cronológica



Fonte: O autor, 2018

2 Computação Quântica

Neste capítulo é realizada uma introdução aos conceitos de computação quântica necessários para o entendimento desta dissertação. Na Seção 2.2 são apresentados os postulados da mecânica quântica. Na Seção 2.3 é definido o bit quântico (qubit). Na Seção 2.4 é definido o produto tensorial. Na Seção 2.5 é definido o emaranhamento quântico. Na Seção 2.6 são definidos as operações sobre um qubit. Na Seção 2.7 são definidos as operações sobre dois qubits. Na Seção 2.8 são descritos os circuitos quânticos e portas quânticas. Na Seção 2.9 é apresentado a propriedade da superposição quântica. Na Seção 2.10 é apresentado o paralelismo quântico. Na Seção 2.11 é apresentado o teorema da não clonagem. Na Seção 2.12 é descrito o algoritmo de Grover.

2.1 Introdução

Desde o ábaco até os supercomputadores, a computação era baseada na física clássica. O estudo da computação quântica (NIELSEN; CHUANG, 2002) teve o seu início na década de 1980. Richard Feynman em 1982 (FEYNMAN, 1982) afirmou que a simulação de sistemas quânticos por um computador clássico admite um elevado custo computacional e este custo poderia ser reduzido utilizando-se um computador quântico. Destaca-se na computação quântica a possibilidade de possuir algoritmos quânticos com custo computacional inferior aos algoritmos clássicos conhecidos, numa mesma classe de problemas. Por exemplo, o algoritmo de fatoração de Shor (SHOR, 1999) com ganho exponencial em relação ao melhor algoritmo clássico conhecido, o algoritmo de busca de Grover (GROVER, 1997) que tem ganho quadrático sobre o melhor algoritmo clássico, a simulação de sistemas quânticos, entre outros.

Ressalta-se nesta área, o princípio da superposição em que um qubit está em mais de um estado e, portanto, trabalha simultaneamente. Esta propriedade de um qubit, contribui na capacidade dos algoritmos quânticos na resolução de problemas, inclusive no desenvolvimento de algoritmos de aprendizagem quântica como árvores de decisão (FARHI; GUTMANN, 1998; LU; BRAUNSTEIN, 2014), algoritmos evolutivos (MALOSSINI et al., 2008), redes neurais sem peso (OLIVEIRA et al., 2008; OLIVEIRA,

2009; GRALEWICZ, 2004; NARAYANAN; MENNEER, 2000) e memórias associativas (VENTURA; MARTINEZ, 2000; TRUGENBERGER, 2001).

2.2 Postulados da Mecânica Quântica

Nesta Seção são descritos os quatro postulados da mecânica quântica, como apresentados em (NIELSEN; CHUANG, 2002). Os postulados da mecânica quântica definidos abaixo, serão utilizados nas Seções 2.3 a 2.10 na apresentação dos conceitos da computação quântica.

1º Postulado. Todo e qualquer sistema físico isolado está associado a um espaço vetorial complexo V com produto interno. O espaço vetorial provido de produto interno (cuja notação $\langle v, w \rangle$), definido pela norma $|v| = \sqrt{\langle v, v \rangle}$. Um sistema é absolutamente descrito por um vetor unitário (vetor de estado) em V .

2º Postulado. A evolução de um sistema quântico fechado é descrito por uma transformação unitária. Ou seja, o estado $|\Psi\rangle$ de um sistema no instante t_1 está relacionado com o estado $|\Psi'\rangle$ do sistema no instante t_2 por uma transformação unitária U que depende apenas de t_1 e t_2 .

$$|\Psi'\rangle = U |\Psi\rangle$$

3º Postulado. Este postulado define a medição quântica como sendo um conjunto de operadores M_m de medição. Estes operadores atuam sobre o espaço vetorial associado ao sistema que está sendo medido. O índice m refere-se ao valor de leitura possível, chamado de observável (saídas) que ocorrem na medição. Se o estado do sistema quântico é $|\Psi\rangle$ imediatamente antes da medição ocorrer, então a probabilidade do resultado m ocorrer é determinada por

$$p(m) = \langle \Psi | M_m^\dagger M_m | \Psi \rangle,$$

O estado do sistema após a medida é:

$$\frac{M_m |\Psi\rangle}{\sqrt{\langle\Psi| M_m^\dagger M_m |\Psi\rangle}}$$

Os operadores de medição que devem satisfazer a equação de completude:

$$\sum_m M_m^\dagger M_m = I$$

4º Postulado. O estado de um sistema físico composto é o produto tensorial dos estados dos sistemas físicos componentes. Sejam V e W dois espaços vetoriais de dimensões x e y respectivamente. O novo espaço vetorial $V \otimes W$ tem dimensão $x \cdot y$ e seus vetores são descritos através de combinações lineares da sua base. Como por exemplo, se os sistemas estiverem numerados de 1 a p e o número i estiver no estado $|\Psi_i\rangle$, então o estado do sistema total é $|\Psi_i\rangle \otimes \dots \otimes |\Psi_p\rangle$.

2.3 Qubits

Em computação quântica, um bit quântico ou qubit é um vetor unitário (YOUNG, 1988) denominado de estado quântico e pode ser representado no espaço vetorial \mathbb{C}^2 , descrito numa sobreposição conforme mostra a Equação 2.3.1,

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2.3.1)$$

onde α e β são os coeficientes complexos e também chamados de amplitudes de probabilidade de um estado quântico, restritos pela condição de normalização $|\alpha|^2 + |\beta|^2 = 1$ e $|0\rangle$ e $|1\rangle$ são os vetores descritos na Equação 2.3.2.¹

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{e} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2.3.2)$$

O bit quântico poderá estar simultaneamente nos estados $|0\rangle$ e $|1\rangle$, mas após uma medição ser realizada altera seu estado, assumindo o estado $|0\rangle$ com probabilidade $|\alpha|^2$ ou o estado $|1\rangle$ com probabilidade $|\beta|^2$.

¹ Em computação quântica usa-se qualquer base ortonormal, porém a base computacional (canônica) é a mais utilizada.

2.4 Produto Tensorial

Representa-se um qubit em um sistema quântico n -dimensional como um vetor unitário no espaço vetorial C^{2^n} com o descritor na Equação 2.4.1.

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |\Psi_i\rangle \quad \text{restrito por} \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1 \quad (2.4.1)$$

Seja $|\Psi\rangle$ um sistema geral constituído por dois sistemas, em que $|\alpha\rangle_1$ e $|\varphi\rangle_2$ são os vetores de estado nos espaços de Hilbert distintos, \hat{H}_1 e \hat{H}_2 . Tem-se que,

$$|\Psi\rangle = |\alpha\rangle_1 \otimes |\varphi\rangle_2.$$

Representa-se \otimes como o produto tensorial que descreve o estado de seus componentes.

2.5 Emaranhamento Quântico

Observe o vetor no estado:

$$|\Psi\rangle = \frac{|0,0\rangle + |1,1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} |0\rangle |0\rangle + \frac{1}{\sqrt{2}} |1\rangle |1\rangle$$

Então

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

Dados dois espaços vetoriais W_1 e W_2 , sendo $W_1 = s_0 |0\rangle + s_1 |1\rangle$ e $W_2 = v_0 |0\rangle + v_1 |1\rangle$

Reescrevendo como produto tensorial, tem-se que

$$(s_0 |0\rangle + s_1 |1\rangle) \otimes (v_0 |0\rangle + v_1 |1\rangle) = s_0 v_0 |00\rangle + s_0 v_1 |01\rangle + s_1 v_0 |10\rangle + s_1 v_1 |11\rangle$$

Observa-se que o estado $|\Psi\rangle$ acima, não pode ser descrito como produto tensorial, pois: $|\Psi\rangle = s_0 v_0 = s_1 v_1 = \frac{1}{\sqrt{2}}$ e $s_0 v_1 = s_1 v_0 = 0$, implica que o estado apresenta os dois qubits emaranhados. Portanto, em geral, se um determinado estado não puder ser descrito como produto tensorial de dois qubits, significa que o sistema está emaranhado.

2.6 Operações sobre um qubit

Um operador quântico que atua em um sistema quântico com n qubits é definido como um operador linear e unitário em \mathbb{C}^{2^n} . Fixada uma base, corresponde a matrizes unitárias de dimensão $2^n \times 2^n$. Uma matriz é unitária se $UU^\dagger = U^\dagger U = I$, onde U^\dagger representa a transposta conjugada de U e I é a matriz identidade.

Os vetores de estados são transformados por matrizes unitárias, sendo que estas transformações conservam o comprimento e a quantidade de informação do sistema que o vetor apresentava ao sistema quântico.

Têm-se como matrizes unitárias, por exemplo, a porta X e a porta Hadamard (H) descritas nas Equações 2.6.1 e 2.6.2

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.6.1)$$

O operador X atua sobre os estados da base computacional, como $X|0\rangle = |1\rangle$ e $X|1\rangle = |0\rangle$.

A porta Hadamard (H) é definida pelo operador:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2.6.2)$$

As operações sobre os qubits em um estado em superposição operam linearmente, conforme Equação 2.6.3, onde X é aplicado a um estado quântico $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle \quad (2.6.3)$$

Alguns exemplos de operadores quânticos são as matrizes de Pauli formado pelos operadores descritos a seguir:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \text{e} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2.6.4)$$

Outro exemplo de operador quântico é a porta quântica CNOT (*controlled not*) que apresenta dois qubits de entrada, sendo um qubit de controle (qubit superior) e o outro chamado de qubit alvo (qubit inferior).

A representação do CNOT por uma matriz unitária é dada conforme a Equação 2.6.5.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (2.6.5)$$

Circuito que implementa a porta CNOT conforme mostra a Figura 2.

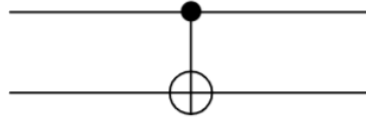


Figura 2 – Porta quântica (CNOT)

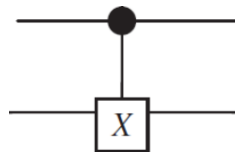


Figura 3 – Outra representação da porta quântica (CNOT)

2.6.1 A porta de Toffoli

Esta porta apresenta três qubits de entrada. É uma porta C-NOT duplamente controlada: o qubit alvo só inverte de estado se os dois qubits de controle forem $|1\rangle$.

Representa-se a porta de Toffoli em um circuito quântico como:

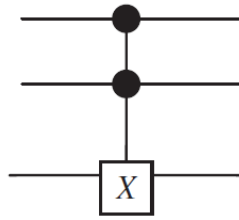


Figura 4 – Porta de Toffoli

A matriz que corresponde a esta porta é

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Figura 5 – Porta de Toffoli

Operações lógicas clássicas podem ser implementadas com operadores quânticos (circuitos quânticos) usando o operador de Toffoli, por ser uma *CNOT* duplamente controlada. Conforme mostra a Equação 2.6.6:

$$T |x, y, z\rangle = |x, y, z \oplus (x \cdot y)\rangle \quad (2.6.6)$$

2.6.2 A porta U-controlada

É uma porta em que U é uma operação unitária sobre dois qubits e cuja ação é descrita pela Figura 6.

2.7 Circuitos quânticos e portas quânticas

Os circuitos quânticos são compostos por um conjunto de portas lógicas (responsáveis em realizar operações básicas em um computador) que operam um conjunto de transformações dos qubits realizadas em “componentes” chamados portas quânticas.

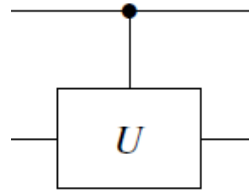


Figura 6 – Porta U-controlada

Na computação quântica, as portas quânticas são representadas por operadores unitários que atuam sobre um qubit. Por exemplo, a porta de Hadamard (é uma das principais portas da computação quântica) e quando aplicada a um estado na base computacional gera uma superposição nas duas bases, conforme descrito na Figura 7.

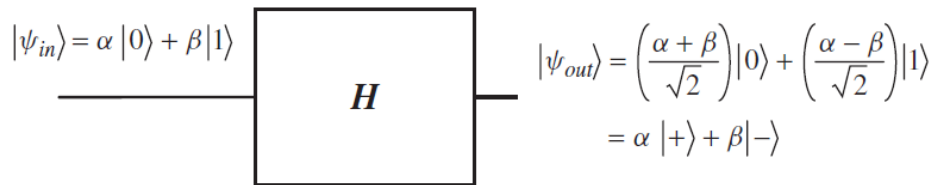


Figura 7 – Circuito de uma porta Hadamard

2.8 Superposição quântica

Um sistema físico pode se encontrar em vários estados. Dessa forma, eles podem estar numa superposição de estados. A superposição é um fenômeno da física quântica que indica que um sistema quântico pode estar em dois ou mais estados simultaneamente, relacionando-se como uma combinação de vetores. Em que a função $|\Psi\rangle$ se apresenta em uma superposição dos estados de base $|\phi\rangle$ também formados pelo conjunto dos estados no espaço de Hilbert que formam uma base e o sistema é descrito por um estado quântico como mostra a Equação 2.8.1.

$$|\Psi\rangle = \sum_i c_i |\phi_i\rangle \quad (2.8.1)$$

Em que os coeficientes c_i podem ser complexos.

2.9 Paralelismo quântico

Um computador quântico torna possível a resolução de um grande número de problemas complexos, com o chamado paralelismo quântico.

Os computadores quânticos realizam esse procedimento em paralelo, em que todas as componentes do sistema são processadas simultaneamente. Por exemplo, considerando uma função $f(x) : \{0, 1\} \rightarrow \{0, 1\}$ criando um operador unitário U_f que implementa f como mostra a Equação 2.9.1. Com uma única operação, calcula-se simultaneamente, os dois valores da função $f(x)$, inicialmente, com um estado $|0\rangle$ e aplicando a porta de Hadamard, conforme a Equação 2.9.2.

$$U_f |x, y\rangle = |x, y \oplus f(x)\rangle \quad (2.9.1)$$

$$U_f \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |0\rangle = \frac{1}{\sqrt{2}} (U_f |00\rangle + U_f |10\rangle) = \frac{|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle}{\sqrt{2}} \quad (2.9.2)$$

2.10 Não Clonagem

Teorema 1. (*Teorema da Não-Clonagem*). *É impossível clonar um bit quântico.*

Demonstração. Suponha que exista U um operador unitário, portanto, linear, possível “candidato” a clonagem de estados quânticos, do estado quântico $|\Psi\rangle$ para o estado alvo $|\chi\rangle$. Sejam $|\Psi\rangle$ e $|\chi\rangle$ dois estados quânticos ortogonais.

Tem-se que $|\Psi\rangle = a|0\rangle + b|1\rangle$. Então,

$$U(|\Psi\rangle \otimes |\chi\rangle) = |\Psi\rangle \otimes |\psi\rangle$$

Portanto

$$(a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) = (a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle) \quad (2.10.1)$$

Pela linearidade de U

$$U(a|0\rangle + b|1\rangle) \otimes |\chi\rangle = U(a|0\rangle \otimes |\chi\rangle + b|1\rangle \otimes |\chi\rangle) \quad (2.10.2)$$

Aplicando o produto interno entre as Equações 2.10.2 e 2.10.1 obtém-se valores diferentes, portanto, nenhum operador unitário é capaz de clonar um estado quântico arbitrário. ■

2.11 Algoritmos Quânticos

Nesta Seção é descrito o algoritmo de Grover que resolve o problema da busca com ganho quadrático em relação ao melhor algoritmo clássico conhecido.

2.11.1 Algoritmo de Grover

Grover (1996) propôs um algoritmo através do qual realiza uma busca para encontrar um elemento em um conjunto de dados não estruturados de forma mais rápida que um algoritmo clássico similar. Ao analisar uma lista não ordenada de N elementos, com o objetivo de encontrar um determinado elemento desta lista, o algoritmo de Grover (GROVER, 1996) custo computacional $O(\sqrt{N})$, onde N é a quantidade de elementos do conjunto de entrada.

O algoritmo de Grover é probabilístico. Este algoritmo também apresenta uma melhora quadrática quando comparado com os algoritmos clássicos de busca (YANOFSKY et al., 2008).

O algoritmo de Grover utiliza dois registradores quânticos: o primeiro registrador com n qubits no estado $|0 \dots 0\rangle$ e o segundo registrador com um qubit auxiliar no estado $|1\rangle$, aplicando o operador de Hadamard nos qubits do primeiro registrador. Portanto, a superposição é denotada por:

$$|\Psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} H |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \quad (2.11.1)$$

Aplicando-se n vezes o operador de Hadamard, obtém-se uma superposição com 2^n estados com igual probabilidade.

O operador linear U_f representado por: $U_f (|x\rangle |y\rangle) = |x\rangle |y \oplus f(x)\rangle$, em que $|x\rangle$ representa a entrada da função e o $|y\rangle$ é um qubit que serve para marcar o elemento

procurado. O operador unitário U_f é definido pela função representada na Equação 2.11.2 a ser implementada pelo operador.

$$f(x) = \begin{cases} 1, & \text{se } x \text{ é o elemento procurado} \\ 0, & \text{se caso contrário} \end{cases} \quad (2.11.2)$$

O efeito do operador U_f sobre o primeiro registrador constituído com um estado computacional e o segundo registrador com um qubit adicional no estado $|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$, onde $|-\rangle$ é o segundo registrador.

Tem-se que:

$$\begin{aligned} |\Psi_1\rangle &= U_f(|x\rangle|-\rangle) = U_f\left(\frac{|x\rangle|0\rangle - |x\rangle|1\rangle}{\sqrt{2}}\right) = \left(\frac{U_f(|x\rangle|0\rangle) - U_f(|x\rangle|1\rangle)}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2}} (|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle) = |x\rangle \left[\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right] \end{aligned}$$

O resultado mostra que somente o elemento que satisfaz a função de U_f será marcado com um sinal negativo, conforme resulta o valor descrito na Equação 2.11.3

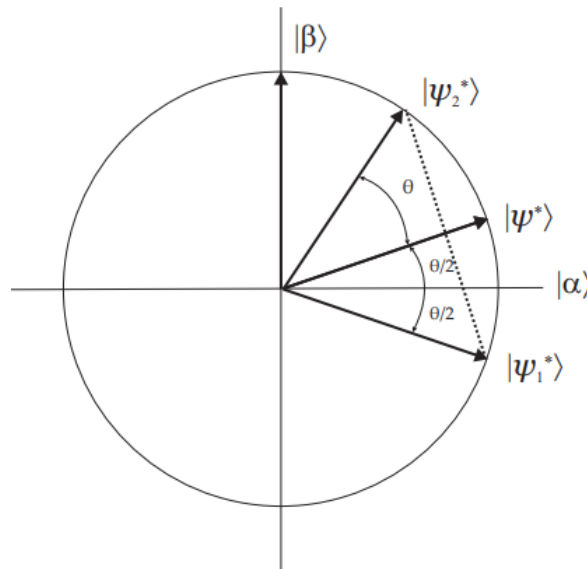
$$|\Psi_2\rangle = (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = \begin{cases} -1 |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \text{se } f(x) = 0 \\ +1 |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \text{se } f(x) = 1 \end{cases} \quad (2.11.3)$$

O estado do primeiro registrador permanece em superposição de todos os possíveis estados associados aos elementos da sequência. No entanto, a amplitude do elemento procurado foi alterado de $\frac{1}{\sqrt{N}}$ para $-\frac{1}{\sqrt{N}}$.

O próximo passo para aumentar a probabilidade do elemento procurado com uma mudança de fase, utiliza-se um procedimento denominado de **inversão sobre a média**. A inversão sobre a média é um operador que aumenta ou diminui a amplitude de um estado, ou seja, aumenta a amplitude quando o estado está abaixo da média e é diminuída quando o estado está acima da média, preservando a distância entre a média e o estado (número), resumidamente, inverte-se cada elemento em relação a média.

Sendo o vetor $|\Psi^*\rangle = a|\alpha\rangle + b|\beta\rangle$, após a ação do operador unitário U_f resulta numa reflexão na direção do vetor unitário $|\beta\rangle$, sendo $|\beta\rangle$ o vetor considerado como o elemento procurado e α como seu vetor ortogonal. A atuação da amplitude resulta na reflexão de $|\Psi^*\rangle$. Observa-se que a composição dessas duas reflexões impostas pelo operador unitário U_f e a amplitude é conhecida como **iteração de Grover**. Como resultado global da aplicação desta iteração, tem-se a rotação do $|\Psi^*\rangle$ por um ângulo θ aproximando do vetor $|\beta\rangle$. Induzindo-se pela Figura 10, que pode refletir o vetor $|\Psi_1^*\rangle$ em relação ao vetor $|\Psi^*\rangle$, para aumentar a amplitude do elemento procurado $|\beta\rangle$, em relação a sua amplitude no estado $|\Psi^*\rangle$.

Figura 8 – Representação gráfica da iteração de Grover



De acordo com o Algoritmo 1, tem-se que M é o número de respostas no espaço de

pesquisa.

Algoritmo 1: ALGORITMO DE GROVER

início

Inicialize o sistema $|\Psi\rangle = |0\rangle_n$

Aplique o operador de Hadamard $|\Psi\rangle = H^{\otimes n} |\Psi\rangle$

Aplique a operação de inversão de fase $U_f(I \otimes H)$

Aplique a inversão sobre a média $(-I + 2M)$

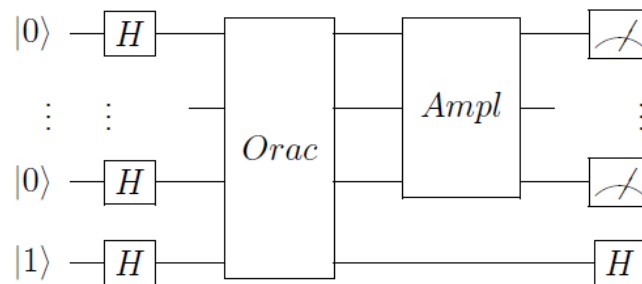
Repita os passos 3 e 4 por $\sqrt{2^n}$ vezes

Realize uma medição dos qubits no estado $|\Psi\rangle$

fim

O circuito é então representado pela Figura 9.

Figura 9 – Circuito quântico que implementa o algoritmo de Grover



3 Memória Quântica Probabilística

Neste capítulo será descrito a memória quântica probabilística, cuja capacidade de armazenamento é incrementada para armazenar 2^n padrões com n qubits quânticos sendo utilizados apenas n qubits. Na Seção 3.2 é apresentado o algoritmo de armazenamento de padrões quânticos em uma memória quântica probabilística, na Seção 3.3 é apresentado o algoritmo para recuperação de informação de uma memória quântica probabilística, cujo processo de recuperação é probabilístico e a Seção 3.4 é um sumário do capítulo.

3.1 Introdução

As Memórias Associativas Quânticas (MAQ) são algoritmos de computação quântica que simulam a propriedade da memória associativa (SCHULD et al., 2014b). As memórias associativas (que permitem o acesso pelo conteúdo) através do qual a recuperação da informação não necessita do conhecimento prévio do endereço da memória apenas, do conhecimento “parcial” do conteúdo. Considerando que a memória dispõe da sua capacidade ampliada nas suas duas fases do processo, tanto no reconhecimento como na classificação de padrões, destaca-se, portanto, a importância da implementação de um algoritmo quântico que permite facilitar a classificação de padrões.

A recuperação de um estado baseia-se no algoritmo de Grover para a busca de um padrão em uma superposição de uma sequência completa, em que o algoritmo de Grover é modificado para o estado inicial $|m\rangle$ sendo que contém apenas uma seleção de estados básicos. Por fim, o algoritmo resultante possibilita a recuperação de todos os padrões que apresentam uma determinada string de entrada (VENTURA; MARTINEZ, 2000).

A memória quântica probabilística descrita por (TRUGENBERGER, 2001), propõe uma melhoria na capacidade de armazenamento das memórias associativas, onde um conjunto de padrões binários p formados com os n bits tem capacidade de armazenamento exponencial no número n de qubits, isto é $p_{max} = 2^n$, ou seja, todos os padrões binários formados com os n bits podem ser armazenados.

O modelo proposto neste trabalho utiliza para a sua implementação alguns operadores quânticos já mencionados neste trabalho, como também, os operadores descritos

a seguir:

$$CS^i = |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes S^i \quad (3.1.1)$$

$$S^i = \begin{pmatrix} \sqrt{\frac{i-1}{i}} & \frac{1}{\sqrt{i}} \\ -\frac{1}{\sqrt{i}} & \sqrt{\frac{i-1}{i}} \end{pmatrix} \quad (3.1.2)$$

É importante salientarmos que além das portas NOT, H (Hadamard), XOR, 2XOR (Toffoli), porta nXOR e a porta de CS^i descrita na Equação 3.1.1 é imprescindível, apresentar dois operadores responsáveis na implementação do algoritmo neste capítulo, descritos nas Equações 3.1.2 e 3.1.3

$$U = \begin{pmatrix} e^{i\frac{\pi}{2n}} & 0 \\ 0 & 1 \end{pmatrix} \quad (3.1.3)$$

Para a implementação do algoritmo de armazenamento dos padrões do modelo proposto é necessário que os dados p dos padrões p^i possam gerar um determinado estado quântico, sendo que os padrões a serem armazenados são colocados em superposição, como na Equação 3.1.4. Empregando-se o modelo proposto por Trugenberger, para colocar este estado em superposição, conforme descrito na Seção 3.2 e para o processo de recuperação de informação será utilizado o algoritmo na Seção 3.3.

$$|m\rangle = \frac{1}{\sqrt{p}} \sum_{i=1}^p |p^i\rangle \quad (3.1.4)$$

3.2 O algoritmo de armazenamento de padrões quânticos

Para o armazenamento de padrões quânticos, usa-se três registros quânticos, descritos a seguir:

- Um primeiro registro p com n qubits em que os padrões p são armazenados ao sistema;

- Um segundo registro denominado de registro auxiliar u contendo dois qubits;
- Um terceiro registro \mathbf{m} com n qubits para manter a memória $|m\rangle$.

A proposta do algoritmo de armazenamento é separar este estado em dois termos, um correspondente aos padrões já armazenados e outro pronto para processar um novo padrão. O estado do segundo qubit auxiliar u_2 é verificar os seguintes padrões:

- Se $u_2 = |0\rangle$ os padrões já foram armazenados e
- Se $u_2 = |1\rangle$ termos em processamento.

Inicialmente, temos que construir o estado quântico $|m\rangle$, iniciando com o estado $|\Psi_0^1\rangle$ descrito na Equação 3.2.1, com o uso de três registros:

Sendo o primeiro registro p com n qubits, em que os padrões p^i serão inseridos no decorrer do processo; um registro utilitário u com dois qubits $|01\rangle$ e um registro $|m\rangle$ com n qubits, iniciando com $0_1, \dots, 0_n$ que deve manter a memória.

$$|\Psi_0^1\rangle = |p_1^1, \dots, p_n^1; 01; 0_1, \dots, 0_n\rangle. \quad (3.2.1)$$

Para cada padrão p^i a ser armazenado, executa-se as operações descritas abaixo:

$$|\Psi_1^i\rangle = \prod_{j=1}^n 2XOR_{p_j^i u_2 m_j} |\Psi_0^i\rangle \quad (3.2.2)$$

A Equação 3.2.2 descreve o operador que copia o padrão p^i do registro p para o registro de memória m

$$|\Psi_2^i\rangle = \prod_{j=1}^n NOT_{m_j} XOR_{p_j^i m_j} |\Psi_1^i\rangle \quad (3.2.3)$$

O operador descrito na Equação 3.2.3 faz que todos os qubits do registro de memória m assumam $|1\rangle$ quando o conteúdo dos registros de padrão e de memória são idênticos, o que é exatamente o caso para o termo em processamento.

$$|\Psi_3^i\rangle = nXOR_{m_1 \dots m_n u_1} |\Psi_2^i\rangle \quad (3.2.4)$$

A operação descrita na Equação 3.2.4, o primeiro qubit utilitário tem seu valor alterado para $|1\rangle$.

$$|\Psi_4^i\rangle = CS_{u_1 u_2}^{p+1-i} |\Psi_3^i\rangle \quad (3.2.5)$$

A operação descrita na Equação 3.2.5 é a operação central do algoritmo de armazenamento, separando o novo padrão a ser armazenado com a sua respectiva normalização.

$$|\Psi_5^i\rangle = nXOR_{m_1 \dots m_n u_1} |\Psi_4^i\rangle \quad (3.2.6)$$

$$|\Psi_6^i\rangle = \prod_{j=n}^1 XOR_{p_j^i m_j} NOT_{m_j} |\Psi_5^i\rangle \quad (3.2.7)$$

As operações das Equações 3.2.6 e 3.2.7 são o inverso das Equações 3.2.4 e 3.2.3, restaurando o qubit utilitário u_1 e o registro de memória m para seus valores iniciais, dessa forma o estado do sistema estará da seguinte maneira:

$$|\Psi_6^i\rangle = \frac{1}{\sqrt{p}} \sum_{k=1}^i |p^i; 00; p^k\rangle + \sqrt{\frac{p-i}{p}} |p^i; 01; p^i\rangle \quad (3.2.8)$$

A operação descrita na Equação 3.2.9 restaura o registro m do termo de processamento, isto é, o segundo termo na Equação 3.2.8 retorna ao valor inicial $0_1, \dots, 0_n$. Pelo exposto, submete-se um novo padrão ao registro p , acarretando a repetição de todo o processo até que o registro m esteja no estado $|m\rangle$.

$$|\Psi_7^i\rangle = \prod_{j=n}^1 2XOR_{p_j^i u_2 m_j} |\Psi_6^i\rangle \quad (3.2.9)$$

3.3 O algoritmo de recuperação de padrões quânticos

Segundo o algoritmo proposto pela memória quântica probabilística, a etapa de recuperação da informação consiste em recuperar o padrão de entrada, porém, logo após esta etapa, a memória precisa ser reiniciada e é realizada uma medição no registro c , em

que uma busca probabilística é feita e retorna com a probabilidade indicativa da memória que o padrão está contido, ou seja, a memória reconhece ou não os padrões.

Para o algoritmo de recuperação (como o de armazenamento), usa-se três registros quânticos:

- O primeiro registro i de n qubits que apresenta o padrão de entrada;
- O segundo registro m também com n qubits, contém a memória $|m\rangle$;
- O terceiro registro c contém um único qubit de controle $|c\rangle$ inicializado com o operador de Hadamard, ficando no estado $(|0\rangle + |1\rangle) / \sqrt{2}$.

O estado inicial é:

$$|\Psi_0\rangle = \frac{1}{\sqrt{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 0\rangle + \quad (3.3.1)$$

$$\sqrt{\frac{1}{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 1\rangle$$

Inicializado o processo, aplicamos uma combinação de operadores quânticos conforme Equação 3.3.2.

$$|\Psi_1\rangle = \prod_{k=1}^n NOT_{m_k} XOR_{i_k m_k} |\Psi_0\rangle \quad (3.3.2)$$

A Equação 3.3.2 descreve a operação que permite que os qubits no registro de memória fiquem no estado $|1\rangle$ se $i_j = p_j^k$ são idênticos e $|0\rangle$ caso contrário.

O estado Ψ_1 é descrito na Equação 3.3.3 em que $d_j^k = 1$ se e somente se $i_j = p_j^k$ e $d_j^k = 0$, caso contrário.

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 0\rangle + \quad (3.3.3)$$

$$\sqrt{\frac{1}{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 1\rangle$$

Considere o seguinte operador dado por:

$$\mathcal{H} = (d_H)_m \otimes (\sigma_3)_c, \quad (3.3.4)$$

$$(d_H)_m = \sum_{k=1}^n \left(\frac{\sigma_3 + 1}{2} \right)_{m_k},$$

O valor de $|\Psi_2\rangle$ é calculado através do operador descrito na Equação 3.3.5.

$$|\Psi_2\rangle = \exp\left(i\frac{\pi}{2n}\mathcal{H}\right)|\psi_1\rangle \quad (3.3.5)$$

Observamos que $|\Psi_2\rangle$ pode ser calculado com o uso de operadores quânticos elementares e com o operador U como descrito na Equação 3.3.6.

$$\exp\left(i\frac{\pi}{2n}\mathcal{H}\right)|\Psi_1\rangle = \prod_{i=1}^n (CU^{-2})_{cm_i} \prod_{j=1}^n U_{m_j} |\Psi_1\rangle, \quad (3.3.6)$$

A operação descrita na Equação 3.3.6 mede o número de zeros no registro m , com um sinal positivo se c está no estado $|0\rangle$ e um sinal negativo se c está no estado $|1\rangle$. Esta operação aplicada ao estado $|\Psi_1\rangle$, determinará o número de qubits entre a entrada e os padrões armazenados na memória (distância de Hamming). O estado $|\Psi_2\rangle$ será descrito na Equação 3.3.7, onde $d_H(i, p^k)$ é a distância de Hamming entre a entrada i e o padrão armazenado p^k .

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^p}} \sum_{k=1}^p \exp\left[i\frac{\pi}{2n}d_H(i, p^k)\right] |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 0\rangle + \quad (3.3.7)$$

$$\frac{1}{\sqrt{2^p}} \sum_{k=1}^p \exp\left[-i\frac{\pi}{2n}d_H(i, p^k)\right] |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 0\rangle,$$

Concluimos a parte determinística do algoritmo, realizando uma operação quântica inversa a Equação 3.3.2, restaurando o registro de memória ao estado $|m\rangle$ e aplica-se o operador Hadamard ao qubit de controle c , como descrito na Equação 3.3.8.

$$|\Psi_3\rangle = H_c \prod_{k=n}^1 \text{XOR}_{i_k} m_k \text{NOT}_{m_k} |\Psi_2\rangle, \quad (3.3.8)$$

Observamos que o estado $|\Psi_3\rangle$ estará como descrito na Equação 3.3.9, observe que se $d_H(i, p^k) \rightarrow 0$ então, $\cos\left[\frac{\pi}{2n}d_H(i, p^k)\right] \rightarrow 1$ e $\sin\left[\frac{\pi}{2n}d_H(i, p^k)\right] \rightarrow 0$ e se $d_H(i, p^k) \rightarrow n$

então, $\cos \left[\frac{\pi}{2n} d_H(i, p^k) \right] \rightarrow 0$ e $\sin \left[\frac{\pi}{2n} d_H(i, p^k) \right] \rightarrow 1$.

$$|\Psi_3\rangle = \frac{1}{\sqrt{p}} \sum_{k=1}^p \cos \frac{\pi}{2n} d_H(i, p^k) |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 0\rangle + \quad (3.3.9)$$

$$\frac{1}{\sqrt{p}} \sum_{k=1}^p \sin \frac{\pi}{2n} d_H(i, p^k) |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 1\rangle.$$

Uma medição é realizada no registro c e as probabilidades que resultam em $|0\rangle$ e $|1\rangle$ são descritas nas Equações 3.3.10 e 3.3.11.

$$P(|c\rangle = |0\rangle) = \sum_{k=1}^p \frac{1}{p} \cos^2 \left(\frac{\pi}{2n} d_H(i, p^k) \right), \quad (3.3.10)$$

$$P(|c\rangle = |1\rangle) = \sum_{k=1}^p \frac{1}{p} \sin^2 \left(\frac{\pi}{2n} d_H(i, p^k) \right) \quad (3.3.11)$$

Apresentando um novo padrão ao registro de entrada, em que é aplicado a parte determinística do algoritmo de recuperação, conforme as Equações 3.3.10 e 3.3.11. Em que, se o padrão de entrada for muito diferente de todos os padrões armazenados, então $d_H(i, p^k) \rightarrow n$, tem uma alta probabilidade de que a medição do qubit de controle seja $|c\rangle = |1\rangle$. Pelo contrário, se então $d_H(i, p^k) \rightarrow 0$ um padrão de entrada próximo de todos os padrões armazenados leva a uma alta probabilidade de medir $|c\rangle = |0\rangle$ e é realizada uma medição no registro de memória para identificá-lo e classificá-lo. Este processo pode ser repetido por T vezes. Caso dentre estas repetições o resultado for $|1\rangle$, o padrão não foi reconhecido.

Algoritmo 2: ALGORITMO DE RECUPERAÇÃO DE INFORMAÇÃO DA MEMÓRIA QUÂNTICA PROBABILÍSTICA

início

Inicialize o sistema com o estado quântico $H|0\rangle$ no registro c
 Aplique os operadores NOT e 2XOR no registro m
 Aplique os operadores CU^{-2} e U no registro m
 Aplique os operadores 2XOR e NOT no registro m e $H|0\rangle$ no registro c
 Realize uma medição no registro c

fim

Visando à necessidade de compreensão da fase de recuperação de padrões do Algoritmo 2, será apresentado um exemplo concreto com o uso de um conjunto de dados artificiais descrito abaixo.

Exemplo 1: Sejam duas classes representadas no conjunto de treinamento:

$ m_1\rangle$	$ m_2\rangle$
011101010000000000000000	101001110000000000000000
010101010100000000000000	101001010100000000000000
011101000100000000000000	101001010000000000000000
001101010100000000000000	101001000100000000000000

Sendo o padrão de entrada $|i\rangle = |011101010100000000000000\rangle$, inicializa-se o registro c com $H|0\rangle$, ou seja, o registro é iniciado com o estado $|c\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$,

obtendo-se o estado, como descrito na Equação 3.3.12

$$\begin{aligned}
|\Psi_0\rangle = & \frac{1}{\sqrt{4}} |i\rangle [|0111010100000000000000000000\rangle + |0101010101000000000000000000\rangle + \\
& |0111010001000000000000000000\rangle + |0011010101000000000000000000\rangle] |c\rangle + \\
& \frac{1}{\sqrt{4}} |i\rangle [|1010011100000000000000000000\rangle + |1010010101000000000000000000\rangle + \\
& |1010010100000000000000000000\rangle + |1010010001000000000000000000\rangle] |c\rangle
\end{aligned}
\tag{3.3.12}$$

Aplica-se o operador descrito na Equação 3.3.2 ao estado inicial, obtendo-se o estado descrito na Equação 3.3.13.

$$\begin{aligned}
|\Psi_1\rangle = & \frac{1}{\sqrt{4}} |i\rangle [|1111111101111111111111111111\rangle + |1101111111111111011111111111\rangle + \\
& |1111110111111111111111111111\rangle + |1011111111111111111111111111\rangle] |c\rangle + \\
& \frac{1}{\sqrt{4}} |i\rangle [|0010110110111111111111111111\rangle + |0010111101111111111111111111\rangle + \\
& |0010111101111111111111111111\rangle + |0010111011111111111111111111\rangle] |c\rangle
\end{aligned}
\tag{3.3.13}$$

Em seguida é aplicado o operador descrito na Equação 3.3.6 e obtém-se o estado

descrito na Equação 3.3.14

$$\begin{aligned}
|\Psi_2\rangle = & \frac{1}{2} \left[e^{\left(\frac{i\cdot\pi}{2n}\cdot 1\right)} |111111110111111111111111\rangle + |1101111111111111011111111111\rangle + \right. \\
& \left. |1111111011111111111111111111\rangle + |1011111111111111111111111111\rangle \right] + \\
& \frac{1}{2} \left[e^{\left(\frac{-i\cdot\pi}{2n}\cdot 1\right)} |11111111011111111111111111\rangle + |1101111111111111011111111111\rangle + \right. \\
& \left. |1111111011111111111111111111\rangle + |1011111111111111111111111111\rangle \right] + \\
& \frac{1}{2} \left[e^{\left(\frac{i\cdot\pi}{2n}\cdot 5\right)} |00101101101111111111111111\rangle + |00101111101111111111111111\rangle + \right. \\
& \left. |00101111101111111111111111\rangle + |00101110111111111111111111\rangle \right] + \\
& \frac{1}{2} \left[e^{\left(\frac{-i\cdot\pi}{2n}\cdot 5\right)} |00101101101111111111111111\rangle + |00101111101111111111111111\rangle + \right. \\
& \left. |00101111101111111111111111\rangle + |00101110111111111111111111\rangle \right]
\end{aligned}
\tag{3.3.14}$$

De acordo com a Equação 3.3.8 que retrata as últimas operações determinísticas

do algoritmo e tem-se para $n = 26$, obtém-se o estado descrito na Equação 3.3.15

$$\begin{aligned}
|\Psi_3\rangle = & \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{52}\right) |i\rangle |01110101000000000000000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{5\pi}{52}\right) |i\rangle |10100111000000000000000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{52}\right) |i\rangle |01110101000000000000000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{5\pi}{52}\right) |i\rangle |10100111000000000000000000000000\rangle |1\rangle \right] + \\
& \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{52}\right) |i\rangle |01010101010000000000000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{5\pi}{52}\right) |i\rangle |10100101010000000000000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{52}\right) |i\rangle |01010101010000000000000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{5\pi}{52}\right) |i\rangle |10100101010000000000000000000000\rangle |1\rangle \right] + \\
& \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{52}\right) |i\rangle |01110100010000000000000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{5\pi}{52}\right) |i\rangle |10100101000000000000000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{52}\right) |i\rangle |01110100010000000000000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{5\pi}{52}\right) |i\rangle |10100101000000000000000000000000\rangle |1\rangle \right] + \\
& \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{52}\right) |i\rangle |00110101010000000000000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{5\pi}{52}\right) |i\rangle |10100100010000000000000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{52}\right) |i\rangle |00110101010000000000000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{5\pi}{52}\right) |i\rangle |10100100010000000000000000000000\rangle |1\rangle \right]
\end{aligned} \tag{3.3.15}$$

Conforme descrito nas Equações 3.3.10 e 3.3.11 do algoritmo de recuperação é realizada uma medição do registro c que resultará nas respectivas probabilidades:

$$\left[\frac{1}{\sqrt{2}} \cos\left(\frac{\pi}{52}\right) \right]^2 = 0,99$$

$$\left[\frac{1}{\sqrt{2}} \cos\left(\frac{5\pi}{52}\right) \right]^2 = 0,91$$

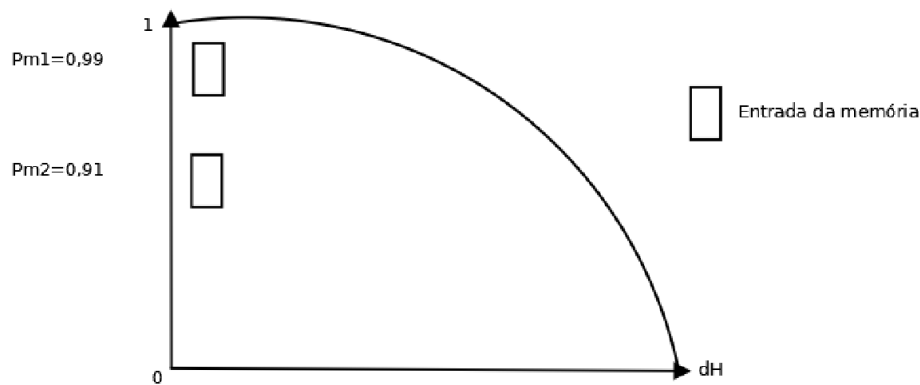
E resultará em $|1\rangle$ com probabilidade:

$$\left[\frac{1}{\sqrt{2}} \sin\left(\frac{\pi}{52}\right) \right]^2 = 0,00$$

$$\left[\frac{1}{\sqrt{2}} \sin\left(\frac{5\pi}{52}\right) \right]^2 = 0,08$$

E o padrão de entrada $|i\rangle = |011101010100000000000000\rangle$ será reconhecido pelas duas memórias $|m_1\rangle$ e $|m_2\rangle$, constatando-se a limitação do algoritmo em associar o padrão de entrada a sua respectiva memória.

Figura 10 – Probabilidade de reconhecimento do padrão $|i\rangle$ para $n = 26$ em uma Memória Quântica Probabilística



3.4 Sumário do capítulo

O objetivo deste capítulo foi apresentar o conceito de uma memória quântica probabilística, em que o número de padrões binários que podem ser armazenados na memória é exponencial ao número de qubits. Também, neste capítulo foi descrito o armazenamento de padrões quânticos e a recuperação de padrões quânticos de uma memória quântica probabilística e um exemplo de recuperação de informação da memória foi demonstrado.

A grande vantagem da implementação desta memória quântica probabilística é sua capacidade de armazenamento de informações, fato este capaz de resolver vários

problemas que envolvem a classificação e o reconhecimento de padrões, incrementando a sua probabilidade de reconhecimento quando a distância de Hamming entre seus padrões são pequenos.

4 Memória Quântica Probabilística Parametrizada

Neste capítulo é apresentado a memória quântica probabilística parametrizada em que esta memória apresenta uma vantagem na classificação dos padrões, através de uma variação feita ao modelo de Trugenberger. Na Seção 4.2 é descrito o problema da memória quântica probabilística. Na Seção 4.3 é descrito a memória quântica probabilística parametrizada. Na Seção 4.4 é um sumário do capítulo.

4.1 Introdução

O modelo proposto em (TRUGENBERGER, 2001) melhora a capacidade de armazenamento da memória associativa e cujos padrões binários podem ser armazenados na memória com um incremento exponencial no número n de qubits, $p_{max} = 2^n$ e seus padrões binários podem ser formados com os n qubits armazenados. Do algoritmo de recuperação de informação, tem-se as Equações 3.3.10 e 3.3.11 provenientes de uma medição no qubit de controle $|c\rangle$ através do cálculo de suas probabilidades, classificando o padrão de entrada se $c = |0\rangle$ em reconhecido e $c = |1\rangle$ caso contrário.

4.2 Limitação da Memória Quântica Probabilística

Segundo (DUNJKO; BRIEGEL, 2017) afirma que a memória probabilística quântica sofre de falta de escalabilidade. Em (BRUN et al., 2003) é realizada uma crítica onde afirma que o modelo não é uma memória, pois a informação colapsa após a recuperação de um padrão na memória. Trugenberger em (TRUGENBERGER, 2003) contradiz, sob a alegação que seu modelo deve apresentar um número de entrada polinomial e que existe a possibilidade de realizar cópias probabilísticas da memória para evitar a perda de informação. Conforme (SCHULD et al., 2014b), relata que quando executa o algoritmo de recuperação e em seguida realiza-se uma medição a memória colapsa. Assegura também que quando a memória apaga, e havendo a necessidade de usá-la terá que iniciá-la novamente. Destacam-se os trabalhos (SCHULD et al., 2014a; ZHOU; DING, 2008) que utilizam este modelo no reconhecimento de padrões.

Uma das etapas que consiste a MQP é a etapa da recuperação da informação, caracterizada pelo modelo descrito pelo Algoritmo 2. Nesta etapa, pode-se destacar a limitação ao modelo descrito no exemplo anterior, pois, quando duas memórias com distância de Hamming próximas entre si e existe a necessidade de classificar um determinado padrão de entrada ao conjunto de memórias, o modelo não conseguirá fazer esta distinção com precisão, porque a probabilidade que cada memória responda é de 0,99 e 0,91, ambas muito próximas, de tal forma que não conseguirá associá-lo ao seu respectivo conjunto. Para resolver a limitação referente ao modelo, incluímos um parâmetro ϕ que permite um ajuste no cálculo da distância entre seus padrões para que esta memória lide com padrões próximos possibilitando ampliar a precisão na distinção para a classificação de seus padrões. No modelo de Trugenberger é definido n como o número de bits da memória, porém, nesta alteração faz-se a inclusão de um parâmetro, substituindo o valor de n e transformando em um valor ajustável, ocorre que com esta substituição ao parâmetro n , a função de probabilidade do algoritmo deverá maximizar o retorno do cálculo de suas probabilidades, pois, possibilitando o retorno com alta probabilidade, apenas da memória que tiver seu padrão reconhecido.

4.3 Memória Quântica Probabilística Parametrizada

Salienta-se que mediante a modificação sugerida é feita uma inclusão de um parâmetro ajustável (ϕ) ao operador representado pela Equação 3.1.3 do algoritmo, esta alteração é definida como memória quântica probabilística parametrizada (MQPP).

O algoritmo da memória quântica probabilística que é probabilístico, utiliza a distância de Hamming como referência para a entrada e o armazenamento de padrões. Neste trabalho, propomos uma modificação em n (tamanho da memória), com a inclusão de um parâmetro ϕ , permitindo que a memória lide com padrões próximos, pois segundo a MQP, se duas memórias apresentam distância de Hamming próximas entre os padrões de entrada e os padrões armazenados, o algoritmo não consegue fazer esta classificação com precisão e com a inclusão do parâmetro ϕ , possibilita-se o retorno com alta probabilidade, apenas da memória que tiver seu padrão reconhecido. A seguir, propomos valores arbitrários ao valor de ϕ . Considera-se que o parâmetro da MQPP apresenta valor igual a $\phi = \frac{1}{a}$, sendo a um valor arbitrário, independente do total de bits da memória, conforme descrito

na Equação 4.3.2.

4.3.1 Escolha do Parâmetro

Destaca-se que para a escolha do parâmetro ajustável ϕ , fez-se o cálculo da derivada da função com seus respectivos pontos críticos. Permitindo-se testar valores que melhor atendiam a característica pretendida, ou seja, adequavam-se ao ajuste dos padrões para o reconhecimento dos padrões.

- Cálculo da derivada da função, para $p = 4$, $d_H = 1$ e $d_H = 5$:

$$f(x) = \frac{1}{4} \cos^2 \left(\frac{\pi}{2n} \cdot 5 \right) = \left[\frac{1}{4} \cos^2 \left(\frac{5\pi}{2n} \right) \right] = ?$$

$$\text{Fazendo: } u = \left(\frac{5\pi}{2n} \right) \Rightarrow \frac{du}{dn} = -\frac{5\pi}{2n^2}$$

$$\text{Temos que: } y = \frac{\cos^2 u}{4} \Rightarrow \frac{dy}{du} = -\frac{1}{2} \sin \left(\frac{5\pi}{2n} \right) \cos \left(\frac{5\pi}{2n} \right) \therefore$$

$$\frac{dy}{dn} = \frac{5\pi \sin \left(\frac{5\pi}{2n} \right) \cos \left(\frac{5\pi}{2n} \right)}{4n^2} \quad (4.3.1)$$

- Pontos Críticos

1. Para $d_H = 1$:

$$n = \frac{1}{m} \quad \text{em que,} \quad m \neq 0$$

2. Para $d_H = 5$:

$$n = \frac{5}{m} \quad \text{em que,} \quad m \neq 0$$

com isso, o valor escolhido para a inclusão do parâmetro ajustável ϕ é $n = \frac{1}{a}$. Acrescentando-se $\phi = \frac{1}{a}$ ao parâmetro, como descrito na Equação 4.3.2.

$$\begin{pmatrix} \exp\left(\frac{i\pi}{2n} \cdot \phi \cdot d_H\right) & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \exp\left(\frac{i\pi}{2} \cdot \frac{1}{a} \cdot d_H\right) & 0 \\ 0 & 1 \end{pmatrix} \quad (4.3.2)$$

Mostraremos detalhadamente que com a modificação proposta ao modelo, continua sendo válida a função do algoritmo de recuperação de informação de Trugenberger, ou seja, permanecem válidas as etapas do algoritmo, como descrito nas equações abaixo.

O estado $|\Psi_0\rangle$ é descrito na Equação 4.3.3

$$\begin{aligned} |\Psi_0\rangle &= \frac{1}{\sqrt{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 0\rangle + \\ &\sqrt{\frac{1}{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 1\rangle \end{aligned} \quad (4.3.3)$$

Daí, o estado $|\Psi_1\rangle$ é descrito na Equação 4.3.4

$$\begin{aligned} |\Psi_1\rangle &= \frac{1}{\sqrt{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 0\rangle + \\ &\sqrt{\frac{1}{2^p}} \sum_{k=1}^p |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 1\rangle \end{aligned} \quad (4.3.4)$$

Observamos que $|\Psi_2\rangle$ também pode ser calculado, com o uso de operadores quânticos elementares e com a aplicação do operador 3.1.3, como descrito na Equação 4.3.5.

$$|\Psi_2\rangle = e^{i\frac{\pi}{2n}\mathcal{H}} |\Psi_1\rangle = \prod_{i=1}^n (CU^{-2})_{cm_i} \prod_{i=1}^n U_{m_j} |\Psi_1\rangle, \quad (4.3.5)$$

Então,

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} \sum_{k=1}^p \left[e^{i\frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k)} \right] |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 0\rangle +$$

$$\frac{1}{\sqrt{2}} \sum_{k=1}^p \left[e^{-i\frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k)} \cdot e^{-2i\frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k)} \right] |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 1\rangle$$

Resumidamente, tem-se

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} \sum_{k=1}^p \left[e^{i\frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k)} \right] |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 0\rangle + \quad (4.3.6)$$

$$\frac{1}{\sqrt{2}} \sum_{k=1}^p \left[e^{-i\frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k)} \right] |i_1, \dots, i_n; d_1^k, \dots, d_n^k; 1\rangle$$

Obtém-se o estado $|\Psi_3\rangle$ como descrito na Equação 4.3.7

$$|\Psi_3\rangle = \frac{1}{\sqrt{p}} \sum_{k=1}^p \cos \frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k) |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 0\rangle + \quad (4.3.7)$$

$$\frac{1}{\sqrt{p}} \sum_{k=1}^p \sin \frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k) |i_1, \dots, i_n; p_1^k, \dots, p_n^k; 1\rangle.$$

Resultando nas seguintes probabilidades, os estados $|0\rangle$ e $|1\rangle$ conforme as Equações 4.3.8 e 4.3.9

$$P(|c\rangle = |0\rangle) = \sum_{k=1}^p \frac{1}{p} \cos^2 \left(\frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k) \right), \quad (4.3.8)$$

$$P(|c\rangle = |1\rangle) = \sum_{k=1}^p \frac{1}{p} \sin^2 \left(\frac{\pi}{2} \cdot \phi \cdot d_H(i, p^k) \right). \quad (4.3.9)$$

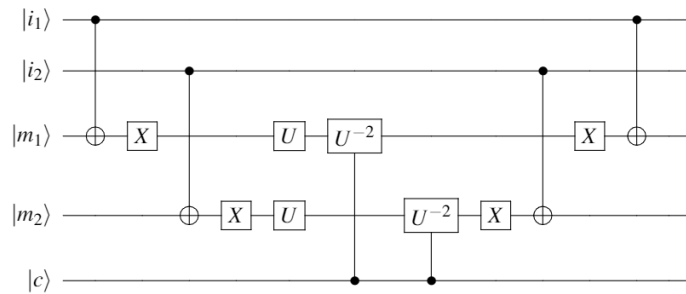


Figura 11 – Circuito recuperação memória quântica probabilística parametrizada

A seguir, será ilustrado um exemplo do funcionamento de uma memória quântica probabilística parametrizada:

Exemplo 2: Dados um conjunto de treinamento e um padrão de entrada $|i\rangle = |01110101010000000000000000\rangle$:

$ m_1\rangle$	$ m_2\rangle$
01110101000000000000000000	10100111000000000000000000
01010101010000000000000000	10100101010000000000000000
01110100010000000000000000	10100101000000000000000000
00110101010000000000000000	10100100010000000000000000

O algoritmo de recuperação [2](#), inicia-se com o estado $|\Psi_0\rangle$ como descrito na Equação [4.3.10](#)

$$\begin{aligned}
 |\Psi_0\rangle = & \frac{1}{\sqrt{4}} |i\rangle [|01110101000000000000000000\rangle + |01010101010000000000000000\rangle + \\
 & |01110100010000000000000000\rangle + |00110101010000000000000000\rangle] |c\rangle + \\
 & \frac{1}{\sqrt{4}} |i\rangle [|10100111000000000000000000\rangle + |10100101010000000000000000\rangle + \\
 & |10100101000000000000000000\rangle + |10100100010000000000000000\rangle] |c\rangle
 \end{aligned}$$

(4.3.10)

Inicializa-se o registro c com $H|0\rangle$, ou seja, o registro é iniciado com o estado

$|c\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$, obtendo-se o estado descrito na Equação 4.3.11.

$$\begin{aligned}
|\Psi_1\rangle = & \frac{1}{\sqrt{4}} |i\rangle [|1111111101111111111111111111\rangle + |1101111111111111011111111111\rangle + \\
& |11111110111111111111111111111111\rangle + |1011111111111111111111111111\rangle] |c\rangle + \\
& \frac{1}{\sqrt{4}} |i\rangle [|0010110110111111111111111111\rangle + |0010111110111111111111111111\rangle + \\
& |00101111101111111111111111111111\rangle + |0010111011111111111111111111\rangle] |c\rangle
\end{aligned} \tag{4.3.11}$$

Aplica-se o operador descrito na Equação 3.3.2, obtendo-se o estado descrito na Equação 4.3.12

$$\begin{aligned}
|\Psi_2\rangle = & \frac{1}{2} \left[e^{\left(\frac{i\pi}{2} \cdot \frac{1}{5} \cdot 1\right)} |1111111101111111111111111111\rangle + |1101111111111111011111111111\rangle + \right. \\
& \left. |11111110111111111111111111111111\rangle + |1011111111111111111111111111\rangle \right] + \\
& \frac{1}{2} \left[e^{\left(\frac{i\pi}{2} \cdot \frac{1}{5} \cdot 1\right)} |1111111101111111111111111111\rangle + |1101111111111111011111111111\rangle + \right. \\
& \left. |11111110111111111111111111111111\rangle + |1011111111111111111111111111\rangle \right] + \\
& \frac{1}{2} \left[e^{\left(\frac{-i\pi}{2} \cdot \frac{1}{5} \cdot 5\right)} |0010110110111111111111111111\rangle + |0010111110111111111111111111\rangle + \right. \\
& \left. |001011111011111111111111111111\rangle + |0010111011111111111111111111\rangle \right] + \\
& \frac{1}{2} \left[e^{\left(\frac{-i\pi}{2} \cdot \frac{1}{5} \cdot 5\right)} |0010110110111111111111111111\rangle + |0010111110111111111111111111\rangle + \right. \\
& \left. |001011111011111111111111111111\rangle + |0010111011111111111111111111\rangle \right]
\end{aligned} \tag{4.3.12}$$

De acordo com a Equação 3.3.8 que descreve as últimas operações determinísticas do algoritmo e usando o parâmetro $\phi = \frac{1}{a}$ com $a = 5$, obtém-se o estado descrito na

Equação 4.3.13

$$\begin{aligned}
|\Psi_3\rangle = & \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{10}\right) |i\rangle |011101010000000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{\pi}{2}\right) |i\rangle |101001110000000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{10}\right) |i\rangle |011101010000000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{\pi}{2}\right) |i\rangle |101001110000000000000000\rangle |1\rangle \right] + \\
& \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{10}\right) |i\rangle |010101010100000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{\pi}{2}\right) |i\rangle |101001010100000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{10}\right) |i\rangle |010101010100000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{\pi}{2}\right) |i\rangle |101001010100000000000000\rangle |1\rangle \right] + \\
& \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{10}\right) |i\rangle |011101000100000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{\pi}{2}\right) |i\rangle |101001010000000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{10}\right) |i\rangle |011101000100000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{\pi}{2}\right) |i\rangle |101001010000000000000000\rangle |1\rangle \right] + \\
& \frac{1}{\sqrt{2}} \left[\cos\left(\frac{\pi}{10}\right) |i\rangle |001101010100000000000000\rangle |0\rangle + \right. \\
& \cos\left(\frac{\pi}{2}\right) |i\rangle |101001000100000000000000\rangle |0\rangle + \\
& i \sin\left(\frac{\pi}{10}\right) |i\rangle |001101010100000000000000\rangle |1\rangle + \\
& \left. i \sin\left(\frac{\pi}{2}\right) |i\rangle |101001000100000000000000\rangle |1\rangle \right]
\end{aligned} \tag{4.3.13}$$

Assim, conforme descrito nas Equações 4.3.8 e 4.3.9 do modelo proposto do algoritmo de recuperação de informação é realizada uma medição no registro c que resulta nas respectivas probabilidades:

$$\left[\frac{1}{\sqrt{2}} \cos\left(\frac{\pi}{10}\right) \right]^2 = 0,90$$

$$\left[\frac{1}{\sqrt{2}} \cos\left(\frac{\pi}{2}\right) \right]^2 = 0,00$$

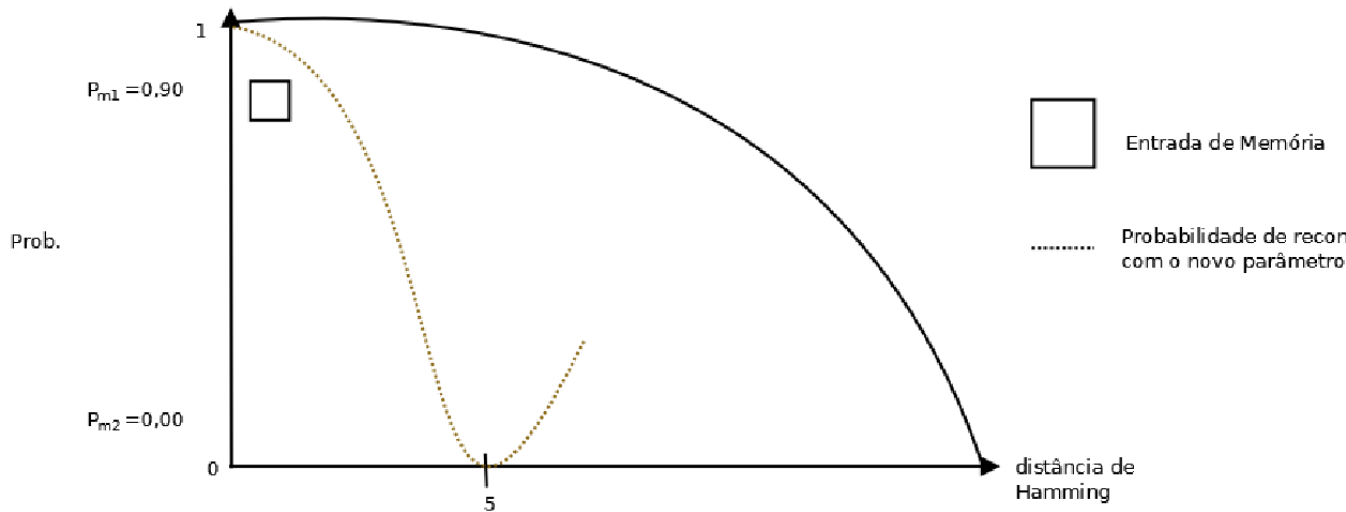
E resultará em $|1\rangle$ com probabilidade:

$$\left[\frac{1}{\sqrt{2}} \sin \left(\frac{\pi}{10} \right) \right]^2 = 0,09$$

$$\left[\frac{1}{\sqrt{2}} \sin \left(\frac{\pi}{2} \right) \right]^2 = 1,00$$

E o novo padrão de entrada $|i\rangle = |011101010100000000000000\rangle$ será reconhecido apenas pela memória $|m_1\rangle$ com probabilidade de 0,90.

Destaca-se a seguir, o gráfico da Figura 12 do Exemplo 2.



5

Figura 12 – Probabilidade de reconhecimento do padrão $|i\rangle$ para $a = 5$ em uma Memória Quântica Probabilística Parametrizada.

É notável o desempenho do algoritmo no reconhecimento do padrão $|i\rangle$ em que a memória m_1 reconhece o padrão com probabilidade de $P_{m_1} = 0,90$ com $a = 5$.

Na comparação entre o modelo de uma MQP e o novo modelo proposto (MQPP), observou-se que no primeiro modelo, o cálculo das probabilidades das duas memórias apresentou $|m_1\rangle = 0,99$ e $|m_2\rangle = 0,91$, respectivamente, as duas memórias com uma alta probabilidade. No segundo modelo, apenas uma das memórias apresenta uma alta probabilidade $|m_1\rangle = 0,90$ e $|m_2\rangle = 0,00$, respectivamente. Isto é, o primeiro modelo não consegue separar o novo padrão de entrada, enquanto que o segundo modelo consegue separá-lo.

Analisando-se o gráfico da Figura 13 do exemplo na Seção 4.3.1, percebe-se que ao fixarmos o valor de $a = 5$, a distância de Hamming gera probabilidades que oscilam entre $P(|c\rangle = |0\rangle)$ ou $P(|c\rangle = |1\rangle)$, variando de cinco em cinco, conforme o comportamento apresentado no gráfico.

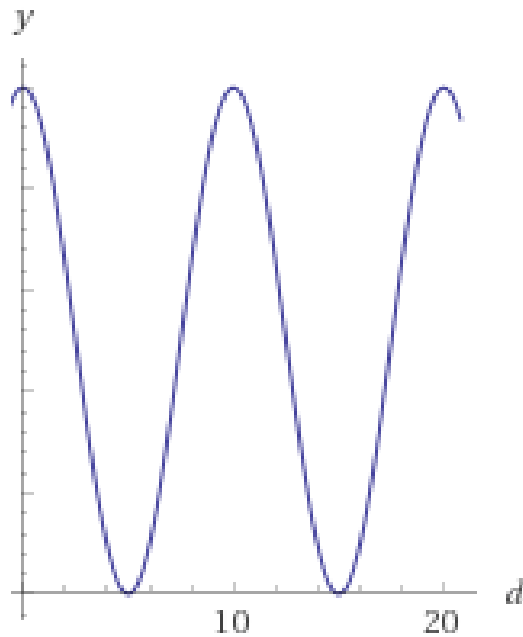


Figura 13 – Ilustração do comportamento da distância de Hamming $d(i, p^k)$ e suas probabilidades (y) em uma Memória Quântica Probabilística Parametrizada.

4.4 Sumário do Capítulo

Este capítulo teve como finalidade, fundamentar a alteração feita ao modelo de Trugenberger, utilizado na classificação de padrões quânticos em que baseia-se em medidas feitas com o uso da distância de Hamming no reconhecimento de padrões, dando ênfase a limitação que ocorre ao modelo de uma memória quântica probabilística. Nesse contexto, o presente trabalho apresenta a variação proposta ao algoritmo de classificação de padrões, definida como memória quântica probabilística parametrizada, abordando seu conceito e principalmente, sua funcionalidade.

A alteração caracterizou-se em substituir n por um parâmetro ϕ , visando aumentar a probabilidade de reconhecimento de padrões, mantendo-se como base a distância de Hamming entre os padrões nos conjuntos de dados. Por fim, utilizamos um exemplo para

melhor compreensão do funcionamento desta alteração ao modelo proposto.

5 Conclusão

Este capítulo caracteriza-se como a conclusão desta dissertação. Na Seção 5.1 são apresentadas algumas considerações finais, na Seção 5.2 é apresentada a contribuição deste trabalho e na Seção 5.3 são apresentados prováveis trabalhos futuros a esta dissertação.

5.1 Considerações finais

O presente trabalho descreve um ajuste feito a uma memória quântica probabilística, com a inserção do parâmetro ao valor fixo de n , para uma melhor funcionalidade da memória na classificação e reconhecimento de padrões.

A principal contribuição deste trabalho foi a proposição de um memória quântica probabilística parametrizada (MQPP). A MQPP foi testada com dados artificiais e a sua eficácia ficou comprovada através dos resultados alcançados.

5.2 Contribuições deste trabalho

Neste trabalho, apresentou-se uma proposta de modificação ao algoritmo de recuperação de informação da memória probabilística quântica (MQP) com a alteração em que n na MQP de Trugenberger era definido como o tamanho da memória do algoritmo, enquanto que com a modificação realizada para ϕ , sendo escolhido um valor arbitrário, tornou-se possível uma adequação no cálculo da distância entre os padrões. Não obstante, com a entrada de um novo padrão, será facilmente reconhecido com uma alta probabilidade, por uma das respectivas memórias armazenadas.

Nesse estudo, observam-se características muito importantes que foram analisadas nesse trabalho, como a fácil implementação do algoritmo e o baixo custo computacional, propiciando o melhoramento de experimentos envolvendo a memória quântica probabilística (MQP).

A proposta do novo modelo, a memória quântica probabilística parametrizada (MQPP) foi testada com o uso dos dados artificiais e comprovou-se, a sua funcionalidade na classificação de padrões.

5.3 Trabalhos Futuros

Como proposta de trabalho futuro, pretende-se realizar experimentos utilizando base de dados reais (binária) para avaliar a eficiência do modelo proposto. Um outro trabalho futuro, será otimizar o desempenho do modelo com a alteração proposta na tarefa de reconhecimento de padrões, onde cada classe do conjunto de dados, será representada por uma memória quântica probabilística parametrizada, proporcionando um melhor desempenho de classificação.

Um outro possível trabalho futuro é combinar diversas memórias com valores de ϕ diferentes, para conseguirmos extrair informações mais detalhadas (e precisas) sobre a memória.

Referências

- BARENDS, R.; KELLY, J.; MEGRANT, A.; VEITIA, A.; SANK, D.; JEFFREY, E.; WHITE, T. C.; MUTUS, J.; FOWLER, A. G.; CAMPBELL, B. et al. Superconducting quantum circuits at the surface code threshold for fault tolerance. **Nature**, Nature Publishing Group, v. 508, n. 7497, p. 500, 2014.
- BIAMONTE, J.; WITTEK, P.; PANCOTTI, N.; REBENTROST, P.; WIEBE, N.; LLOYD, S. Quantum machine learning. **Nature**, Nature Publishing Group, v. 549, n. 7671, p. 195, 2017.
- BRUN, T.; KLAUCK, H.; NAYAK, A.; RÖTTELER, M.; ZALKA, C. Comment on “probabilistic quantum memories”. **Phys. Rev. Lett.**, American Physical Society, v. 91, p. 209801, Nov 2003. Disponível em: <<https://link.aps.org/doi/10.1103/PhysRevLett.91.209801>>.
- CHIAPPETTA, P.; COLANGELO, P.; FELICE, P. D.; NARDULLI, G.; PASQUARIELLO, G. Higgs search by neural networks at lhc. **Physics Letters B**, Elsevier, v. 322, n. 3, p. 219–223, 1994.
- CHILDS, A. M.; KOTHARI, R.; SOMMA, R. D. Quantum linear systems algorithm with exponentially improved dependence on precision. **arXiv preprint arXiv:1511.02306**, 2015.
- CLADER, B. D.; JACOBS, B. C.; SPROUSE, C. R. Preconditioned quantum linear system algorithm. **Physical review letters**, APS, v. 110, n. 25, p. 250504, 2013.
- DEUTSCH, D. Quantum theory, the church–turing principle and the universal quantum computer. **Proc. R. Soc. Lond. A**, The Royal Society, v. 400, n. 1818, p. 97–117, 1985.
- DIVINCENZO, D. P. et al. The physical implementation of quantum computation. **arXiv preprint quant-ph/0002077**, 2000.
- DUNJKO, V.; BRIEGEL, H. J. Machine learning & artificial intelligence in the quantum domain. **arXiv preprint arXiv:1709.02779**, 2017.
- DUNJKO, V.; TAYLOR, J. M.; BRIEGEL, H. J. Quantum-enhanced machine learning. **Physical review letters**, APS, v. 117, n. 13, p. 130501, 2016.
- FARHI, E.; GUTMANN, S. Quantum computation and decision trees. **Physical Review A**, APS, v. 58, n. 2, p. 915, 1998.
- FEYNMAN, R. P. Simulating physics with computers. **International journal of theoretical physics**, Springer, v. 21, n. 6, p. 467–488, 1982.
- GRALEWICZ, P. Quantum computing in neural networks. **arXiv preprint quant-ph/0401127**, 2004.
- GROVER, L. K. A fast quantum mechanical algorithm for database search. In: **ACM. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**. [S.l.], 1996. p. 212–219.

- _____. Quantum mechanics helps in searching for a needle in a haystack. **Physical review letters**, APS, v. 79, n. 2, p. 325, 1997.
- HARROW, A. W.; HASSIDIM, A.; LLOYD, S. Quantum algorithm for linear systems of equations. **Physical review letters**, APS, v. 103, n. 15, p. 150502, 2009.
- HIRVENSALO, M. Quantum computing. In: **Encyclopedia of Sciences and Religions**. [S.l.]: Springer, 2013. p. 1922–1926.
- JOSÉ, M. A.; PIQUEIRA, J. R. C.; LOPES, R. d. D. Introduction to quantum programming. **Revista Brasileira de Ensino de Física**, SciELO Brasil, v. 35, n. 1, p. 1–9, 2013.
- KAK, S. On quantum neural computing. **Information Sciences**, Elsevier, v. 83, n. 3-4, p. 143–160, 1995.
- LLOYD, S.; MOHSENI, M.; REBENTROST, P. Quantum algorithms for supervised and unsupervised machine learning. **arXiv preprint arXiv:1307.0411**, 2013.
- _____. Quantum principal component analysis. **Nature Physics**, Nature Publishing Group, v. 10, n. 9, p. 631, 2014.
- LU, S.; BRAUNSTEIN, S. L. Quantum decision tree classifier. **Quantum information processing**, Springer, v. 13, n. 3, p. 757–770, 2014.
- MAGLOGIANNIS, I. G. **Emerging artificial intelligence applications in computer engineering: real word ai systems with applications in ehealth, hci, information retrieval and pervasive technologies**. [S.l.]: Ios Press, 2007. v. 160.
- MALLOSSINI, A.; BLANZIERI, E.; CALARCO, T. Quantum genetic optimization. **IEEE Transactions on Evolutionary Computation**, IEEE, v. 12, n. 2, p. 231–241, 2008.
- MANIN, Y. I. Classical computing, quantum computing, and shor’s factoring algorithm. **arXiv preprint quant-ph/9903008**, 1999.
- MITCHELL, T. M. et al. **Machine learning**. WCB. [S.l.]: McGraw-Hill Boston, MA:, 1997.
- NARAYANAN, A.; MENNEER, T. Quantum artificial neural network architectures and components. **Information Sciences**, Elsevier, v. 128, n. 3, p. 231–255, 2000.
- NEIGOVZEN, R.; NEVES, J. L.; SOLLACHER, R.; GLASER, S. J. Quantum pattern recognition with liquid-state nuclear magnetic resonance. **Physical Review A**, APS, v. 79, n. 4, p. 042321, 2009.
- NEVEN, H.; DENCHEV, V. S.; ROSE, G.; MACREADY, W. G. Training a large scale classifier with the quantum adiabatic algorithm. **arXiv preprint arXiv:0912.0779**, 2009.
- NIELSEN, M. A.; CHUANG, I. **Quantum computation and quantum information**. [S.l.]: AAPT, 2002.
- NIELSEN, M. A.; CHUANG, I. L. **Quantum computation and quantum information**. [S.l.]: Cambridge university press, 2010.

NILSSON, N. J. **Artificial intelligence: A modern approach: Stuart Russell and Peter Norvig**, (Prentice Hall, Englewood Cliffs, NJ, 1995); xxviii+ 932 pages. [S.l.]: Elsevier, 1996.

NJAJA, J.-P. T.; ENGO, S. N.; WOAFO, P. Quantum associative memory with improved distributed queries. **International Journal of Theoretical Physics**, Springer, v. 52, n. 6, p. 1787–1801, 2013.

OLIVEIRA, W. R. de. Quantum ram based neural networks. In: **ESANN**. [S.l.: s.n.], 2009. v. 9, p. 331–336.

OLIVEIRA, W. R. de; SILVA, A. J.; LUDERMIR, T. B.; LEONEL, A.; GALINDO, W. R.; PEREIRA, J. C. Quantum logical neural networks. In: IEEE. **Neural Networks, 2008. SBRN'08. 10th Brazilian Symposium on**. [S.l.], 2008. p. 147–152.

ÖMER, B. A procedural formalism for quantum computing. Citeseer, 1998.

PUDENZ, K. L.; LIDAR, D. A. Quantum adiabatic machine learning. **Quantum information processing**, Springer, v. 12, n. 5, p. 2027–2070, 2013.

REBENTROST, P.; MOHSENI, M.; LLOYD, S. Quantum support vector machine for big data classification. **Physical review letters**, APS, v. 113, n. 13, p. 130503, 2014.

REBENTROST, P.; STEFFENS, A.; MARVIAN, I.; LLOYD, S. Quantum singular-value decomposition of nonsparse low-rank matrices. **Physical review A**, APS, v. 97, n. 1, p. 012327, 2018.

RIGATOS, G. G.; TZAFESTAS, S. G. Neurodynamics and attractors in quantum associative memories. **Integrated Computer-Aided Engineering**, IOS Press, v. 14, n. 3, p. 225–242, 2007.

ROSENBLATT, F. The perceptron: a probabilistic model for information storage and organization in the brain. **Psychological review**, American Psychological Association, v. 65, n. 6, p. 386, 1958.

RUSSELL, S. J.; NORVIG, P. **Artificial intelligence: a modern approach**. [S.l.]: Malaysia; Pearson Education Limited, 2016.

SASAKI, M.; CARLINI, A. Quantum learning and universal quantum matching machine. **Physical Review A**, APS, v. 66, n. 2, p. 022303, 2002.

SASAKI, M.; CARLINI, A.; JOZSA, R. Quantum template matching. **Physical Review A**, APS, v. 64, n. 2, p. 022317, 2001.

SCHULD, M.; SINAYSKIY, I.; PETRUCCIONE, F. Quantum computing for pattern classification. In: SPRINGER. **Pacific Rim International Conference on Artificial Intelligence**. [S.l.], 2014. p. 208–220.

_____. The quest for a quantum neural network. **Quantum Information Processing**, Springer, v. 13, n. 11, p. 2567–2586, 2014.

_____. An introduction to quantum machine learning. **Contemporary Physics**, Taylor & Francis, v. 56, n. 2, p. 172–185, 2015.

- SCHÜTZHOLD, R. Pattern recognition on a quantum computer. **Physical Review A**, APS, v. 67, n. 6, p. 062311, 2003.
- SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM review**, SIAM, v. 41, n. 2, p. 303–332, 1999.
- SILVA, A. J. D.; OLIVEIRA, W. R. D.; LUDERMIR, T. B. Classical and superposed learning for quantum weightless neural networks. **Neurocomputing**, Elsevier, v. 75, n. 1, p. 52–60, 2012.
- SILVA, A. J. da; LUDERMIR, T. B.; OLIVEIRA, W. R. de. Quantum perceptron over a field and neural network architecture selection in a quantum computer. **Neural Networks**, Elsevier, v. 76, p. 55–64, 2016.
- SILVA, A. J. da; OLIVEIRA, W. R. de; LUDERMIR, T. B. Weightless neural network parameters and architecture selection in a quantum computer. **Neurocomputing**, Elsevier, v. 183, p. 13–22, 2016.
- SIMON, D. R. On the power of quantum computation. **SIAM journal on computing**, SIAM, v. 26, n. 5, p. 1474–1483, 1997.
- SINGH, M. P.; RADHEY, K.; SARASWAT, V.; KUMAR, S. Classification of patterns representing apples and oranges in three-qubit system. **Quantum Information Processing**, Springer, v. 16, n. 1, p. 16, 2017.
- TRUGENBERGER, C. A. Probabilistic quantum memories. **Physical Review Letters**, APS, v. 87, n. 6, p. 067901, 2001.
- _____. Quantum pattern recognition. **Quantum Information Processing**, Springer, v. 1, n. 6, p. 471–493, 2002.
- _____. Trugenberger replies. **Physical Review Letters**, APS, v. 91, n. 20, p. 209802, 2003.
- VENTURA, D.; MARTINEZ, T. Quantum associative memory. **Information Sciences**, Elsevier, v. 124, n. 1-4, p. 273–296, 2000.
- WIEBE, N.; BRAUN, D.; LLOYD, S. Quantum algorithm for data fitting. **Physical review letters**, APS, v. 109, n. 5, p. 050505, 2012.
- WIEBE, N.; KAPOOR, A.; SVORE, K. Quantum algorithms for nearest-neighbor methods for supervised and unsupervised learning. **arXiv preprint arXiv:1401.2142**, 2014.
- YANOFSKY, N. S.; MANNUCCI, M. A.; MANNUCCI, M. A. **Quantum computing for computer scientists**. [S.l.]: Cambridge University Press Cambridge, 2008. v. 20.
- YOUNG, N. **An introduction to Hilbert space**. [S.l.]: Cambridge university press, 1988.
- ZHOU, R.; DING, Q. Quantum pattern recognition with probability of 100%. **International Journal of Theoretical Physics**, Springer, v. 47, n. 5, p. 1278–1285, 2008.