

UNIVERSIDADE DE SÃO PAULO  
Instituto de Física de São Carlos

Estêvão Vilas Boas de Oliveira

## **Computação Quântica com o IBM Q Experience**

Trabalho de conclusão de curso apresentado ao Programa de Graduação em Física do Instituto de Física de São Carlos da Universidade de São Paulo, para obtenção do título de Bacharel em Física

Orientador: Prof. Dr. Frederico Borges de Brito

São Carlos

2019

# Resumo

Este projeto teve como objetivo inicial um estudo dos elementos fundamentais da computação quântica, bem como a familiarização com a implementação de circuitos quânticos simples utilizando a plataforma de acesso público da IBM, a IBM Q Experience<sup>1</sup>. Assim, propomos aqui a elaboração de algoritmo quântico, que caracteriza-se de uma calculadora simples para a realização do procedimento de soma entre dois números de 1 qbit, cuja aplicação, tanto em um dispositivo quântico real quanto em um simulador clássico que implementa um computador quântico ideal, serviu para uma análise mais geral de certos aspectos da computação quântica. A partir desta análise constatou-se a origem de erros quânticos intrínsecos à implementação física do problema em questão. Ainda, está incluído neste trabalho uma apresentação sucinta do Algoritmo de Shor como forma de estabelecer um comparativo entre ele e o código aqui proposto, no que diz respeito à exploração efetivamente vantajosa das propriedades da mecânica quântica para a computação.

## 1 Introdução Teórica

Nesta seção serão apresentados, de maneira sucinta, apenas alguns conceitos essenciais para o entendimento deste projeto, tendo como base os postulados e fundamentos da mecânica quântica.

### 1.1 Introdução à mecânica quântica

O primeiro conceito a ser introduzido é o conceito de vetor de estado, pertencente à um espaço de estados contido no espaço de Hilbert, como representação de um sistema físico. Aqui o sistema físico de interesse, o qbit, apresenta um espaço de estados bidimensional com base ortonormal  $\{|0\rangle, |1\rangle\}$ . Qualquer vetor estado  $|\Psi\rangle$  nesse espaço de estados pode ser representado como um estado de superposição entre os vetores da base da forma

$$|\Psi\rangle = a|0\rangle + b|1\rangle, \quad (1)$$

com  $a^2 + b^2 = 1$  sendo a condição de normalização, e

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ e } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2)$$

na notação matricial. Ainda, podemos gerar estados compostos de dois ou mais qbits, da forma

$$|\Psi_t\rangle = |\Psi_0\rangle \otimes |\Psi_1\rangle \otimes \dots \otimes |\Psi_n\rangle, \quad (3)$$

com o espaço de estados  $2^n$ -dimensional.

A evolução temporal de  $|\Psi\rangle$  é dada por uma operação unitária  $U$  tal que

$$|\Psi(t_2)\rangle = U(t_1, t_2) |\Psi(t_1)\rangle, \quad (4)$$

e a unitariedade de  $U$  preserva a norma de  $|\Psi\rangle$  uma vez que

$$\langle\Psi|\Psi\rangle = \langle\Psi(t)|\Psi(t)\rangle = \langle\Psi|U^\dagger \cdot U|\Psi\rangle = 1 \implies U^\dagger \cdot U = Id, \quad (5)$$

em que  $Id$  é o operador identidade, definido como sendo a matriz identidade de dimensão  $n \times n$ , em que  $n$  é a dimensão do espaço vetorial. Para um sistema de 1 qbit temos

$$Id = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad (6)$$

A operação unitária  $U$  é obtida a partir da equação de Schrödinger

$$i\hbar \frac{\partial}{\partial t} |\Psi\rangle = \mathcal{H} |\Psi\rangle, \quad (7)$$

e se o operador Hamiltoniano  $\mathcal{H}$  do sistema não depende explicitamente do tempo temos<sup>2;3</sup>

$$U(t_1, t_2) = \exp\left\{\frac{-i\mathcal{H}(t_2 - t_1)}{\hbar}\right\} \quad (8)$$

Em computação quântica a base ortonormal do espaço de estados apresentada é definida como sendo a base computacional<sup>2</sup> ou base  $z$ , uma vez que os vetores de estado da base são auto-vetores da matriz de Pauli  $Z$ , definida como

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (9)$$

Introduziremos, agora, uma apresentação alternativa à descrição de um sistema físico em termos dos vetores de estado: a matriz densidade, ou operador densidade  $\rho$ , definido como

$$\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|, \quad (10)$$

em que  $p_i$  é a probabilidade de o sistema estar no estado  $|\Psi_i\rangle$ . Esta formulação é útil para descrever um *ensemble* de estados quântico, pois sua formulação evidencia o caráter estatístico do problema físico já que os elementos de matriz da diagonal principal representam as probabilidades clássicas dos resultados de medidas feitas no estado  $|\Psi\rangle$ . Uma consequência disso é o traço de  $\rho$  ser igual à

unidade. Para o estado puro dado segundo a equação 1 temos

$$\rho = a^2 |0\rangle\langle 0| + ab |0\rangle\langle 1| + ab |1\rangle\langle 0| + b^2 |1\rangle\langle 1| = \begin{bmatrix} a^2 & ab \\ ab & b^2 \end{bmatrix}, \quad (11)$$

e ainda, os termos fora da diagonal principal estão relacionados à coerência do estado quântico<sup>3</sup>.

Analogamente ao vetor de estado  $|\Psi\rangle$ , a evolução temporal da matriz densidade  $\rho$  é dada, também, através da operação unitária  $U$  da forma

$$\rho(t) = |\Psi(t)\rangle\langle\Psi(t)| = U |\Psi\rangle\langle\Psi| U^\dagger = U\rho U^\dagger \quad (12)$$

## 1.2 Introdução à computação quântica

A computação quântica, em analogia à computação clássica, é construída a partir de um circuito quântico composto por objetos que carregam e manipulam a informação quântica.

Munidos dos conceitos introduzidos anteriormente, podemos, então, definir aqui os instrumentos responsáveis por manipular a informação quântica no processo computacional. Esses objetos são as portas lógicas quânticas e são definidos como sendo quaisquer operações unitárias agindo no vetor de estado do sistema.

Serão introduzidas as principais portas lógicas quânticas utilizadas na composição dos algoritmos quânticos deste trabalho. Além das operações  $Id$  e  $Z$  definidas nas equações (6) e (9), definimos as seguintes portas lógicas de 1 qbit:

Matriz de Pauli X dada por

$$X = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \implies \begin{cases} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{cases}, \quad (13)$$

cuja operação é inverter o vetor de estado;

A porta Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \implies H|i\rangle = \frac{|0\rangle + (-1)^i |1\rangle}{\sqrt{2}}, \quad (14)$$

cuja atuação cria um estado de superposição entre os vetores de estado da base com igual amplitude de probabilidade;

E a operação  $R_y(\theta)$

$$R_y(\theta) = \begin{bmatrix} \cos \frac{\theta}{2} & \sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}, \quad (15)$$

que representa um rotação de  $\theta$  do vetor de estado ao redor do eixo  $y$ .

Defindo as operações de 2 qbits temos a porta lógica CNOT, ou "não controlado"  $U_{CN_{c \rightarrow t}}$ , em que  $c$  representa o qbit de controle e  $t$  o qbit alvo. Sua atuação varia o estado do qbit alvo dependendo do valor do qbit de controle

$$U_{CN_{c \rightarrow t}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \implies \begin{cases} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{cases}; \quad (16)$$

A porta lógica de troca ou *swap*  $S_w$

$$S_w = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad (17)$$

que opera trocando os estados dos dois qbits.

Por fim, definimos a porta lógica Toffoli  $U_{T_{c,c \rightarrow t}}$  de 3 qbits, sendo dois deles qbits de controle e o último sendo o alvo, da forma

$$U_{T_{c,c \rightarrow t}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad (18)$$

que de maneira análoga à porta CNOT, atua mudando o estado do qbit alvo dependo do valor dos qbits de controle.

## 2 Materiais e métodos

Nesta seção será apresentado um breve resumo sobre a plataforma online da IBM para computação quântica, a IBM-Q Experience<sup>1</sup>, utilizada para o processamento dos algoritmos quânticos aqui propostos, bem como, para a aquisição de todos os dados. A plataforma é aberta e exige apenas um cadastro inicial e verificação de conta para sua utilização e oferece uma interface gráfica para a criação de circuitos quânticos, mostrada na figura 1, bem como a possibilidade processá-los, através de uma submissão *online*, em computadores quânticos reais dos laboratórios de pesquisa da IBM.

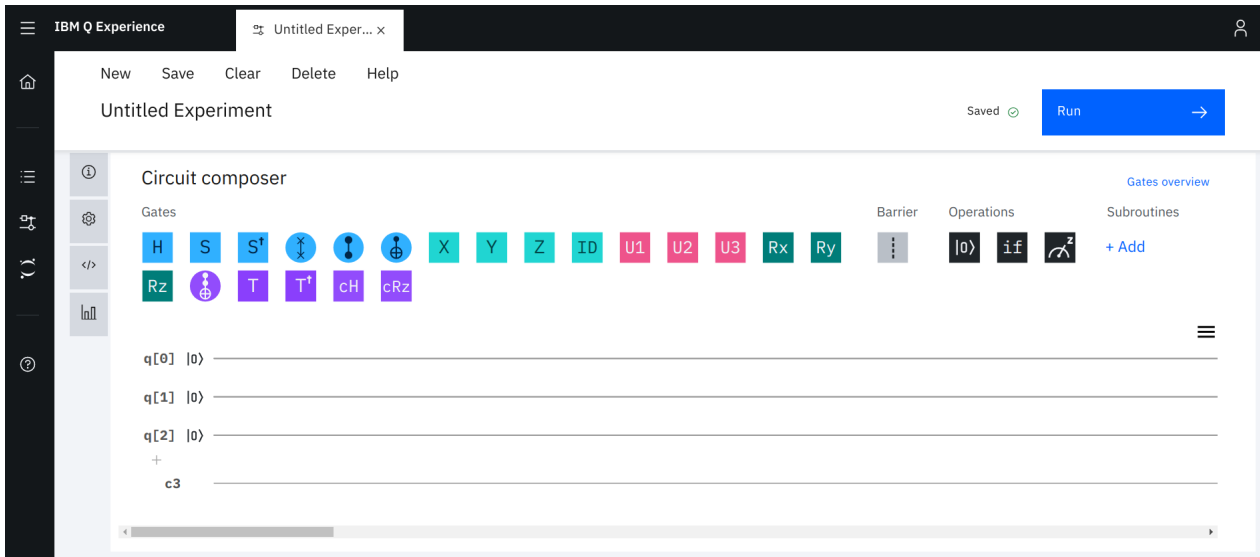


Figura 1 – Interface gráfica utilizada para a criação de circuitos quânticos.  
Fonte: IBM Q<sup>1</sup>

Da figura 1 vemos que as 3 primeiras linhas (q[0] à q[2]) correspondem cada uma a um registro quântico configurado com um estado inicial *default* de entrada  $|0\rangle$ . A última linha (c3 no caso da gravura acima) corresponde a um registro clássico das medições dos qbits, sendo cada registro quântico relacionado a 1 bit no registro clássico. Cada ícone na figura corresponde a alguma porta lógica quântica ou a alguma operação. A montagem do circuito é feita clicando-se nos ícones, correspondentes às portas lógicas ou operações que se deseja implementar, e arrastando-os até a posição desejada nos registros quânticos, de modo que a sua ordem, da esquerda para a direita, representam linhas de comando. Em todos os algoritmos criados aqui utilizaremos as portas lógicas quânticas, já introduzidas na seção 1.2, e operações ilustradas na figura 2

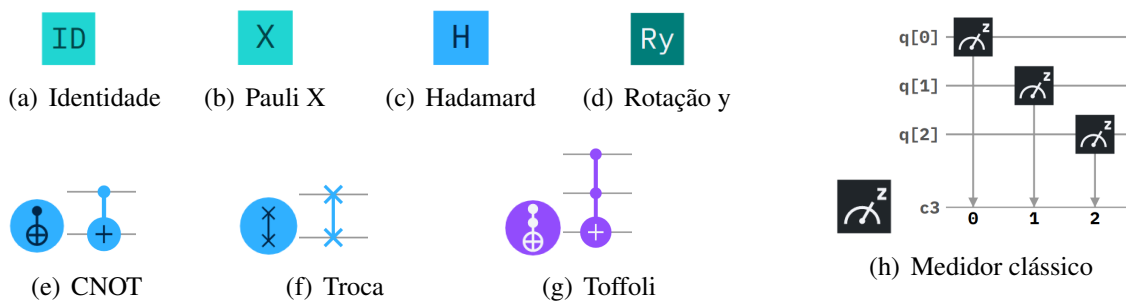


Figura 2 – Ícones e representações referentes às portas lógicas quânticas de um, dois e três qbits utilizadas e à operação de medição na base computacional Z quânticos  
Fonte: IBM Q<sup>1</sup>

A operação de medição, ilustrada na figura 2(h), é definida como sendo a medição dos qbits na base computacional, ou seja, a base Z. A operação de medição converte o valor obtido para os estados quânticos dos qbits em bits, e armazena no registro clássico, em que o primeiro qbit (referente ao

registro  $q[0]$  é o primeiro dígito (menor base de 2) do número binário no registro clássico, e assim por diante, de modo que o resultado da medição do estado  $|110\rangle$  seria o número binário 011, por exemplo.

A submissão online dos códigos pode ser feita clicando-se no ícone "Run", mostrado na figura 1, e em seguida, ajustando-se as condições do experimento, de acordo com a figura 3

Run your circuit

1. Select an available backend  
Backends availability and functionality can vary depending on the provider.

2. Select number of shots  
Increase the number of shots to improve statistical accuracy.

ibmq\_qasm\_simulator in ibmq-open/main ▼

1024 ▼

Cancel Run

Figura 3 – Tela de ajuste das opções do experimento, sendo elas a escolha do computador quântico à processar o código, e o número de vezes que esse código será processado

Fonte: IBM Q<sup>1</sup>

A primeira opção consiste na escolha de qual dispositivo da IBM deseja-se processar o circuito quântico. Dentre estes, estão alguns computadores quânticos e também um simulador clássico sendo este último um dispositivo que implementa um computador quântico ideal, ou seja, aquele constituído de um sistema quântico perfeitamente isolado, não apresentando, portanto, erros quânticos relacionados à processos de dissipação e descoerência. Diferentemente, os dispositivos quânticos reais são susceptíveis à tais erros e uma discussão mais detalhada das implicações disto será dada mais adiante, na seção 3.

A segunda opção consiste na escolha do número de vezes que o código será executado, sendo, num contexto ideal, cada execução equivalente à uma idêntica\* preparação, manipulação e medição de  $n$  sistemas quânticos com as mesmas características, podendo,  $n$  ser 1, 1024, 4096 ou 8196, segundo as opções da plataforma, e neste trabalho a utilização dos termos, "número de medições", "quantidades de medidas tomadas", ou sinônimos, se referirão à esse aspecto. Destaca-se ainda que a opção permite uma melhora na precisão estatística dos resultados das aferições do circuito quântico proposto, e uma explicação mais detalhada disto será dada, também, na seção 3.

Ao final os resultados dos experimentos são dados na forma de um histograma das possíveis respostas de uma medição dos qbits do circuito elaborado. Entretanto, por uma questão de clareza os resultados serão apresentados em histogramas personalizados elaborados utilizando o software *Mathematica* 11.3<sup>4</sup>.

\* É importante ressaltar que em um contexto não ideal existe uma limitação experimental associada à essa condição de construção de sistemas idênticos, o que também levará à erros.

Foram utilizados para executar os códigos, além do simulador clássico, os dispositivos quânticos **ibmq\_5\_yorktown-ibmqx2 (v2.0.0)** e **ibmq\_ourense (v1.0.1)** com as características definidas segundo a figura 4, em que as setas ligando os qbits representam a conectividade entre eles, ou seja, como eles interagem entre si. A escala de cores representa o erro associado a cada operação básica realizada, relativa à cada qbit. Ambos apresentam como operações básicas as portas lógicas  $U_1$ ,  $U_2$ ,  $U_3$ , que atuam como operações de rotações,  $C_x$ , que é a operação CNOT, e  $Id$  a operação identidade.

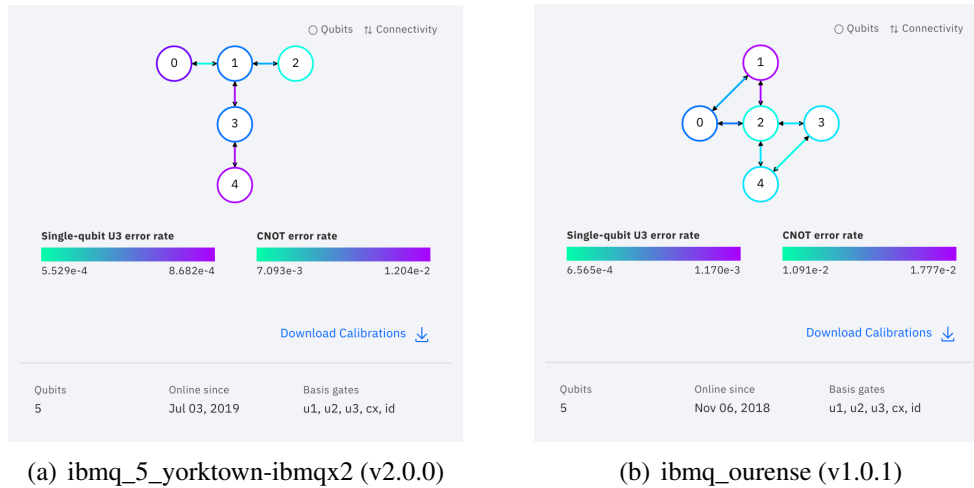


Figura 4 – *Set-ups* dos dispositivos quânticos utilizados no processamento dos circuitos quânticos. As setas representam a conectividade dentre os qbits e a escala de cores representam os erros de cada qbit com relação às operações dadas

Fonte: IBM Q<sup>1</sup>

A predileção por tais dispositivos se deu, primeiro, pelo fato de que os códigos criados aqui são de no máximo três qbits, e portanto um dispositivo que apresente uma conectividade maior entre esses qbits utilizados seria mais interessante, e, segundo, por uma questão de praticidade visto que a execução de algoritmos respeita uma fila de submissão, sendo tais dispositivos os que apresentavam uma concorrência menor.

### 3 Resultados e discussão

#### 3.1 Algoritmo para a geração de dois qbits emaranhados

Inicialmente será pautada a construção de um sistema físico mais simples com o intuito de se analisar suas principais características no contexto da mecânica quântica e da computação quântica. Tal construção foi dada pela montagem do seguinte circuito, ilustrado na figura 5

O estado inicial e a atuação das portas Hadamard e CNOT, respectivamente, são dadas por

$$|\Psi\rangle = U_{CN_{q[0] \rightarrow q[1]}} (H \otimes Id) |\Psi_0\rangle = U_{CN_{q[0] \rightarrow q[1]}} (H \otimes Id) |00\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (19)$$

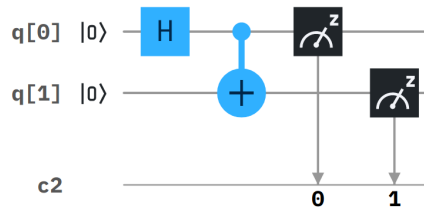


Figura 5 – Representação do circuito quântico de um sistema de 2 qbits emaranhados  
 Fonte: IBM Q<sup>1</sup>

Vemos que o resultado de uma medida no primeiro qbit inevitavelmente revela qual será o resultado de uma medida no segundo qbit, antes mesmo que essa medida seja realizada. Assim, fazendo-se uma medição do primeiro e segundo qbit respectivamente, os dois únicos possíveis resultados são 00 e 11, ambos com 50% de probabilidade. O código foi processado tanto no simulador clássico quanto num computador quântico, e os resultados para diferentes quantidades de medidas em sistemas idênticamente preparados são mostrados na figura 6.

Aqui é interessante notar dois fatores. O primeiro deles está relacionado ao caráter probabilístico da mecânica quântica, se repararmos apenas nas medidas realizadas no simulador, onde vemos que a estatística do problema se torna mais apurada a medida que o espaço amostral (número de medições realizadas em 1, 1024, 4096 ou 8192 sistemas idênticamente preparados) aumenta.

O segundo fator notório são as probabilidades não nulas para os resultados 01 e 10 em uma medida, presentes nos histogramas referentes ao computador quântico. A ressalva de que, devido à definição do estado  $|\Psi\rangle$  na equação (19), seria, num sistema físico ideal impossível obter-se resultados de medições diferentes de 00 e 11, nos leva a indagar de onde surgem os erros ligados à essas probabilidades não nulas.

Conforme mencionado na seção 2 anterior, o simulador implementa um computador quântico ideal, ou seja, um sistema quântico perfeitamente isolado de qualquer meio interagente, e, portanto, não suscetível a processos de dissipação e descoerência, e como podemos constatar os histogramas da primeira coluna não apresenta erros relacionados à tais processos.

De fato, conforme<sup>5</sup> vemos que o ambiente nas vizinhanças de um sistema quântico desempenha um papel crucial nestes processos. Ainda, em<sup>6</sup> um modelo quantizado da interação de um sistema quântico com sua vizinhança mostra que até mesmo flutuações do vácuo contribuem com a descoerência, sendo, então, impossível construir-se um sistema quântico perfeitamente isolado.

Portanto, diferentemente do simulador, um computador quântico real sempre apresentará erros associados aos processos de dissipação e descoerência, por mais minimizados que sejam. Ainda que presentes, esses erros não impossibilitam o refinamento da estatística do problema (até o limite imposto pelo erro), à medida que espaço amostral aumenta, de maneira similar ao que foi discutido anteriormente, e pode ser visto nos histogramas da segunda coluna na figura 6.

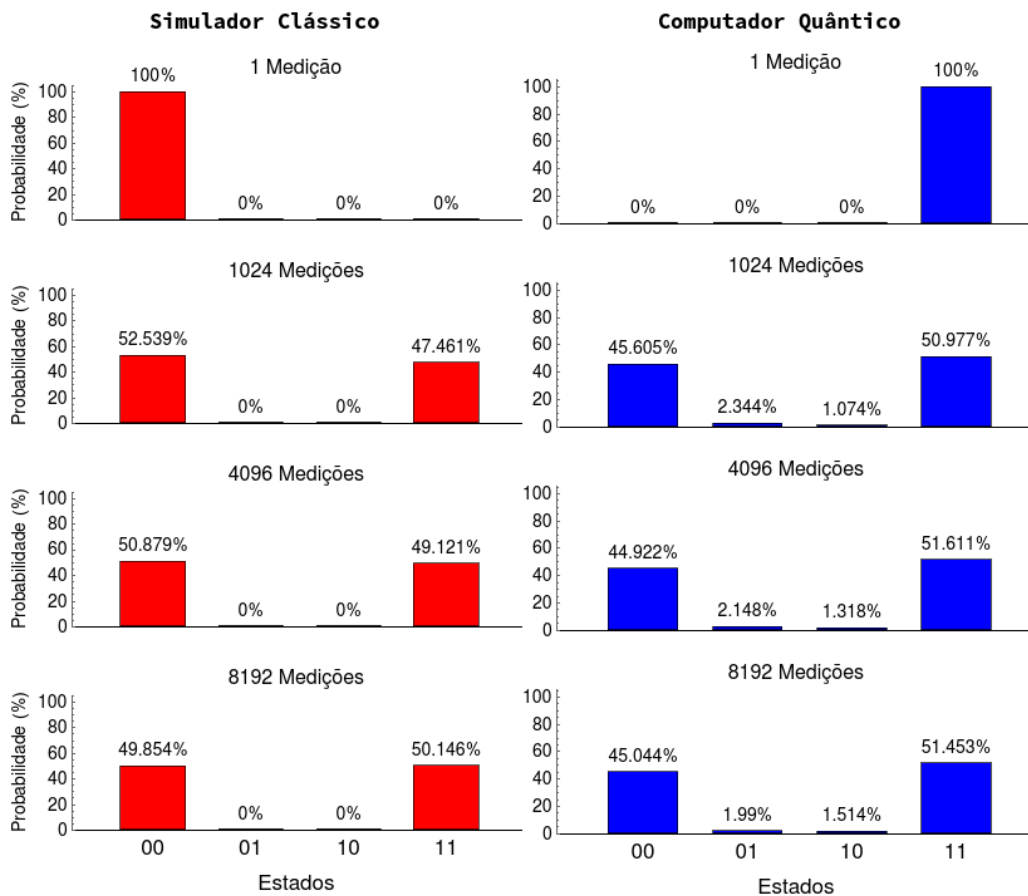


Figura 6 – Histogramas de probabilidades para medidas no sistema de 2qbits emaranhados utilizando tanto um simulador clássico quanto uma máquina real (computador quântico)  
 Fonte: Elaborada pelo autor.

### 3.2 Calculadora de soma de 2 registros de 1 qbit

Aqui propõe-se a implementação de algoritmos quânticos que realizem a operação de soma entre qbits. Os algoritmos aqui propostos são formulados com base em aritmética modular e soma de números binários. Assim, ressalta-se que todos os passos realizados pelos algoritmos quânticos implementados nesta seção poderiam ser realizados, também, em um computador clássico utilizando as portas lógicas clássicas devidas. Sendo assim, a motivação desta proposta é apenas a exploração de algumas propriedades quânticas dos sistemas apresentados, com um viés didático de estudo do tema "computação quântica".

Nesta implementação configurou-se o algoritmo da seguinte maneira:

**Entrada:** Dois registros de 1 qbit, representando os números à serem somados

**Saída:** Um número, de até 2 bits, resultado da soma entre os números da entrada

Para isso necessitou-se de 3 registros quânticos iniciais e 2 medidores clássicos, ao final do código.

Cada um dos dois primeiros registros (q[0] e q[1]) é composto de 1 qbit, e o terceiro composto por um estado de ancila. A figura 7 ilustra a montagem do sistema.

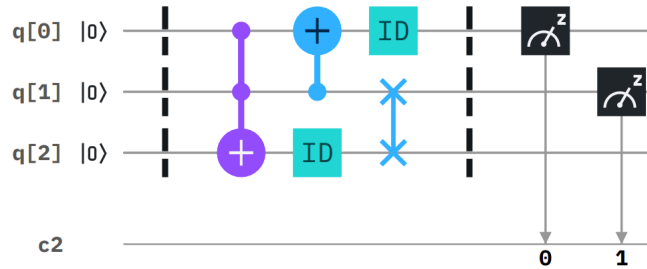


Figura 7 – Representação do circuito quântico de soma de dois registros de 1 qbit  
Fonte: IBM Q<sup>1</sup>

A função do estado de ancila é armazenar o qbit excedente da soma módulo 2. O algoritmo pode ser dividido em 3 partes, ilustradas na figura 7 pelas linhas verticais pontilhadas:

**Primeira parte:** Entrada do usuário nos registros q[0] e q[1] dos números que se deseja somar, de modo que o estado inicial é  $|\Psi\rangle = (U_1 |0\rangle) \otimes (U_2 |0\rangle) \otimes |0\rangle$ , em que  $U_1$  e  $U_2$  são quaisquer portas lógicas de 1 qbit;

**Segunda parte:** algoritmo de soma representado pelo operador unitário  $U_S$ , dado por  $U_S = (Id \otimes S_{W_{q[1] \leftrightarrow q[2]}}) (U_{CN_{q[1] \rightarrow q[0]}} \otimes Id) U_{T_{q[0], q[1] \rightarrow q[2]}}$ . Tal algoritmo realiza a operação de soma clássica entre os números representados pelos dois primeiros qbits;

**Terceira parte:** Medidores clássicos nos registros q[0] e q[1], nessa ordem.

Introduziremos agora quatro casos diferentes de entradas no algoritmo quântico, que abrangem todas as possibilidades de soma binária clássica de dois números de 1 bit (0 + 0, 0 + 1, 1 + 0 e 1 + 1). Os circuitos que representam esses casos são dados na figura 8.

Aqui, a matriz de Pauli  $X$  foi usada pra inverter o estado de um dos registros (ou dos dois primeiros registros na figura 8(d)) do estado *default*  $|0\rangle$  para o estado  $|1\rangle$ . A resposta obtida na saída de cada circuito dado será dada pela medida dos dois primeiros qbits no estado resultante da atuação do operador  $U_S$  em cada um estados iniciais dados.

$$\begin{aligned}
 |000\rangle &\xrightarrow{U_S} |000\rangle \xrightarrow{\text{medição}} 00 \\
 |010\rangle &\xrightarrow{U_S} |100\rangle \xrightarrow{\text{medição}} 01 \\
 |100\rangle &\xrightarrow{U_S} |100\rangle \xrightarrow{\text{medição}} 01 \\
 |110\rangle &\xrightarrow{U_S} |011\rangle \xrightarrow{\text{medição}} 10
 \end{aligned} \tag{20}$$

Os histogramas resultante de um conjunto de várias medições, por conta do erro experimental, de sistemas igualmente preparados conforme os circuitos ilustrados na figura 8 são mostrados nos gráficos na figura 9.

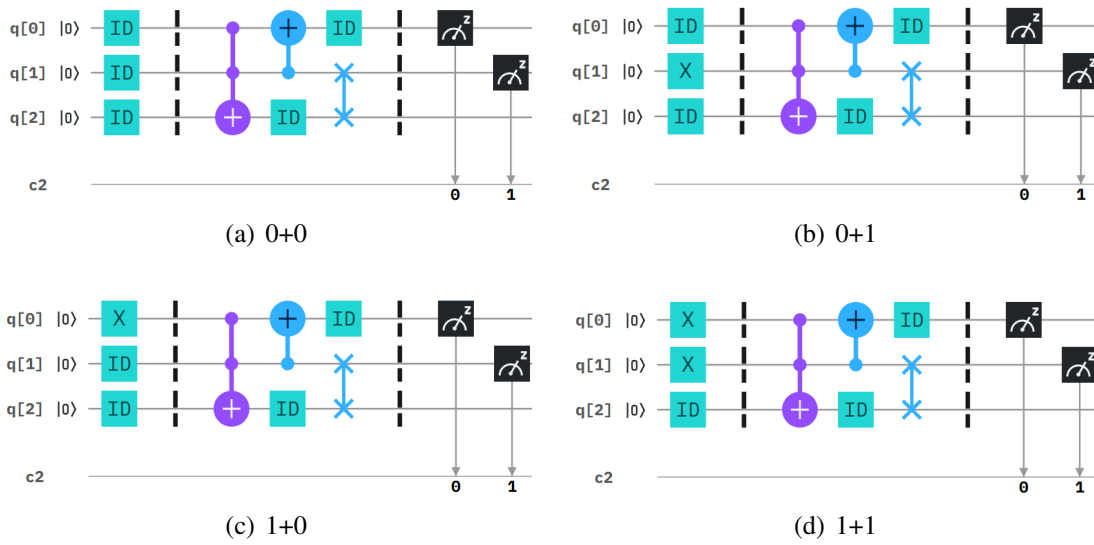


Figura 8 – Circuitos (a), (b), (c) e (d) que mostram as diferentes entradas usadas para representar a soma clássica binária de dois números de 1bit, 0 + 0, 0 + 1, 1 + 0 e 1 + 1 respectivamente  
 Fonte: IBM Q<sup>1</sup>

Analisando os histogramas dos resultados das medidas utilizando o simulador, para cada um dos casos, vemos que os resultados esperados numa medida, ou seja, o resultado da soma binária clássica para cada um dos casos, aparecem com 100% de probabilidade, seguindo a expectativa.

Aqui, novamente vemos, no processamento do algoritmo no CQ real, probabilidades não nulas para certos resultados, não esperados em um sistema quântico ideal. Ainda sobre esse aspecto, podemos ver que, diferente do algoritmo para a geração de dois qubits emaranhados, que utiliza apenas duas portas lógicas, a utilização de um número maior de operações no algoritmo de soma (tanto as do próprio operador  $U_S$  em si, quanto àquelas introduzidas pelo usuário) promove um aumento dos erros associados aos processos de decoerência e dissipação, seja pelo número maior de passos ou pelo aumento no tempo de processamento do algoritmo.

Ainda assim, observamos que as probabilidades de se obter os resultados esperados numa medida, em cada um dos casos, são expressamente majoritárias, tornando satisfatória a implementação do algoritmo, mas ainda longe do limite de uma computação robusta à erro.

Até agora vemos que o algoritmo implementado, no que diz respeito à inserção da entrada e obtenção dos resultados, não apresenta, ainda, diferenças com relação a um algoritmo clássico com a mesma função. Assim, exploraremos algumas propriedades quânticas do sistema introduzindo entradas constituídas por estados de superposição. Iniciando o código com  $|q[0]\rangle$  e  $|q[1]\rangle$  estados arbitrários temos

$$\begin{aligned} |q[0]\rangle &= a |0\rangle + b |1\rangle, \\ |q[1]\rangle &= c |0\rangle + d |1\rangle, \end{aligned} \tag{21}$$

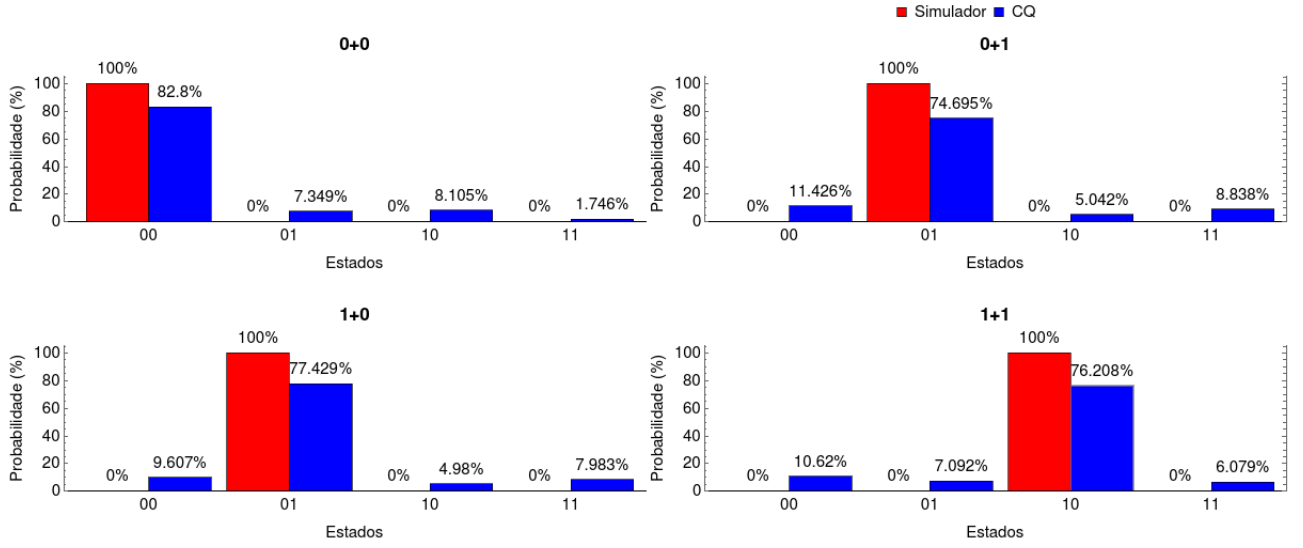


Figura 9 – Histogramas resultantes de um conjunto de 8192 medições para cada um dos circuitos da figura 8. As medidas foram tomadas tanto em um computador quântico (CQ) quanto no simulador clássico.

Fonte: Elaborada pelo autor.

com  $a^2 + b^2 = c^2 + d^2 = 1$ . Portanto, o estado  $|\Psi\rangle$  inicial de entrada do algoritmo pode ser representado por  $|\Psi\rangle = |q[0]\rangle \otimes |q[1]\rangle \otimes |q[2]\rangle$ , e atribuindo a arbitrariedade dos estados  $|q[0]\rangle$  e  $|q[1]\rangle$  (entrada do usuário), e mantendo o estado de ancila, temos

$$\begin{aligned} |\Psi\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \otimes |0\rangle \\ &= ac|000\rangle + ad|010\rangle + bc|100\rangle + bd|110\rangle \end{aligned} \quad (22)$$

Aqui será conveniente representar  $|\Psi\rangle$  e  $U_S$  na notação matricial. Da definição de  $U_S$  na seção 3.2 e da equação (22), na base computacional, obtemos

$$U_S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad (23)$$

e,

$$|\Psi\rangle = [ac \ 0 \ ad \ 0 \ bc \ 0 \ bd \ 0]^T. \quad (24)$$

Para a análise do problema e de sua evolução, ou seja, a atuação do operador  $U_S$  no estado inicial  $|\Psi\rangle$  (processamento do algoritmo) será útil a introdução do operador densidade evoluído  $\rho'$ , segundo a equação (12)

$$\rho' = |\Psi(t)\rangle \langle \Psi(t)| = U_S |\Psi\rangle \langle \Psi| U_S^\dagger \quad (25)$$

$$\rho' = \begin{bmatrix} a^2c^2 & 0 & 0 & abcd & abc^2 & a^2cd & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ abcd & 0 & 0 & b^2d^2 & b^2cd & abd^2 & 0 & 0 \\ abc^2 & 0 & 0 & b^2cd & b^2c^2 & abcd & 0 & 0 \\ a^2cd & 0 & 0 & abd^2 & abcd & a^2d^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (26)$$

Assim, o operador densidade na equação (26) contém toda a informação do processamento de uma estado arbitrário no algoritmo de soma. Como ao final do código os medidores clássicos fazem medições correspondentes apenas aos registros quânticos  $q[0]$  e  $q[1]$ , a informação útil ao nosso problema se restringe às informações relativas aos dois primeiros qbits. Logo, tomando o traço parcial do operador  $\rho'$  com relação ao terceiro qbit temos

$$\text{Tr}_3 \rho' = \rho'^{12} = \begin{bmatrix} a^2c^2 & 0 & abc^2 & 0 \\ 0 & b^2d^2 & abd^2 & 0 \\ abc^2 & abd^2 & b^2c^2 + a^2d^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (27)$$

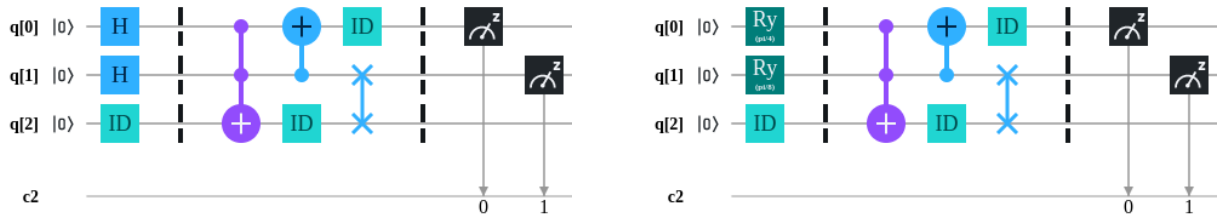
Desse modo estendemos a análise dos resultados da soma de dois números de 1 bit, aos possíveis resultados de uma medida no sistema de qbits dado.

A análise probabilística dos possíveis resultados das medidas realizadas pelos registradores clássicos pode ser dada em termos da matriz densidade reduzida (27) de modo que

$$\begin{aligned} P(00) &= \langle 00 | \rho'^{12} | 00 \rangle = a^2c^2 \\ P(01) &= \langle 10 | \rho'^{12} | 10 \rangle = b^2c^2 + a^2d^2 \\ P(10) &= \langle 01 | \rho'^{12} | 01 \rangle = b^2d^2 \\ P(11) &= \langle 11 | \rho'^{12} | 11 \rangle = 0 \end{aligned} \quad (28)$$

Agora, serão testadas duas entradas iniciais com diferentes coeficientes  $a, b, c$  e  $d$ , ambas mostradas na figuras 10.

Da figura 10(a) temos



(a) Estados de superposição aplicando portas Hadamard

(b) Estados de superposição aplicando portas Ry

Figura 10 – Circuitos (a) e (b) que mostram diferentes entradas de estados de superposição

Fonte: IBM Q<sup>1</sup>

$$|\Psi\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \otimes \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \otimes |0\rangle \implies a = b = c = d = \frac{1}{\sqrt{2}} \quad (29)$$

e, segundo a equação (28) obtemos

$$\boxed{P(00) = 0,25} ; \boxed{P(01) = 0,50} ; \boxed{P(10) = 0,25} ; \boxed{P(11) = 0} \quad (30)$$

Da figura 10(b), e da definição da operação  $R_y$  na equação (15), temos

$$|\Psi\rangle = R_{y_{\pi/4}}|0\rangle \otimes R_{y_{\pi/8}}|0\rangle \otimes |0\rangle = \left(\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle\right) \otimes \left(\cos\frac{\pi}{16}|0\rangle + \sin\frac{\pi}{16}|1\rangle\right) \otimes |0\rangle \implies \begin{cases} a = \cos\frac{\pi}{8} \\ b = \sin\frac{\pi}{8} \\ c = \cos\frac{\pi}{16} \\ d = \sin\frac{\pi}{16} \end{cases} \quad (31)$$

e, novamente, segundo a equação (28) obtemos

$$\boxed{P(00) = 0,82107} ; \boxed{P(01) = 0,17336} ; \boxed{P(10) = 0,00557} ; \boxed{P(11) = 0} \quad (32)$$

Os histogramas resultantes de um conjunto de várias medições de sistemas igualmente preparados conforme os circuitos ilustrados na figura 10 são mostrados nos gráficos na figura 11.

Analisando os histogramas e as equações (30) e (32), em ambos os casos, notamos novamente a presença de probabilidades não nulas para o resultado 11 devido aos erros relacionados à implementação física do computador quântico, discutidos anteriormente.

Outra vez, a fidelidade nas probabilidades dos resultados das medições realizadas no simulador dependem exclusivamente da formulação estatística do problema no que diz respeito à quantidade de medições efetuadas num certo número de sistemas identicamente preparados. Constata-se que o

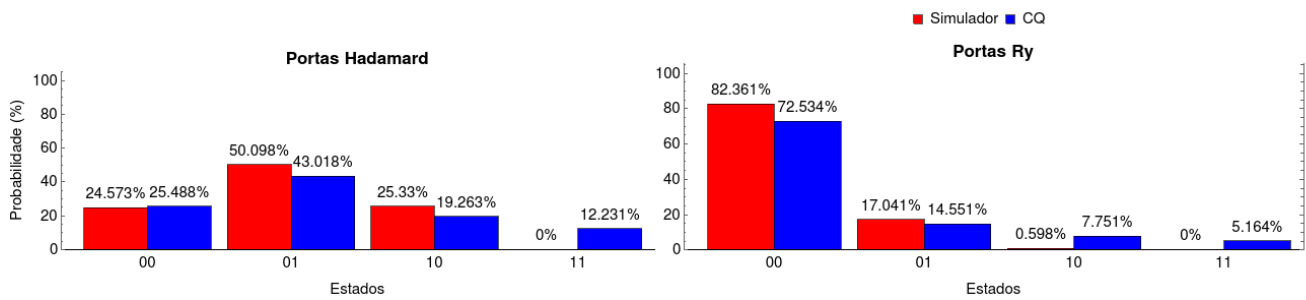


Figura 11 – Histogramas resultantes de um conjunto de 8192 medições para cada um dos circuitos da figura 10. As medidas foram tomadas tanto em um computador quântico (CQ) quanto em um simulador.

Fonte: Elaborada pelo autor.

simulador sempre dá  $P(11) = 0$ , diferentemente do que ocorre para as probabilidades resultantes do computador quântico. Além disso, observa-se que este último apresenta uma perda de fidelidade para probabilidades esperadas com valor pequeno, já que nestes casos os erros se tornam mais expressivos, como na probabilidade esperada para o resultado 10 no segundo histograma.

É importante salientar que a principal motivação para a introdução de entradas constituídas de estados de superposição no algoritmo de soma é sua circunstancial vantagem com relação aos algoritmos clássicos usuais já que aqui foi possível a realização de todas as possíveis operações de soma de dois números de 1bit em apenas uma execução do algoritmo. Assim, ao final do código temos um estado final que é a superposição de todas as possíveis respostas esperadas classicamente.

Entretanto, o caráter probabilístico da mecânica quântica nos deixa refém do ato da medição no sentido de que embora tenhamos em mão um "oráculo" ciente de todas as respostas somos obrigados aceitar o fato de que a cada pergunta apenas uma das respostas será fornecida e todas as outras serão perdidas. Assim, é necessário realizar esse procedimento por diversas vezes até que se obtenha uma distribuição estatística fiel de todos os possíveis resultados.

Desse modo, realizar todas as operações de possíveis soma entre dois números de 1bit de uma só vez, mas ser obrigado a executar esse processo várias vezes, ao invés de realizar todas as possíveis operações de soma entre dois números de 1 bit, individualmente, aparenta não ser uma troca tão vantajosa assim, conforme foi enunciado.

De fato esta última observação está correta já que aqui a introdução dos estados de superposição no algoritmo de soma teve um caráter puramente didático e de investigação das propriedades quânticas do sistema implementado, apesar de, na prática, tal implementação não ser tão engenhosa assim, no que diz respeito à exploração destas propriedades. Todavia essa apresentação abriu um interessante precedente para a formulação de um comparativo entre o sistema proposto e um sistema que, de maneira extremamente sagaz, efetivamente beneficia-se do caráter quântico do problema. Esse breve comparativo será introduzido na seção a seguir com a exposição do algoritmo de Shor.

### 3.3 O algoritmo de Shor

O algoritmo de Shor é um algoritmo quântico de fatoração de números inteiros em fatores primos criado em 1994 pelo matemático Peter Shor<sup>7</sup>. A importância do algoritmo de Shor no contexto da computação quântica é creditada justamente à sua eficiência frente aos algoritmos clássicos de fatoração.

Em ciência da computação uma das características que definem um algoritmo eficiente é o seu processamento ser dado em "tempo polinomial", ou seja, o número de passos crescer como um polinômio do *input* inicial. Assim, dado um número  $N \in \mathbb{Z}$ , sua fatoração via Shor em números primos requer  $O(n^2 \log n \log(\log n))$  operações, em que  $n$  é o número de *bits* da entrada inicial  $N$ , enquanto o análogo clássico requer  $\exp(O(n^{2/3} \log^{2/3} n))$  operações.<sup>2</sup>

Ainda assim o algoritmo pode ser entendido como sendo composto de duas partes: uma **parte clássica**, que diz respeito a todos os passos que poderiam reproduzidos exatamente em algoritmos clássicos de fatoração usuais, e têm base na teoria dos números e aritmética modular, e uma **parte quântica**, que explora, de maneira extremamente engenhosa, as propriedades da mecânica quântica de superposição de estados e interferência quântica para a obtenção da resposta, sendo esta última a principal motivação desta seção.

Para dar mais clareza à maneira como o algoritmo de Shor opera e o que é responsável por sua maior eficiência será necessário introduzir um tópico sobre a transformada de Fourier quântica.

#### 3.3.1 Transformada de Fourier quântica (QFT)

A transformada de Fourier é uma transformação matemática que mapeia uma função em um novo espaço de funções, denominado espaço recíproco. Em física, sua principal aplicação é o mapeamento de funções de domínio temporal para o domínio das frequências. No algoritmo de Shor, a aplicação da QFT parte da mesma premissa: explorar a periodicidade de uma função. Assim sendo, podemos definir a QFT. Dado uma base ortonormal  $\{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$ , a transformada de Fourier quântica (QFT) pode ser definida como sendo a operação linear que age nos estados da base de modo que

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |k\rangle, \quad (33)$$

sendo  $|j\rangle$  um dos quaisquer estados. Deste modo podemos definir um operador linear  $U_{QFT}$  tal que

$$U_{QFT} |j\rangle \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} jk} |k\rangle \quad (34)$$

É importante ressaltar que a QFT é uma operação unitária, ou seja,  $U^\dagger \cdot U = I$ , sendo, então, possível a construção de um circuito quântico que compute tal transformação. Assim, para sua implementação, em termos das portas lógicas quânticas usuais, é conveniente introduzir a **representação**

**produto** da QFT, representando os estados da base ortonormal em termos da base computacional (base binária).

Se tomarmos  $N = 2^n$  para algum  $n \in \mathbb{Z}$ , temos que os estados da base ficam:  $|0\rangle, |1\rangle, \dots, |2^n - 1\rangle$ . Então, para um estado  $|j\rangle$  qualquer, temos que  $j$  em base binária fica  $j_1 j_2 \dots j_n$  com  $j = 0, 1$ , ou seja,  $j = 2^{n-1} j_1 + 2^{n-2} j_2 + \dots + 2^1 j_{n-1} + 2^0 j_n$ .

Da equação (33)

$$\begin{aligned}
|j\rangle &\longrightarrow \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j \frac{(2^{n-1} k_1 + 2^{n-2} k_2 + \dots + 2^1 k_{n-1} + 2^0 k_n)}{2^n}} |k_1 k_2 \dots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j \sum_{l=1}^n k_l 2^{-l}} |k_1 k_2 \dots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 \left[ \bigotimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[ \sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] = \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[ |0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \\
&= \frac{(|0\rangle + e^{2\pi i j/2} |1\rangle) (|0\rangle + e^{2\pi i j/2^2} |1\rangle) \dots (|0\rangle + e^{2\pi i j/2^n} |1\rangle)}{2^{n/2}}
\end{aligned} \tag{35}$$

Ainda, podemos escrever o termo  $\frac{j}{2^l}$  em termos de **frações binárias**, sendo

$$0.j_l j_{l+1} \dots j_m = \sum_{n=l}^m j_n 2^{-n+l-1} \tag{36}$$

Assim

$$\boxed{U_{QFT} |j\rangle = \frac{(|0\rangle + e^{2\pi i 0.j_n} |1\rangle) (|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n} |1\rangle)}{2^{n/2}}} \tag{37}$$

Aqui, vê-se que a representação produto coloca a QFT em termos da base computacional, facilitando a busca de um circuito quântico que compute a transformação. Tal circuito é representado na figura 12, em que a operação  $R_k$  é dada por

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}. \tag{38}$$

O número de portas lógicas utilizadas para  $n$  qbits é então, para o primeiro qbit: uma Hadamard e  $(n - 1) R_k$ , sendo  $n$  no total; para o segundo qbit: uma Hadamard e  $(n - 2)$ , sendo  $(n - 1)$ ; e assim sucessivamente, de modo que o número total de portas lógicas Hadamard e  $R_k$  é dada pela progressão aritmética

$$n + (n - 1) + (n - 2) + \dots + 2 + 1 = \frac{n(n + 1)}{2}. \quad (39)$$

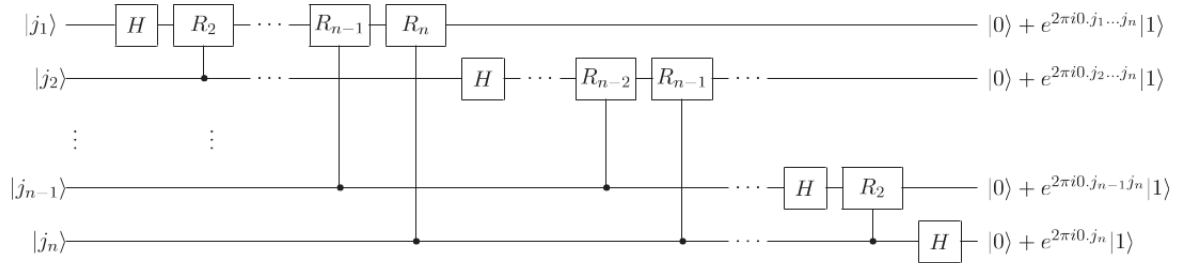


Figura 12 – Representação da QFT em um circuito quântico , omitindo-se os fatores de normalização e as portas *swap* para inverter a ordem dos qbits, conforme vemos na representação produto

Fonte: NIELSEN, M. A.; CHUANG, I.<sup>2</sup>

Ainda, utiliza-se uma porta *Swap* para cada par de qbits, de modo totalizar  $n/2$  portas, no máximo. Aqui vemos que o número de portas lógicas utilizadas é da ordem de  $O(n^2)$ , em contra partida à implementação clássica da transformada de Fourier, que requer exponencialmente mais portas lógicas.

### 3.3.2 Fatoração em números primos

Dado  $\{N | N \in \mathbb{Z}, N > 1\}$  a partir do **teorema fundamental da aritmética**<sup>2</sup>, sempre é possível escrever  $N$  da forma  $N = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ , em que  $p_i$  é um número primo e  $a_i$  é um inteiro positivo.

Para  $x$  e  $N$  inteiros positivos e co-primos, ou seja, o máximo divisor entre eles é 1, a ordem de  $x$  módulo  $N$  é o inteiro positivo  $r$  tal que  $x^r = 1 \pmod{N}$ .

Mais genericamente, dado um inteiro positivo  $N$ , escolhendo arbitrariamente  $x \neq 1$ , co-primo e menor que  $N$  temos que  $x^r - 1$  é um múltiplo de  $N$ , assim

$$x^r - 1 = mN \implies (x^{r/2} + 1)(x^{r/2} - 1) = mN, \quad (40)$$

com  $m$  um inteiro qualquer.

Vemos aqui que a partir da busca da ordem  $r$  é possível obter-se a fatoração de  $N$  em fatores não triviais  $\frac{(x^{r/2} \pm 1)}{m}$ . Mesmo  $m$  sendo desconhecido, pode-se executar algoritmos clássicos, como o **algoritmo de Euclides**<sup>2</sup>, para se computar o máximo divisor comum (m.d.c) entre  $(x^{r/2} \pm 1)$  e  $N$ .

Assim, o problema da fatoração de  $N$  em números primos se resume ao problema de busca da ordem  $r$ . Partindo desse princípio definimos a função  $f(k)$  tal que

$$f(k) = x^k \pmod{N}, \quad (41)$$

para  $k \in \mathbb{Z}$ .

Da estrutura da  $f(k)$  podemos verificar que ela é  $r$ -periódica, sendo  $r$  a ordem definida acima,

$$f(k+r) = x^{k+r} \pmod N = x^k x^r \pmod N = x^k (1 \pmod N) = x^k \pmod N = f(k) \quad (42)$$

Assim, podemos iniciar o algoritmo com o estado de dois registros  $|0\rangle|0\rangle$ .

Aplicamos  $t$  transformações de Hadamard no primeiro registro (note que a representação do estado quântico em termos da base decimal é mais ilustrativo para o propósito deste trabalho):

$$(H^t \otimes I) |0\rangle|0\rangle = (H^t |0\rangle) |0\rangle = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle |0\rangle \quad (43)$$

Ainda, calculamos  $f(k)$  para cada  $k$  e armazenamos no segundo registro:

$$\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle |x^k \pmod N\rangle, \quad (44)$$

e assim teremos:

$$\frac{1}{2^{t/2}} [|0\rangle|0\rangle + |1\rangle|1\rangle + \dots + |k_j\rangle|f(k_j)\rangle + |k_{j+1}\rangle|f(k_{j+1})\rangle + \dots + |2^{t-1}\rangle|f(2^{t-1})\rangle] \quad (45)$$

Aqui, realizando uma medição no segundo registro, obteríamos um certo estado  $|f(k_n)\rangle$  de modo que a função de onda total colapsaria num estado emaranhado de todos os  $|k_n\rangle$  cuja  $f(k) = f(k_n)$ . Mas explorando a periodicidade da função  $f(k)$  obtemos o seguinte estado:

$$C [|k_n\rangle|f(k_n)\rangle + |k_n+r\rangle|f(k_n)\rangle + |k_n+2r\rangle|f(k_n)\rangle + \dots], \quad (46)$$

em que  $C$  é a constante de normalização.

Por fim, a aplicação da QFT no primeiro registro, a partir de uma série de padrões de interferências construtivas e destrutivas, leva-o à um estado de superposição  $\sum_l \alpha_l |l\rangle$ , em que  $\alpha_l$  é zero para qualquer  $l$  não múltiplo de  $r$ , de modo que em uma única medida de  $|l\rangle$  é possível se obter a ordem  $r$  com uma certa precisão.

## 4 Conclusões e considerações finais

A partir da implementação dos algoritmos propostos nas seções 3.1 e 3.2, tanto no simulador clássico quanto num dispositivo quântico, foi possível constatar certos aspectos de extrema relevância no contexto da computação quântica. O primeiro deles está relacionado às fontes de erros gerados por processos de descoerência e dissipação nos resultados das implementações físicas de sistemas quânticos. A inexistência desses erros é observada no simulador clássico que implementa um sistema perfeitamente isolado.

O segundo aspecto está relacionado ao caráter probabilístico da mecânica quântica, em que a descrição dos possíveis resultados das medidas dos sistemas propostos apresentaram um aumento na precisão estatística com o aumento do espaço amostral, ou seja, número de execução dos códigos. Esse resultado foi observado tanto para o simulador clássico quanto para o computador quântico, com a ressalva de que neste último a acurácia estatística era limitada pelos erros associados aos processos de dissipação e descoerência mencionados acima.

Ainda, a implementação da calculadora de soma partindo-se de estados iniciais constituídos de estados de superposição, apesar de promover o processamento em paralelo de todos os possíveis cálculos de soma de dois números de 1bit, mostrou-se pouco inventiva com relação à exploração da propriedades da mecânica quântica em prol da obtenção eficiente das respostas do problema proposto. Diferente desta, vimos na seção 3.3 que o Algoritmo de Shor, a partir da implementação da transformada de Fourier quântica, promove uma serie de padrões de interferência construtiva e destrutiva de modo a resultar num estado final formado pela superposição apenas dos estados que correspondem à resposta esperada para o problema. Assim, em uma única medida é possível obter-se, com certa precisão, os fatores primos de um número inteiro  $N$ , no caso da apresentação feita aqui.

## Referências

- 1 IBM Corporation 1994-2019. **IBM Q Experience**. Disponível em: [https:// quantum-computing.ibm.com/](https://quantum-computing.ibm.com/). Acesso em: 20 out. 2019.
- 2 NIELSEN, M. A.; CHUANG, I. **Quantum computation and quantum information**: 10th anniversary edition. Cambridge: Cambridge University Press, 2011.
- 3 COHEN-TANNOUJDI, C.; DIU, B.; LALOE, F. **Quantum mechanics**. New York: John Wiley & Sons, 1991. v.1.
- 4 WOLFRAM RESEARCH. **Mathematica for students for sites - versão 11.3.0.0**. Distribuição de Software CCE - USP, out 2019. Disponível em: <https://atendimentosti.usp.br/otrs/public.pl?Action=PublicFAQZoom;ItemID=287>. Acesso em: 25 nov. 2020.
- 5 ZUREK, W. H. Environment-induced decoherence and the transition from quantum to classical. **Vistas in Astronomy**, v.37 p.185–196, 1993.
- 6 PALMA, G. M.; SUOMINEN, K.; EKERT, A. Quantum computers and dissipation. **Proceedings Mathematical Physical and Engineering Sciences**, v.452, p.567–584, 1996. doi:10.1098/rspa.1996.0029.
- 7 SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE, 35th, Santa Fe, NM, USA. **Proceedings 35th Annual Symposium on Foundations of Computer Science**, Santa Fe: 1994. p. 124–134.