COMPUTAÇÃO QUÂNTICA: COMPLEXIDADE E ALGORITMOS

CARLOS H. CARDONHA
MARCEL K. DE CARLI SILVA
CRISTINA G. FERNANDES (ORIENTADORA)

Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo

Resumo. O problema da fatoração de inteiros em primos é um dos mais famosos em computação, tanto do ponto de vista teórico quanto prático. Apresentamos o modelo quântico de computação, introduzido nos anos 80, e o algoritmo de Shor, que fatora inteiros em primos eficientemente nesse modelo. A seguir, passamos a um estudo mais aprofundado desse modelo, por meio do conceito de máquinas de Turing quânticas. Concluímos exibindo os principais resultados de complexidade computacional envolvendo o modelo quântico.

1. Introdução

Em 1900, em uma palestra marcante no Congresso Internacional de Matemáticos realizado em Paris, Hilbert postulou 23 problemas matemáticos, que tratam de temas diversos em matemática e áreas afins. O décimo problema na lista de Hilbert (*determination of the solvability of a diophantine equation*) pergunta se é possível determinar se uma equação diofantina arbitrária tem ou não solução por meio de um "processo finito":

Financiado parcialmente pela FAPESP 03/13236-0.
Financiado parcialmente pela FAPESP 03/13237-7.

> *Given a diophantine equation with any number of unknown quantities and with rational numerical coefficients: to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Esse problema pode ser postulado em uma linguagem mais atual como o seguinte: existe um algoritmo que, dada uma equação diofantina, determina se esta tem ou não solução?

Note que a questão postulada por Hilbert precede de décadas a invenção de computadores. Foi apenas nos anos 30 que tais questões foram formuladas e tratadas dentro do que ficou depois conhecido como *teoria da computabilidade*. Esta é a parte da teoria da computação especializada em lidar com esse tipo de questão.

Foi nos anos 30, após um trabalho de Gödel em lógica, que a idéia de algoritmo começou a ser formalizada. Gödel [Göd31] introduziu o conceito de *função primitiva recursiva* como uma formalização dessa idéia. Church [Chu33, Chu36] introduziu o λ-*cálculo* e Kleene [Kle36] definiu o conceito de *funções recursivas parciais* e mostrou a equivalência entre esse e o λ-cálculo. Turing [Tur36, Tur37] por sua vez propôs a sua formalização da idéia de algoritmo: as chamadas *máquinas de Turing*. Nesses trabalhos, Turing mostrou também a equivalência do conceito de máquinas de Turing e de funções recursivas parciais. Vale mencionar que o conceito de máquinas de Turing foi independentemente proposto por Post [Pos36], um professor de colegial de Nova Iorque. Cada uma dessas propostas diferentes do conceito de algoritmo é chamada de *modelo de computação*.

Foi Kleene [Kle52] quem chamou de *tese de Church* a afirmação de que todo modelo de computação *razoável* é equivalente ao da máquina de Turing. A afirmação é propositalmente vaga, pois visa capturar mesmo modelos que ainda venham a ser propostos, e cuja natureza não podemos prever. Por *razoável* entende-se um modelo que seja realista, no sentido de poder (mesmo que de maneira aproximada) ser construído na prática.

A teoria da computabilidade no fundo diferencia os problemas *decidíveis* (para os quais existe um algoritmo) dos *indecidíveis* (para os quais não existe um algoritmo). O surgimento dos computadores

nas décadas de 30 e 40 aos poucos evidenciou uma diferença entre os problemas decidíveis: muitos parecem ser bem mais difíceis que outros, no sentido de que se conhece apenas algoritmos extremamente lentos para eles. Com isso, surgiu a necessidade de refinar a teoria de computabilidade para tentar explicar essas diferenças. Foi apenas nos anos 60 que a *teoria de complexidade*, que trata de tais questões, tomou corpo, com a formalização da idéia de *algoritmo eficiente*, independentemente introduzida por Cobham [Cob65] e Edmonds [Edm65], e a proposta de reduções eficientes entre problemas, feita por Karp [Kar72].

Foi nessa época que surgiram as definições das classes de complexidade **P** e **NP** e do conceito de **NP**-*completude*, que captura de certa maneira a dificuldade de se conseguir algoritmos eficientes para certos problemas. Grosseiramente, um problema em **NP** é dito **NP**-*completo* se qualquer outro problema da classe **NP** pode ser reduzido eficientemente a ele. A mais famosa questão na área de teoria da computação é se **P** é ou não igual a **NP**. Se for mostrado que algum problema **NP**-completo está em **P**, então tal questão é resolvida e fica provado que $\mathbf{P} = \mathbf{NP}$.

Um marco na teoria de complexidade é o *teorema de Cook* [Coo71, Lev73], que prova a existência de problemas **NP**-completos. Cook mostrou que o problema conhecido como SAT, de decidir se uma fórmula booleana em forma normal conjuntiva é ou não satisfatível, é **NP**-completo. Após o teorema de Cook e o trabalho de Karp [Kar72], que mostrou que vários outros problemas conhecidos são **NP**-completos, essa teoria se desenvolveu amplamente, tendo estabelecido a dificuldade computacional de problemas das mais diversas áreas, como mostram Garey e Johnson [GJ79].

Um dos problemas mais famosos cuja complexidade continua em aberto, mesmo após várias décadas de esforço da comunidade no sentido de resolvê-lo, é o *problema da fatoração de inteiros*: dado um inteiro, determinar a sua fatoração em números primos. Recentemente, o seu parente próximo, o problema de decidir se um número inteiro é primo ou não, chamado de *problema da primalidade*, teve sua complexidade totalmente definida, com o algoritmo AKS, de Agrawal, Kayal e Saxena [AKS02a, AKS02b]. Esse algoritmo mostra que o problema da primalidade está na classe **P**, resolvendo com isso uma questão em aberto há anos. Não se sabe até hoje, no entanto, se

há um algoritmo eficiente para resolver o problema da fatoração de inteiros!

Na verdade, a dificuldade computacional do problema da fatoração de inteiros tem sido usada de maneira crucial em alguns sistemas criptográficos bem-conhecidos. Se for descoberto um algoritmo eficiente para resolver o problema da fatoração, vários sistemas criptográficos importantes seriam quebrados, incluindo o famoso sistema RSA de chave pública, criado por Rivest, Shamir e Adleman [RSA78].

O assunto de nossa iniciação científica — Computação Quântica — trata de um novo modelo de computação, o modelo quântico, que vem levantando questões intrigantes dentro da teoria de complexidade, e pode ter impactos práticos dramáticos no mínimo na área de criptologia. O modelo quântico de computação não infringe a validade da tese de Church, porém questiona a validade de uma versão mais moderna dessa, a chamada *tese de Church estendida*, que diz que todo modelo de computação razoável pode ser simulado *eficientemente* por uma máquina de Turing.

Pode-se dizer que a teoria de computação quântica iniciou-se nos anos 80, quando Feynman [Fey82] observou que um sistema quântico de partículas, ao contrário de um sistema clássico, parece não poder ser simulado eficientemente em um computador clássico, e sugeriu um computador que explorasse efeitos da física quântica para contornar o problema. Desde então, até 1994, a teoria de computação quântica desenvolveu-se discretamente, com várias contribuições de Deutsch [Deu85, Deu89], Bernstein e Vazirani [BV97], entre outros, que colaboraram fundamentalmente para a formalização de um modelo computacional quântico.

Foi apenas em 1994 que a teoria recebeu um forte impulso e uma enorme divulgação. Isso deveu-se principalmente ao algoritmo de Shor [Sho94, Sho97], um algoritmo quântico eficiente para o problema da fatoração de inteiros, considerado o primeiro algoritmo quântico combinando relevância prática e eficiência. O algoritmo de Shor é uma evidência de que o modelo computacional quântico proposto pode superar de fato o modelo clássico, derivado das máquinas de Turing. O resultado de Shor impulsionou tanto a pesquisa prática, objetivando a construção de um computador segundo o modelo quântico, quanto a busca por algoritmos criptográficos alternativos e algoritmos quânticos eficientes para outros problemas difíceis. Essas

e várias outras questões, relacionadas tanto com a viabilidade do modelo quântico quanto com as suas limitações, têm sido objeto de intensa pesquisa científica.

Do ponto de vista prático, busca-se descobrir se é ou não viável construir um computador segundo o modelo quântico que seja capaz de manipular números suficientemente grandes. Tal viabilidade esbarra em uma série de questões técnicas e barreiras físicas e tecnológicas. Já se tem notícia de computadores construídos segundo o modelo quântico, mas todos ainda de pequeno porte. Em 2001, por exemplo, foi construído um computador quântico com 7 *qubits* (o correspondente aos bits dos computadores tradicionais). Nesse computador, foi implementado o algoritmo de Shor que, nele, fatorou o número 15. Uma parte dos cientistas da computação acredita que a construção de computadores quânticos de maior porte será possível, enquanto outra parte não acredita nisso.

Do ponto de vista de teoria de complexidade, busca-se estabelecer a relação entre as classes de complexidade derivadas do modelo quântico e as classes de complexidade tradicionais. Também busca-se, claro, estabelecer a complexidade no modelo quântico de problemas bem conhecidos, ou seja, busca-se por algoritmos quânticos eficientes para outros problemas relevantes.

Selecionamos para apresentar nesse trabalho os pontos que consideramos mais relevantes nessa área: o algoritmo de Shor e os principais resultados de complexidade computacional na área. Para apresentar o algoritmo de Shor, descrevemos uma das possíveis formalizações do modelo computacional quântico, mais adequada à descrição de resultados algorítmicos. Para mostrar os resultados de complexidade computacional, apresentamos uma segunda possível formalização do modelo quântico — as máquinas de Turing quânticas. Essas duas formalizações são equivalentes, porém a demonstração desse fato não é trivial e optamos por não incluí-la nesse trabalho.

Assim mesmo, esperamos dar uma visão do que é esta área nova e intrigante, e das suas potencialidades e dificuldades. O tema é multidisciplinar, no sentido de que depende de uma série de conceitos da mecânica quântica, e empresta a notação usada nessa área, o que dificulta um pouco a apresentação dos conceitos para pessoas de outras áreas, como computação e matemática. Um texto mais completo foi

preparado durante essa iniciação científica e pode ser encontrado no endereço `http://www.ime.usp.br/~magal/quantum/`.

2. O modelo quântico de computação

Nesta seção apresentamos uma formalização do modelo quântico de computação mais adequada à descrição de algoritmos quânticos. Esta consiste primeiramente na formalização dos principais componentes de um computador quântico e do seu funcionamento básico. Depois disso, segue a formalização do conceito de algoritmo quântico. Um exemplo simples é incluído no final da seção para ajudar na assimilação dos conceitos apresentados.

2.1. **Bits quânticos.** Seja $\mathcal{H}_2$ um espaço de Hilbert de dimensão 2. Fixe uma base ortonormal $B_2 := \{|0\rangle, |1\rangle\}$ de $\mathcal{H}_2$. Um *qubit* ou *bit quântico* é um vetor unitário em $\mathcal{H}_2$, isto é, um vetor $|\phi\rangle \in \mathcal{H}_2$ é um qubit se

$$|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle, \tag{1}$$

com $\alpha_0, \alpha_1 \in \mathbb{C}$ e $|\alpha_0|^2 + |\alpha_1|^2 = 1$. Dizemos que os vetores $|0\rangle$ e $|1\rangle$ são os *estados básicos* e que o qubit $|\phi\rangle$ está numa *superposição* de estados básicos (contraste isto com o modelo clássico, onde um bit assume apenas um dos valores 0 ou 1). Chamamos ao coeficiente complexo α_j de *amplitude* do estado básico $|j\rangle$, para $j = 0, 1$.

No modelo clássico, se tivermos em mãos um bit b, podemos descobrir sem problemas se b vale 0 ou 1 e isso em nada afeta o valor de b. Já no modelo quântico, não é possível determinar o valor de um qubit $|\phi\rangle$. Se tentarmos, o que observamos é o resultado de um evento probabilístico que tem como efeito colateral a alteração irreversível do valor $|\phi\rangle$. Mais precisamente, ao medirmos o estado de um qubit $|\phi\rangle$ dado pela equação (1), enxergaremos o "valor" $|0\rangle$ com probabilidade $|\alpha_0|^2$ e o "valor" $|1\rangle$ com probabilidade $|\alpha_1|^2$. Se o "valor" observado for $|0\rangle$, o estado do qubit $|\phi\rangle$, imediatamente após a medição, será $|0\rangle$, e analogamente se o estado observado for $|1\rangle$. Note então que, apesar de um qubit armazenar uma superposição de estados, usando medições, só conseguimos obter dele um dos estados da superposição.

Existem apenas duas portas lógicas operando sobre um bit clássico: a porta identidade e a negação. No modelo quântico de computação,

qualquer transformação unitária em $\mathcal{H}_2$ é uma porta quântica. Uma matriz $U \in \mathbb{C}^{2\times 2}$ é dita *unitária* se $U^*U = UU^* = I$, onde I é a matriz identidade e U^* é a transposta conjugada de U. Para trabalharmos com tais transformações, convencionamos que um qubit $|\phi\rangle$ dado pela equação (1), tem a seguinte representação na base B_2:

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = |\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle. \tag{2}$$

Assim, a matriz de Hadamard

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3}$$

transforma o qubit $|0\rangle$ no qubit

$$H|0\rangle = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big). \tag{4}$$

Será útil convencionarmos uma representação gráfica para circuitos quânticos, indicando a ordem de aplicação de portas e medições. Por exemplo, o circuito ilustrado na figura 1 indica que a matriz de Hadamard H deve ser aplicada ao qubit $|\phi\rangle$ e depois o qubit resultante deve ser medido para obtermos o qubit $|\phi'\rangle$. Se $|\phi\rangle$ for inicializado com $|0\rangle$, então $|\phi'\rangle$ será $|0\rangle$ ou $|1\rangle$ equiprovavelmente, de acordo com a equação (4).

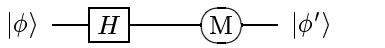

FIGURA 1. Um circuito quântico.

É interessante observar como as medições afetam o comportamento do circuito. Por exemplo, se inicializarmos $|\phi\rangle$ com $|0\rangle$, então $|\phi'\rangle$ no circuito quântico da figura 2 sempre será $|0\rangle$. Já no circuito da figura 3, o estado $|\phi'\rangle$ será $|0\rangle$ ou $|1\rangle$ equiprovavelmente.

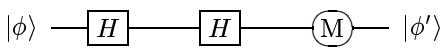

FIGURA 2. Mais um circuito.

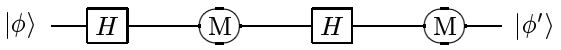

FIGURA 3. Circuito com medição intercalada.

2.2. **Registradores quânticos.** Seja $\mathcal{H}_{2^n}$ um espaço de Hilbert de dimensão 2^n. Fixe $B_{2^n} := \{|x\rangle : x \in \{0,1\}^n\}$ uma base ortonormal de $\mathcal{H}_{2^n}$, onde $\{0,1\}^n$ denota o conjunto das cadeias de caracteres de comprimento n sobre o alfabeto $\{0,1\}$. Por exemplo, para $n = 2$ temos $B_4 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Um registrador quântico de n qubits é um vetor unitário em $\mathcal{H}_{2^n}$, isto é, um vetor $|\phi\rangle \in \mathcal{H}_{2^n}$ é um registrador quântico de n qubits se

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle, \tag{5}$$

com $\alpha_x \in \mathbb{C}$ para todo $x \in \{0,1\}^n$ e

$$\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1. \tag{6}$$

A nomenclatura para qubits se estende para os registradores: os estados $|x\rangle$ com $x \in \{0,1\}^n$ são os *estados básicos*, o qubit $|\phi\rangle$ é dito uma *superposição* de estados básicos e o coeficiente complexo α_x é chamado de *amplitude* do estado básico $|x\rangle$ para todo $x \in \{0,1\}^n$.

Será conveniente expressarmos o estado (5) como

$$|\phi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle, \tag{7}$$

onde estamos substituindo as cadeias de caracteres de $\{0,1\}^n$ pelos valores numéricos que essas cadeias representam, se interpretadas como representação binária de números. Por exemplo, para $n = 2$, temos

$$\begin{aligned} |\phi\rangle &= \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \\ &= \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|3\rangle. \end{aligned}$$

Continuando a estender a notação de qubits para registradores, a representação na base B_{2^n} do registrador quântico dado por (7) é

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix} = |\phi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle.$$

A seguinte questão surge naturalmente: dado um registrador $|\phi\rangle$ com n qubits cujos qubits, de menos para mais significativos, são $|\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{n-1}\rangle$, qual é o estado quântico do registrador $|\phi\rangle$? A resposta é: $|\phi\rangle = |\phi_{n-1}\rangle \otimes |\phi_{n-2}\rangle \otimes \cdots \otimes |\phi_0\rangle$, onde $\otimes$ denota o produto tensorial, que definimos a seguir.

Sejam

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1q} \\ \vdots & \ddots & \vdots \\ b_{p1} & \cdots & b_{pq} \end{pmatrix}$$

matrizes. O produto tensorial de A e B, denotado por $A \otimes B$, é definido como

$$A \otimes B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}. \tag{8}$$

Assim, um registrador $|\phi\rangle$ cujos qubits são $|\phi_1\rangle$ e $|\phi_0\rangle$, com $|\phi_1\rangle := \alpha_0|0\rangle + \alpha_1|1\rangle$ e $|\phi_0\rangle := \beta_0|0\rangle + \beta_1|1\rangle$, está no estado

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_0\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

e, portanto,

$$\begin{aligned} |\phi\rangle &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle \\ &= \alpha_0\beta_0|0\rangle + \alpha_0\beta_1|1\rangle + \alpha_1\beta_0|2\rangle + \alpha_1\beta_1|3\rangle. \end{aligned} \tag{9}$$

A medição de um registrador quântico funciona de modo semelhante à medição de qubits: se medirmos um registrador quântico $|\phi\rangle$ dado por (7), obtemos o estado básico $|x\rangle$ com probabilidade $|\alpha_x|^2$ e, imediatamente após a medição, o estado do registrador será $|x\rangle$. Ou

seja, a superposição que existia anteriormente foi irreversivelmente perdida.

Não é necessário, porém, medirmos todos os qubits do registrador: pode-se medir qubits individuais ou grupos de qubits. Por exemplo, se medirmos apenas o qubit $|\phi_1\rangle$ do registrador $|\phi\rangle$ descrito acima na equação (9), existem duas possibilidades de resposta:

- O valor observado é $|0\rangle$. Esse evento ocorre com probabilidade $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 = |\alpha_0|^2$. Neste caso, o estado do registrador $|\phi\rangle$, imediatamente após a medição, será
$$|\phi'\rangle = \frac{\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle}{|\alpha_0|^2},$$
ou seja, projetou-se o estado $|\phi\rangle$ no subespaço gerado por $|00\rangle$ e $|01\rangle$, normalizando-se o resultado para obtermos um vetor unitário.
- O valor observado é $|1\rangle$. Esse evento ocorre com probabilidade $|\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = |\alpha_1|^2$. Neste caso, o estado do registrador $|\phi\rangle$, imediatamente após a medição, será
$$|\phi'\rangle = \frac{\alpha_1\beta_0|10\rangle + \alpha_1\beta_1|01\rangle}{|\alpha_1|^2},$$
ou seja, projetou-se o estado $|\phi\rangle$ no subespaço gerado por $|10\rangle$ e $|11\rangle$, normalizando-se o resultado para obtermos um vetor unitário.

Para o caso geral, suponha que seu registrador quântico com n qubits está no estado dado pela equação (5) e que você está medindo o qubit $|\phi_j\rangle$, onde o qubit menos significativo é $|\phi_0\rangle$ e o mais significativo é $|\phi_{n-1}\rangle$. Para cada cadeia de caracteres $x \in \{0,1\}^n$, escreva $x = x_{n-1}\cdots x_0$, com $x_k \in \{0,1\}$ para todo k. Existem duas possibilidades para o resultado da medição de $|\phi_j\rangle$:

- O valor observado é $|0\rangle$. A probabilidade de ocorrência desse evento é
$$p_0 := \sum \big\{|\alpha_x|^2 \colon x \in \{0,1\}^n \text{ e } x_j = 0\big\}.$$

Neste caso, o estado do registrador, imediatamente após a medição, será

$$|\phi'\rangle = \frac{\sum \{\alpha_x |x\rangle \colon x \in \{0,1\}^n \text{ e } x_j = 0\}}{p_0},$$

onde p_0 é simplesmente um fator de normalização.

- O valor observado é $|1\rangle$. A probabilidade de ocorrência desse evento é

$$p_1 := \sum \{|\alpha_x|^2 \colon x \in \{0,1\}^n \text{ e } x_j = 1\}.$$

Neste caso, o estado do registrador, imediatamente após a medição, será

$$|\phi'\rangle = \frac{\sum \{\alpha_x |x\rangle \colon x \in \{0,1\}^n \text{ e } x_j = 1\}}{p_1},$$

onde p_1 é simplesmente um fator de normalização.

O mecanismo de medição de um número arbitrário de qubits de um registrador é análogo.

2.3. **Reversibilidade.** Falemos agora de portas quânticas operando sobre mais de um qubit. Uma *porta quântica* sobre n qubits é uma função bijetora de $\mathcal{V}_{2^n}$ para $\mathcal{V}_{2^n}$, onde $\mathcal{V}_{2^n}$ é o conjunto de vetores unitários de $\mathcal{H}_{2^n}$. Em outras palavras, uma porta quântica é uma matriz unitária em $\mathcal{H}_{2^n}$.

Uma conseqüência disso é que toda porta quântica é reversível, isto é, existe uma bijeção entre o domínio e a imagem da função correspondente. Por exemplo, suponha que temos uma porta quântica U e um registrador $|\phi\rangle$ com dimensões compatíveis. Se aplicarmos U a $|\phi\rangle$ para obtermos $|\phi'\rangle := U|\phi\rangle$, então podemos obter o estado original $|\phi\rangle$ a partir de $|\phi'\rangle$ através da aplicação da porta quântica U^* (claramente U^* é unitária), pois $U^*|\phi'\rangle = U^*U|\phi\rangle = I|\phi\rangle = |\phi\rangle$. Em outras palavras, a aplicação de U não causa "perda de informação".

Esse não é o caso, por exemplo, da porta lógica $\vee$, o "ou" lógico do modelo clássico: suponha que temos dois bits clássicos a e b e que aplicamos a porta $\vee$ nesses bits, obtendo $c := a \vee b$. Se tivermos $c = 1$, não temos como obter os valores de a e b, pois podia valer que $a = 1$ e $b = 0$, ou que $a = 0$ e $b = 1$, ou ainda, que $a = 1$ e $b = 1$. Dizemos, por esse motivo, que a porta $\vee$ não é reversível.

Não é difícil, porém, construirmos uma "versão" da porta "ou" que seja reversível. Considere a função $f : \{0,1\}^3 \longrightarrow \{0,1\}^3$ dada por $f(x,y,z) := \big(x, y, z \oplus (x \vee y)\big)$, onde $\oplus$ denota a operação lógica "ou exclusivo". Em outras palavras, a aplicação da função f muda o valor do bit z se, e somente se, $x \vee y = 1$. Da imagem da f, é trivial obtermos os valores originais de x, y e z, pois x e y fazem parte dos valores que saem da porta e, com eles e o terceiro valor de saída, podemos recuperar z. É evidente que f é uma bijeção, de modo que f é reversível. A única diferença é que estamos armazenando informações a mais, o suficiente para sermos capazes de obter x e y (e z) a partir de $f(x,y,z)$.

Assim sendo, existe uma matriz unitária U_f que "implementa" a função f. Dado um registrador $|\phi\rangle := |x\rangle \otimes |y\rangle \otimes |z\rangle$, onde $|x\rangle, |y\rangle$ e $|z\rangle$ são qubits, a porta quântica U_f transforma o estado $|\phi\rangle$ no estado $|\phi'\rangle = |x\rangle \otimes |y\rangle \otimes \big|z \oplus (x \vee y)\big\rangle$. Será mais conveniente usarmos a seguinte notação: dado um registrador $|\phi\rangle := |x,y,z\rangle$, a aplicação de U_f a $|\phi\rangle$ leva o estado deste registrador a $|\phi'\rangle = \big|x, y, z \oplus (x \vee y)\big\rangle$. Veja que estamos simplesmente separando os qubits individuais por vírgulas. Na verdade, podemos utilizar essa notação para separar grupos arbitrários de qubits num registrador, quando isso for conveniente.

O "truque" de carregar informações a mais nas aplicações de portas lógicas pode ser utilizado para transformar qualquer porta lógica do modelo clássico numa porta reversível e que, portanto, pode ser implementada por uma matriz unitária no modelo quântico.

Na verdade, Bennett [Ben73] mostrou que qualquer circuito (no modelo clássico) pode ser convertido em reversível, ou seja, num circuito cujas portas são todas reversíveis, e mostrou que isso pode ser feito com um aumento no máximo polinomial no tamanho do circuito, isto é, no número de portas utilizadas. Isso implica, como veremos a seguir, que todo algoritmo polinomial no modelo clássico pode ser implementado por um algoritmo polinomial no modelo quântico.

2.4. **Circuitos e algoritmos quânticos.** A notação para circuitos apresentada anteriormente se estende facilmente para circuitos operando sobre múltiplos qubits. Por exemplo, a figura 4 mostra um circuito operando sobre 3 qubits e com uma única porta, dada pela matriz U_f implementando a versão reversível da operação lógica "ou".

De acordo com nossa especificação de U_f, temos $|x'\rangle = |x\rangle$, $|y'\rangle = |y\rangle$ e $|z'\rangle = \big|z \oplus (x \vee y)\big\rangle$.

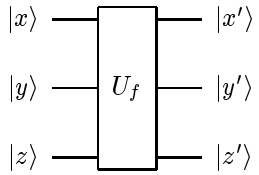

FIGURA 4. Circuito com porta "ou" reversível.

Seja $V_f \in \mathbb{C}^{2\times 2}$ uma matriz unitária. Então a notação utilizada no circuito da figura 5 indica que o operador V_f deve ser aplicado ao qubit $|y\rangle$ se, e somente se, $|x\rangle = |1\rangle$. Em outras palavras, o circuito da figura 5 é equivalente ao circuito da figura 6, onde

$$V_f' := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & v_{11} & v_{12} \\ 0 & 0 & v_{21} & v_{22} \end{pmatrix} \qquad \text{e} \qquad V_f := \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}.$$

A porta indicada no circuito da figura 5 é chamada *porta V_f controlada por $|x\rangle$*.

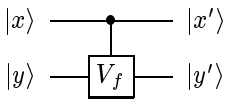

FIGURA 5. Circuito com porta V_f controlada por $|x\rangle$.

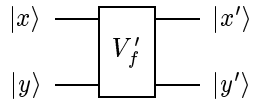

FIGURA 6. Circuito equivalente ao da figura 5.

Para fazermos a análise do consumo de tempo de um algoritmo quântico, vamos nos basear em circuitos quânticos. Algoritmos quânticos devem ser expressos utilizando-se circuitos acíclicos. Estamos

interessados em circuitos de tamanho polinomial no tamanho da entrada, onde o tamanho do circuito é simplesmente o número de portas quânticas utilizadas.

Ademais, cada uma das portas do circuito construído deve operar sobre, no máximo, um número previamente fixo de qubits. Esclarecendo melhor, fixe um inteiro k. Para todo n, o circuito construído para resolver uma instância de tamanho n deve utilizar portas quânticas que operam, no máximo, sobre k qubits. Essa exigência é razoável, já que computações geralmente são realizadas localmente, isto é, a cada passo uma quantidade limitada de informações é processada.

Além disso, o circuito deve poder ser construído por um algoritmo polinomial. Em outras palavras, deve existir um algoritmo polinomial que, ao receber qualquer instância I de um dado problema, constrói o circuito que resolve o problema para a instância I. Essa exigência impede que o circuito construído contenha informações "difíceis de calcular" codificadas em sua estrutura: se o algoritmo de construção do circuito não precisasse ser limitado polinomialmente, então tal algoritmo poderia calcular, digamos em tempo exponencial, a solução da instância em questão e codificar isso no circuito, que poderia ter até tamanho constante.

Nesse contexto, um algoritmo quântico é dito polinomial se, para toda instância do problema, existe um circuito quântico construtível em tempo polinomial e utilizando portas operando sobre, no máximo, um número fixo de qubits, que resolve a instância do problema.

2.5. **O problema de Deutsch.** Vamos apresentar um algoritmo quântico para ver os conceitos apresentados em funcionamento.

Dizemos que uma função f é dada como uma *caixa preta* se só podemos obter informações acerca de f através de sua aplicação a elementos de seu domínio. O problema de Deutsch [Deu85] consiste no seguinte. Seja $f : \{0,1\} \longrightarrow \{0,1\}$ uma função dada como uma caixa preta. Determine se $f(0) = f(1)$ ou se $f(0) \neq f(1)$. Em outras palavras, determine se f é constante ou balanceada.

Para se resolver o problema no modelo clássico, são necessárias duas aplicações de f: é preciso usar a caixa preta de f duas vezes, para as entradas 0 e 1. Já no modelo quântico, este problema pode ser resolvido utilizando-se apenas uma chamada à caixa preta. Vamos mostrar um algoritmo quântico, devido a Cleve, Ekert, Macchiavello

e Mosca [CEMM98], que resolve o problema no modelo quântico com uma única chamada à caixa preta.

Seja U_f a transformação unitária de dimensão 4 que leva $|x, y\rangle$ a $\big|x, y \oplus f(x)\big\rangle$. No modelo quântico, U_f é a nossa caixa preta.

O circuito que resolve o problema está descrito na figura 7. Vamos detalhar melhor o funcionamento do algoritmo.

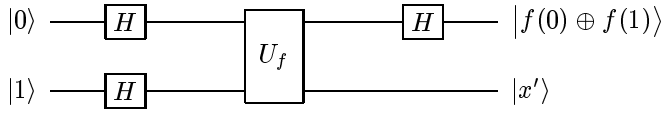

FIGURA 7. Circuito para o problema de Deutsch.

Vamos usar um registrador $|\phi_0\rangle$ de 2 qubits. Inicialmente, tomamos $|\phi_0\rangle := |0, 1\rangle$.

Primeiro aplicamos a transformação de Hadamard aos 2 qubits do registrador, obtendo

$$\begin{aligned} |\phi_1\rangle &:= \big(H|0\rangle\big) \otimes \big(H|1\rangle\big) = \frac{1}{2}\Big[\Big(|0\rangle + |1\rangle\Big) \otimes \Big(|0\rangle - |1\rangle\Big)\Big] \\ &= \frac{1}{2}\Big[|0\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big] + \frac{1}{2}\Big[|1\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big]. \end{aligned}$$

Neste ponto a caixa preta U_f é aplicada a $|\phi_1\rangle$ para obtermos $|\phi_2\rangle$:

$$\begin{aligned} |\phi_2\rangle := U_f|\phi_1\rangle &= \frac{1}{2}\left\{U_f\Big[|0\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big]\right\} \\ &\quad + \frac{1}{2}\left\{U_f\Big[|1\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big]\right\}. \end{aligned} \tag{10}$$

Vamos escrever $|\phi_2\rangle$ de outra maneira. Queremos mostrar que

$$U_f\Big[|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big] = (-1)^{f(x)}\Big[|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big] \tag{11}$$

para $x \in \{0, 1\}$. Temos

$$\begin{aligned} |\psi\rangle &:= U_f\Big[|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big] = U_f\Big[|x, 0\rangle - |x, 1\rangle\Big] \\ &= \big|x, f(x)\big\rangle - \big|x, 1 \oplus f(x)\big\rangle. \end{aligned}$$

- Se $f(x) = 0$, então

$$\begin{aligned} |\psi\rangle &= |x,0\rangle - |x,1\rangle = |x\rangle \otimes \Big(|0\rangle - |1\rangle\Big) \\ &= (-1)^{f(x)}\Big[|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big]. \end{aligned}$$

- Se $f(x) = 1$, então

$$\begin{aligned} |\psi\rangle &= |x,1\rangle - |x,0\rangle = |x\rangle \otimes \Big(|1\rangle - |0\rangle\Big) \\ &= (-1)^{f(x)}\Big[|x\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big]. \end{aligned}$$

Provamos então a equação (11), de modo que,

$$\begin{aligned} |\phi_2\rangle &= \frac{1}{2}\Big\{(-1)^{f(0)}\Big[|0\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big]\Big\} \\ &\qquad + \frac{1}{2}\Big\{(-1)^{f(1)}\Big[|1\rangle \otimes \Big(|0\rangle - |1\rangle\Big)\Big]\Big\} \\ &= \frac{1}{2}\Big[\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big) \otimes \Big(|0\rangle - |1\rangle\Big)\Big]. \end{aligned}$$

Vamos temporariamente omitir o segundo qubit de $|\phi_2\rangle$ no que segue:

$$\begin{aligned} |\phi_2\rangle &= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}(-1)^{f(0)}(-1)^{f(0)}|1\rangle\Big) \\ &= \frac{(-1)^{f(0)}}{2}\Big(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\Big). \end{aligned}$$

Voltando a levar em conta o segundo qubit de $|\phi_2\rangle$, concluímos que

$$\begin{aligned} |\phi_2\rangle &= (-1)^{f(0)}\Bigg\{\Big[\frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\Big)\Big] \\ &\qquad \otimes \Big[\frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)\Big]\Bigg\}. \end{aligned}$$

Agora podemos aplicar a transformação de Hadamard ao primeiro qubit de $|\phi_2\rangle$ para obter

$$|\phi_3\rangle := (-1)^{f(0)}\Bigg\{\Big[|f(0)\oplus f(1)\rangle\Big] \otimes \Big[\frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)\Big]\Bigg\}.$$

Uma medição do primeiro qubit de $|\phi_3\rangle$ fornece agora o valor de $f(0) \oplus f(1)$ e portanto o algoritmo descobre se f é constante ou balanceada através de uma única aplicação da caixa preta.

3. O algoritmo de fatoração de Shor

O algoritmo de Shor resolve o problema da fatoração de inteiros em primos e consome tempo polinomial no tamanho da entrada. Apresentamos a seguir os detalhes fundamentais do funcionamento deste algoritmo.

3.1. **Visão geral do algoritmo.** O algoritmo de Shor [Sho97] é um algoritmo quântico que, dado um inteiro n composto ímpar que não é potência de primo, devolve um fator (divisor não-trivial) de n com probabilidade limitada de erro.

As restrições para o valor de n não representam problema algum. De fato, é trivial encontrar um fator de um número par. Além disso, existe um algoritmo clássico eficiente que decide se $n = a^k$, para inteiros a e $k > 1$, e que devolve a e k neste caso. Veja o artigo de Bernstein [Ber98] para mais detalhes.

Ademais, podemos verificar em tempo polinomial se n é composto, utilizando o algoritmo AKS. Outra opção é executar testes probabilísticos de primalidade um número suficiente de vezes. Na prática, isso é mais eficiente, pois os testes probabilísticos são, em geral, mais simples e rápidos que o AKS. O teste de Miller-Rabin [Mil75, Mil76, Rab80, CLRS01] é uma ótima escolha para esta verificação, por ser de fácil implementação e ter complexidade de tempo $O\big(\lg^3 n\big)$, onde $\lg n$ denota o logaritmo de n na base 2. Outra vantagem desse teste é que a constante escondida pela notação assintótica é pequena.

Como n é produto de no máximo $\lceil \lg n \rceil$ inteiros, o algoritmo de Shor pode ser utilizado para resolver o problema da fatoração em tempo polinomial no tamanho da entrada.

O algoritmo de Shor baseia-se numa redução do problema da busca de um fator de n ao problema da busca do período de uma seqüência. Como a redução utiliza aleatorização, é possível que ela falhe, isto é, que nenhum fator de n seja encontrado. Porém, a probabilidade de ocorrência deste evento é limitada.

Na seção 3.2 apresentamos essa redução e uma delimitação superior para a probabilidade de falha. Na seção 3.3, mostramos um algoritmo quântico eficiente para a busca do período da seqüência gerada pela redução. Esse algoritmo utiliza a transformada quântica de Fourier, que pode ser implementada eficientemente, como mostramos na seção 3.4.

O algoritmo de busca de período apresentado na seção 3.3 pode ser facilmente generalizado para buscar eficientemente o período de qualquer seqüência. Mais formalmente, dado um oráculo U_f que computa uma função f de $\{0,\ldots,2^m-1\}$ em $\{0,\ldots,2^a-1\}$ com período r, a generalização do algoritmo faz uma única chamada a U_f e usa um circuito quântico de tamanho polinomial em m para descobrir r com probabilidade limitada de erro.

3.2. **Redução à busca do período.** Seja n um inteiro composto ímpar que não é potência de primo. Vamos mostrar como reduzir o problema de encontrar um fator de n ao problema de encontrar o período de uma função. Essa redução utiliza aleatorização, de modo que precisaremos limitar a probabilidade de falha do procedimento.

Algoritmo SHOR (n)

1 escolha um inteiro $1 < x < n$ aleatoriamente
2 se $\mathrm{mdc}(x,n) > 1$
3 então devolva $\mathrm{mdc}(x,n)$
4 seja r o período da função $f(a) := x^a \bmod n$
5 se r for ímpar ou $x^{r/2} \equiv -1 \pmod{n}$
6 então o procedimento falhou
7 devolva $\mathrm{mdc}(x^{r/2}+1, n)$

Note que o algoritmo de Shor utiliza um único passo quântico: o cálculo do período da função na linha 4.

Agora vamos mostrar que, se a redução devolve uma resposta, ela está correta. Depois vamos delimitar superiormente a probabilidade de falha deste procedimento, isto é, a probabilidade de o algoritmo terminar na linha 6.

Começamos observando que, se o algoritmo executa a linha 3, então o valor devolvido de fato é um fator de n.

Já se $\mathrm{mdc}(x, n) = 1$, então x está em $\mathbb{Z}_n^*$, o grupo multiplicativo módulo n, de modo que a função $f(a) = x^a \bmod n$ é periódica com período dado pela ordem de x, módulo n. Isto é, o período r é o tamanho do subgrupo de $\mathbb{Z}_n^*$ gerado por x. Equivalentemente, r é o menor inteiro positivo tal que $x^r \equiv 1 \pmod{n}$.

Suponha que r é par, de modo que $(x^{r/2}+1)(x^{r/2}-1) \equiv 0 \pmod{n}$, ou seja, n divide o produto $(x^{r/2}+1)(x^{r/2}-1)$. Se tivermos $x^{r/2} \not\equiv -1 \pmod{n}$, então n não divide $x^{r/2}+1$, o primeiro fator do produto. Como r é o menor inteiro positivo tal que $x^r \equiv 1 \pmod{n}$, temos também que $x^{r/2} \not\equiv 1 \pmod{n}$, de modo que n não divide $x^{r/2}-1$. Mas então os fatores de n devem estar separados entre $x^{r/2}+1$ e $x^{r/2}-1$. Logo, $\mathrm{mdc}(x^{r/2}+1, n)$ é um fator de n, como queremos.

Resta limitarmos a probabilidade de falha do procedimento, ou seja, dado um inteiro $1 < x < n$ escolhido aleatoriamente com probabilidade uniforme, precisamos limitar a probabilidade de que r, a ordem de x, módulo n, seja ímpar ou satisfaça $x^{r/2} \equiv -1 \pmod{n}$ se for par.

Suponha que a fatoração de n em primos é dada por $n = \prod_{i=1}^{m} p_i^{k_i}$, onde p_i é primo para todo i e $m > 1$, já que n não é potência de primo. Para cada i, seja $n_i := {p_i}^{k_i}$, de modo que $n = n_1 \cdots n_m$. Sejam $1 < x < n$ um inteiro,

$$r \text{ a ordem de } x, \text{ módulo } n,$$

e

$$r_i \text{ a ordem de } x, \text{ módulo } n_i,$$

para $i = 1, \ldots, m$. Pelo teorema chinês do resto, a equação $x^r \equiv 1 \pmod{n}$ é equivalente ao sistema

$$\begin{aligned} x^r &\equiv 1 \pmod{n_1} \\ x^r &\equiv 1 \pmod{n_2} \\ &\vdots \\ x^r &\equiv 1 \pmod{n_m}. \end{aligned} \tag{12}$$

Sabemos que r_i é o menor inteiro positivo tal que $x^{r_i} \equiv 1 \pmod{n_i}$. Ademais, temos $x^r \equiv 1 \pmod{n_i}$ se, e somente se, r é múltiplo de r_i. Como r é o menor inteiro positivo tal que $x^r \equiv 1 \pmod{n}$, segue que

$$r = \mathrm{mmc}(r_1, \ldots, r_m). \tag{13}$$

Seja

$$r_i = 2^{c_i} q_i, \text{ com } q_i \text{ ímpar}, \tag{14}$$

para $i = 1, \ldots, m$. É fácil ver que r é ímpar se, e somente se, r_i é ímpar para todo i, isto é, se, e somente se, $c_i = 0$ para todo i.

Suponha agora que r_i é par para algum i. Então r é par. Vamos descobrir em que condições temos $x^{r/2} \equiv -1 \pmod{n}$. Novamente, pelo teorema chinês do resto, a equação $x^{r/2} \equiv -1 \pmod{n}$ é equivalente ao sistema

$$\begin{aligned} x^{r/2} &\equiv -1 \pmod{n_1} \\ x^{r/2} &\equiv -1 \pmod{n_2} \\ &\vdots \\ x^{r/2} &\equiv -1 \pmod{n_m}. \end{aligned} \tag{15}$$

Suponha que existam $i, j \in \{1, \ldots, m\}$ tais que $c_i > c_j$. Então $r = 2r_j u$ para algum inteiro u, pela equação (13). Segue que $x^{r/2} \equiv x^{r_j u} \pmod{n_j}$. Mas então temos $x^{r/2} \equiv 1 \pmod{n_j}$, de modo que $x^{r/2} \not\equiv -1 \pmod{n}$. Portanto, para que r seja par e $x^{r/2} \equiv -1 \pmod{n}$, é necessário que $c_1 = c_2 = \cdots = c_m > 0$.

Estabelecemos assim que, para que o procedimento falhe, é preciso que $c_1 = \cdots = c_m$. Vamos limitar a probabilidade de ocorrência desse evento, dada a escolha aleatória de x.

Pelo teorema chinês do resto, existe uma bijeção entre $\mathbb{Z}_n$ e o produto cartesiano $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$:

$$\mathbb{Z}_n \ni x \leftrightarrow (x_1, \ldots, x_m) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}. \tag{16}$$

Assim, escolher um inteiro $0 \leq x < n$ aleatoriamente é equivalente a escolher, independentemente para cada $1 \leq i \leq m$, um inteiro $0 \leq x_i < n_i$. Vamos supor que $\mathrm{mdc}(x, n) = 1$, já que a redução não se aplica se $\mathrm{mdc}(x, n) > 1$. Então $x \in \mathbb{Z}_n^*$. É fácil ver que $x \in \mathbb{Z}_n^*$ se, e somente se, $x_i \in \mathbb{Z}_{n_i}^*$ para todo i. Portanto estamos escolhendo aleatoriamente um $x_i \in \mathbb{Z}_{n_i}^*$, independentemente, para cada $i = 1, \ldots, m$:

$$\mathbb{Z}_n^* \ni x \leftrightarrow (x_1, \ldots, x_m) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_m}^*, \tag{17}$$

Para cada $i = 1, \ldots, m$, o grupo $\mathbb{Z}_{n_i}^*$ é cíclico, pois $n_i = {p_i}^{k_i}$ com p_i primo. Seja g_i um gerador de $\mathbb{Z}_{n_i}^*$, para cada i. Seja

$$x_i = g_i^{l_i}, \text{ com } 0 \leq l_i < \phi(n_i), \text{ para } i = 1, \ldots, m, \tag{18}$$

onde $\phi(n_i) := \left|\mathbb{Z}^*_{n_i}\right|$ é a função totiente de Euler. Estamos então escolhendo aleatoriamente um $0 \leq l_i < \phi(n_i)$ para cada i, independente e uniformemente:

$$\mathbb{Z}^*_n \ni x \leftrightarrow (g_1^{l_1}, \ldots, g_m^{l_m}) \in \mathbb{Z}^*_{n_1} \times \cdots \times \mathbb{Z}^*_{n_m}, \tag{19}$$

Para $i = 1, \ldots, m$, seja

$$\phi(n_i) = 2^{d_i} s_i, \text{ com } s_i \text{ ímpar},$$

e lembre-se que

$$r_i = 2^{c_i} q_i \text{ é a ordem de } x_i, \text{ módulo } n_i, \text{ com } q_i \text{ ímpar}.$$

Como $\phi(n_i) = \phi\left(p_i^{k_i}\right) = p_i^{k_i - 1}(p_i - 1)$ e p_i é ímpar, então $d_i > 0$.

Pelo teorema de Lagrange, a ordem do subgrupo de $\mathbb{Z}^*_{n_i}$ gerado por x divide a ordem do grupo $\mathbb{Z}^*_{n_i}$. Em outras palavras, r_i divide $\phi(n_i)$, e portanto $c_i \leq d_i$. Sabemos que r_i é o menor inteiro positivo tal que $g_i^{l_i r_i} \equiv 1 \pmod{n_i}$ e que $l_i r_i = 2^{c_i} q_i l_i$ é múltiplo de $\phi(n_i) = 2^{d_i} s_i$. Se l_i é ímpar, então devemos ter $c_i = d_i$, pois $q_i l_i$ é ímpar. Já se l_i é par, então necessariamente teremos $c_i < d_i$: se $c_i = d_i$, então $r_i/2$ também é inteiro e $l_i r_i/2$ também é múltiplo de $\phi(n_i)$, um absurdo. Portanto, a probabilidade de que $c_i = c$, para qualquer c, é limitada por $1/2$, já que $0 \leq l_i < \phi(n_i)$ e $\phi(n_i)$ é par.

Concluímos então que a probabilidade de falha dessa redução, ou, na verdade, a probabilidade de que $c_1 = \cdots = c_m$ é, no máximo, $1 - 1/2^{m-1} \leq 1/2$, pois $m > 1$ e a escolha de cada c_i é independente de todas as outras.

3.3. **Busca do período.** Seja n um inteiro composto ímpar que não é potência de primo e seja $1 < x < n$ um inteiro relativamente primo a n. Vamos apresentar um algoritmo quântico que descobre, com probabilidade limitada de erro, a ordem de x, módulo n, que é o período da seqüência

$$\langle x^0 \bmod n, x^1 \bmod n, x^2 \bmod n, \ldots \rangle. \tag{20}$$

Seja $\beta := \lfloor \lg n \rfloor + 1$ o número de bits da representação binária de n e seja $q := 2^l$ a única potência de 2 tal que $n^2 \leq q < 2n^2$. Vamos precisar de um registrador $|\phi\rangle$ com $l + \beta$ qubits. Os l primeiros qubits formam o primeiro sub-registrador. Os β qubits restantes farão parte do segundo sub-registrador. Todos os qubits do registrador $|\phi\rangle$ devem ser inicializados com $|0\rangle$.

Após a aplicação da transformação de Hadamard a cada um dos qubits do primeiro sub-registrador, o estado do registrador $|\phi\rangle$ será

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle. \tag{21}$$

Seja U_f a transformação unitária que, para todo $0 \leq a < q$, leva um estado básico $|a, 0\rangle$, ao estado $|a, x^a \bmod n\rangle$. É fácil pensar num algoritmo clássico para a exponenciação modular que consome $O(\beta^3)$ operações sobre bits. Então, para todo n, existe um circuito com $O(\beta^3)$ portas, cada uma operando sobre no máximo um número fixo de qubits, que efetua a transformação U_f. Em outras palavras, U_f pode ser implementada eficientemente (veja o artigo de Shor [Sho97] para mais detalhes).

Aplicando a transformação U_f ao registrador $|\phi\rangle$, obtemos o estado

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \bmod n\rangle. \tag{22}$$

Medindo o estado do segundo sub-registrador de $|\phi\rangle$, obtemos algum $x^b \bmod n$, onde $0 \leq b < q$. Com isso, o estado do registrador $|\phi\rangle$ colapsa para uma superposição dos estados básicos de (22) cujos β qubits menos significativos representam $x^b \bmod n$.

Seja r a ordem de x, módulo n. Então os valores de $0 \leq a < q$ tais que $x^a \equiv x^b \pmod{n}$ são da forma $a_0 + jr$, com $0 \leq a_0 < r$, já que a seqüência (20) é periódica com período r. A medição do segundo sub-registrador em (22) selecionará os seguintes valores de a, no primeiro sub-registrador: $a_0, a_0+r, a_0+2r, \ldots, a_0+(A-1)r$, onde $A := \lceil q/r \rceil$. O estado do registrador $|\phi\rangle$ será então

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |a_0 + jr, x^b \bmod n\rangle.$$

De agora em diante, vamos ignorar o segundo sub-registrador. Então o estado de $|\phi\rangle$ será

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |a_0 + jr\rangle. \tag{23}$$

Note que os estados básicos de $|\phi\rangle$ que podem ser obtidos numa medição estão uniformemente espaçados a partir de a_0, com espaço r.

Seja M_q a transformação unitária dada por

$$M_q : |x\rangle \longrightarrow \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} \exp(2\pi i x y/q)|y\rangle. \tag{24}$$

Vamos mostrar, na seção 3.4, que esta transformação, conhecida como matriz de Vandermonde, pode ser implementada eficientemente por um circuito quântico. A aplicação de M_q ao registrador $|\phi\rangle$, dado por (23), gera o estado

$$\begin{aligned} |\phi\rangle &= \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} \left[\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} \exp\left\{2\pi i(a_0 + jr)y/q\right\}|y\rangle \right] \\ &= \frac{1}{\sqrt{qA}} \sum_{y=0}^{q-1} \left[\exp\{2\pi i a_0 y/q\} \sum_{j=0}^{A-1} \exp\{2\pi i j r y/q\}|y\rangle \right]. \end{aligned}$$

Então a amplitude de um estado básico $|y\rangle$ é

$$\frac{1}{\sqrt{qA}} \exp\{2\pi i a_0 y/q\} \sum_{j=0}^{A-1} \exp\{2\pi i j r y/q\}, \tag{25}$$

de modo que a probabilidade de obtenção de $|y\rangle$ numa medição de $|\phi\rangle$ é

$$p_y := \frac{1}{qA} \left| \sum_{j=0}^{A-1} \exp\{2\pi i j r y/q\} \right|^2. \tag{26}$$

Aqui vamos apenas analisar o caso em que r é uma potência de 2, de modo que $A = q/r$. Os demais casos seguem a mesma idéia porém são mais técnicos.

Suponha que y não é múltiplo de A. Então ry/q não é inteiro, de modo que $\exp\{2\pi i r y/q\} \neq 1$. Pela fórmula da soma de uma

progressão geométrica, temos

$$\begin{aligned}\sum_{j=0}^{A-1} \exp\{2\pi ijry/q\} &= \sum_{j=0}^{A-1} \big(\exp\{2\pi iry/q\}\big)^j \\ &= \frac{\big(\exp\{2\pi iry/q\}\big)^A - 1}{\exp\{2\pi iry/q\} - 1} \\ &= \frac{\exp\{2\pi iy\} - 1}{\exp\{2\pi iry/q\} - 1} \;=\; 0,\end{aligned}$$

pois $A = q/r$.

Suponha agora que y é um múltiplo de A. Então ry/q é inteiro, de modo que $\exp\{2\pi ijry/q\} = 1$ para todo $0 \le j < A$. Então

$$\sum_{j=0}^{A-1} \exp\{2\pi ijry/q\} \;=\; A.$$

Concluímos que a probabilidade de obtenção de $|y\rangle$ na medição do registrador $|\phi\rangle$ no estado (25) é

$$p_y \;=\; \begin{cases} 1/r, & \text{se } y \text{ é múltiplo de } q/r \\ 0, & \text{caso contrário.}\end{cases} \tag{27}$$

Assim, uma medição de $|\phi\rangle$ nos fornece um valor $y = cq/r$, com $0 \le c < r$ escolhido equiprovavelmente. Teremos então um y satisfazendo $y/q = c/r$, onde c e q são conhecidos. Se $\mathrm{mdc}(c, r) = 1$, então basta obter a fração irredutível correspondente a y/q para chegarmos ao período r. A probabilidade de obtenção de um $0 \le c < r$ com $\mathrm{mdc}(c, r) = 1$ é $\phi(r)/r$. Pode-se provar [HW54] que existe uma constante δ tal que $\phi(r)/r > \delta/\log\log r$. Assim, a probabilidade de falha deste procedimento é, no máximo, $1 - \delta/\log\log r$.

Se repetirmos o procedimento acima $z := \log\log r/\delta$ vezes, a probabilidade de falha passará a ser $(1 - 1/z)^z \le 1/e$, de modo que a probabilidade de sucesso é, no mínimo, $1 - 1/e$, uma constante. Portanto, obtemos o período r com probabilidade limitada inferiormente por uma constante.

3.4. **A transformada quântica de Fourier.** Vamos ver agora que a transformação unitária M_q, dada por (24), pode ser implementada eficientemente sempre que q for uma potência de 2. Ou seja, para todo $q = 2^m$, vamos mostrar que existe um circuito de tamanho

polinomial em m, utilizando apenas portas quânticas que operam sobre um número fixo de qubits, cuja aplicação a um registrador com m qubits é equivalente à aplicação da matriz M_q.

Primeiro vamos escrever o estado

$$\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} \exp(2\pi i x y/q)|y\rangle \tag{28}$$

de uma forma mais conveniente. Considere $q := 2^m$, com m um inteiro positivo. Denotaremos por $(x_{m-1} \cdots x_0)_2$ a representação binária de $0 \leq x < 2^m$, ou seja, $x = \sum_{j=0}^{m-1} x_j 2^j$, com $x_j \in \{0,1\}$ para todo j. Além disso, utilize $(0.\, x_1 \cdots x_p)_2$ para denotar a representação binária de $0 \leq x < 1$, isto é, $x = \sum_{j=1}^{p} x_j 2^{-j}$, com $x_j \in \{0,1\}$ para todo j.

Então o estado (28) pode ser fatorado como

$$\begin{aligned} &\left[\frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\left\{2\pi i (0.\, x_0)_2\right\}|1\rangle\Big)\right] \otimes \\ &\quad \left[\frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\left\{2\pi i (0.\, x_1 x_0)_2\right\}|1\rangle\Big)\right] \otimes \cdots \otimes \\ &\qquad \left[\frac{1}{\sqrt{2}}\Big(|0\rangle + \exp\left\{2\pi i (0.\, x_{m-1} \cdots x_0)_2\right\}|1\rangle\Big)\right]. \end{aligned} \tag{29}$$

Para mostrar que o estado quântico (28) é o mesmo que o estado (29), vamos mostrar que, para todo estado básico $|y_{m-1} \cdots y_0\rangle$, temos

$$\begin{aligned} &\exp\{2\pi i x y/2^m\}|y_{m-1} \cdots y_0\rangle = \\ &\quad \Big(\exp\left\{2\pi i (0.\, x_0)_2 y_{m-1}\right\}|y_{m-1}\rangle\Big) \otimes \\ &\quad \Big(\exp\left\{2\pi i (0.\, x_1 x_0)_2 y_{m-2}\right\}|y_{m-2}\rangle\Big) \otimes \cdots \otimes \\ &\qquad \Big(\exp\left\{2\pi i (0.\, x_{m-1} \cdots x_0)_2 y_0\right\}|y_0\rangle\Big), \end{aligned} \tag{30}$$

onde o lado direito da equação (30) mostra como se forma o estado básico $|y_{m-1}\cdots y_0\rangle$ em (29). Será então suficiente mostrar que

$$\begin{aligned}
&\exp\{2\pi i xy/2^m\} \\
&\quad = \exp\left\{2\pi i (0.\,x_0)_2 y_{m-1}\right\}\ \exp\left\{2\pi i (0.\,x_1x_0)_2 y_{m-2}\right\}\cdots \\
&\qquad\qquad \exp\left\{2\pi i (0.\,x_{m-1}\cdots x_0)_2 y_0\right\} \\
&\quad = \exp\Big\{2\pi i\big[(0.\,x_0)_2 y_{m-1} + (0.\,x_1x_0)_2 y_{m-2} + \cdots + \\
&\qquad\qquad (0.\,x_{m-1}\cdots x_0)_2 y_0\big]\Big\}.
\end{aligned} \tag{31}$$

Observe que

$$\frac{yx}{2^m} = \frac{1}{2^m}\sum_{k=0}^{m-1}\left[y_k 2^k \sum_{k=0}^{m-1} x_k 2^k\right] = \sum_{j=0}^{m-1}\left[y_j \sum_{k=0}^{m-1} x_k 2^{k-m+j}\right]. \tag{32}$$

Na equação (31), o termo $xy/2^m$ aparece multiplicando $2\pi i$. Então apenas a parte fracionária de $xy/2^m$ é relevante: se $xy/2^m = u + r$, com $0 \le r < 1$ e $u \in \mathbb{Z}$, então $\exp(2\pi i xy/2^m) = \exp(2\pi i r)$. Na equação (32), para $k \ge m - j$, o valor 2^{k-m+j} é inteiro, de modo que podemos reescrever (32) como

$$\frac{yx}{2^m} = \sum_{j=0}^{m-1}\left[y_j u_j + y_j \sum_{k=0}^{m-j-1} x_k 2^{k-m+j}\right], \tag{33}$$

onde u_j é um inteiro. É fácil verificar agora que

$$\sum_{k=0}^{m-j-1} x_k 2^{k-m+j} = (0.\,x_{m-j-1}\cdots x_0)_2.$$

Mas então

$$\begin{aligned}
xy/2^m = u + y_{m-1}(0.\,x_0)_2 + y_{m-2}(0.\,x_1x_0)_2 \\
+ \cdots + y_0(0.\,x_{m-1}\cdots x_0)_2,
\end{aligned} \tag{34}$$

onde u é um inteiro. A equação (31) segue imediatamente da equação (34), de modo que fica provado que o estado (28) pode ser fatorado como (29).

Considere o circuito quântico apresentado na figura 8, referente ao caso em que $m = 3$.

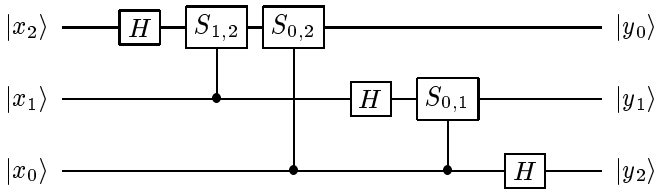

FIGURA 8. Circuito para a transformada quântica de Fourier, com $m = 3$.

Nesta figura, a matriz $S_{j,k}$, para $j < k$ é definida por

$$S_{j,k} = \begin{bmatrix} 1 & 0 \\ 0 & \exp\{2\pi i/2^{k-j+1}\} \end{bmatrix}. \tag{35}$$

É muito fácil ver como este circuito se estende para qualquer m. Para cada qubit $|x_k\rangle$, aplicamos a matriz de Hadamard, seguida de k portas $S_{j,k}$, onde $S_{j,k}$ é controlada por $|x_j\rangle$ para todo $0 \leq j < k$.

Para ver que esse circuito de fato calcula a transformada quântica de Fourier, vamos analisar sua operação sobre o qubit $|x_2\rangle$ na figura 8. Após a aplicação da matriz de Hadamard, o estado deste qubit será $|0\rangle + \exp\left\{2\pi i(0.\,x_2)_2\right\}|1\rangle$. Note que estamos desprezando o fator de normalização $1/\sqrt{2}$, para maior clareza. Depois da aplicação da porta $S_{1,2}$, o estado passa a ser $|0\rangle + \exp\left\{2\pi i(0.\,x_2x_1)_2\right\}|1\rangle$. Por fim, aplicando agora a porta $S_{0,2}$, teremos $|0\rangle + \exp\left\{2\pi i(0.\,x_2x_1x_0)_2\right\}|1\rangle$. Mas isso é justamente $|y_0\rangle$, conforme a equação (29). Repetindo esses cálculos com os outros qubits, obteremos os estados desejados, de acordo com a equação (29).

Note que os qubits da saída deste circuito estão na ordem inversa. É óbvio que isso não representa qualquer problema para nós.

Observe também que o circuito utiliza $m(m+1)/2$ portas, o que é quadrático em m. Assim, a transformada quântica de Fourier pode ser implementada por um circuito de tamanho limitado por $\Theta(m^2)$.

4. MÁQUINAS DE TURING

Agora mudamos de assunto, nos voltando à teoria de complexidade computacional. Os resultados dessa área são usualmente apresentados por meio do mais tradicional modelo de computação — a máquina

de Turing (MT), que nada mais é que um computador bastante rudimentar com memória infinita.

Vamos apresentar três variantes desse modelo: a máquina de Turing determinística, a não-determinística e a probabilística. Depois disso, apresentamos a segunda formalização do modelo quântico de computação, a máquina de Turing quântica, fazendo um paralelo com o modelo clássico de computação. Como observamos na introdução, essa segunda formalização é equivalente à primeira. A demonstração desse fato não é trivial e não será mostrada nesse texto.

4.1. **Máquina de Turing determinística.** Uma máquina de Turing determinística (MTD) é composta por uma central de controle, uma cabeça de leitura e uma fita dividida em células. Essa fita tem um final à esquerda e contém infinitas células à direita.

Cada célula da fita armazena um símbolo pertencente a um conjunto finito Σ. O conjunto Σ é chamado de *alfabeto* da máquina e contém, entre outros, dois símbolos especiais: o símbolo $\sqcup$, chamado de *branco*, e o símbolo $\triangleright$, que fica armazenado o tempo todo na célula mais à esquerda da fita.

A cabeça de leitura da máquina é um apontador móvel para uma determinada célula da fita. O conteúdo dessa célula pode ser lido e alterado pela máquina.

A cada instante, a central de controle da máquina está em um dos estados de um conjunto finito Q de estados. No instante inicial, a máquina começa em um estado particular de Q, chamado de estado *inicial* e denotado por s. Existe ainda um conjunto especial de estados $H \subseteq Q$, chamados de estados *finais*.

Uma MTD funciona da seguinte maneira. Ela recebe como entrada uma cadeia de caracteres em $\left(\Sigma \setminus \{\sqcup, \triangleright\}\right)^*$. Inicialmente a cabeça de leitura aponta para a célula mais à esquerda da fita, e a partir da célula seguinte está armazenada a entrada da máquina, seguida por brancos. A máquina efetua uma seqüência de passos até terminar a execução. Se q é o estado corrente da máquina e q está em H, então ela termina a execução. Do contrário, ela realiza três ações, determinadas pelo par (q, σ), onde σ é o símbolo de Σ contido na célula que está sob a cabeça de leitura.

A primeira ação consiste na alteração do estado da máquina de q para um estado q' em Q. A segunda ação é a escrita de um símbolo σ'

na célula que está sob a cabeça de leitura. A terceira ação consiste no deslocamento da cabeça de leitura, que pode se mover uma posição para a esquerda, uma posição para a direita ou pode continuar apontando para a mesma célula.

A cabeça de leitura da fita sempre desloca-se para a direita quando atinge a célula mais à esquerda e nunca altera o conteúdo dessa posição da fita. Por conveniência, assume-se que a máquina não pode escrever o símbolo $\triangleright$ em qualquer posição da fita que não seja a célula mais à esquerda.

A cadeia de caracteres escrita na fita quando a máquina termina a execução, ignorando-se o símbolo $\triangleright$ e os brancos à direita, é a saída da máquina para a entrada em questão.

Formalmente, define-se uma máquina de Turing determinística como uma quíntupla $M := (Q, \Sigma, \delta, s, H)$, onde Q é o conjunto de estados, Σ é o alfabeto de símbolos, δ é uma função de $(Q \setminus H) \times \Sigma$ em $Q \times \Sigma \times \{\leftarrow, \downarrow, \rightarrow\}$, $s \in Q$ é o estado inicial e $H \subseteq Q$ é o conjunto de estados finais. O conjunto $\{\leftarrow, \downarrow, \rightarrow\}$ descreve os possíveis movimentos da cabeça de leitura da máquina.

A função δ, chamada usualmente de *função de transição*, descreve um passo arbitrário da máquina e satisfaz as restrições mencionadas acima. Suponha que a máquina esteja num estado q em $Q \setminus H$ e que sob a cabeça de leitura esteja o símbolo σ. Se $\delta(q, \sigma) = (q', \sigma', d)$, o próximo estado será q', o símbolo σ' será escrito no lugar de σ e a cabeça de leitura de M moverá de acordo com d.

A *configuração atual* de M é uma tripla $(w_1, q, w_2) \in \Sigma^* \times Q \times \Sigma^*$, onde w_1 é a palavra que aparece na fita à esquerda da cabeça de leitura, q é o estado atual e w_2 é a palavra à direita da cabeça de leitura ignorando-se brancos à direita. A cabeça de leitura aponta para a posição que contém o último símbolo de w_1. A configuração inicial é a tripla $(\triangleright, s, x)$, onde x é a entrada para a máquina.

Dizemos que uma configuração (w_1, q, w_2) *produz em k passos* uma configuração (w_1', q', w_2'), denotado por $(w_1, q, w_2) \vdash_M^k (w_1', q', w_2')$, se a máquina sai da primeira configuração e vai para a segunda em exatos k passos.

4.2. **Máquinas de Turing não-determinísticas.** A máquina de Turing não-determinística (MTND) é uma generalização da máquina

de Turing determinística. Essa máquina tem um papel fundamental na teoria de complexidade pois está na base da definição da classe **NP**, conforme será mostrado posteriormente.

A maior parte das definições e idéias envolvidas na descrição das MTDs também se aplica às MTNDs. A diferença entre a MTND e a MTD está na função de transição e na maneira como as transições são feitas a cada passo. Nas máquinas determinísticas, existe uma única transição possível a partir de uma dupla (q, σ), onde q é um estado não-final e σ é um símbolo em Σ. Já nas máquinas não-determinísticas, pode existir mais de uma transição válida a partir de uma dupla (q, σ). Em cada passo da MTND, uma transição válida é escolhida arbitrariamente e é executada.

O número de transições válidas a partir de uma dupla (q, σ) é limitado superiormente por $3 \times |\Sigma| \times |Q|$. Logo, o número de configurações que podem ser produzidas a partir de cada configuração também é limitado superiormente por $3 \times |\Sigma| \times |Q|$. A transição numa MTND é portanto uma *relação* e não necessariamente uma função.

Formalmente, uma máquina de Turing não-determinística é uma quíntupla $M := (Q, \Sigma, \Delta, s, H)$, onde Q é o conjunto de estados, Σ é o alfabeto de símbolos, Δ é uma relação de $(Q \setminus H) \times \Sigma$ em $Q \times \Sigma \times \{\leftarrow, \downarrow, \rightarrow\}$, $s \in Q$ é o estado inicial e $H \subseteq Q$ é o conjunto de estados finais.

É evidente que as MTDs são casos particulares de MTNDs em que Δ é uma função, já que toda função é uma relação.

Uma transição (q', σ', d) em $\Delta(q, \sigma)$, onde $q \in Q$ e $\sigma \in \Sigma$, é interpretada como antes. Assim, q' será o próximo estado da máquina, σ' deve ser escrito no lugar de σ e d indicará o deslocamento da cabeça de leitura. Tal transição será válida somente se $(q', \sigma', d) \in \Delta(q, \sigma)$. A definição de configuração é igual à que usamos na definição da máquina de Turing determinística. Para MTNDs, dizemos que uma configuração (w_1, q, w_2) produz a configuração (w_1', q', w_2') em k passos se, estando a máquina na primeira configuração, após k passos válidos ela pode estar na segunda a partir de uma seqüência de transições válidas.

A existência de várias transições possíveis para cada par (q, σ) numa MTND permite a ocorrência de computações distintas para uma mesma entrada. Como as MTNDs podem ter várias computações válidas possíveis para uma mesma entrada, elas podem produzir

saídas diferentes para uma mesma entrada. Comentaremos mais sobre isso quando falarmos das linguagens decididas por uma máquina de Turing.

4.3. **Máquina de Turing probabilística.** Uma máquina de Turing probabilística (MTP) é uma MTND $M = (Q, \Sigma, \Delta, s, H)$ que funciona de maneira diferente.

A cada passo, em vez de uma transição ser escolhida arbitrariamente dentre todas as transições aplicáveis, escolhe-se uma com probabilidade uniforme. Assim, pode-se falar na probabilidade da MTP produzir, numa computação para uma certa entrada, uma saída específica. Todas as definições dadas para as MTNDs aplicam-se de maneira natural a uma MTP. Observe que uma MTD é uma MTP em que, a cada passo, há apenas uma transição aplicável.

Uma MTP corresponde à formalização do conceito de um computador acoplado a um gerador de números aleatórios.

É possível descrever o funcionamento de uma MTP postergando as escolhas aleatórias para o final. Ou seja, pode-se calcular a probabilidade de se estar em uma configuração específica a cada passo e só ao final fazer um único sorteio para determinar a configuração em que a máquina termina.

4.4. **Máquina de Turing quântica.** A definição de uma máquina de Turing quântica (MTQ) assemelha-se à de uma MTP. Uma máquina de Turing quântica é uma MTND $M = (Q, \Sigma, \Delta, s, H)$ com a relação Δ substituída por uma função

$$\alpha : Q \times \Sigma \times Q \times \Sigma \times \{\leftarrow, \downarrow, \rightarrow\} \longrightarrow \mathbb{C}$$

tal que, para cada (q, σ) em $Q \times \Sigma$, vale que

$$\sum_{(q', \sigma', d) \in T} |\alpha(q, \sigma, q', \sigma', d)|^2 = 1,$$

onde $T := Q \times \Sigma \times \{\leftarrow, \downarrow, \rightarrow\}$.

Cada número $\alpha(q_1, \sigma_1, q, \sigma, d)$ é chamado de *amplitude*. Note que α determina uma distribuição de probabilidade nas possíveis transições aplicáveis a um par (q_1, σ_1).

Define-se *superposição de configurações* como uma combinação linear de configurações, onde o coeficiente de uma configuração c é um número complexo α_c e $\sum_c |\alpha_c|^2 = 1$, sendo que o somatório é sobre

todas as configurações c que estão na superposição. O coeficiente α_c é a *amplitude* da configuração c.

A primeira diferença no funcionamento de uma MTQ frente às máquinas anteriores é que esta, a cada instante, encontra-se numa superposição de configurações. Para que a transição de uma MTQ esteja bem definida, é preciso que a máquina satisfaça a seguinte propriedade: se, numa superposição obtida depois de k passos a partir da configuração inicial, há uma configuração com amplitude não-nula num estado final, então todas as configurações com amplitude não-nula nessa superposição estão num estado final.

Se todas as configurações da MTQ com amplitude não-nula forem finais, a MTQ termina a execução. Caso contrário, ela efetua uma transição, que consiste no seguinte. Digamos que $\psi := \sum_{j=1}^{t} \alpha_j c_j$ é a superposição corrente, onde $\sum_{j=1}^{t} |\alpha_j|^2 = 1$ e $\alpha_j \neq 0$ para todo j. Para cada j, seja C_j o conjunto das configurações que podem ser obtidas de c_j em um passo por meio de uma transição cuja amplitude é não-nula. Para cada c em C_j, seja α_c^j a amplitude correspondente à transição de c_j para c. Então, temos que a superposição resultante da transição é $\psi' = \sum_{j=1}^{t} \alpha_j \sum_{c \in C_j} \alpha_c^j c$.

Quando uma mesma configuração c aparece em mais de um conjunto C_j e $\left|\sum_{j:c \in C_j} \alpha_j \alpha_c^j\right|^2 \neq \sum_{j:c \in C_j} \left|\alpha_j \alpha_c^j\right|^2$, dizemos que houve *interferência*. A interferência é *negativa* se o lado esquerdo é menor que o direito e *positiva* caso contrário. O fenômeno de interferência é o principal responsável pela diferença entre uma MTQ e uma MTP.

A segunda diferença no funcionamento de uma MTQ frente às máquinas anteriores é que, ao final de sua execução, a MTQ efetua o que chamamos de *medição*. Digamos que $\psi := \sum_{j=1}^{t} \alpha_j c_j$ é a superposição final da máquina, com $\sum_{j=1}^{t} |\alpha_j|^2 = 1$ e $\alpha_j \neq 0$ para todo j. Uma medição consiste na escolha aleatória de uma configuração $c = c_j$ com probabilidade $|\alpha_j|^2$, e na transição da superposição ψ para a superposição $\psi' := c$, ou seja, para a superposição em que apenas a configuração c tem amplitude não-nula (mais exatamente, c tem amplitude 1 em ψ'). A saída da MTQ é o que está escrito na fita após a medição. Assim como uma MTP, uma MTQ pode produzir diferentes saídas para uma mesma entrada, cada uma com uma probabilidade.

Chamamos de *paralelismo quântico* à capacidade da MTQ estar numa superposição de configurações, e, num passo, efetuar transições múltiplas, envolvendo diversas configurações. Potencialmente é possível explorar o fenômeno de interferência bem como o paralelismo quântico para se obter algoritmos quânticos eficientes para problemas considerados difíceis no modelo clássico de computação.

5. Teoria clássica de complexidade

Apresentamos alguns resultados e definições do modelo clássico de computação com o intuito de estabelecer um paralelo durante a apresentação dos correspondentes quânticos desses resultados e definições.

5.1. **Principais classes de complexidade.** Vamos falar agora sobre as classes de complexidade mais importantes no modelo clássico de computação, baseados na abordagem apresentada por Papadimitriou [Pap94].

Para isso, definiremos o significado de tempo e espaço consumido nas máquinas do modelo clássico. Em seguida, falaremos das linguagens decididas por cada uma dessas máquinas e finalmente definiremos as principais classes do modelo clássico de computação.

Tempo consumido pelas máquinas de Turing. Durante a descrição da MTD, foi definido que $(w_1, q, w_2) \vdash_M^k (w_1', q', w_2')$ se a máquina M sai da primeira configuração e vai para a segunda em exatos k passos. Se (w_1, q, w_2) é a configuração inicial de M e q' é um de seus estados finais, então dizemos que k é o tempo consumido por M para a entrada w_2.

Dada uma MTD M, se existe um polinômio $p(n) : \mathbb{N} \longrightarrow \mathbb{N}$ tal que, para qualquer entrada x, o tempo consumido por M é limitado superiormente por $p(|x|)$, onde $|x|$ denota o comprimento da palavra x, então dizemos que M é *polinomialmente limitada.*

Se M é uma MTND, o maior tempo consumido em uma computação válida de M para uma entrada determinada é considerado o tempo consumido por M para essa entrada. Analogamente, M é polinomialmente limitada se existe um polinômio $p(n) : \mathbb{N} \longrightarrow \mathbb{N}$ tal que, para qualquer entrada x, o tempo consumido por M em qualquer computação válida é limitado superiormente por $p(|x|)$.

Por fim, se M é uma MTP, valem as mesmas definições usadas para as MTNDs. Vale destacar que no caso das MTPs também aplica-se o conceito de tempo *esperado* de computação, que formalmente é a esperança do tempo consumido por uma computação de M para uma dada entrada x.

Espaço consumido pelas máquinas de Turing. Existem também classes de problemas que são definidas em função do espaço consumido pelas máquinas de Turing que os resolvem. Da mesma forma que no estudo do consumo de tempo, temos interesse especial nos problemas que podem ser resolvidos por máquinas de Turing que consomem espaço polinomial no tamanho das entradas.

As diferenças entre as máquinas de Turing de naturezas distintas não são muito grandes no consumo de espaço. Mais adiante, ao enunciarmos um resultado de Savitch [Sav70], ficará mais claro o porquê dessa afirmação.

Dizemos que o *espaço consumido* por uma MT é a maior quantidade de células distintas usadas pela máquina para realizar uma computação válida para uma determinada entrada. No caso das MTDs, é o número de células usadas na única computação possível. Já para MTNDs e MTPs, é o maior número de células utilizadas em uma computação válida.

Como em toda MT a cabeça de leitura só pode se deslocar de uma célula a cada passo, claramente o espaço consumido em uma computação é limitado superiormente pelo número de passos utilizados pela máquina.

Dizemos que uma MT *consome espaço polinomial* se o espaço consumido pela MT é limitado superiormente por um polinômio definido em função do tamanho da entrada.

Linguagens e máquinas de Turing. Ao definir as máquinas de Turing, utilizamos como parâmetro um alfabeto Σ. Esse alfabeto é um conjunto que contém todos os símbolos reconhecidos pela máquina de Turing em questão. Logo, uma entrada válida para a máquina deve ser uma palavra composta apenas por símbolos de Σ.

Um conjunto de palavras cujas letras pertencem a um alfabeto Σ é chamado de *linguagem*. Algumas linguagens possuem propriedades

que as tornam especialmente interessantes. Geralmente estamos interessados em verificar se uma determinada palavra pertence ou não a uma particular linguagem L.

Máquinas de Turing que devolvem respostas binárias podem ser usadas para efetuar essa tarefa. Uma das respostas indica que a palavra fornecida como entrada pertence à linguagem L (aceitação) e a outra que a palavra não pertence (rejeição).

Em muitos casos, porém, deseja-se fornecer uma entrada para uma máquina de Turing para a obtenção de uma saída que não pode ser descrita apenas com duas respostas distintas. Por exemplo, uma máquina que recebe a representação binária de um número inteiro x qualquer como entrada e devolve como resposta a representação binária do número $x + 2$ claramente deve ser capaz de devolver mais do que duas respostas distintas. Nesse caso, dizemos que estamos lidando com um *problema*, e não com uma linguagem. Rigorosamente, existem diferenças entre problemas e linguagens, mas como podemos transformar uma coisa na outra de maneira razoavelmente simples, vamos falar de problemas e linguagens de maneira indistinta. Mostraremos agora as relações entre as linguagens e as máquinas de Turing determinísticas, não-determinísticas e probabilísticas.

Se existe uma MTD M que, dada uma palavra x, responde se x pertence ou não a uma determinada linguagem L, então dizemos que M *decide* a linguagem L. As respostas são devolvidas por M através dos símbolos 0 e 1, que indicam rejeição e aceitação, respectivamente, da palavra x. Esses símbolos devem aparecer sozinhos na fita da máquina após a mesma ter parado, na segunda célula da esquerda para a direita.

No caso das MTNDs, já vimos que podem existir várias computações e várias saídas possíveis para uma máquina e uma entrada. Assim, dizemos que uma MTND M decide uma linguagem L se toda palavra $x \in L$ é aceita por M em alguma de suas computações, e se toda palavra $x \notin L$ é rejeitada por M em todas as suas computações. Essa definição acaba mostrando a característica das MTNDs que faz com que elas pareçam ser mais eficientes computacionalmente e menos realistas do que as MTDs.

Por fim, a decisão de linguagens por MTPs têm um aspecto um pouco diferente das demais máquinas de Turing. Assim como as MTNDs, as MTPs também podem produzir respostas distintas

para uma mesma entrada. Porém, nas MTPs, atribuímos a cada computação válida (e conseqüentemente a cada possível resposta) uma determinada probabilidade. A decisão de uma linguagem por uma MTP envolve as probabilidades de obtenção das respostas.

Em alguns casos estamos interessados em fixar uma probabilidade máxima para as rejeições incorretas, em outros para as aceitações incorretas e em outros para as duas simultaneamente. A decisão de linguagens em MTPs, portanto, não possui uma definição única como no caso das MTDs e das MTNDs. Logo, ao utilizar esse conceito mais adiante no texto, definiremos exatamente o significado adequado dentro do contexto.

As classes **P** *e* **PSPACE**. A partir do conceito de máquinas de Turing polinomialmente limitadas, vamos definir as linguagens *polinomialmente decidíveis*. Dizemos que uma linguagem é polinomialmente decidível se existe uma máquina de Turing determinística polinomialmente limitada que a decide.

A classe **P** (*polynomial-time*) é o conjunto de todas as linguagens polinomialmente decidíveis. Esta classe é extremamente importante, pois contém a maior parte dos problemas que podem ser resolvidos de maneira eficiente. Dizemos que um problema é resolvido de maneira eficiente se existe um algoritmo para resolvê-lo que consome tempo polinomial no tamanho da entrada. A classe **P** é fechada sob união, intersecção, concatenação e estrela de Kleene. Essas propriedades são importantes e suas provas são interessantes, mas serão omitidas nesse texto.

De maneira bastante parecida com a que definimos a classe **P**, podemos definir a classe **PSPACE** (*polynomial-space*). Vale ressaltar que, enquanto a primeira faz a classificação das linguagens em função do tempo consumido, a segunda o faz em função do espaço consumido. Dizemos que uma linguagem pertence à classe **PSPACE** se ela é decidida por uma máquina de Turing determinística que consome espaço polinomial no tamanho da entrada.

É fácil ver que $\mathbf{P} \subseteq \mathbf{PSPACE}$: como já observamos, toda MTD que consome tempo polinomial certamente consome espaço polinomial, já que, a cada passo, a cabeça de leitura da máquina só pode se mover de no máximo uma célula à direita. Por outro lado, o inverso não é verdade. É fácil imaginar uma MTD que consome tempo

superpolinomial mas espaço polinomial. Assim, é concebível (e até de se esperar) que existam linguagens em **PSPACE** que não estejam em **P**. Surpreendentemente, não se sabe até hoje se este é o caso ou não. Ou seja, não se sabe se **P** = **PSPACE**.

As classes **NP** *e* **coNP**. As classes **NP** e **coNP** podem ser descritas de maneira parecida com a que descrevemos a classe **P**. Conforme explicaremos adiante, essas classes são muito importantes no estudo da teoria de complexidade clássica.

Vamos definir **NP** (*nondeterministic polynomial-time*) e **coNP** em função das máquinas de Turing não-determinísticas polinomialmente limitadas. Dizemos que uma linguagem pertence à classe **NP** se ela pode ser decidida por uma máquina de Turing não-determinística polinomialmente limitada.

A classe das linguagens cujo complemento pertence a **NP** é denominada **coNP**, onde o complemento de uma linguagem L sob um alfabeto Σ é a linguagem $\Sigma^* \setminus L$. De maneira geral, o complemento de uma classe de complexidade arbitrária **C** é denotado por **coC** e definido como o conjunto das linguagens cujo complemento está em **C**.

Por exemplo, ao definir a classe **P**, também poderíamos ter definido a classe **coP**, seguindo a definição acima. Nesse caso, temos uma classe que é igual ao seu complemento. Dada uma linguagem L em **P** ou em **coP**, e uma máquina M polinomialmente limitada que a decide, basta trocar aceitação por rejeição e vice-versa na descrição de M para obter uma máquina polinomialmente limitada que decide o complemento de L.

As classes **NP** e **coNP** contêm vários problemas para os quais não se conhece algoritmo polinomial, e formam com a classe **P** a fronteira entre o que pode e o que não pode ser resolvido eficientemente no modelo clássico. Essas classes também são importantes porque contêm uma grande quantidade de problemas de interesse prático.

Claramente, toda linguagem que está em **P** também está em **NP** e em **coNP**, visto que uma MTD é uma MTND. Porém, não sabemos muito mais a respeito da relação entre essas três classes. A questão mais importante e conhecida é se **P** é igual a **NP**. Se isso for verdade, saberemos que muitos problemas para os quais hoje não se conhecem algoritmos exatos razoáveis terão uma solução polinomial. Porém, são poucos os que acreditam nessa hipótese.

NP $\subseteq$ **PSPACE**. Uma relação conhecida entre classes de complexidade é que **NP** $\subseteq$ **PSPACE**. Isso significa que toda linguagem decidida por uma MTND limitada polinomialmente pode ser decidida por uma MTD que consome espaço polinomial.

Vamos apresentar a prova de maneira razoavelmente informal, pois o que queremos mostrar é a idéia que está por trás da simulação de uma MTND por uma MTD.

Dada uma MTND M polinomialmente limitada que decide uma linguagem L, queremos mostrar que essa máquina pode ser simulada por uma MTD M' que consome espaço polinomial e decide a mesma linguagem L.

A diferença entre as máquinas M e M' é o não-determinismo. Sendo uma MTND, M requer apenas que uma de suas possíveis computações aceite uma palavra da linguagem L, e também requer que todas as computações rejeitem as palavras que não estão em L.

Logo, ao simular M, a máquina M' deve ser capaz de simular todas as computações possíveis de M para poder rejeitar uma palavra corretamente. A conclusão de que uma palavra está na linguagem pode ser rápida (basta encontrar a primeira computação que aceita a palavra de entrada), mas de qualquer forma em geral não é possível determinar a priori quantas simulações precisam ser feitas.

Assim, considerando o pior caso, é fácil ver que toda simulação de M por M' que consiste em testar cada uma das computações possíveis pode consumir tempo exponencial no tamanho da entrada. Porém, sabemos que M é polinomialmente limitada. Logo, todas as suas computações consomem tempo, e portanto espaço, polinomial no tamanho da entrada.

Assim, uma simulação de M por M' que testa cada computação possível consumindo espaço polinomial e que sempre consegue reaproveitar esse espaço nas próximas computações é suficiente para mostrar que **NP** está contida em **PSPACE**.

A construção da M' é razoavelmente simples. A idéia principal consiste numa espécie de busca em largura num grafo. Mais especificamente, M' simula todas as computações possíveis de M com t passos antes de simular qualquer computação com $t+1$ passos.

Para representar as computações, M' pode indexar as transições das computações com números. Esses números serão obtidos a partir de um contador, que será representado na base binária. Logo, mesmo

se o número de computações for exponencial, o espaço consumido por M' para armazenar tal contador será polinomial no tamanho da entrada.

A cada passo da simulação, M' incrementa seu contador e simula a computação de M referente a seu valor. O conteúdo da fita de M para cada computação pode ser guardado numa fita auxiliar durante a simulação, e antes da próxima computação essa fita é apagada. Dessa forma, é claro que o espaço usado para guardar as computações também será polinomial no tamanho da entrada.

Como toda transição de M pode ser simulada em tempo polinomial por M', a simulação pode ser feita consumindo espaço polinomial no tamanho da entrada. Assim, $\mathbf{NP} \subseteq \mathbf{PSPACE}$. Analogamente, mostra-se que $\mathbf{coNP} \subseteq \mathbf{PSPACE}$.

Dizemos que uma linguagem pertence à classe **NPSPACE** se ela é decidida por uma máquina de Turing não-determinística que consome espaço polinomial no tamanho da entrada. Uma simulação semelhante a essa foi proposta por Savitch [Sav70] para mostrar que $\mathbf{NPSPACE} = \mathbf{PSPACE}$.

As classes **RP** *e* **coRP**. As classes discutidas a seguir envolvem computações probabilísticas e são de fundamental importância tanto no modelo clássico como no modelo quântico.

Primeiro definimos a classe **RP** (*randomized polynomial-time*). Na literatura, essa classe é definida em função das *máquinas de Turing Monte-Carlo*. Infelizmente não há um consenso quanto a definição dessas máquinas (algumas fontes falam que elas devem ser limitadas polinomialmente, enquanto outras não estabelecem essa restrição). Logo, vamos fazer a definição da classe em função de suas propriedades principais.

Para que uma linguagem L pertença à classe **RP**, deve existir uma MTP M limitada polinomialmente satisfazendo o seguinte:

(1) Se uma palavra x dada na entrada não está na linguagem L, então a máquina M sempre rejeita a palavra x.
(2) Se uma palavra x dada na entrada está na linguagem L, então a máquina M aceita x com probabilidade pelo menos 0,5.

Essas duas propriedades caracterizam a máquina de Turing Monte-Carlo. Diz-se neste caso que M decide a linguagem L com probabilidade de aceitação 0,5.

O valor da probabilidade de aceitação na definição de **RP** não é muito importante, no sentido de que qualquer outro valor em $(0; 1]$ leva à mesma classe **RP**. Isso porque, de uma MTP limitada polinomialmente que decide uma linguagem L com probabilidade de aceitação p, para um valor p qualquer em $(0, 1]$, é possível obter uma MTP limitada polinomialmente que decide L com probabilidade de aceitação 0,5. De fato, se $p \geq 0{,}5$, não há nada a fazer. Se $p < 0{,}5$, executa-se k vezes, com $k = \lceil -1/\log p \rceil$, a máquina original e rejeita-se a palavra se pelo menos uma vez a máquina original a rejeitou. Do contrário, aceita-se a palavra. Esse procedimento aumenta a probabilidade de aceitação para pelo menos 0,5.

O uso da repetição da execução das máquinas de Turing Monte-Carlo é bastante útil, pois pode deixar a probabilidade de falsas rejeições arbitrariamente pequena. Por isso, esse recurso é bastante utilizado na prática, mesmo quando as probabilidades de rejeição incorreta são pequenas (menores que 0,5).

A classe **coRP**, das linguagens cujo complemento está em **RP**, pode também ser vista como a classe das linguagens L para as quais existe uma MTP M limitada polinomialmente com as seguintes propriedades:

(1) Se uma palavra x dada na entrada não está na linguagem L, então a máquina M rejeita x com probabilidade maior ou igual a 0,5.
(2) Se uma palavra x dada na entrada está na linguagem L, então a máquina M nunca rejeita a palavra x.

As definições deixam claro o caráter complementar das duas classes. Enquanto as linguagens que estão em **RP** admitem máquinas que fazem rejeições incorretas, as linguagens de **coRP** admitem máquinas que fazem aceitações incorretas.

A classe **RP** claramente está contida em **NP**. Basta notar que uma máquina de Turing Monte-Carlo para uma linguagem L é uma máquina de Turing não-determinística que decide L (existe pelo menos uma computação dessa máquina que aceita cada palavra que está em L e todas as computações rejeitam palavras que não estão em L). Um argumento análogo mostra que a classe **coRP** está contida na classe **coNP**.

Também é claro que **P** está contida nessas duas classes, pois uma MTD é um caso especial de uma máquina de Turing Monte-Carlo, onde as palavras sempre são aceitas e rejeitadas corretamente.

As classes **ZPP** *e* **BPP**. Na última seção, vimos classes de linguagens que são decididas por MTPs limitadas polinomialmente que podem ou aceitar ou rejeitar erroneamente uma determinada palavra.

Agora, vamos definir uma classe de linguagens que exige das máquinas que as respostas sejam corretas, mas que abre mão da certeza da polinomialidade na execução.

Para que uma linguagem L pertença à classe **ZPP** (*zero-error probability polynomial-time*), deve existir uma máquina de Turing probabilística M que sempre aceita palavras que pertencem a L e sempre rejeita palavras que não pertencem a L, e cujo tempo esperado de execução para qualquer entrada é polinomial.

Pela definição, podemos perceber que a classe **ZPP** é muito parecida com a classe **P**, diferindo apenas no fato de que as máquinas utilizadas podem consumir tempo superpolinomial em algumas computações.

Outra definição possível é a seguinte: **ZPP** é a classe das linguagens que pertencem tanto a **RP** como a **coRP**. Se uma linguagem está tanto em **RP** como em **coRP**, executa-se de maneira alternada cada uma das máquinas envolvidas até que uma delas obtenha uma resposta certamente correta. O número de passos desse algoritmo é indeterminado (não há sequer garantias de que ele pára em algum momento), mas a esperança do número de passos é um valor polinomial no tamanho da entrada, pois a probabilidade de obtenção de respostas erradas diminui exponencialmente a cada execução das máquinas.

Outra classe de complexidade importante, que também pode ser relacionada com as demais classes probabilísticas já citadas, é a classe **BPP** (*bounded-error probabilistic polynomial-time*), que contém as linguagens para as quais existem máquinas de Turing que devolvem respostas erradas (tanto rejeições como aceitações) com probabilidade estritamente menor que 0,5. Na verdade, qualquer delimitação da probabilidade no intervalo $(0; 0{,}5)$ resultaria na mesma classe. Porém, Papadimitriou [Pap94] mostrou que delimitações maiores ou iguais a 0,5 podem levar a uma classe diferente.

A definição dessa classe é simétrica, pois rejeição e aceitação são feitas corretamente na maioria absoluta das computações feitas por essas máquinas. Assim, utilizando um argumento análogo ao do resultado $\mathbf{P} = \mathbf{coP}$, obtemos que $\mathbf{BPP} = \mathbf{coBPP}$.

Além disso, é fácil ver que $\mathbf{RP} \subseteq \mathbf{BPP}$. Dadas uma linguagem L em $\mathbf{RP}$ e uma máquina M associada, basta executar M com a entrada desejada duas vezes para que a probabilidade de falsa rejeição seja de no máximo 0,25. Como a probabilidade de falsa aceitação é zero, as condições necessárias para que L pertença a $\mathbf{BPP}$ estão satisfeitas. O argumento que mostra que $\mathbf{coRP} \subseteq \mathbf{BPP}$ é análogo.

Por fim, vale destacar que não sabemos ainda se a classe $\mathbf{BPP}$ está contida na classe $\mathbf{NP}$.

6. Classes quânticas de complexidade

Vamos agora apresentar as duas principais classes quânticas de complexidade e demonstrar alguns resultados que as relacionam às classes clássicas.

6.1. **Tempo, espaço e linguagens no modelo quântico.**

Durante as discussões sobre o modelo clássico de computação, fizemos considerações sobre o consumo de tempo e de espaço pelas máquinas de Turing determinísticas, não-determinísticas e probabilísticas.

O tempo consumido por uma MTQ com entrada x é o número de passos que a máquina efetua até terminar a execução. Essa definição é consistente, porque exigimos que, quando uma configuração da superposição atinge um estado final, todas as demais configurações também o fazem.

O espaço consumido por uma MTQ M com entrada x é definido de maneira análoga ao espaço consumido por uma MTND. Dentre todas as configurações que durante a execução de M tiveram amplitude não-nula, seja c aquela com o maior número possível de células em que M escreveu algo. O número de células utilizadas em c é o espaço consumido por M com a entrada x.

No contexto de linguagens, estamos interessados em MTQs que, para cada entrada x, têm saída ou $x1$ ou $x0$ (MTQs devem ser reversíveis, por isso a resposta usualmente binária é precedida pela entrada).

Diz-se que uma MTQ M desse tipo decide de maneira exata uma linguagem L se, para todo x em L, a máquina M produz como saída $x1$, e, para todo x fora de L, a máquina M tem como saída $x0$.

Por fim, para um número p entre 0 e 1, diz-se que uma MTQ M decide L com probabilidade p se M, com entrada x em L, produz $x1$ com probabilidade pelo menos p e, com entrada x fora de L, produz $x0$ com probabilidade pelo menos p.

6.2. **As classes EQP e BQP.** As duas classes de complexidade que iremos introduzir aqui foram propostas por Bernstein e Vazirani [BV97].

A classe **EQP** é o conjunto das linguagens que são decididas de maneira exata por uma MTQ que consome tempo polinomial no tamanho da entrada. Essa classe corresponde à classe **P** do modelo clássico.

A classe **BQP** é o conjunto das linguagens para as quais existem máquinas de Turing quânticas que devolvem respostas erradas (tanto rejeições como aceitações) com probabilidade estritamente menor que 0,5. A classe correspondente no modelo clássico é **BPP**, e assim como no caso dela, a probabilidade de erro pode ser qualquer valor no intervalo $(0; 0{,}5)$.

A seguir, vamos mostrar algumas relações envolvendo essas classes e as classes tradicionais de complexidade.

6.3. **Relações envolvendo as classes quânticas.** Inicialmente, vamos mostrar que $\mathbf{P} \subseteq \mathbf{EQP}$ e que $\mathbf{BPP} \subseteq \mathbf{BQP}$, pois as demonstrações e as idéias envolvidas são mais simples. Em seguida, mostraremos que $\mathbf{BQP} \subseteq \mathbf{PSPACE}$. Seguem abaixo demonstrações breves das duas primeiras relações, apresentadas no artigo de Bernstein e Vazirani [BV97].

Teorema 6.1. $\mathbf{P} \subseteq \mathbf{EQP}$.

Demonstração. Seja L uma linguagem que pertence à classe **P**. É fácil ver que existe uma MTD limitada polinomialmente que, para cada entrada x, produz como saída $x1$ se $x \in L$ e $x0$ caso contrário. Para toda MTD polinomialmente limitada, existe uma MTD reversível equivalente, que também é limitada polinomialmente. Para obtê-la, modifica-se a máquina original de modo que cada um de seus estados só possa ser atingido por movimentos da cabeça de leitura em uma

única direção (as transições cujas triplas têm o mesmo estado devem fazer o mesmo deslocamento da cabeça de leitura da máquina).

Isso pode ser obtido duplicando-se os estados da máquina. Com isso, a função de transição torna-se bijetora quando a direção é ignorada, e pode-se, de uma configuração arbitrária da máquina, deduzir-se a configuração "anterior". Ou seja, a máquina é reversível. Além disso, o número de passos executados pela máquina até que ela pare é o mesmo da máquina original.

Mas se uma MTD é reversível, então essa máquina é uma MTQ onde cada superposição de configurações contém apenas uma configuração com amplitude não-nula.

Logo, existe uma MTQ limitada polinomialmente que, para cada entrada x, devolve $x1$ como resposta sempre que x está em L, e devolve $x0$ sempre que x está fora de L. Então, L é decidida de maneira exata por uma MTQ, e portanto pertence a **EQP**. Concluímos assim que $\mathbf{P} \subseteq \mathbf{EQP}$. □

A demonstração a seguir mostra como uma MTQ engloba naturalmente um gerador de números aleatórios.

Teorema 6.2. $\mathbf{BPP} \subseteq \mathbf{BQP}$.

Demonstração. Sejam L uma linguagem em **BPP** e M uma MTP para L dada pela definição de **BPP**. Para mostrar que $L \in \mathbf{BQP}$, vamos descrever uma MTQ que simula M com um aumento apenas polinomial no consumo de tempo.

Para simplificar, vamos assumir que M tem k opções de transição em cada um de seus passos, para algum k fixo. Se numa simulação de M por uma MTQ M' conseguimos, a cada passo, escolher aleatoriamente um símbolo do alfabeto $\{1, \ldots, k\}$, então M pode ser simulada por M'. Cada símbolo do alfabeto é usado para definir qual transição se aplica no passo que está sendo simulado de M. Esses símbolos podem ser gerados da seguinte maneira.

A cada passo, se o estado atual não é final, a cabeça de leitura desloca-se para uma determinada posição da fita e escreve-se o símbolo j com amplitude $1/\sqrt{k}$, para $j = 1, \ldots, k$, em uma única transição, que representa um sorteio aleatório. Feito isso, o conteúdo da célula é lido, a cabeça retorna para a posição original da fita e a transição representada pelo símbolo lido é realizada.

A célula utilizada no sorteio deve ser tal que não haja interferência no resto da fita. Como M é polinomialmente limitada, existem números c e e tais que qualquer computação de M não consome mais do que cn^e passos. Assim, basta inserir os caracteres dos sorteios seqüencialmente, começando na (cn^{e+1})-ésima célula da fita.

Como cada transição do passo de sorteio tem amplitude $1/\sqrt{k}$, então cada configuração no final terá amplitude $(1/\sqrt{k})^t$, onde t é o número de passos de M, lembrando que não ocorrerá interferência entre as configurações geradas. Logo, com a medição, a probabilidade de obtenção de um determinado resultado em M' será igual à da obtenção do mesmo resultado em M.

Como M pode ser simulada por M', a linguagem L pode ser decidida com a mesma probabilidade $p > 0{,}5$ por uma MTQ limitada polinomialmente. Logo, $L \in \mathbf{BQP}$, e portanto temos que $\mathbf{BPP} \subseteq \mathbf{BQP}$. □

As duas provas mostradas acima servem para reforçar idéias que devem ser intuitivas após a leitura das definições envolvidas. Nosso objetivo agora é mostrar uma relação menos imediata e mais importante, que envolve o consumo de espaço na simulação de uma MTQ por uma MTD.

Quando falamos em simulação de uma MTQ por uma MTD, estamos nos referindo a uma simulação onde queremos saber a probabilidade de cada saída possível ser produzida. Não conhecemos nenhuma simulação de uma MTQ por uma MTD que consuma tempo polinomial no tempo consumido pela MTQ, porém o teorema abaixo mostra que é possível fazer uma simulação utilizando espaço polinomial no espaço consumido pela MTQ. Nesse texto, mostraremos apenas as linhas gerais da prova desse teorema.

Teorema 6.3. $\mathbf{BQP} \subseteq \mathbf{PSPACE}$.

Demonstração. Seja $L \in \mathbf{BQP}$ e $M := (Q, \Sigma, \alpha, s, H)$ uma MTQ polinomialmente limitada que decide L com probabilidade p maior que 0,5. Vamos descrever uma MTD M' que decide L em espaço polinomial no tempo consumido por M. A máquina M' calcula, para cada entrada x, a probabilidade p_x de M aceitar x (ou seja, de M produzir $x1$ como saída). No final, M' aceita ou rejeita x de acordo com o valor de p_x.

Dizemos que uma configuração (w_1, q, w_2) tem *tamanho* k se a cadeia de caracteres $w_1 w_2$ tem k caracteres. Dadas duas configurações c_1 e c_2, denotamos por $\alpha(c_1, c_2)$ o valor da amplitude correspondente à transição de M que leva c_1 a c_2. Se não há nenhuma transição que leva c_1 a c_2, então $\alpha(c_1, c_2) = 0$. Seja $c_0 := (\triangleright, s, x)$ a configuração inicial.

A máquina M', para cada inteiro t a partir de $|x|$, simula t passos de M e calcula a probabilidade p_x de M produzir, em t passos, a saída $x1$. Essa probabilidade é dada por

$$p_x = \left| \sum_{c_1,\ldots,c_t} \prod_i \alpha(c_{i-1}, c_i) \right|^2,$$

onde o somatório é sobre todas as configurações $c_1, \ldots, c_t$ de tamanho no máximo t onde $c_t = (\triangleright, h, x_1)$, para algum h em H. Note que o número de termos no somatório é no máximo $T = t|\Sigma|^{2t}|Q|$.

A máquina M' deve portanto calcular o somatório descrito acima. O primeiro problema que aparece é a incapacidade de M' fazer cálculos com números irracionais. MTDs só podem armazenar valores inteiros limitados, enquanto que cada $\alpha(c_{i-1}, c_i)$ pode nem mesmo ser racional. Logo, a simulação será uma aproximação, que deverá ter um erro tolerável. Por fim, vale destacar que cada um dos no máximo T termos do somatório terá t fatores.

Se cada $\alpha(c_{i-1}, c_i)$ for representado com m bits tanto na parte inteira como na parte imaginária dos números, onde m é grande comparado a $\log T$, o erro será pequeno (da ordem de 2^{-m}). Assim, a primeira dificuldade já foi eliminada.

O que M' deve fazer é computar cada termo do somatório e guardar a soma dos termos. Como cada operação de adição usa pouco espaço auxiliar (ou seja, consome espaço polinomial em m) e só é necessário guardar a cada operação a soma atual, podemos garantir que o espaço necessário para efetuar o somatório é polinomial. No caso dos produtos, os mesmos comentários se aplicam.

O que resta considerar agora é a obtenção de cada $\alpha(c_{i-1}, c_i)$. É fácil, em tempo polinomial nos comprimentos de c_{i-1} e c_i, detectar se c_i pode ou não ser derivada de c_{i-1} em um passo. Se não pode, então $\alpha(c_{i-1}, c_i) = 0$. Se pode, então ao mesmo tempo pode-se determinar a transição $(q_1, \sigma_1, q, \sigma, d)$ em $Q \times \Sigma \times Q \times \Sigma \times \{\leftarrow, \downarrow, \rightarrow\}$ que,

quando aplicada a c_{i-1}, leva a c_i. A máquina M' então aciona uma "subrotina" que recebe um número m e devolve, em espaço polinomial em m, o valor de $\alpha(q_1, \sigma_1, q, \sigma, d)$ com precisão 2^{-m}. O valor devolvido pela subrotina é a aproximação desejada de $\alpha(c_{i-1}, c_i)$. Mostrar que de fato há uma MTD que efetua tal subrotina e consome espaço polinomial em m não é tarefa trivial e envolve uma série de etapas. Omitiremos essa prova nesse texto.

É importante notar que o número de tais subrotinas não depende da entrada, mas apenas da máquina M. Assim M' está bem definida, desde que existam MTDs que executem tais subrotinas. Mais do que isso, cada etapa que M' executa consome espaço polinomial (assumindo que as subrotinas consumam espaço polinomial), portanto de fato $\mathbf{BQP} \subseteq \mathbf{PSPACE}$. □

Dos resultados acima, temos que $\mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$. Assim, não é possível mostrar que $\mathbf{BPP} \neq \mathbf{BQP}$ sem resolver a clássica questão de se $\mathbf{P}$ está propriamente contido em $\mathbf{PSPACE}$ ou não. Por outro lado, no mesmo artigo, Bernstein e Vazirani [BV97] mostram um oráculo em relação ao qual $\mathbf{BPP} \neq \mathbf{BQP}$. Outros resultados nessa linha, porém direcionados à questão "$\mathbf{P} \neq \mathbf{NP}$?", foram provados por Bennet *et al.* [BBBV97]. Por exemplo, Bennet *et al.* mostraram que, em relação a um oráculo, $\mathbf{NP} \not\subseteq \mathbf{BQP}$.

7. Comentários finais

A área de computação quântica aborda um tema que de início se mostra atraente e amedrontador ao mesmo tempo. O seu aspecto amedrontador vem principalmente do seu caráter multidisciplinar, que em particular implicou na adoção de uma notação que mistura a tradicionalmente usada em mecânica quântica com a empregada em teoria da computação e em álgebra booleana.

Acrescentado a isso, há o fato de que, por ser ainda uma área jovem, são raros os bons textos introdutórios disponíveis (textos didáticos, objetivos e auto-contidos). Esperamos que esse nosso texto sirva como uma introdução ao assunto, senão didática, pelo menos objetiva e, dentro do possível, auto-contida.

Shor [Sho03], num artigo onde ele discute possíveis razões para a escassez de resultados algorítmicos novos nessa área, comenta que é curioso que os dois resultados algorítmicos mais famosos da área

digam respeito a problemas ligados à teoria dos números: o problema da fatoração e o problema do cálculo do logaritmo discreto. Ele levanta a possibilidade de que o modelo quântico seja mais adequado para resolver problemas dessa natureza.

Para ver o texto completo que resultou dessa iniciação científica, visite a página `http://www.ime.usp.br/~magal/quantum/`.

Referências

[AKS02a] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. Preprint. `http://www.cse.iitk.ac.in/news/primality.pdf`, 2002.

[AKS02b] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. Revised. `http://www.cse.iitk.ac.in/news/primality_v3.pdf`, 2002.

[BBBV97] C.H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

[Ben73] C.H. Bennett. Logical reversibility of computation. *IBM J. Res. Develop.*, 17:525–532, 1973.

[Ber98] D.J. Bernstein. Detecting perfect powers in essentially linear time. *Math. Comp.*, 67(223):1253–1283, 1998.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411–1473, 1997.

[CEMM98] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci.*, 454(1969):339–354, 1998.

[Chu33] A. Church. A set of postulates for the foundation of logic. *Annals of Mathematics*, 25:839–864, 1933.

[Chu36] A. Church. An unsolvable problem of elementary number theory. *Annals of Mathematics*, 58:345–363, 1936.

[CLRS01] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein. *Introduction to Algorithms*. MIT Press, Cambridge, MA, second edition, 2001.

[Cob65] A. Cobham. The intrinsic computational difficult of functions. In Y. Bar-Hillel, editor, *Logic, Methodology and Philosophy of Science*, pages 24–30. North-Holland, 1965.

[Coo71] S. Cook. The complexity of theorem proving procedures. In *Proc. 3rd ACM Symposium on Theory of Computing*, pages 151–158, 1971.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Roy. Soc. London Ser. A*, 400(1818):97–117, 1985.

[Deu89] D. Deutsch. Quantum computational networks. *Proc. Roy. Soc. London Ser. A*, 425(1868):73–90, 1989.

[Edm65] J. Edmonds. Paths, trees, and flowers. *Canadian Journal of Mathematics*, 17:449–467, 1965.

[EJ96] A. Ekert and R. Jozsa. Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.*, 68(3), 1996.

[Fey82] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6 & 7):467–488, 1982.

[Göd31] K. Gödel. On formally undecidable propositions of Principia Mathematica and related systems. *Monatshefte fur Math. und Physik*, 38:173–198, 1931.

[GJ79] M.R. Garey and D.S. Johnson. *Computers and Intractability: a Guide to the Theory of NP-Completeness*. Freeman, 1979.

[HW54] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford, at the Clarendon Press, 1954. 3rd ed.

[Joy] D.E. Joyce. Mathematical problems by professor David Hilbert. `http://aleph0.clarku.edu/~djoyce/hilbert/problems.html`.

[Kar72] R.M. Karp. Reducibility among combinatorial problems. In *Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972)*, pages 85–103. Plenum, New York, 1972.

[Kle36] S. Kleene. General recursive functions of natural numbers. *Mathematische Annalen*, 112:727–742, 1936.

[Kle52] S. Kleene. *Introduction to Metamathematics*. D. Van Nostrand, Princeton, NJ, 1952.

[Lev73] L.A. Levin. Universal sorting problems. *Problems of Information Transmission*, 9:265–266, 1973.

[Mil75] G.L. Miller. Riemann's hypothesis and tests for primality. In *Seventh Annual ACM Symposium on Theory of Computing (Albuquerque, N.M., 1975)*, pages 234–239. Assoc. Comput. Mach., New York, 1975.

[Mil76] G.L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. System Sci.*, 13(3):300–317, 1976. Working papers presented at the ACM-SIGACT Symposium on the Theory of Computing (Albuquerque, N.M., 1975).

[MM04] D.C. Marinescu and G.M. Marinescu. Lectures on quantum computing. `http://www.cs.ucf.edu/~dcm/Fall2003Class-QC/QCTextBookIndex.htm`, 2004.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, Cambridge, 1995.

[Pap94] C.H. Papadimitriou. *Computational Complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994.

[Pos36] E. Post. Finite combinatory process. *Journal of Symbolic Logic*, 1:103–105, 1936.

[Pre04] J. Preskill. Lecture notes for Physics 219/Computer Science 219. `http://www.theory.caltech.edu/people/preskill/ph229`, 2004.

[Rab80] M.O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12(1):128–138, 1980.

[RP00] E. Rieffel and W. Polak. Introduction to quantum computing. *ACM Computing Surveys*, 32(3):300–335, 2000.

[RSA78] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[Sav70] W.J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *Journal of Computer and System Sciences*, 4(2):177–192, 1970.

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124–134. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

[Sho97] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[Sho03] Peter W. Shor. Why haven't more quantum algorithms been found? *J. ACM*, 50(1):87–90, 2003.

[Tur36] A. Turing. On computable numbers with an application to the entscheidungsproblem. *Proc. London Math. Soc.*, 2:230–265, 1936.

[Tur37] A. Turing. Rectifications to 'on computable numbers...'. In *Proc. London Mathematical Society*, volume 4, pages 544–546, 1937.

Instituto de Matemática e Estatística, Universidade de São Paulo, Rua do Matão 1010, 05508–900 São Paulo, SP

Endereços Eletrônicos: {magal,cardonha,cris}@ime.usp.br

URL: http://www.ime.usp.br/~magal/quantum