

Quantum Finance: um tutorial de computação quântica aplicada ao mercado financeiro

Quantum Finance: a tutorial on quantum computing applied to the financial market

Askery Canabarro^{1,2}, Taysa M. Mendonça¹, Ranieri Nery¹, George Moreno¹,
Anton S. Albino³, Gleydson F. de Jesus³, Rafael Chaves^{1,4}

¹Universidade Federal do Rio Grande do Norte, Instituto Internacional de Física, 59078-970, Natal, RN, Brasil.

²Universidade Federal de Alagoas, Núcleo de Ciências Exatas, Grupo de Física da Matéria Condensada, 57072-970, Arapiraca, AL, Brasil.

³Latin American Quantum Computing Center/Senai Cimatec, 41650-010, Salvador, BA, Brasil.

⁴Universidade Federal do Rio Grande do Norte, Escola de Ciências e Tecnologia, 57078-970, Natal, RN, Brasil.

Recebido em 25 de março de 2022. Revisado em 08 de agosto de 2022. Aceito em 27 de setembro de 2022.

Antes restrita a uma área de fronteira da Física, a computação quântica é uma das áreas que mais tem crescido atualmente, justamente por suas aplicações tecnológicas em problemas de otimização, aprendizagem de máquina, segurança da informação e simulações. O objetivo deste artigo é introduzir os fundamentos da computação quântica, tendo como foco um algoritmo quântico promissor e sua aplicação a um problema do mercado financeiro. Mais especificamente, discutimos o problema da otimização de portfólio usando o *Quantum Approximate Optimization Algorithm* (QAOA). Não somente descrevemos os principais conceitos envolvidos, mas também consideramos exemplos simples práticos, envolvendo ativos financeiros disponíveis na bolsa brasileira, com códigos, tanto clássicos quanto quânticos, disponíveis livremente em um Jupyter Notebook. Também analisamos em detalhes a qualidade das soluções de otimização combinatória de portfólio por meio do QAOA usando o simulador quântico ATOS QLM do SENAI/CIMATEC.

Palavras-chave: Computação Quântica, Mercado Financeiro, Finança Quântica.

Previously only considered a frontier area of Physics, nowadays quantum computing is one of the fastest growing research field, precisely because of its technological applications in optimization problems, machine learning, information security and simulations. The goal of this article is to introduce the fundamentals of quantum computing, focusing on a promising quantum algorithm and its application to a financial market problem. More specifically, we discuss the portfolio optimization problem using the Quantum Approximate Optimization Algorithm (QAOA). We not only describe the main concepts involved but also consider simple practical examples, involving financial assets available on the Brazilian stock exchange, with codes, both classic and quantum, freely available as a Jupyter Notebook. We also analyze in details the quality of the combinatorial portfolio optimization solutions through QAOA using SENAI/CIMATEC's ATOS QLM quantum simulator.

Keywords: Quantum Computing, Financial Market, Quantum Finance.

1. Introdução

Desenvolvida ao longo das primeiras décadas do século 20 para explicar fenômenos na escala atômica da matéria, a teoria quântica mudou radicalmente os fundamentos da Física [1, 2]. Até o advento da teoria quântica, sempre assumimos que os átomos e outros constituintes microscópicos tivessem sua posição e velocidade muito bem definidas. As probabilidades refletiam apenas nosso desconhecimento destas quantidades. Mas ao contrário da Física Clássica, a incerteza na Física Quântica é fundamental. Mesmo que saibamos tudo que há para saber sobre um elétron – ou seja, a sua função de onda – só podemos fazer previsões probabilísticas

sobre suas propriedades. Ao contrário do que estávamos acostumados até então, o papel da medição passou a ter um papel central, algo que na interpretação mais ortodoxa da mecânica quântica, conhecida como interpretação de Copenhagen, pode ser resumido nas palavras de Pascual Jordan: “*Observações não somente perturbam o que vai ser medido, elas o produzem [...] Nós compelimos o elétron a assumir uma posição bem definida [...] Nós próprios somos os responsáveis por produzir os resultados das medições que observamos*”. Ou como disse Asher Peres certa vez: “*Experimentos não realizados não tem resultados*”.

Mas nem todos no entanto concordaram com essa nova visão, certamente radical. Em particular, em 1935, Albert Einstein, Boris Podolsky e Nathan Rosen argumentaram que mecânica quântica apesar de correta – afinal ela prediz com total acurácia as probabilidades

* Endereço de correspondência: askery@gmail.com

† Endereço de correspondência: rchaves@iip.ufrn.br

de observação em experimentos realizados – seria uma teoria incompleta [3]. No “paradoxo de EPR”, como viria a ficar conhecido esse artigo, o chamado emaranhamento quântico, inicialmente identificado por Erwin Schrödinger [4], tem um papel fundamental. Mas ao contrário do que o trio EPR poderia supor, esse emaranhamento é de fato uma característica fundamental da natureza, conforme demonstrado pelo teorema de Bell [5] e seus variados testes experimentais [6, 7] que provam de maneira categórica a inadequação do realismo local invocado por Einstein para chegar ao seu paradoxo.

Apesar de questões conceituais da mecânica quântica continuarem mais atuais do que nunca, a chamada primeira revolução quântica possibilitou avanços nas mais diversas áreas e o desenvolvimento de variadas tecnologias. A moderna teoria da computação, formulada por Alan Turing [8], por exemplo, certamente não teria tido o mesmo impacto se não fosse pelo processo de miniaturização permitido pelos transistores e outras multitudes de componentes eletrônicos que operam de acordo com as leis quânticas. Alguns anos mais tarde, em 1948, seria a vez de Claude Shannon definir matematicamente o conceito de informação [9]. Shannon não somente definiu a unidade básica de informação, o dígito binário, ou bit, como também estabeleceu a teoria que quantifica os recursos físicos necessários para armazenar, comunicar e recuperar os dados de uma fonte de informação (ou seja, o número de bits), mesmo na presença de ruído no canal. Novamente sem a quântica, neste caso responsável pelo desenvolvimento do *laser* e dispositivos capazes e armazenar grandes quantidades de informação, dificilmente estaríamos a nos indagar sobre a atual era da informação.

Não obstante essas revoluções primordiais, foi somente no início da década de 1980 que as reais possibilidades abertas pela teoria quântica no processamento da informação começariam a tomar forma. Em 1982, Richard Feynman [10] mostrou que devido às propriedades do espaço de Hilbert no qual a informação quântica é codificada, nenhuma máquina clássica seria capaz de simular fenômenos quânticos em larga escala sem que um fator exponencial fosse introduzido em seu desempenho. Como pode ser lido em mais detalhes na edição especial da RBEF [11] sobre o legado de Feynman, ele propôs então que apenas um “simulador quântico universal” seria capaz de fazê-lo eficientemente. Com trabalhos tais como de Benioff [12, 13], propondo uma versão quântica da máquina de Turing, e de Deutsch [14], que construiu uma situação matemática onde as características próprias dos sistemas quânticos foram usadas explicitamente para resolver um problema com funções binárias, generalizando a pedra fundamental da computação para o regime quântico, tivemos o primeiro vislumbre da computação quântica.

Em paralelo, o pioneirismo de Bennett e Brassard ao proporem a criptografia quântica [15] e a descoberta da não-clonagem quântica por Wootters e Zurek [16]

trouxeram à tona possibilidades antes impossíveis no limite clássico. Com a descoberta dos primeiros algoritmos quânticos práticos com vantagens computacionais, tais como o de Shor [17] para fatoração em número primos e o de Grover [18] para a busca em um banco de dados, foi mostrada em definitivo o potencial da informação quântica. Desde então, a chamada segunda revolução quântica amadureceu rapidamente em um campo de pesquisa multidisciplinar, com efeitos de longo alcance tanto em ciência fundamental quanto em aplicações tecnológicas como a computação quântica [19], simulação quântica [20], comunicação quântica [21] e metrologia quântica [22], que prometem moldar o século 21.

Contudo, muito embora todas as promessas e apesar dos avanços experimentais impressionantes, os protótipos de computadores quânticos atuais são extremamente ruidosos. Processadores quânticos baseados em circuitos supercondutores, tal como aquele usado pela Google na primeira demonstração da supremacia quântica [23], operam com uma taxa de ruído por operação quântica fundamental de aproximadamente 0.6%. Em contraste, a taxa de ruído dos computadores clássicos modernos é insignificante, com componentes típicos com uma taxa de falhas da ordem de 10^{-17} . Enquanto para os computadores clássicos a correção de erros é irrelevante, para as máquinas quânticas ela é essencial. Caso contrário, os erros se acumularão exponencialmente rápido obliterando qualquer vantagem computacional. Na prática, isso implica uma sobrecarga enorme na qual cada qubit lógico é composto de centenas ou mesmo milhares de qubits físicos. Um computador quântico universal tolerante a falhas que possa resolver, de forma eficiente, problemas como a fatoração de inteiros e a pesquisa em um banco de dados não estruturado requerem milhões de qubits com baixas taxas de erro e longos tempos de coerência.

Ainda que o avanço experimental para criar tais dispositivos possa levar décadas de pesquisa, a era NISQ [24], do inglês *Noisy Intermediate-Scale Quantum*, com até algumas centenas de qubits, tempo de coerência limitado e sem correção de erros, já é uma realidade. Algo que tem motivado uma variedade de novos algoritmos para os quais pode-se garantir o desempenho na presença de erros e assim atingir vantagens computacionais [25]. Uma das principais aplicações vislumbradas para os dispositivos quânticos da era NISQ ocorre em problemas de otimização. Algoritmos tais como o QAOA [26], do inglês *Quantum Approximate Optimization Algorithm*, o VQE [27, 28], do inglês *Variational Quantum Eigensolver* ou aqueles baseados no anelamento quântico [29–31] formam a base para aplicações que variam desde simulações moleculares [32] e de novos materiais [33] até problemas de aprendizagem de máquina [34] e análise de redes complexas [35].

Algoritmos quânticos de otimização tem tido particular destaque em problemas financeiros [36, 37], incluindo métodos de Monte Carlo, otimização de portfólio, gestão

de risco financeiro e melhoramento de algoritmos de aprendizado de máquina [25, 36, 38–44]. Essa nova linha de pesquisa, chamada *quantum finance*, tem tido um número crescente de artigos científicos [37, 45] e até mesmo o surgimento de startups focadas na área como, por exemplo, a DualQ [46] e a Multiverse [47]. A motivação para isso é, entre outras coisas, a promessa de resolver problemas de forma mais rápida e a necessidade de garantir a segurança de dados diante de uma nova tecnologia.

Por ora, enquanto o desenvolvimento do hardware não é suficiente para ultrapassar a era NISQ, o desafio mais urgente é a prova de princípio de que algoritmos quânticos possam executar uma gama de tarefas com desempenho ao menos comparável ao dos computadores clássicos e entender sob quais condições vantagens quânticas podem ser esperadas. Na própria RBEF, há diversos tutoriais explicando como usar circuitos para implementar algoritmos quânticos no computador quântico da empresa IBM [48–52].

Dentro deste contexto, o objetivo deste tutorial é proporcionar o entendimento básico da computação quântica usando um problema central do mercado financeiro: a otimização de portfólio [53–59]. Para tanto, após uma breve introdução aos conceitos básicos em computação quântica, focaremos nossa atenção na solução baseada no QAOA [26, 59]. Por fim, com o intuito de melhor entender e motivar a aplicação da computação quântica para finanças, preparamos um Jupyter Notebook que pode ser acessado através da Ref. [60], onde detalhamos conceitos centrais do mundo das finanças, além de disponibilizar códigos tanto clássicos quanto quânticos para a resolução do problema da otimização de portfólio.

2. Computação Quântica

Ao contrário da informação clássica, codificada em bits 0 ou 1, a informação quântica permite a superposição de estados, o bit quântico, também chamado de qubit [61, 62], do inglês *quantum bit*. O qubit é associado a qualquer sistema quântico com dois estados bem definidos, na chamada base computacional, são descritos pelos estados $|0\rangle$ e $|1\rangle$. Diferentemente de bits clássicos, os qubits podem estar em uma superposição de estados, ou seja,

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

ou, em forma matricial,

$$|\psi\rangle = a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad (2)$$

onde, $a, b \in \mathbb{C}$ são amplitudes de probabilidade. Mais precisamente, se uma medição for realizada na base computacional, encontraremos o qubit no estado $|0\rangle$ com probabilidade $|a|^2$, ou com probabilidade $|b|^2 = 1 - |a|^2$ para o qubit no estado $|1\rangle$. Note na Eq. (2), que $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

e $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Vemos, portanto, que a base computacional $(|0\rangle, |1\rangle)$ é composta pelos autovetores da matriz de Pauli Z , apresentada adiante na Eq. (8).

Em sua versão mais usual, a computação quântica trabalha com a evolução do estado descrevendo um sistema quântico. Para isso há basicamente dois paradigmas de tecnologias: a computação por portas lógicas e a computação adiabática, sobre as quais faremos uma breve descrição a seguir. Para alternativas ao modelo de computação quântica por circuito e a computação quântica adiabática, pode-se consultar as seguintes referências [63–66].

2.1. Modelo de circuitos da computação quântica

Um dos principais e mais utilizados modelos de computação quântica é aquele baseado em circuitos no qual um algoritmo é realizado através da aplicação sequencial de portas lógicas quânticas em um certo estado quântico de entrada. Tipicamente, um estado de referência onde os n qubits a serem processados são inicializados no estado $|0\rangle^{\otimes n}$. O que um computador quântico que usa tecnologia de portas faz é simplesmente aplicar uma operação unitária U neste estado de entrada, gerando um estado final $|\psi\rangle_{final} = U|0\rangle^{\otimes n}$ que codifica a resposta da computação que pode ser acessada através de medições apropriadas. Apesar de U ser um operador atuando em um espaço de n qubits, um dos resultados fundamentais da computação quântica nos mostra que esta operação unitária genérica pode ser arbitrariamente bem aproximada por operações unitárias atuando apenas em um único qubit, além de unitárias emaranhantes em dois qubits. Em outras palavras, com um conjunto finito de portas lógicas quânticas podemos realizar uma computação quântica universal.

De modo geral, transformações em sistemas quânticos controlados, sem acesso a graus de liberdade externos, devem ser reversíveis e precisam preservar a probabilidade total dos resultados de uma medida em 100%. Por conta disso, portas lógicas devem corresponder a transformações unitárias no estado quântico sobre o qual atuam. Matematicamente, uma transformação é dita unitária quando seu operador adjunto correspondente é também sua transformação inversa, isto é

$$U^\dagger U = U U^\dagger = I, \quad (3)$$

onde U^\dagger é o operador adjunto de U , obtido a partir da transposta de U tomando-se o complexo conjugado dos seus elementos, e I é a matriz identidade. A reversibilidade é garantida pela existência de inversa, enquanto a preservação da normalização dos estados é dada pela Eq. (3) junto do fato que $(U|\psi\rangle)^\dagger = \langle\psi|U^\dagger$, o que leva a

$$|\langle\psi|U^\dagger U|\psi\rangle|^2 = |\langle\psi|\psi\rangle|^2 = 1. \quad (4)$$

Pode-se mostrar que, a menos de uma fase global arbitrária, operações unitárias que atuam sobre um

único qubit correspondem a operadores com a mesma forma de um operador de rotação de um sistema com spin 1/2. Dessa forma, toda unitária sobre um qubit pode ser descrita a partir de um eixo de rotação \hat{n} e um ângulo θ na forma

$$U = e^{-i\theta\hat{n}\cdot\sigma/2} = \cos(\theta/2)I - i\sin(\theta/2)\hat{n}\cdot\sigma, \quad (5)$$

onde $\hat{n}\cdot\sigma$ é uma notação reduzida para o operador $n_x X + n_y Y + n_z Z$, sendo X e Z as matrizes de Pauli descritas respectivamente nas Eq. (7) e (8) e Y é a matriz de Pauli restante tal que

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \quad (6)$$

Note, em particular, que as portas X , Z e H , apresentadas a seguir, correspondem a rotações de um ângulo π em torno dos eixos \hat{x} , \hat{z} e $(\hat{x} + \hat{z})/\sqrt{2}$, respectivamente, a menos de uma fase global, que não interfere no resultado de medidas.

A noção de transformações unitárias como rotações em um espaço abstrato pode ser realizada de maneira mais concreta. Cada estado de um qubit pode ser visualizado como um ponto em uma esfera, tal esfera é conhecida como esfera de Bloch. Na Figura 1 mostramos a representação das operações das portas X e Y na esfera de Bloch aplicadas a partir do estado $|0\rangle$, ou seja, a trajetória da evolução de θ da Eq. (5) quando σ equivale às portas X (Eq. (7)) e Y (Eq. (6)). Enfatizamos que estas evoluções ocorrem tão rapidamente que podemos considerar que a mudança de estado ocorre instantaneamente após a aplicação de U .

As portas apresentadas a seguir fazem parte do circuitos quânticos mostrados mais adiante, discutidos detalhadamente mais a frente quando introduzirmos o Algoritmo de Otimização Quântica Aproximada (em tradução livre do inglês *Quantum Approximate Optimization Algorithm*, ou QAOA).

As portas lógicas X e Z , são portas de um único qubit e correspondem, respectivamente, às matrizes de Pauli

X e Z , ou seja

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (7)$$

e

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (8)$$

A porta X é o análogo da porta clássica NOT, a porta Z também é conhecida como porta de fase – por colocar um fase negativa no estado $|1\rangle$. Quando atuam na base computacional, teremos como resultado

$$X|0\rangle \rightarrow |1\rangle, \quad (9)$$

$$X|1\rangle \rightarrow |0\rangle, \quad (10)$$

e

$$Z|0\rangle \rightarrow |0\rangle, \quad (11)$$

$$Z|1\rangle \rightarrow -|1\rangle. \quad (12)$$

Outra importante porta quântica é a chamada Hadamard. Representada por H , a porta Hadamard é uma porta de um qubit e é responsável por gerar superposições de estados a partir da base computacional $|0\rangle$ e $|1\rangle$, tal que

$$H|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad (13)$$

$$H|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad (14)$$

onde o termo $1/\sqrt{2}$ promove a normalização do estado após a aplicação da porta. A representação matricial da porta Hadamard é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (15)$$

Por fim, a que talvez seja a porta lógica quântica mais importante já que gera o emaranhamento entre os qubits, condição necessária para potenciais vantagens quântica, é a chamada CNOT. A porta Não-Controlada, ou *Controlled-NOT* (CNOT), atua sobre dois qubits, um sendo chamado de qubit controle e o segundo de qubit alvo. Sua representação matricial é dada por

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (16)$$

Quando aplicada, por exemplo, a dois qubits no estado $|10\rangle$, teremos

$$CNOT|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad (17)$$

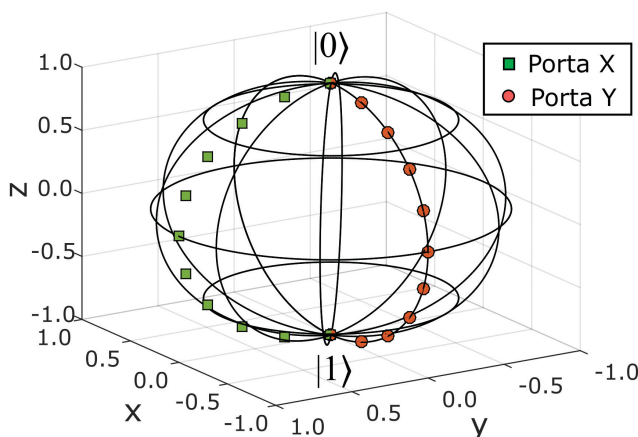


Figura 1: Representação da esfera de Bloch para a implementação dos operadores X e Y em um qubit com estado inicial $|0\rangle$.

Observe que a matriz que representa a porta CNOT (Eq. 16) só irá atuar no segundo qubit, já que os primeiros termos da diagonal principal representam uma identidade. No entanto, o primeiro qubit irá atuar como um qubit controle na operação e no caso dele estar no estado $|0\rangle$ nada acontece com o segundo qubit (qubit alvo). Caso contrário, se o controle está em $|1\rangle$, uma porta NOT quântica (a porta X) é aplicada ao qubit alvo, atuando na base computacional como

$$\begin{aligned} CNOT|00\rangle &\rightarrow |00\rangle, \\ CNOT|01\rangle &\rightarrow |01\rangle, \\ CNOT|10\rangle &\rightarrow |11\rangle, \\ CNOT|11\rangle &\rightarrow |10\rangle. \end{aligned}$$

Operações lógicas e algoritmos podem ser descritos por um diagrama similar ao usado em computação clássica, denominado circuito quântico. Em particular, na Seção 5 explicamos mais detalhadamente sobre os elementos que compõem o circuito para implementação do algoritmo QAOA adiante.

2.2. Computação Quântica Adiabática

A computação quântica adiabática [67] é um paradigma alternativo, no qual o estado fundamental de um Hamiltoniano codifica a resposta de uma dada computação. Pelo teorema adiabático, temos a garantia de que um sistema no estado fundamental de um Hamiltoniano inicial, irá se manter neste mesmo estado caso a evolução até um Hamiltoniano final seja vagarosa o suficiente, tempo este que é inversamente proporcional ao *gap* entre os níveis de energia do sistema quântico em questão [29, 31, 67, 68].

Assim, diferentemente da computação por portas, a computação adiabática tem como fundamento a evolução Hamiltoniana dependente do tempo, tal que

$$H(s) = A(s)H_i + B(s)H_f, \quad (18)$$

onde H_i e H_f são, respectivamente, os Hamiltonianos inicial e final. s é a parametrização do tempo e varia entre 0 e 1 enquanto $A(s)$ e $B(s)$ são as funções que descrevem variação temporal do Hamiltoniano, obedecendo condições de contorno dadas por $A(0) \neq 0$, $B(1) \neq 0$, $A(1) = B(0) = 0$. Ou seja, quando $t = 0$ o Hamiltoniano H_i prevalecerá enquanto que para $t = t_f$ o termo H_f será dominante.

Segundo o Teorema Adiabático [29, 30]: *Um sistema físico permanece em seu autoestado instantâneo, não degenerado, ao longo da evolução temporal, se sobre ele é aplicada uma perturbação suficientemente pequena.* Portanto, para ser adiabática, a evolução do Hamiltoniano descrita na Eq. (18) deve acontecer da forma mais lenta possível, evitando-se transição entre níveis energéticos e garantido que o sistema permaneça em seu estado fundamental.

Pelo enunciado do Teorema Adiabático podemos entender porque tecnologia chamada *annealing* quântico é

comumente usada no modelo de computação adiabática. Em analogia com o termo *annealing*, que em português pode ser traduzido como recozimento e, no mundo clássico, envolve problemas termodinâmicos onde um sistema é iniciado em um estado aleatório e em seguida a temperatura é reduzida de forma suficientemente lenta de modo que sempre seja garantido que o estado de maior entropia seja atingido. Durante esse processo o sistema evolui gradualmente até atingir seu estado fundamental [69]. Assim, o *annealing* quântico fornece uma ponte conceitual entre a computação quântica adiabática e a otimização clássica. Contudo, na computação quântica adiabática, o termo *annealing* quântico está relacionado à transição lenta entre os Hamiltonianos, portanto, neste caso, o *annealing* está relacionado à mudança temporal, e não térmica, como no caso clássico.

A computação quântica adiabática é capaz de implementar qualquer algoritmo quântico [70], o que significa que também é um computador quântico universal. Entretanto, na prática, a tecnologia de *annealing* quântico nos restringe a problemas que podem ser escritos como um problema tipo Ising ou QUBO (Otimização Binária Quadrática Irrestrita, em tradução livre). Vale ressaltar que, com o objetivo de tornar a computação quântica adiabática mais popular, a empresa D-Wave, líder nesta área, disponibiliza uma ferramenta que fornece interoperabilidade entre o computadores quânticos que funcionam usando a técnica de *annealing* e aqueles usando circuitos quânticos [71]. Mais detalhes sobre computação quântica adiabática podem ser encontrados em [72].

Como discutiremos mais abaixo, é interessante notar que o QAOA (Quantum Approximate Optimization Algorithm) é um algoritmo implementado através da computação de portas que de fato pode ser entendido como uma discretização da evolução temporal contínua de uma computação quântica adiabática.

3. Fundamentos Básicos do Mercado Financeiro

Dois dos elementos básicos do sistema financeiro são: (i) Ações, que são títulos de posse de frações de uma determinada empresa e (ii) *commodities*, que são bens fungíveis, como por exemplo, ouro, açúcar e dinheiro. Nos referimos de forma genérica a esses elementos como ativos. Ambos são atribuídos de um valor relativo que varia de acordo com a oferta e procura: um produto escasso e muito demandado torna-se valioso, ao passo que outro, ofertado em quantidades que superam sua procura perde seu valor. Uma carteira, ou portfólio, de um investidor é basicamente o seu investimento em diferentes tipos de ativos. Por exemplo, se você tem investimentos em ações de 5 empresas (por exemplo: Google, Amazon, Tesla, Petrobras e Vale), as ações dessas empresas compõem sua carteira de investimentos.

As ações, que serão os ativos de exemplo neste artigo, são, como já dito, frações do capital social de uma empresa. Em geral, as empresas oferecem tais ações aos investidores no mercado financeiro com o intuito de arrecadar recurso para expandir seu negócio. A bolsa de valores corresponde a um ambiente de negociação onde investidores podem comprar ou vender ações e diversos outros produtos financeiros como *commodities* e derivativos.

Nesta seção discutiremos os elementos básicos para entender o mundo das finanças. No material suplementar a este artigo, um Jupyter Notebook [60], pode-se encontrar uma descrição mais detalhada de conceitos do mercado financeiro, como bolsa de valores, ações, fundos de investimentos, criptomoedas, entre outros.

3.1. Abordagem Clássica

Os retornos esperados de um ativo são simplesmente a média da variação percentual nos preços de suas ações. Portanto, o valor do retorno esperado que obtemos aqui são os retornos esperados diários. Considerando o ativo i , o seu retorno no dia t será dado por $R_t^{(i)} = (P_{t+1}^{(i)} - P_t^{(i)})/P_t^{(i)}$, onde $P_t^{(i)}$ e $P_{t+1}^{(i)}$ são os preços da ação i nos dias t e $t + 1$ [73]. Podemos definir $R^{(i)}$ como um vetor (coluna) de retornos referente a cada tempo (dia) t da ação i . Ou seja, cada componente do vetor $R^{(i)}$ será um valor dado por $R_t^{(i)}$. Chamaremos de Δt o intervalo de tempo (cada dia), t o tempo decorrido a partir do dia inicial, M é o número total de passos (dias) considerado e T_{tot} é o tempo total tal que $T_{tot} = M\Delta t$.

O retorno esperado (média dos retornos) para a ação i será dado por:

$$\mu^{(i)} = \frac{1}{M} \sum_{t=1} R_t^{(i)}, \quad (19)$$

no nosso exemplo usamos a média de retornos diários no período de um ano, ver Ref. [60] para detalhes práticos.

Precisamos entender como o comportamento de ações distintas estão relacionadas, para isso é preciso encontrar a matriz de covariância, esta é usada para calcular o risco de uma carteira de ações. Podemos escrever uma matriz onde a diferença entre o retorno de cada ativo e o seu retorno médio está representado em uma coluna, ou seja

$$R = \begin{bmatrix} R_1^{(1)} - \mu^{(1)} & R_1^{(2)} - \mu^{(2)} & \dots & R_1^{(q)} - \mu^{(q)} \\ R_2^{(1)} - \mu^{(1)} & R_2^{(2)} - \mu^{(2)} & \dots & R_2^{(q)} - \mu^{(q)} \\ \vdots & \vdots & \ddots & \vdots \\ R_{T_{tot}}^{(1)} - \mu^{(1)} & R_{T_{tot}}^{(2)} - \mu^{(2)} & \dots & R_{T_{tot}}^{(q)} - \mu^{(q)} \end{bmatrix}_{M \times q} \quad (20)$$

onde q é número total de ativos.

A matriz de covariância será dada por

$$\Sigma = \frac{1}{M-1} R^T R, \quad (21)$$

onde R^T é a matriz transposta de R . Σ é a matriz de covariância de ordem $q \times q$ onde cada uma de suas

componentes será a relação entre dois ativos i e j tal que

$$\Sigma_{ij} = \frac{1}{M-1} \sum_{t=1}^M \left[\left(R_t^{(i)} - \mu^{(i)} \right) \left(R_t^{(j)} - \mu^{(j)} \right) \right]. \quad (22)$$

Uma covariância positiva significa que os retornos dos dois ativos se movem juntos (ambos caem ou sobem), enquanto uma covariância negativa significa que eles se movem inversamente (quando um sobe ou outro tende a cair e vice-versa).

No mercado financeiro, o risco quantifica a possibilidade de que o retorno obtido do ativo possa ser diferente da estimativa de retorno, portanto, a medida do risco depende da distribuição dos retornos. É preciso analisar o comportamento do ativo e assim estimar o risco de um portfólio de investimentos (com a combinação apropriada de ativos), algo que pode ser feito através do histórico de informações de mercado. De fato, o desvio padrão dos retornos nos fornece o grau de variação de uma série de preços de negociação ao longo do tempo, ou seja, como os retornos podem flutuar.

4. O problema da otimização de portfólio

Uma figura importante para gestão de risco no mercado financeiro é a construção de portfólios. Introduzida por Markowitz [53], um portfólio consiste em um conjunto de q ativos nos quais se deseja investir um determinado capital. A decisão de quanto e quando investir em cada ativo é tomada diante da estimativa de retorno $R^{(i)}$ e de previsão de riscos de perda Σ [74]. Tal processo de estimativa de risco e retorno é chamado de otimização de portfólio. Ou seja, para um determinado risco, existe um portfólio que maximiza o retorno. Por outro lado, para um determinado retorno, existe um portfólio que minimiza o risco.

O problema de otimização de portfólio pode ser definido simplesmente como um problema cuja finalidade é encontrar os valores ótimos dos pesos que maximizam os retornos esperados enquanto minimizam o risco (volatilidade).

Dado uma matriz de pesos w que representará a alocação percentual dos investimentos entre essas q ações, dado por

$$w = [w_1 \quad w_2 \quad \dots \quad w_q], \quad (23)$$

e tal que a soma deste pesos deve ser $\sum_{i=1}^q w_i = 1$. Para $q = 4$ ações, por exemplo, podemos ter uma alocação uniforme $w = [0.25, 0.25, 0.25, 0.25]$ ou, inclusive, uma matriz aleatória, como mostrado na resolução prática com 30000 portfólios, ver [60].

O retorno esperado do portfólio R_p é dado por

$$R_p = w_1 \mu^{(1)} + \dots + w_q \mu^{(q)}, \quad (24)$$

onde $\mu^{(i)}$ é o retorno esperado para cada ativo i . Observe que $R_p \equiv \mu^T w$.

A volatilidade mede a dispersão dos retornos. Ela está relacionada com a medida de risco, quanto mais o preço de uma ação varia em um determinado período de tempo, maior o risco de se ganhar ou perder dinheiro. A volatilidade do portfólio é dada por:

$$\sigma(R_p) = \sqrt{\sum_{i=1}^q \sum_{j=1}^q w_i w_j \Sigma_{ij}}, \tag{25}$$

onde w_i e w_j denotam os pesos dos ativos de 1 a q (no nosso exemplo, de 1 a 4) e Σ_{ij} é a covariância das duas ações denotadas por i e j (Eq. (22)).

Na prática, como existem investimentos com risco nulo, ou praticamente nulo, a carteira ideal não é escolhida apenas olhando o maior retorno ou o menor risco. De fato, há um índice denominado *Sharpe Ratio* (SR) – índice de Sharpe, em português – que expressa o retorno médio obtido em excesso da taxa livre de risco. A taxa de retorno livre de risco, ou fator de risco, é o retorno de um investimento com risco zero, o que significa que é o retorno que os investidores poderiam esperar sem correr risco.

Por exemplo, se um portfólio A produz um retorno $R_A = 2 * R_f$ duas vezes maior que o retorno de um hipotético ativo livre de risco (R_f), mas com um risco σ_A e um portfólio B um retorno $R_B = 2 * R_f$ quatro vezes maior que o ativo livre de risco, mas ao custo de um risco σ_B , mas digamos que $\sigma_B > 2 * \sigma_A$. Assim, a carteira B, embora com maior retorno absoluto (o dobro), não é a carteira ideal pois não ofereceu um prêmio de risco adequado, pois o risco mais que dobrou. Para mais detalhes metodológicos sobre o *Sharpe Ratio*, verificar Refs. [75, 76].

Dentro deste contexto, a carteira de risco ideal é aquela com o maior *Sharpe Ratio* [77], definido como

$$SR = \frac{R_p - R_f}{\sigma}, \tag{26}$$

onde R_p é o retorno do portfólio, R_f é taxa de lucro livre de risco e σ é o desvio padrão do portfólio (volatilidade). Cabe mencionar que retorno e risco são médias de janelas de 12 meses, considerado o ano como tendo 250 dias de negociação, conforme detalhado no material suplementar [60]. Outra observação importante é que, na prática, investimentos livre de risco não existem e as taxas apresentadas adiante, como CDI e outras, são meras referências numéricas com taxas semelhantes às taxas hipotéticas.

Um dos pontos fortes do trabalho de Markowitz foi mostrar que a busca por taxas de retorno maiores implica necessariamente em montar portfólios com maiores níveis de risco. Em termos práticos, se buscamos um maior retorno, precisaremos expor nossa carteira de investimentos a um risco mais elevado, que significa maiores variações percentuais, ou seja, uma maior volatilidade.

4.1. Exemplo prático

De um modo geral, um bom portfólio é aquele que nos fornece o máximo retorno com um mínimo de risco. Assim, assume-se que os investidores são avessos ao risco, ou seja, se houver uma escolha entre carteiras de baixo e alto riscos com os mesmos retornos, um investidor escolherá uma com baixo risco. Portanto, para decidirmos, entre a infinidade de combinações possíveis de carteiras, aquela que é ótima, i.e. para fazer a otimização de portfólio, devemos escolher a carteira com máximo retorno dado um certo grau de risco.

Como exemplo, consideramos os preços diários das ações das empresas Braskem (BRKM5), Itaú (ITUB4), Klabin (KLBN4) e Vale (VALE3) para o período entre 01 de janeiro de 2016 até 20 de setembro de 2021 obtidos com o pacote “yfinance” provido pelo *Yahoo! Finance*, cujos preços estão apresentados na Fig. 2.

Conforme discutido, precisamos obter dois ingredientes fundamentais: o vetor de retorno para cada ativo e a matriz de covariância para uma dada periodicidade (ver Ref. [60] para mais detalhes). Para o intervalo estabelecido e a periodicidade anual, o vetor de retorno médio anual e a matriz de covariância são apresentados, respectivamente, nas Tabelas 1 e 2 conforme calculado na Ref. [60].

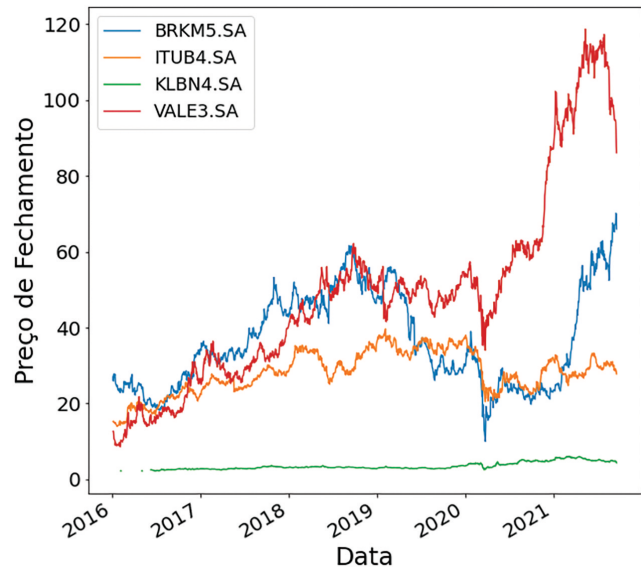


Figura 2: Exemplo da evolução temporal do preço de fechamento de ativos (disponíveis na bolsa brasileira) que formam uma carteira composta com ações das empresas Braskem, Itaú, Klabin e Vale.

Tabela 1: Retorno anual médio dos preços de fechamento das ações da Braskem (BRKM5), Itaú (ITUB4), Vale (VALE3) e Klabin (KLBN4) referentes ao período entre 01 de janeiro de 2016 até 20 de setembro de 2021.

Ativos	BRKM5	ITUB4	KLBN4	VALE3
Retorno (μ)	0.32	0.06	0.11	0.30

Tabela 2: Matriz de covariância dos preços de fechamento das ações da Braskem (BRKM5), Itaú (ITUB4), Vale (VALE3) e Klabin (KLBN4) referentes ao período entre 01 de janeiro de 2016 até 20 de setembro de 2021.

Ativos	BRKM5	ITUB4	KLBN4	VALE3
BRKM5	1.00	0.37	0.28	0.33
ITUB4	0.37	1.00	0.18	0.36
KLBN4	0.28	0.18	1.00	0.24
VALE3	0.33	0.36	0.24	1.00

Usando a teoria moderna de portfólio, conhecida também como a abordagem de Markowitz, nós geramos 30000 vetores pesos $w \in \mathbb{R}^4$ aleatoriamente, onde cada componente de um vetor específico representam, nesta ordem, a alocação em Braskem, Itaú, Klabin e Vale. Em cada iteração, consideramos os diferentes pesos individuais para cada ativo e calculamos o retorno e a volatilidade dessa alocação particular do portfólio. Assim, para cada w , calculamos o retorno anual da carteira por meio da Eq. (24) e dos retornos individuais apresentados na Tabela 1, bem como o risco (volatilidade) anual através da Eq. (25) e dos dados da Tabela 2. Ver Ref. [60] para maiores detalhes práticos de todos os exemplos dessa seção.

Observe que a criação da carteira, nesta vertente clássica, consiste em determinar o percentual que aplicamos em cada uma das ações (BRKM5, ITUB4, KLBN4 e VALE3). Através do plot do Retorno em função do Risco para os 30000 portfólios (ver Fig. 3), podemos determinar carteiras com diversas características. Podemos, por exemplo, selecionar a carteira com retorno máximo para um determinado risco ou uma carteira com risco mínimo para um determinado retorno ou ainda, podemos simplesmente selecionar a carteira com Sharpe Ratio máximo para determinados fatores de risco, como definido na Eq. (26).

Tais portfólios ideais para distintos níveis de risco formam o que se chama de curva de Fronteira Eficiente, representada na linha tracejada na Fig. 3. Sobre tal curva encontram-se os portfólios com a melhor relação risco/retorno, sendo mais vantajosos que todos os demais portfólios situados abaixo dela. Como precisaremos de alguns pontos (portfólios) para traçar a curva de Fronteira Eficiente, vamos explicar alguns deles. Na Tabela 3 é feita uma compilação de alguns portfólios,

Tabela 3: Apresentação de alguns portfólios conforme destacados na Fig. 3, contendo: *i*) as frações (ou pesos) de cada ação na carteira, bem como *ii*) o risco e *iii*) o retorno correspondentes, obtidos usando a abordagem clássica de Markowitz. Em destaque, as duas maiores alocações de cada carteira.

Descrição do Portfólio	BRKM5	ITUB4	KLBN4	VALE3	Risco	Retorno
Risco Mínimo	0.009	0.404	0.503	0.083	0.244	0.108
Retorno Máximo	0.919	0.006	0.009	0.066	0.492	0.311
Melhor SR ($R_f = 0.015$)	0.370	0.000	0.193	0.436	0.347	0.270
Melhor SR ($R_f = 0.028$)	0.403	0.002	0.099	0.496	0.372	0.287
Melhor SR ($R_f = 0.100$)	0.451	0.000	0.022	0.526	0.395	0.303

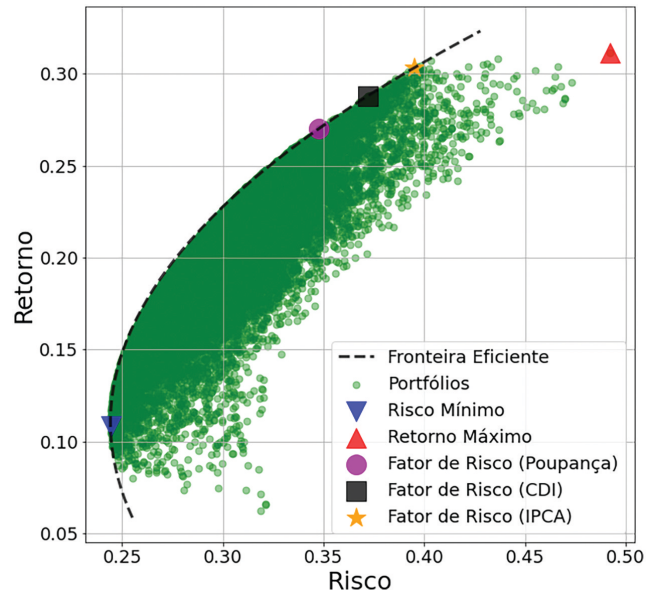


Figura 3: O conflito entre Risco (Σ) e Retorno (μ) ilustrado com o gráfico da Fronteira Eficiente. Cada ponto verde representa uma carteira com diferentes proporções (pesos) de ações das empresas Braskem, Itaú, Klabin e Vale. Observe como a busca por retornos maiores implica em assumir maiores níveis de risco. Confira a Ref. [60] para verificar a obtenção da Fronteira Eficiente na prática.

conforme destacados na Fig. 3, com as frações (ou pesos) de cada ação na carteira, bem como o risco e o retorno correspondentes.

Após o cálculo do risco e do retorno para cada um dos 30000 pesos gerados aleatoriamente, podemos investigar a composição de cada um dos portfólios. Como sabemos, um portfólio de interesse é o com menor risco que, na Figura 3, corresponde ao triângulo para baixo em azul. Na Tabela 3, mostra-se que equivale a um risco de cerca de 24.4%, significando que a carteira variou em média em torno de 24.4% por ano, com um retorno anual médio de cerca 10.8%. A composição desta carteira é concentrada em Itaú (40.4%) e Klabin (50.3%).

Outro portfólio natural a ser investigado é a carteira com retorno máximo, que corresponde ao triângulo para cima em vermelho na Fig. 3. Vemos, na Tabela 3, que a composição deste portfólio é fortemente concentrado em Braskem (92%), com uma alocação residual em Vale

(6.6%), o que já era esperado dado o destaque em performance das ações da Braskem e Vale com relação às demais ações apresentadas na Fig. 2. A carteira apresenta retorno anual de cerca de 31% com risco de 50%. Observe que o risco é aproximadamente o dobro da carteira de risco mínimo, porém com o triplo do retorno.

Seguindo a hipótese de que os investidores são naturalmente avessos ao risco, surge a necessidade de comparar o desempenho dos portfólio com investimentos livres de risco, através do cálculo do Sharpe Ratio (SR), conforme já prescrito na Eq. (26). Suponha que exista no mercado uma Taxa Livre de Risco equiparada com a taxa de poupança, CDI e IPCA. Na Figura 3, para descobrir o portfólio com máximo SR, usamos três fatores de risco R_f (três cenários qualitativamente distintos): a taxa de poupança, a CDI e o IPCA, aproximadamente. Note que, para cada fator de risco, temos um portfólio ideal, que não coincide com o portfólio de retorno máximo. Ou seja, para bater um benchmark cada vez mais alto (taxa de retorno sem risco crescente), precisamos tomar riscos cada vez maiores, caso o apetite do investidor não seja satisfeito com a taxa livre de risco.

Em um cenário onde a taxa livre de risco disponível seja em torno de $R_f = 1.6\%$, como a nossa poupança atual, o portfólio com maior SR, após testar 30000 composições (pesos) de portfólios, de igual modo, com Braskem, Itaú, Klabin e Vale apresenta a seguinte composição para proporção de alocação w , nesta ordem, $w = [37\%, 0\%, 19\%, 43\%]$, com um risco de cerca de 35% e um retorno de 27%. Veja o círculo roxo na Fig. 3 e a terceira linha de dados na Tab. 3. Note que mais de 80% da alocação do recursos concentra-se em Braskem e Vale.

Para um fator de risco de $R_f = 2.86\%$ (aproximadamente a CDI), obtemos os seguintes pesos de alocação correspondente a um SR máximo: $w = [40.3\%, 0\%, 10\%, 49.7\%]$. Tal portfólio é indicado na Fig. 3 pelo quadrado preto. Observe que quase 90% da carteira é concentrada em Braskem e Vale. O retorno do portfólio é de 28.7% e o risco gira em torno de 37%.

Por fim, para um cenário onde exista investimento livre de risco com taxa $R_f = 10\%$ (e.g., aproximadamente o IPCA), temos $w = [45.1\%, 0\%, 2.2\%, 52.6\%]$, representado pela estrela laranja na Fig. 3. Em primeiro lugar, observe que quase 98% da carteira é alocada, de igual modo, em Braskem e Vale. O retorno é praticamente igual ao da carteira com retorno máximo, cerca de 30.3%, porém o com um risco cerca 25% menor, em torno de 40%.

Apresentados tais pontos (portfólios) contidos na Fronteira Eficiente, podemos proceder um ajuste polinomial para a determinação precisa da curva. Confira nosso Jupyter Notebook [60] onde apresentamos um ajuste polinomial de grau 2 do Risco em função do Retorno para obtenção da Fronteira Eficiente.

A dificuldade computacional que envolve o problema de otimização de portfólio aumenta quando se adicionam

restrições (como o da Eq. (28)) mais realistas ao problema. Por exemplo, pode-se desejar impor restrições de positividade (de modo que só se possa comprar e não vender ativos), ou restrições de número inteiro (de modo que só se pode investir em ativos em incrementos fixos), ou limites superiores sobre o valor que se pode investir em um determinado ativo (devido, por exemplo, à liquidez). Além disso, os retornos ou correlações entre os ativos podem variar no tempo, podendo haver custos de transação para a compra e venda de ativos.

Com essas restrições mais realistas, o problema de otimização de portfólio pode se tornar substancialmente mais desafiador de resolver, mesmo aproximadamente, e é um desafio das finanças computacionais modernas. Uma variedade de abordagens algorítmicas quânticas [25, 57, 78–83] foram desenvolvidas para resolver, ao menos aproximadamente, este problema. Abaixo definimos matematicamente o problema de otimização, para o qual analisaremos a solução quântica proporcionada pelo QAOA.

Considere o seguinte problema de otimização de portfólio, cujo objetivo é minimizar a expressão

$$\min_{x \in \{0,1\}^n} bx^T \sigma x - \mu^T x \tag{27}$$

com a restrição

$$1^T x = B, \tag{28}$$

onde $x \in \{0,1\}^n$ é um vetor de variáveis binárias no qual quando $x = 1$ indica quais ativos escolher e $x = 0$ indica quais não escolher. O parâmetro $b > 0$ é um controle de risco do gestor de ativos, já que ao aumentar b precisamos de maiores retornos para alcançar o mínimo da função objetiva. Fato que, pela fronteira eficiente discutida anteriormente (Fig. 3), exige maiores riscos. O parâmetro B denota o orçamento, neste caso específico, o número de ativos a serem selecionados dentre q disponíveis. Note que, com variáveis binárias, a otimização apenas nos diz quais ativos devemos investir, mas não a quantidade ou proporção com a qual devemos fazê-lo.

A restrição estabelecida na Eq. (28) pode ser entendida como oriunda de um termo de penalidade do tipo

$$P(x) = \alpha(B - f(x))^2 \tag{29}$$

onde $f(x)$ é uma função de penalidade e α é um coeficiente de escala de penalidade. Quando $f(x) = B$, $P(x) = 0$ então a restrição é atendida. Quando $f(x) \neq B$, $P(x) > 0$ então a restrição é violada [59]. No nosso exemplo da Eq. (28), $f(x) = 1^T x$. Observe que o termo de regularização penaliza carteiras com um número de ativos diferente de B . Veja [60] para conferir na prática. Caso o leitor(a) deseje assumir uma taxa de retorno livre de risco diversa das que utilizamos como exemplo, ele(a) pode executar o código com qualquer valor que desejar, fazendo as mudanças correspondentes no código disponibilizado. Para uma lista de títulos públicos mundiais e o os respectivos rendimentos, sugerimos consultar Ref. [84].

5. O algoritmo QAOA

O Algoritmo de Otimização Quântica Aproximada (em tradução livre do inglês *Quantum Approximate Optimization Algorithm*, ou QAOA) é um algoritmo híbrido (isto é, parcialmente quântico e clássico) que busca encontrar soluções aproximadas para problemas de otimização, sendo bastante adequado para resolver problemas de otimização combinatória.

Proposto originalmente por Farhi et al. [26] em 2014, o algoritmo segue o modelo de um método variacional, onde o problema de otimização é mapeado em um Hamiltoniano de custo, H_C , que passa a codificar a solução do problema no seu menor autovalor. Busca-se, então, minimizar o valor esperado desse Hamiltoniano, $\langle \psi | H_C | \psi \rangle$, sobre estados $|\psi\rangle$ que pertençam a uma determinada família de estados parametrizados a partir da otimização (clássica) dos parâmetros, na expectativa de encontrar uma cota superior ao mínimo verdadeiro do espectro de H_C , ou o próprio valor mínimo, atingível apenas com o autoestado correspondente.

O QAOA propõe uma forma específica de produzir estados quânticos parametrizados com uma garantia de eventual convergência ao valor ótimo do problema para uma quantidade suficientemente grande de parâmetros. Por sua simplicidade e possibilidade de aplicação imediata nos primeiros computadores quânticos e pelas garantias teóricas de convergência e de eficiência [45, 78], um crescente interesse da comunidade em algoritmos variacionais vem ocorrendo ao longo dos últimos anos [25, 57, 78–83].

Apesar de ter aplicabilidade geral, o algoritmo do QAOA é comumente usado em problemas de otimização combinatória [25, 78], isto é, problemas onde buscamos minimizar (ou maximizar) funções que tomam variáveis binárias como argumentos. A razão para isso tem a ver com a facilidade em codificar este tipo de problema no Hamiltoniano de custo correspondente e também com o fato de problemas dessa forma nem sempre possuírem algoritmos clássicos eficientes para sua solução.

Na falta de um algoritmo clássico eficiente para a solução de um problema envolvendo n variáveis binárias x_i , pode-se pensar em uma estratégia de varredura sobre todas as 2^n combinações de valores possíveis, ou seja, uma solução por “força bruta”. Mesmo que se leve um tempo pequeno para cada teste individual, como por exemplo $1 \mu s$, o crescimento exponencial do número de possibilidades rapidamente leva a tempos impraticáveis para o uso desse método. Enquanto um problema de 30 variáveis, por exemplo, levaria em torno de 17 minutos para ser resolvido nesse cenário, o mesmo problema com 50 variáveis já levaria mais de 35 anos. Compare isso com um algoritmo que levasse um tempo proporcional ao quadrado do número de variáveis, o tempo necessário para resolução do problema com 50 variáveis seria apenas $(50/30)^2 \approx 2.77$ vezes mais demorado que o problema de 30 variáveis. Supondo ainda 17 minutos

para este último problema, levaríamos agora em torno de 47 minutos para o problema maior, o que é consideravelmente menor que o esperado pelo método de força bruta. Apesar de não se acreditar que algoritmos quânticos possam reduzir drasticamente o tempo de *todos* os problemas que tenham esse incremento exponencial a um problema com incrementos polinomiais, entende-se que em alguns casos alguma vantagem pode ser apresentada em relação a algoritmos clássicos, o que tornaria tratáveis algumas instâncias do problema.

A parametrização proposta pelo QAOA se baseia fundamentalmente na aplicação sucessiva de duas operações unitárias: a unitária de custo, U_C , correspondente à evolução do Hamiltoniano de custo H_C e a unitária de mistura, U_B , correspondente ao Hamiltoniano de mistura, H_B , dado por

$$H_B = \sum_{i=1}^n X_i, \quad (30)$$

onde X_i é o operador de Pauli X (porta X) atuando no espaço do i -ésimo qubit. A “duração” da evolução de cada Hamiltoniano corresponde aos parâmetros a serem otimizados. Considerando parâmetros reais β e γ , temos as operações unitárias

$$U_C(\gamma) := e^{-i\gamma H_C}, \quad (31)$$

$$U_B(\beta) := e^{-i\beta H_B}. \quad (32)$$

O algoritmo então prescreve a preparação de estados $|\psi(\boldsymbol{\gamma}, \boldsymbol{\beta})\rangle$, com $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_p)$ e $\boldsymbol{\beta} = (\beta_1, \dots, \beta_p)$, a partir de um estado inicial $|\psi_{\text{ini}}\rangle$ (também prescrito pelo algoritmo), de acordo com a sequência de evoluções unitárias

$$|\psi(\boldsymbol{\beta}, \boldsymbol{\gamma})\rangle = U_B(\beta_p)U_C(\gamma_p) \dots U_B(\beta_1)U_C(\gamma_1)|\psi_{\text{ini}}\rangle, \quad (33)$$

e então buscamos encontrar o valor da expressão

$$F_p := \min_{\boldsymbol{\beta}, \boldsymbol{\gamma}} \langle \psi(\boldsymbol{\beta}, \boldsymbol{\gamma}) | H_C | \psi(\boldsymbol{\beta}, \boldsymbol{\gamma}) \rangle, \quad (34)$$

a partir de algum algoritmo clássico de otimização sobre os parâmetros. Vale notar que, como o espectro de $H_B = \sum_i X_i$ contém apenas valores inteiros (mais precisamente, $\{-1, 1\}$), então os valores de β podem ser tomados no intervalo $[0, \pi]$. Os valores de γ podem ser buscados no intervalo $[0, 2\pi]$.

Na Fig. 4 apresentamos o circuito de implementação do QAOA. Um circuito quântico determina quais e

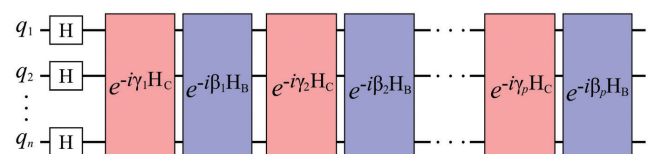


Figura 4: Circuito para implementação do QAOA.

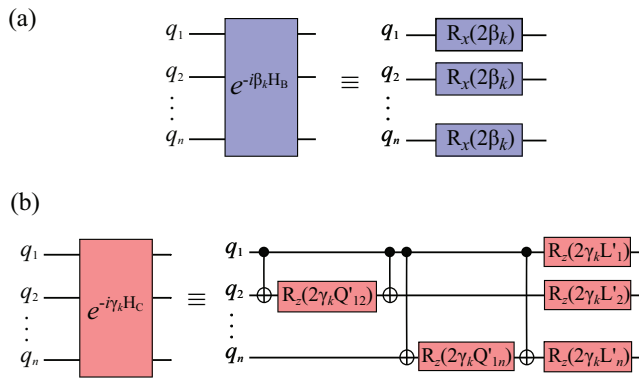


Figura 5: Circuitos implementando as unitárias (a) U_B e (b) U_C .

em que ordem as chaves lógicas são aplicadas a um ou mais qubits de um sistema. Estes são compostos de linhas e símbolos onde as linhas representam os qubits (uma linha para cada qubit) e cada símbolo representa uma chave lógica. Por sua vez, as chaves lógicas (descritas por caixas, com letras) descrevem um conjunto de operações quânticas aplicadas a um ou mais qubits. No circuito do QAOA vemos que temos n qubits, primeiramente aplicamos a porta Hadamard em todos os qubits. Em seguida intercalamos operações que implementam o Hamiltoniano de mistura (U_B) – em azul – e o Hamiltoniano de custo (U_C) – em vermelho. Na Fig. 5 mostramos com mais detalhes as etapas para implementação de U_B e U_C .

O algoritmo toma como estado inicial a superposição de todos os estados da base computacional com igual amplitude, isto é,

$$|\psi_{\text{ini}}\rangle = \sum_{x_i \in \{0,1\}} |x_1 \dots x_n\rangle / \sqrt{2^n}. \quad (35)$$

Note que este estado pode ser preparado de forma imediata a partir do estado $|0\rangle^{\otimes n}$ e da porta Hadamard (Eq. (15)), aplicando-a independentemente sobre todos os qubits. O resultado da combinação é a superposição de todas as possibilidades de estados da base computacional para todos os qubits, todos com a mesma amplitude. Isto é representado na equação a seguir e também na parte inicial do circuito na Fig. 4, tal que

$$|\psi_{\text{ini}}\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)^{\otimes n}. \quad (36)$$

Veremos mais adiante que há um motivo para estabelecer essa prescrição para o estado inicial, exatamente como o autoestado de maior autovalor do Hamiltoniano de mistura, H_B , o que está conectado com o modelo de computação adiabática.

Outro ponto interessante de notar é que o aumento no número de parâmetros usados, implicitamente estabelecido acima como $2p$ (p valores de γ e p valores de β), tende a melhorar a aproximação do valor ótimo real

do problema (embora na prática possam haver flutuações, como mostrado adiante): a estrutura sequencial de operadores unitários faz com que uma preparação envolvendo $p + 1$ iterações de U_C e U_B sempre inclua preparações com p iterações, uma vez que, se usarmos $\gamma_{p+1} = 0$ e $\beta_{p+1} = 0$, obtemos $U_C(\gamma_{p+1}) = I$ e $U_B(\beta_{p+1}) = I$, de modo que

$$F_{p+1} \leq F_p, \quad (37)$$

lembrando que F_p é o valor resultante da otimização sobre os parâmetros, como definido na Eq. (34). Veremos que, também por conta da conexão com o modelo de computação adiabática, de fato esta melhora não só deve ser garantida para um número suficientemente grande de p , como deve convergir ao valor real do problema original.

Particularizando o QAOA para problemas de otimização combinatória, temos ainda uma maneira concreta de estabelecer o Hamiltoniano de custo como um operador diagonal na base computacional e, portanto, em termos de combinações de produtos de operadores de Pauli Z_i , como num modelo de Ising. Para ilustrar isso e também por ser mais pertinente a problemas de otimização de portfólio, consideramos mais particularmente problemas tipo QUBO, onde a função custo a ser minimizada pode ser descrita como

$$C(x_1, \dots, x_n) = \sum_{i,j=1}^n Q_{i,j} x_i x_j + \sum_{i=1}^n L_i x_i. \quad (38)$$

Mapeando as variáveis binárias clássicas x_i em operadores quânticos na base z , ou seja, $\hat{x}_i = |1\rangle\langle 1| = (I - Z_i)/2$, obtemos a propriedade

$$\hat{x}_i |x\rangle = x_i |x\rangle, \quad (39)$$

onde $x \in \{0, 1\}$. Realizando esse mapa em todas as variáveis da função custo C acima, obtemos o Hamiltoniano H_C desejada, que possui agora a propriedade

$$H_C |x_1 \dots x_n\rangle = C(x_1 \dots x_n) |x_1 \dots x_n\rangle, \quad (40)$$

para um estado $|x_1 \dots x_n\rangle$ da base computacional. Além disso, H_C possui a forma genérica

$$H_C = \sum_{i,j=1}^n Q'_{ij} Z_i \otimes Z_j + \sum_{i=1}^n L'_i Z_i + K, \quad (41)$$

onde os novos coeficientes são obtidos dos coeficientes originais a partir da expansão de \hat{x}_i em termos de Z_i . Em implementações práticas, o termo constante K pode ser ignorado, uma vez que ele não altera o autoestado que minimiza o autovalor de H_C .

Como todos os termos em H_C comutam entre si, a unitária associada U_C pode ser expandida em um produto de unitárias associadas a cada termo, em qualquer ordem desejada. Os termos “lineares”, envolvendo apenas operadores na base z para um único qubit, são

imediatamente identificados como rotações em torno do eixo z da esfera de Bloch para esse qubit, que costumam ser facilmente implementáveis em plataformas de computação quântica remota já disponíveis atualmente [85]. Já para os termos envolvendo operadores sobre dois qubits, nos valem da identidade

$$\exp(-ikZ_i \otimes Z_j) = \text{CNOT}_{ij} \exp(-ikZ_j) \text{CNOT}_{ij}, \quad (42)$$

onde CNOT_{ij} é a porta não-controlada (Eq. (16)) com controle no qubit i e atuando sobre o qubit j . Essas portas também são implementáveis nessas plataformas de computação quântica, apesar de serem ainda bastante ruidosas e terem a conectividade entre os qubits ainda consideravelmente limitadas (isto é, nem todos os pares i e j são conectados diretamente, o que envolve a aplicação de mais portas CNOT para realizar uma conexão indireta).

Na Fig. 5(a) mostramos as portas lógicas necessárias para construir a operação U_B . Nela aplicam-se rotações em todos os qubits no eixo x sob um ângulo $2\beta_k$. Ou seja, ocorre uma rotação na esfera de Bloch de cada um dos qubits, essa rotação acontece como representado na Porta X da Fig. 1 mas o ângulo de rotação é de $2\beta_k$. O subíndice k representa o contador de cada iteração. Já a Fig. 5(b) mostra a implementação de U_C , aqui é usado o modelo estabelecido para a Hamiltoniana H_C na Eq. (41). Para tal implementação, aplicam-se rotações no eixo z sob ângulos de $2\gamma_k Q'_{1j}$ onde os coeficientes Q'_{1j} são determinados individualmente em relação às operações entre os qubits 1 e j . Antes e depois das rotações R_z , aplicam-se portas CNOT, como demonstrado na Eq. 42. Por fim aplicam-se rotações, também no eixo z , com ângulos $2\gamma_k L'_j$. Observe que estas operações ocorrem entre pares de qubits sempre envolvendo o qubit q_1 (qubit controle) e os outros qubits q_j (qubit alvo).

Note que os valores de Q'_{ij} e Q'_{ji} podem ser agregados em um só coeficiente, uma vez que Z_i e Z_j comutam entre si. Também é possível incorporar termos diagonais nos termos lineares, no problema clássico original, uma vez que variáveis binárias satisfazem $x_i^2 = x_i$. Usamos também a identidade (42) para implementar as unitárias associadas aos termos quadráticos.

A vantagem quântica do algoritmo QAOA foi investigada na Ref. [86], onde foi mostrado que a amostragem eficiente da distribuição de saída de QAOA, mesmo para o caso de menor profundidade de $p = 1$, implica no colapso da hierarquia polinomial, um forte indício de que não haja uma simulação clássica eficiente deste algoritmo.

De um modo geral, métodos variacionais, como o QAOA, fornecem limites superiores para a energia mais baixa de uma função custo com forma/simetria mapeada em um Hamiltoniano. Contudo, vale dizer, que a relativa aceleração do algoritmo quântico e a garantia de convergência são questões de pesquisa ainda em

aberto. Ou seja, é possível que novos algoritmos clássicos mais eficientes sejam descobertos, bem como classe de problemas onde a convergência dos métodos quânticos é desafiada. Uma desvantagem conhecida dos métodos variacionais, famosa no domínio da química quântica, é a não extensividade da solução com o tamanho do sistema. Dito de outro modo, a energia calculada usando tais ferramentas pode não escalar com o tamanho do sistema [87]. Porém, no domínio da otimização combinatória, este fato não é particularmente preocupante, uma vez que escalar o problema (acrescentar novos ativos, por exemplo), em geral, significa ter um novo sistema e todo cálculo precisa ser necessariamente refeito. Muito embora as limitações do método, há uma projeção de que uma demonstração de supremacia quântica baseada no QAOA assim que um computador quântico de 420 qubits (com correção de erros) esteja disponível [88].

5.1. Relação do QAOA com a Computação Adiabática

A conexão do QAOA com a computação adiabática se dá pela aplicação repetida dos operadores de custo e do misturador, que podem ser entendidas como uma discretização de uma evolução adiabática contínua. A forma geral do problema adiabático é descrito na Eq. (18), relembremos aqui a equação já com os Hamiltonianos inicial e final pertinentes ao problema do QAOA:

$$H(t) = \left(1 - \frac{t}{T}\right) H_B + \left(\frac{t}{T}\right) H_C. \quad (43)$$

O Hamiltoniano do misturador H_B será nosso Hamiltoniano inicial e o Hamiltoniano de custo H_C será nosso Hamiltoniano final. Na formulação adiabática, a evolução é contínua e t é o tempo transcorrido desde o começo da evolução, T é o tempo final de evolução entre H_B e H_C , isto é $t \in [0, T]$.

Notemos então que, de acordo com o teorema adiabático, para T suficientemente grande (de modo que $H(t)$ varie lentamente), um autoestado de H_B seria continuamente transformado no autoestado correspondente de H_C . Se o problema de otimização que queremos resolver com H_C é um problema de minimização, começamos com o autoestado de menor autovalor de H_B . Analogamente, podemos começar com o autoestado de maior autovalor de H_B , como o estado inicial do QAOA, $|\psi_{\text{ini}}\rangle$, descrito na Eq. (35), para resolvermos um problema de maximização. Podemos também começar com o mesmo estado e substituímos H_B por $-H_B$ no Hamiltoniano $H(t)$ para permanecermos com um problema de minimização.

Acima mostramos que o QAOA é um algoritmo projetado para ser implementado em um computador quântico no modelo de circuito. No entanto, as portas quânticas são construídas realizando a evolução de um estado quântico a partir de um Hamiltoniano tal que $U(\alpha, H) = e^{-i\alpha H}$. No caso da evolução de $H(t)$, dada $U(T, t_0)$ uma

matriz que descreve a evolução de um estado quântico entre os tempos t_0 e T , podemos discretizar a evolução tal que

$$U(T, t_0) = U(T, t_m)U(t_m, t_{m-1}) \dots U(t_1, t_0), \quad (44)$$

onde m é o número de divisões da evolução, ou seja, número de passos de tempo. Conforme m aumenta, a aproximação se torna mais precisa e cada passo da evolução passa a envolver um intervalo de tempo cada vez menor. Com um número suficientemente grande para m , cada termo da discretização pode ser bem aproximado por termos de primeira ordem no tempo, de modo que podemos reescrever a Eq. (44) como uma função de diversas exponenciais:

$$U(T, t_0) \approx e^{-\frac{i}{\hbar}H_n(T-t_n)} e^{-\frac{i}{\hbar}H_{n-1}(t_n-t_{n-1})} \dots e^{-\frac{i}{\hbar}H_0(t_1-t_0)}. \quad (45)$$

Podemos também separar a evolução de cada Hamiltoniano em evoluções de termos individuais. Como os Hamiltonianos H_B e H_C não comutam entre si, não podemos simplesmente separar a evolução deles em termos individuais, já que para operadores A e B que não comutam, vale que $e^{A+B} \neq e^A e^B$. Podemos, no entanto, decompor tal expressão usando a decomposição de Suzuki-Trotter [89–92]:

$$e^{A+B} = \lim_{p \rightarrow \infty} \left(e^{A/p} e^{B/p} \right)^p. \quad (46)$$

A evolução final aproximada pode ser escrita então como um produto alternado de exponenciais de H_B e H_C , avaliadas em instantes diferentes. Isso dá o seguinte aspecto ao operador de evolução total

$$U(t, t_0) \approx e^{-i\beta'_n H_B} e^{-i\gamma'_n H_C} \dots e^{-i\beta'_1 H_B} e^{-i\gamma'_1 H_C}, \quad (47)$$

que possui exatamente a forma da expressão (33), sendo que agora os parâmetros β' e γ' englobam a duração de cada evolução e o fator da decomposição de Suzuki-Trotter.

A importância da Eq. (47) é a de mostrar que, para um número de iterações do algoritmo QAOA $p \rightarrow \infty$, existem parâmetros β' e γ' , pelo menos em princípio, que permitiriam o algoritmo simular com exatidão uma evolução adiabática. Com isso, e usando que a convergência ao valor ótimo do problema de otimização é garantido pelo teorema adiabático, obtemos uma garantia de que uma otimização adequada dos parâmetros β e γ do QAOA deve também permitir convergência ao valor ótimo do problema. Em outras palavras, podemos sempre encontrar um p e um conjunto de ângulos γ_k e β_k que tornam F_p (Eq. (34)) o mais próximo do menor nível de energia do espectro em questão [26].

Apesar dessa condição ser suficiente para garantir a convergência, nada implica que ela seja necessária. Consequentemente, o QAOA pode ser mais eficiente que a computação adiabática, uma vez que, através da otimização dos parâmetros, possivelmente fugindo da prescrição dada pela evolução adiabática, podemos encontrar boas aproximações para o problema de otimização com poucas iterações do QAOA.

5.2. Aplicação à Otimização de Portfólio

Para a abordagem quântica do problema de otimização de portfólio, ao invés de pesar as diferentes ações, determinaremos quais ações incluir e quais excluir de uma carteira, usando método do QAOA para a tarefa de otimização de portfólio [59]. É, assim, um problema relacionado ao problema clássico, porém distinto.

Conforme a Eq. (27), além dos ingredientes usados na abordagem clássica (os retornos e a matriz de covariância), precisamos informar alguns parâmetros. Um deles é o apetite ao risco b , que fixamos em $b = 0.5$, correspondente ao maior risco observado na abordagem clássica. O outro é o parâmetro B , que representa o orçamento, neste caso quantas ações colocar na carteria. Como utilizamos as mesmas ações anteriores e sabendo que o portfólio com máximo Sharpe Ratio na abordagem clássica se concentra majoritariamente em duas ações, fixamos $B = 2$ com um intuito de contrastar com os resultados anteriores. Observe que o termo de restrição provoca uma penalização ao construir um portfólio com um número de ações diferente de B , ver Ref. [60].

Dito de outro modo, ao fixar $B = 2$ pretendemos responder a seguinte pergunta: será que o QAOA retornará como portfólio ideal uma carteira semelhante à carteria clássica? Ou seja, uma carteira com Braskem e Vale, tal qual obtido anteriormente? Observe que as carteiras com melhores Sharpe Ratio na Tabela 3 são concentradas praticamente em proporções iguais em BRKM5 e VALE3. Veja também a Ref. [60] para mais detalhes.

Assim, usando a Tabela 2 podemos escrever a função objetiva (relacionada ao Hamiltoniano) a ser minimizada usando o QAOA como

$$\begin{aligned} C(x) = & -x_1 - x_2 - x_3 - x_4 + (0.37x_1x_2) \\ & + (0.28x_1x_3)(0.33x_1x_4) + (0.18x_2x_3) \\ & + (0.36x_2x_4) + (0.24x_3x_4) \\ & - (2 - x_1 - x_2 - x_3 - x_4)^2, \end{aligned} \quad (48)$$

onde x_1 , x_2 , x_3 e x_4 equivalem, respectivamente, a BRKM5, ITUB4, KLBN e VALE3, sendo variáveis binárias, ou seja, podem assumir valores de 0 ou 1. Observe como o termo de de restrição penaliza carteiras com número de ações diferentes do orçamento ($B = 2$). Por exemplo, verifique o valor da função objetiva para a escolha das 4 ações ou nenhuma delas em Ref. [60], visto que escolher exatamente duas ações anula a penalidade.

Por meio do QAOA, encontramos, para cada uma das $2^4 = 16$ combinações possíveis das variáveis binárias, ou seja, para cada um dos vetores de estado ($|0000\rangle, |0001\rangle, \dots, |1110\rangle, |1111\rangle$), um valor para a energia associada e a probabilidade de o respectivo vetor ser a solução ideal. Como vimos na Seção 5, o QAOA permite transformar o estado de superposição uniforme no autoestado correspondente à menor energia por meio da otimização dos parâmetros β, γ .

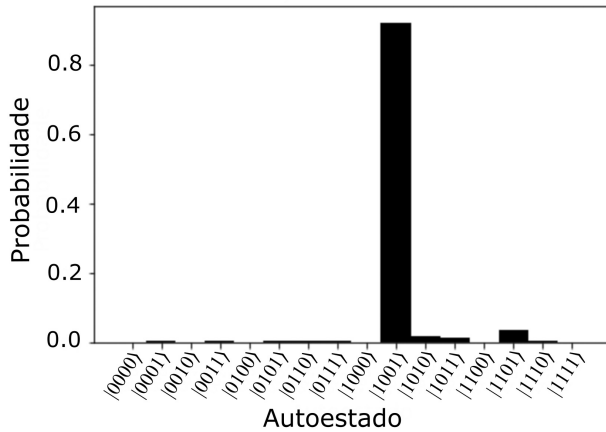


Figura 6: Histograma da distribuição de probabilidades de medição de cada estado da base computacional, considerando-se a solução ótima obtida pelo QAOA com 20 camadas.

Na Fig. 6 mostramos que, ao utilizar o QAOA com 20 camadas a solução ótima encontrada, sendo aquela com menor energia associada H_{\min} , representa o vetor $|1001\rangle$, que corresponde a uma carteira com incluindo Braskem ($x_1 = 1$) e Vale ($x_4 = 1$) e excluindo Itaú ($x_2 = 0$) e Klabin ($x_3 = 0$). Note que a probabilidade máxima, de quase 90%, é justamente aquela associada à solução do problema, o autoestado $|1001\rangle$, aquele com a menor energia para o Hamiltoniano considerado.

Assim, o resultado da otimização combinatória de portfólio encontrado usando o QAOA é condizente com a carteira ótima encontrada com o método clássico, embora seja válido mencionar novamente que são problemas semelhantes, porém distintos. Ocorre, ainda, que o QAOA é um método heurístico, de modo que não sabemos, de antemão, o melhor valor para o número de camadas. Além disto, a convergência pode variar para execuções distintas do algoritmo. Deste modo, investigamos, na Fig. 7, como a probabilidade de que o estado $|\psi(\beta, \gamma)\rangle$ encontrado pelo QAOA seja medido no autoestado fundamental $|1001\rangle$ varia com número de camadas após tomar a média das duas melhores dentre 10 execuções do código, ver Ref. [60]. Note que o comportamento não é monotônico, ou seja, aumentar o número de camadas nem sempre melhora a probabilidade associada ao vetor $|1001\rangle$ ser a solução ideal.

A mesma investigação pode ser feita olhando-se para a energia da solução encontrada pelo QAOA e compará-la com o valor mínimo associado ao vetor $|1001\rangle$, o que é apresentado na Fig. 8. Note que a energia tem um comportamento mais suave, porém também oscila mesmo tomando-se a média das duas melhores dentre 10 diferentes otimizações para um dado número de camadas. Notamos um comportamento assintótico em torno de 16 a 20 camadas.

Cabe mencionar que a qualidade da solução obtida por meio do QAOA para um determinado problema depende da performance do otimizador clássico usado

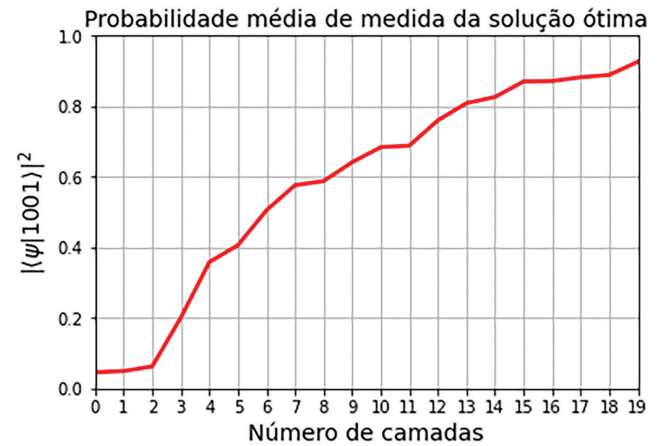


Figura 7: Probabilidade $|\langle \psi(\beta, \gamma) | 1001 \rangle|^2$ de que o estado encontrado pelo QAOA seja encontrado na solução ótima $|1001\rangle$, plotada em função do número de camadas no QAOA. Para cada número de camadas, consideramos uma média sobre as duas melhores dentre 10 otimizações.

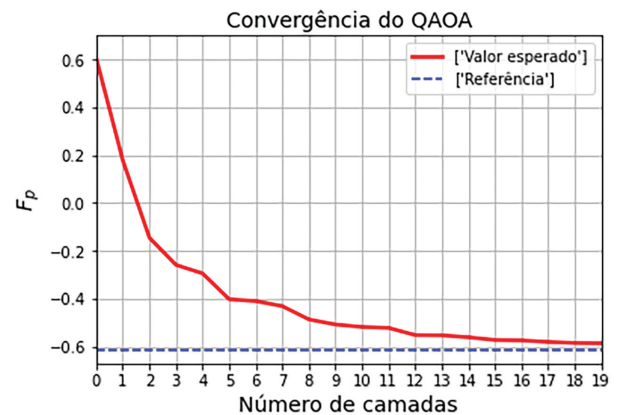


Figura 8: A energia da solução F_p (Eq. (34)) encontrada pelo QAOA como função do número de camadas. Como referência plotamos em azul a energia fundamental, associada ao autoestado $|1001\rangle$ do Hamiltoniano dado por $\langle H \rangle_{\min} = -0,6165$. Para cada número de camadas, consideramos uma média sobre as duas melhores dentre 10 otimizações.

para otimizar os parâmetros variacionais. Deste modo, nossa análise com relação ao número de camadas não é a mais ampla possível. Entretanto, foge ao escopo desse artigo comparar as soluções obtidas com distintos otimizadores como, por exemplo, COBYLA, BOBYQA, Nelder-Mead, SLSQP, SPSA, entre outros [93]. Fazendo uso do Jupyter Notebook disponível na Ref. [60], pode-se realizar extensivas simulações e, até mesmo, adaptar livremente o código para problemas de seu interesse.

Para este artigo, o QAOA foi implementado através do ATOS Quantum Learning Machine (QLM) [94] que é um ambiente de teste para a computação quântica desenvolvida pela empresa francesa ATOS e adquirido pelo SENAI CIMATEC para o desenvolvimento de algoritmos quânticos no Centro de Computação Quântica da América Latina. O dispositivo é capaz de simular até

35 qubits e inclui a simulação de ruídos, emulando a arquitetura de computadores quânticos reais. A escolha por trazer uma solução de certo modo completamente nacional visa fortalecer as colaborações e pesquisas científicas em tecnologias quânticas.

O QLM também possui interoperabilidade com outros frameworks de computação quântica, o que possibilita o uso de computadores quânticos através da plataforma. Além disso, o myQLM, framework disponibilizado gratuitamente, possibilita também o desenvolvimento e simulação de algoritmos quânticos por usuários domésticos, podendo ser instalado localmente. Por sua completeza, a utilização do QLM para o desenvolvimento de algoritmos de computação quântica se torna interessante, podendo ser utilizado em diferentes etapas do desenvolvimento de algoritmos quânticos. Algumas outras vantagens são: a existência de plug-ins especiais para realizar métodos variacionais orientados a era NISQ (como VQE, QAOA), bem como uma interface para conectar-se com os processadores quânticos disponíveis e as principais estruturas de programação quântica, tais como Qiskit, ProjectQ, Cirq etc.¹

6. Conclusão

Após um longo período sendo apenas uma área acadêmica, mais notadamente nas fronteiras da Física, a computação quântica tem atraído crescente atenção de governos, empresas e indústrias por suas promessas tecnológicas. Mesmo que um computador quântico com correção de erros ainda não seja uma realidade, o panorama traçado por empresas do setor mostram que tal feito pode ser alcançado. Em seu *roadmap* [95], a IBM aposta em chips quânticos com mais de 1000 qubits até 2023 e uma plataforma escalável atingindo 1 milhão de qubits até o final desta década. Em contrapartida, a IonQ planeja um computador quântico com mais de 1000 qubits [96], já com correção de erros, até 2028. Razão mais que suficiente para que comecemos a nos preparar e entendamos como estas máquinas quânticas de um futuro próximo poderão ser operadas.

Dentro deste contexto, o objetivo deste artigo foi o de apresentar um algoritmo de destaque na literatura, o QAOA, *Quantum Approximation Optimization Algorithm*, e uma de suas aplicações em um importante problema financeiro, a otimização de portfólios. Não só expusemos de forma concisa os principais conceitos, mas também fornecemos provas de princípio desta aplicação, considerando um problema simples com 4 ativos disponíveis na bolsa brasileira. Como forma de motivação, disponibilizamos um Jupyter Notebook com explicações

¹ Para instalação do myQLM recomendamos seguir a própria documentação do software, disponível em: https://myqlm.github.io/myqlm_specific/install.html. Na nossa documentação, também apresentamos um roteiro de como fazer a instalação: <https://github.com/askery/computacao-quantica-aplicada-ao-mercado-financeiro>

detalhadas do mercado financeiro e dos algoritmos tanto clássico quanto quânticos que foram utilizados.

A segunda revolução quântica, com dispositivos tecnológicos que exploram toda a capacidade informacional da mecânica quântica, já é uma realidade. Esperamos que este artigo possa impulsionar ainda mais esta área em nosso país, que apesar de grande qualidade acadêmica no tema, ainda carece de uma maior integração com setores privados da sociedade. A ciência quântica promete moldar o desenvolvimento de tecnologias do século 21. Ainda é tempo para que o Brasil reassuma sua posição de destaque neste tema.

Agradecimentos

Agradecemos ao Instituto Serrapilheira (Grant n. Serra-1708-15763), a John Templeton Foundation via o projeto Q-CAUSAL No 61084, a Simons Foundations (Grant Number 884966, AF), ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) por meio do Instituto Nacional de Ciência e Tecnologia de Informação Quântica (INCT-IQ) e das Bolsas: (N. 423713/2016-7, N. 307172 / 2017-1, N. 406574 / 2018-9 e N. 307295/2020-6), ao Ministério da Ciência, Tecnologia e Inovação do Brasil, e Comunicações (MCTIC) e ao Ministério da Educação (MEC). A.C. agradece à Universidade Federal de Alagoas (UFAL) por um licença de cooperação científica na Universidade Federal do Rio Grande do Norte (UFRN).

Referências

- [1] M. Kumar, *Quantum: Einstein, Bohr and the great debate about the nature of reality* (Icon Books Ltd, London, 2008).
- [2] R. Chaves, *Incerteza Quântica: O mistério de uma teoria e a nova era da informação* (Editora Zahar, Grupo Companhia das Letras, Rio de Janeiro, 2022).
- [3] A. Einstein, B. Podolsky e N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [4] E. Schrödinger, *Proceedings of the American Philosophical Society* **124**, 323 (1935).
- [5] J. Bell, *Physics Physique Fizika* **1**, 195 (1964).
- [6] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten e C. Abellán, *Nature* **526**, 682 (2015).
- [7] M. Giustina, M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Larsson e C. Abellán, *Physical Review Letters* **115**, 250401 (2015).
- [8] A. Turing, *Proceedings of the London Mathematical Society* **42**, 230 (1936).
- [9] C. Shannon, *The Bell System Technical Journal* **27**, 379 (1948).
- [10] R. Feynman, *International Journal of Theoretical Physics* **21**, 467 (1982).
- [11] A. Caldeira, *Rev. Bras. Ensino Fís.* **40**, e4211 (2018).
- [12] P. Benioff, *Journal of Statistical Physics* **22**, 563 (1980).

- [13] P. Benioff, *Journal of Statistical Physics* **29**, 515 (1982).
- [14] D. Deutsch, *A. Mathematical and Physical Sciences* **400**, 97 (1985).
- [15] C. Bennett e G. Brassard, *Theoretical Computer Science* **560**, 7 (2014).
- [16] W. Wootters e W. Zurek, *Nature* **299**, 802 (1982).
- [17] P. Shor, *SIAM Journal On Computing* **26**, 1484 (1997).
- [18] L. Grover, *Physical Review Letters* **79**, 325 (1997).
- [19] C. Chang, A. Gambhir, T. Humble e S. Sota, *Scientific Reports* **9**, 1 (2019).
- [20] I. Georgescu, S. Ashhab e F. Nori, *Reviews of Modern Physics* **86**, 153 (2014).
- [21] N. Gisin e R. Thew, *Nature Photonics* **1**, 165 (2007).
- [22] C. Degen, F. Reinhard e P. Cappellaro, *Reviews of Modern Physics* **89**, 035002 (2017).
- [23] F. Arute, K. Arya, R. Babbush, D. Bacon, J. Bardin, R. Barends, R. Biswas, S. Boixo, F. Brandao e D. Buell, *Nature* **574**, 505 (2019).
- [24] J. Preskill, *Quantum* **2**, 79 (2018).
- [25] A. Bouland, W. Dam, H. Joorati, I. Kerenidis e A. Prakash, arXiv:2011.06492 (2020).
- [26] E. Farhi, J. Goldstone e S. Gutmann, arXiv:1411.4028 (2014).
- [27] A. Peruzzo, J. McClean, P. Shadbolt, M. Yung, X. Zhou, P. Love, A. Aspuru-Guzik e J. O'Brien, *Nature Communications* **5**, 1 (2014).
- [28] J. McClean, J. Romero, R. Babbush e A. Aspuru-Guzik, *New Journal of Physics* **18**, 023023 (2016).
- [29] M. Born e V. Fock, *Zeitschrift Für Physik* **51**, 165 (1928).
- [30] T. Kato, *Journal of the Physical Society of Japan* **5**, 435 (1950).
- [31] E. Farhi, J. Goldstone, S. Gutmann e M. Sipser, arXiv:quant-ph/0001106 (2000).
- [32] P. O'Malley, R. Babbush, I. Kivlichan, J. Romero, J. McClean, R. Barends, J. Kelly, P. Roushan, A. Tranter e N. Ding, *Physical Review X* **6**, 031007 (2016).
- [33] B. Bauer, S. Bravyi, M. Motta e G. Chan, *Chemical Reviews* **120**, 12685 (2020).
- [34] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe e S. Lloyd, *Nature* **549**, 195 (2017).
- [35] G. Paparo, M. Müller, F. Comellas e M. Martin-Delgado, *Scientific Reports* **3**, 1 (2013).
- [36] D. Egger, C. Gambella, J. Marecek, S. McFaddin, M. Mevissen, R. Raymond, A. Simonetto, S. Woerner e E. Yndurain, *IEEE Transactions On Quantum Engineering* **1**, 1 (2020).
- [37] R. Orús, S. Mugel e E. Lizaso, *Reviews in Physics* **4**, 100028 (2019).
- [38] B. Baaquie, *Journal De Physique I* **7**, 1733 (1997).
- [39] E. Haven, *Physica A: Statistical Mechanics and its Applications* **304**, 507 (2002).
- [40] Z. Jiang, A. Canabarro, B. Podobnik, H. Stanley e W. Zhou, *Quantitative Finance* **16**, 1713 (2016).
- [41] Z. Jiang, G. Wang, A. Canabarro, B. Podobnik, C. Xie, H. Stanley e W. Zhou, *Quantitative Finance* **18**, 353 (2017).
- [42] A. Canabarro, S. Brito e R. Chaves, *Phys. Rev. Lett.* **122**, 200401 (2019).
- [43] A. Canabarro, F. Fanchini, A. Malvezzi, R. Pereira e R. Chaves, *Phys. Rev. B* **100**, 045129 (2019).
- [44] C. Goes, A. Canabarro, E. Duzzioni e T. Maciel, *Quantum Information Processing* **20**, 99 (2021).
- [45] D. Egger, J. Mareček e S. Woerner, *Quantum* **5**, 479 (2021).
- [46] <https://dualq.tech>, acesso em: 20/06/2022.
- [47] <https://www.multiversecomputing.com/>, acesso em: 20/06/2022.
- [48] G. Jesus, M. Silva, T. Netto, L. Galvão, F. Souza e C. Cruz, *Rev. Bras. Ensino Fís.* **43**, e20210033 (2021).
- [49] A. Oliveira, A. Santos e C. Villas-Boas, *Rev. Bras. Ensino Fís.* **44**, e20210333 (2022).
- [50] W. Rabelo e M. Costa, *Rev. Bras. Ensino Fís.* **40**, e4306 (2018).
- [51] M. José, J. Piqueira e R.D. Lopes, *Rev. Bras. Ensino Fís.* **35**, 1 (2013).
- [52] A. Santos, *Rev. Bras. Ensino Fís.* **39**, e1301 (2016).
- [53] H. Markowitz, *The Journal of Finance* **7**, 77 (1952).
- [54] G. Rosenberg, P. Haghnegahdar, P. Goddard, P. Carr, K. Wu e M. Prado, *IEEE Journal of Selected Topics in Signal Processing* **10**, 1053 (2016).
- [55] J. Cohen, A. Khan e C. Alexander, arXiv:2007.01430 (2020).
- [56] D. Venturelli, D. Marchand e G. Rojo, arXiv:1506.08479 (2016).
- [57] P. Rebentrost, B. Gupt e T. Bromley, *Phys. Rev. A* **98**, 022321 (2018).
- [58] I. Kerenidis, A. Prakash e D. Szilágyi, arXiv:1908.08040 (2019).
- [59] M. Hodson, B. Ruck, H. Ong, D. Garvin e S. Dulman, arXiv:1911.05296 (2019).
- [60] <https://github.com/askery/computacao-quantica-apli-cada-ao-mercado-financeiro>
- [61] B. Schumacher, *Physical Review A* **51**, 2738 (1995).
- [62] M. Nielsen e I. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2011).
- [63] R. Raussendorf, D. Browne e H. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [64] M. Nielsen, *Reports On Mathematical Physics* **57**, 147 (2006).
- [65] P. Zanardi e M. Rasetti, *Physics Letters A.* **264**, 94 (1999).
- [66] A. Kitaev, *Annals of Physics* **303**, 2 (2003).
- [67] T. Albash e D. Lidar, *Reviews of Modern Physics* **90**, 015002 (2018).
- [68] J. Roland e N. Cerf, *Physical Review A.* **65**, 042308 (2002).
- [69] S. Kirkpatrick, C. Gelatt e M. Vecchi, *Science* **220**, 671 (1983).
- [70] D. Aharonov, W.V. Dam, J. Kempe, Z. Landau, S. Lloyd e O. Regev, *SIAM Review* **50**, 755 (2008).
- [71] <https://bityli.com/Kosxl>, acessado: 08/09/2021.
- [72] P.J. Souza, T.M. Mendonça, E.V.B. Oliveira e C.J. Villas-Boas, *Rev. Bras. Ensino Fís.* **43**, e20210049 (2021).
- [73] P. Wilmott, *Introduces Quantitative Finance* (Wiley, Hoboken, 2007).

- [74] V. Ziemann, *Physics and Finance* (Springer International Publishing, New York, 2021).
- [75] https://www.b3.com.br/pt_br/market-data-e-indices/indices/indices-de-segmentos-e-setoriais/di/metodologia-de-calculo-acumulado-de-di/, acesso em: 20/06/2022.
- [76] https://www.b3.com.br/pt_br/market-data-e-indices/indices/indices-de-segmentos-e-setoriais/serie-historica-do-di.htm, acesso em: 20/06/2022.
- [77] W.F. Sharpe, *The Journal of Business* **39**, 119 (1966).
- [78] K. Bharti, A. Cervera-Lierta, T.H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J.S. Kottmann, T. Menke, W.K. Mok et al., arXiv:2101.08448 (2021).
- [79] N. Moll, P. Barkoutsos, L.S. Bishop, J.M. Chow, A. Cross, D.J. Egger, S. Filipp, A. Fuhrer, J.M. Gambetta, M. Ganzhorn, *Quantum Science and Technology* **3**, 030503 (2018).
- [80] D.J. Egger, R.G. Gutiérrez, J.C. Mestre e S. Woerner, arXiv:1907.03044 (2019).
- [81] S. Woerner e D.J. Egger, *Npj Quantum Information* **5**, 15 (2019).
- [82] N. Stamatopoulos, D.J. Egger, Y. Sun, C. Zoufal, R. Iten, N. Shen e S. Woerner, *Quantum* **4**, 291 (2020).
- [83] C. Zoufal, A. Lucchi e S. Woerner, *Npj Quantum Information* **5**, 103 (2019).
- [84] <https://br.investing.com/rates-bonds/world-government-bonds>, acesso em: 20/06/2022.
- [85] <https://zenodo.org/record/4660156#.Y0luCXbMKUk>
- [86] E. Farhi e A.W. Harrow, arXiv:1602.07674 (2016).
- [87] J.A. Pople, *Theoretical Models for Chemistry, Proceedings of the Summer Research Conference on Theoretical Chemistry, Energy Structure and Reactivity* (John Wiley & Sons, New York, 2008).
- [88] A. Dalzell, A. Harrow, D. Koh e R. La Placa, *Quantum* **4**, 264 (2020).
- [89] M. Suzuki, *Communications in Mathematical Physics* **51**, 183 (1976).
- [90] M. Suzuki, *Progress of Theoretical Physics* **56**, 1454 (1976).
- [91] M. Suzuki, *Communications in Mathematical Physics* **57**, 193 (1977).
- [92] M. Suzuki, *Journal of Mathematical Physics* **26**, 601 (1985).
- [93] S. Khairy, R. Shaydulin, L. Cincio, Y. Alexeev e P. Balaprakash, *Proceedings of the AAAI Conference On Artificial Intelligence* **34**, 2367 (2020).
- [94] <https://myqlm.github.io/index.html>, acesso em: 20/06/2022.
- [95] <https://research.ibm.com/blog/ibm-quantum-roadmap>
- [96] <https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap>, acesso em: 20/06/2022.