KIT QUANTUM (Q)

Computação Quântica:

Laboratório para Alunos do Ensino Médio

Manual do professor

WS2

WOMEN SUPPORTING
WOMEN IN THE SCIENCES

Declaração de missão

A missão deste laboratório é ensinar alunos do ensino médio (idades entre 12 e 18 anos) sobre conceitos de computação quântica por meio de experimentos relacionados à mecânica quântica.

Indice

1. Introdução aos kits de laboratório WS2

1.1. Informações sobre WS2

A Women Supporting Women in the Sciences (WS2), uma organização internacional que une e apoia mulheres de nível de pós-graduação e profissional e aliadas em ciência, tecnologia, engenharia e matemática (STEM), recebeu um Fundo de Inovação da Sociedade Americana de Física (APS) em 2020 para formar equipes internacionais para projectar e distribuir kits de laboratório de física e ciência dos materiais de baixo custo para alunos do ensino fundamental e médio, predominantemente na África Oriental. Os kits de laboratório utilizaram recursos locais e incluíram tópicos especialmente relevantes para meninas, a fim de estimular seu interesse em disciplinas STEM. De 2020 a 2023, mais de 5.100 alunos da África Oriental em mais de 40 escolas se envolveram com nossos kits de laboratório, sendo 62% meninas.

A WS2 recebeu seu segundo Fundo de Inovação da APS em 2025 para apoiar outra Iniciativa de Kits de Laboratório, desta vez com foco em tópicos quânticos. Para mais informações sobre a WS2, visite nosso site em ws2global.org.

O WS2 é patrocinado pelo Fundo de Inovação da APS, pelo Fórum de Educação da APS, pelo Centro de Pesquisa em Ciência e Engenharia de Materiais da Northwestern University e pelo Departamento de Assuntos Estudantis Multiculturais da Northwestern University. O WS2 é extremamente grato aos voluntários responsáveis pelo projecto do kit de laboratório (John Bakayana, Celline Omondi, Alice Flarend, Elvira Khwatenge, Babra Mwimali e Sserugo Enock) e aos consultores externos (SciBridge e Projekt Inspire) por sua orientação. O WS2 também agradece e reconhece o PhysicsQuest (https://www.aps.org/initiatives/physics-education/physicsquest) e o Quantum Explorations Student Toolbox (QuEST) pelos experimentos que serviram de base para o conteúdo do kit de laboratório.

1.2. Informações sobre este Kit

Bem-vindo ao emocionante mundo da ciência quântica — um reino onde partículas podem estar em vários lugares ao mesmo tempo, a luz se comporta tanto como onda quanto como partícula e objectos distantes podem influenciar uns aos outros instantaneamente. Parece ficção científica, mas não é!

Este manual foi elaborado para guiá-lo por experimentos práticos simples que dão vida a alguns dos conceitos mais fascinantes da física quântica. Usando materiais do dia a

dia, você explorará grandes ideias como superposição, interferência e entrelaçamento — conceitos que desafiam nossa compreensão clássica de como o universo funciona.

Não se preocupe se esses termos forem novos ou complicados. Cada experimento inclui:

- Declaração clara do propósito para indicar o que você está aprendendo
- Perguntas pré-laboratoriais para fazer você pensar
- Procedimentos passo a passo que você pode seguir com facilidade
- Ferramentas simples que você provavelmente já tem em casa ou na sala de aula
- Tabelas de observação para registar seus resultados
- Perguntas pós-experimento bem pensadas para ajudar a conectar o que você viu aos mistérios da ciência quântica

Esses experimentos têm como objectivo despertar a curiosidade, a criactividade e o pensamento mais profundo. Você não precisa ser físico (ainda!) para apreciá-los — basta ter a mente aberta, um senso de admiração e a disposição para explorar ideias que expandam os limites do que consideramos possível. Ao realizar essas actividades, lembre-se: até os cientistas mais famosos começaram fazendo perguntas simples e realizando pequenos experimentos. Quem sabe a que descobertas sua curiosidade pode levar?

1.3. Usando o Guia

Este manual deve ser utilizado pelo professor ou facilitador do kit de laboratório e possui conteúdo semelhante ao manual do aluno, mas pode conter material adicional, a saber: Conceitos Fundamentais de Ciências Abordados, Habilidades Práticas, Resumo de Experimentos, Pré-Laboratório do Professor e Solução de Problemas. Essas seções adicionais visam fornecer ao professor o conhecimento e a base essenciais para a implementação bem-sucedida deste kit de laboratório em sala de aula. Recomenda-se que os professores deste kit de laboratório leiam o guia do início ao fim para se familiarizarem com o conteúdo antes de ensinar o kit de laboratório aos alunos. Dúvidas sobre o conteúdo podem ser direcionadas a qualquer momento para ws2global.org@gmail.com, usando o assunto "Dúvidas sobre o Conteúdo do Kit de Laboratório".

<u>OBSERVAÇÕES IMPORTANTES:</u>

- Este kit de laboratório destina-se ao uso com alunos do ensino médio (idades entre 12 e 18 anos), mas, dependendo da formação educacional específica dos alunos, o conteúdo pode precisar ser modificado pelo professor para torná-lo mais simples ou mais complexo. O professor também é incentivado a abordar o conteúdo no ritmo que for mais adequado para os alunos; alguns alunos mais jovens podem precisar de mais tempo e atenção do professor e/ou facilitador para analisar as questões e os experimentos, enquanto alunos mais velhos podem ser mais independentes e exigir menos atenção do professor e/ou facilitador. Portanto, o conteúdo abordado, a profundidade da abordagem e o ritmo ficam a critério do professor e/ou facilitador.
- O conteúdo deste manual de kit de laboratório pode não se adequar ao currículo específico da escola em que está sendo ensinado. Fica a critério do(s) facilitador(es) e do(s) professor(es) se desejam introduzir novos conteúdos ou pular determinadas seções que não se aplicam às suas salas de aula.
- Em certas áreas, pode ser necessário fazer modificações na lista de materiais, dependendo da disponibilidade de materiais na área específica em que o laboratório está sendo ministrado. Tentamos listar algumas alternativas na lista de materiais, mas entendemos que esta lista de alternativas não é exaustiva.
- Nos experimentos, os alunos são divididos em grupos de três a quatro. Se os materiais permitirem, os alunos podem ser divididos em grupos de dois.

1.4. Vocabulário-chave

- Bit (clássico): os 0s e 1s que os computadores clássicos tradicionais usam
- Qubit (bit quântico): unidade fundamental de informação quântica na computação quântica que pode existir como 0 ou 1 simultaneamente
- Medição: o processo de colapso do estado de superposição de um qubit em um estado definido (0/1)
- Superposição: um sistema (como um qubit) que existe em múltiplos estados simultaneamente até ser medido
- Entrelaçamento: a ligação de estados em objectos, independentemente da distância entre eles
- Porta quântica: um dispositivo que altera o estado quântico de um qubit
- Criptografia quântica: um método de comunicação segura que codifica mensagens em qubits

1.5. Perguntas-chave

- O que é um qubit e como ele difere de um bit clássico?
    - <u>Resposta:</u> *As diferenças fundamentais entre bits clássicos e qubits residem em seu comportamento, capacidades e física subjacente.*
        - *Um bit clássico existe em um estado definitivo de 0 ou 1, muito parecido com um interruptor de luz tradicional que está ligado ou desligado. Em nítido contraste, um qubit opera no reino quântico, onde pode incorporar simultaneamente os estados 0 e 1 por meio de superposição – uma propriedade quântica fundamental que não possui equivalente clássico.*
        - *Embora os sistemas clássicos não consigam atingir a superposição, esse fenômeno permite que os qubits processem informações em paralelo em múltiplos estados. O entrelaçamento, outra exclusividade quântica, permite que os qubits formem estados interconectados que permanecem correlacionados mesmo quando separados por grandes distâncias, criando um poderoso recurso computacional ausente na computação clássica.*
        - *A capacidade de informação é escalável de forma drasticamente diferente entre os dois sistemas: os bits clássicos armazenam dados em unidades discretas de 1 bit, enquanto os qubits utilizam a mecânica quântica para atingir o potencial de escalonamento exponencial. Essa capacidade de processamento paralelo e correlação quântica forma a base do poder revolucionário da computação quântica.*
- O que é superposição?
    - <u>Resposta:</u> *A superposição não é análoga a uma moeda lançada (que cai como cara ou coroa). Em vez disso, ela representa um sistema quântico que existe em múltiplos estados simultaneamente até ser medido. Por exemplo, o spin de um elétron não é meramente "desconhecido", mas está genuinamente nos estados de spin para cima e para baixo ao mesmo tempo.*

- Como um computador quântico difere de um computador clássico que usa números binários 0 e 1?
    - <u>Resposta:</u> *Computadores clássicos processam dados binários sequencialmente. Computadores quânticos usam superposição para explorar múltiplas soluções simultaneamente e entrelaçamento para*

correlacionar os estados dos qubits. Por exemplo, enquanto um sistema clássico de 2 bits pode representar quatro estados (00, 01, 10, 11) um de cada vez, dois qubits em superposição podem representar todos os quatro simultaneamente.

1.6. Objectivo

O objectivo deste manual de laboratório é aprender sobre computação quântica por meio de experimentos e actividades. Os alunos aprenderão a diferença entre bits clássicos e qubits e os conceitos de superposição e entrelaçamento. Os alunos também participarão de actividades que os ensinarão sobre criptografia quântica e computação quântica por meio de jogos e analogias.

1.7. Conceitos científicos fundamentais abordados

Este kit de laboratório apresenta os tópicos de computação quântica e criptografia quântica, relevantes para diversas áreas, incluindo Física e Computação, para alunos do ensino fundamental e médio/secundário. Especificamente, o kit de laboratório incentiva os alunos a refletir sobre os princípios por trás da computação quântica e como ela difere da computação clássica, explorando conceitos-chave como superposição, interferência de ondas e entrelaçamento por meio de jogos e actividades. Os alunos obterão as seguintes conclusões principais: (1) superposição significa que algo pode existir em múltiplos estados simultaneamente antes da medição; (2) fótons polarizados passados por um canal quântico formam a base para a criação de uma chave segura em certos protocolos de criptografia quântica; (3) portas quânticas utilizam superposição e entrelaçamento para manipular o estado e a fase do qubit de maneiras não acessíveis por portas de computação clássicas.

1.8. Habilidades práticas

- Os alunos compreenderão como os computadores clássicos são diferentes dos computadores quânticos.
- Os alunos ganharão experiência com probabilidade e aleatoriedade no contexto da estatística.
- Os alunos utilizarão lógica e regras para prever resultados.

2. Contexto dos Tópicos Principais

2.1. Bits quânticos (Qubits) e computadores quânticos

A computação quântica, que utiliza propriedades da mecânica quântica, é procurada porque pode realizar cálculos impossíveis para computadores clássicos. Como funciona um computador tradicional? Computadores tradicionais processam informações usando unidades fundamentais de dados chamadas bits clássicos (0s ou 1s). Esses bits são manipulados por meio de operações lógicas que permitem ao computador concluir tarefas simples e complexas. Como um computador quântico é diferente? Ao contrário dos bits clássicos que representam 0 ou 1, os bits quânticos, ou qubits, em computadores quânticos podem existir em superposição, que é um estado em que o bit existe como 0 e 1 simultaneamente (veja a Figura 1). Para colapsar um estado de superposição, o qubit é medido, o que significa que o qubit não é mais 0 e 1 simultaneamente, mas sim um 0 ou 1 definido.

Qual é outra maneira de pensar sobre superposição? Imagine um interruptor de luz. Ele pode estar LIGADO (1) ou DESLIGADO (0). É como um bit de computador tradicional. Agora, imagine um interruptor de luz especial que pode estar LIGADO, DESLIGADO ou ambos ao mesmo tempo! Isso seria como um qubit. Essa capacidade de superposição "dos dois ao mesmo tempo" é o que dá poder aos computadores

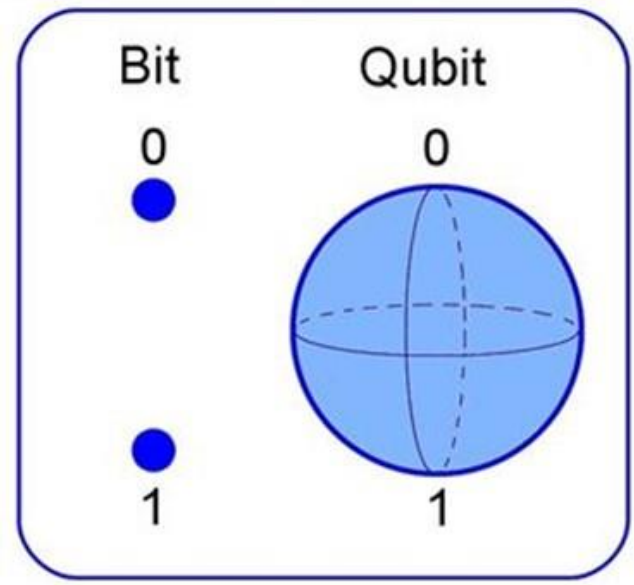


Figura 1. Ilustração do bit clássico (esquerda) e do qubit (direita). O bit clássico pode ser 0 ou 1, e o qubit pode existir em superposição como 0 e 1 simultaneamente. Esta foto de autor desconhecido está licenciada sob CC BY.

quânticos. Enquanto os computadores tradicionais só conseguem processar bits tradicionais (0 ou 1), os computadores quânticos podem processar 0, 1 ou ambos, o que significa que podem explorar múltiplas possibilidades simultaneamente.

Assim como os computadores tradicionais, os computadores quânticos seguem conjuntos de instruções chamados algoritmos que empregam portas lógicas para manipular bits em uma ordem específica. Em vez de usar portas clássicas (como "E", "OU"), os computadores quânticos usam portas lógicas quânticas, que são dispositivos que manipulam qubits usando a mecânica quântica. Por exemplo, uma porta de Hadamard coloca um qubit em um estado de superposição (0 e 1).

Quais são outros fenômenos da mecânica quântica que os computadores quânticos utilizam? O entrelaçamento, que é a ligação de estados (como qubits), independentemente da distância entre eles, é usado em computadores quânticos para criar algoritmos quânticos e métodos de comunicação poderosos. Se você se lembrar da analogia do interruptor de luz da superposição, imagine dois interruptores de luz entrelaçados. Se você acionar um, o outro também aciona instantaneamente, mesmo que estejam distantes! Essa é uma conexão assustadora!

Como os computadores quânticos podem ser úteis em nossas vidas? Como os computadores quânticos podem explorar múltiplas possibilidades simultaneamente com qubits, eles podem trabalhar de forma mais rápida e eficiente do que os computadores tradicionais. Isso pode ser extremamente útil em diversos campos, incluindo descoberta de medicamentos, ciência dos materiais e inteligência artificial. Os computadores quânticos também podem ser usados em criptografia, que é a forma como as informações são protegidas contra acesso não autorizado. A criptografia clássica usa matemática para embaralhar mensagens. A criptografia quântica usa qubits e mecânica quântica para criar códigos inquebráveis. Se alguém tentar espionar uma mensagem quântica, o espião perturbará os qubits e o remetente saberá que alguém está ouvindo!

3. Resumo dos Experimentos

Este kit de laboratório consiste em um experimento, duas actividades, um procedimento complementar opcional de programação de computadores e um desafio de design para compreender conceitos relacionados à computação quântica. Esta investigação começará fornecendo informações básicas relevantes sobre computação quântica, antes de demonstrar os fenômenos que surgem nesses sistemas. Se sua escola não tiver acesso a computadores, a Actividade Complementar pode ser ignorada. Os objectivos dos experimentos e do desafio de design são os seguintes:

Parte I: Demonstrar a superposição com o lançamento de uma moeda e o colapso da superposição com sua medição

Parte II: Compreender o protocolo de criptografia quântica BB84 usando doces e cores para representar fótons e polarização

Parte III: Demonstrar portas de computação quântica, que incluem superposição e entrelaçamento de qubits, usando um jogo

Desafio de Design: Projectar um desafio que altere o estado e a fase de um qubit usando portas de computação quântica

3.1. Lista de suprimentos

- Moedas (de metal com dois lados distintos)
- Copos opacos
- Papel
- Doces embrulhados (ou pequenos pedaços de papel)
- Baldes ou potes
- Marcadores
- Fita adesiva colorida (vermelha e verde) (outras duas cores também podem ser usadas)
- Guarde as peças do jogo do Gato de Schrödinger para cada grupo:
    - 8 fichas de gato azul/gato vermelho para actuarem como qubits
    - 8 fichas de gato amarelo/gato verde para actuarem como qubits
    - 2 portas X
    - 2 portas Y
    - 2 portas X
    - 2 portas S
    - 2 portas H
    - 1 porta CNOT
    - 1 tabela de mudança de fase da porta de qubit
    - 1 tabela de interferência de qubit
- Tesoura
- Fita adesiva transparente

3.2. Informações de segurança

Antes de os alunos iniciarem o laboratório, levem em consideração as seguintes questões de segurança:

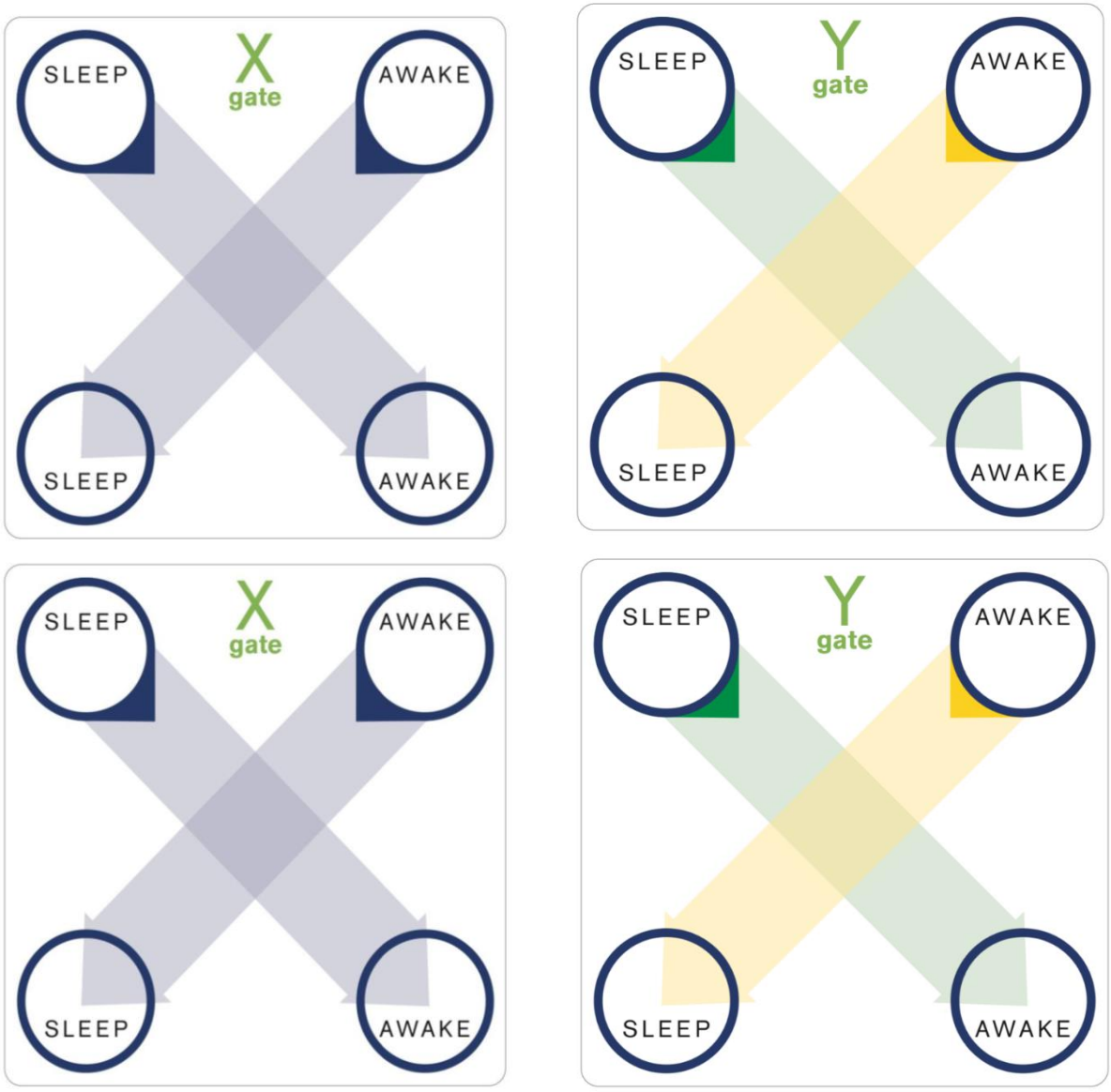
- Este kit de laboratório não apresenta grandes preocupações de segurança associadas a ele.

3.3. Pré-laboratório do professor

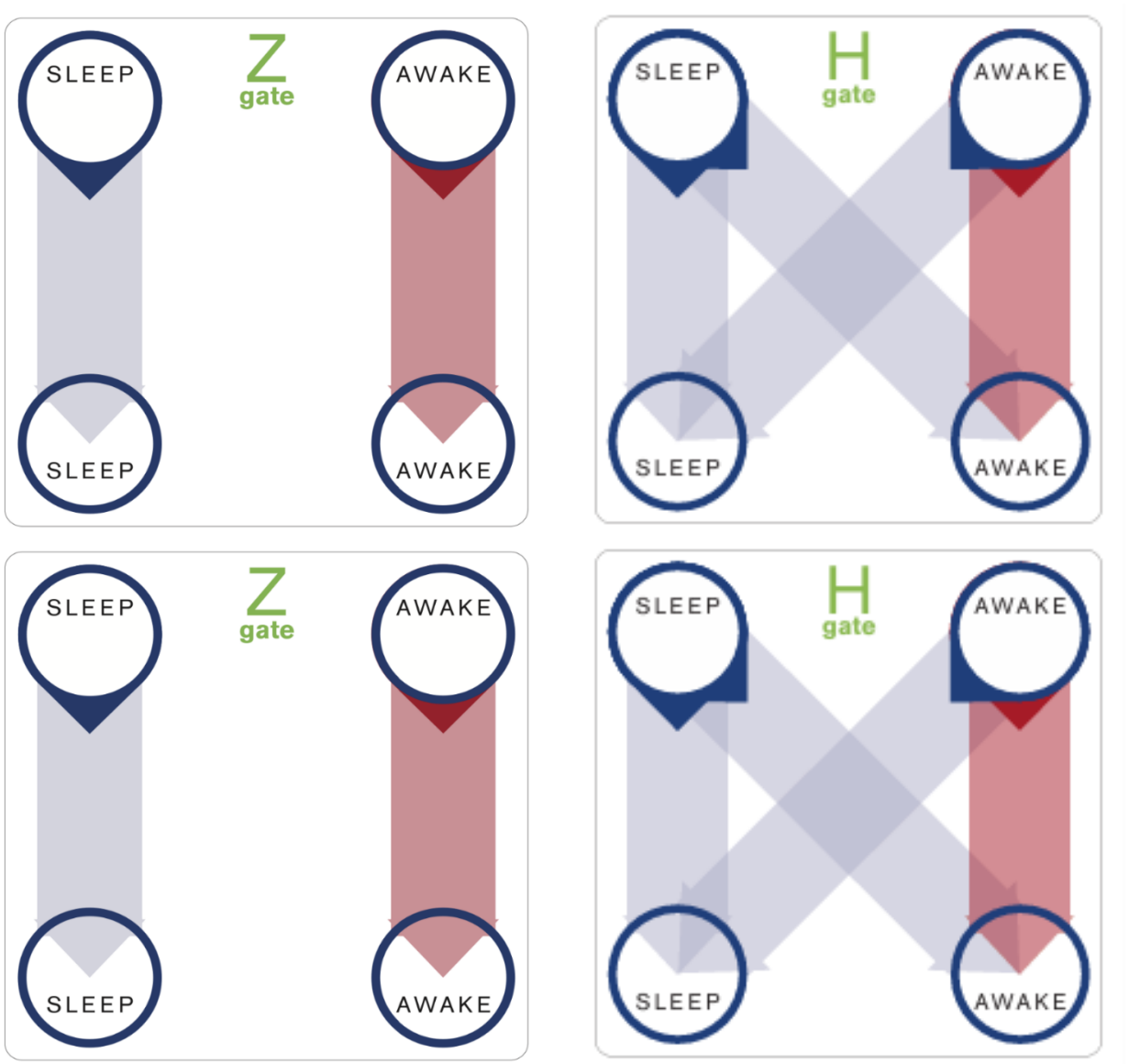
Os professores podem organizar os materiais para os experimentos e actividades com antecedência. Para cada aluno ou grupo de 2 a 4 alunos, os materiais necessários são: 1 moeda (com dois lados distintos), 1 copo opaco, 40 balas embrulhadas (ou 40 pedaços de papel), 2 baldes ou potes, as peças do jogo para a Parte III (veja abaixo) e uma caneta ou lápis. Deve haver fita adesiva colorida e marcadores que a turma possa partilhar. Se estiver realizando a actividade suplementar opcional, cada grupo deve ter acesso a um computador com Python instalado, ou o professor pode projectar o programa para os alunos em uma tela ou quadro.

Os professores podem assistir a uma demonstração do jogo na Parte III no YouTube em https://www.youtube.com/watch?v=1OEqjGWOUhM. Os professores devem imprimir e preparar o seguinte para cada grupo para a Parte III:

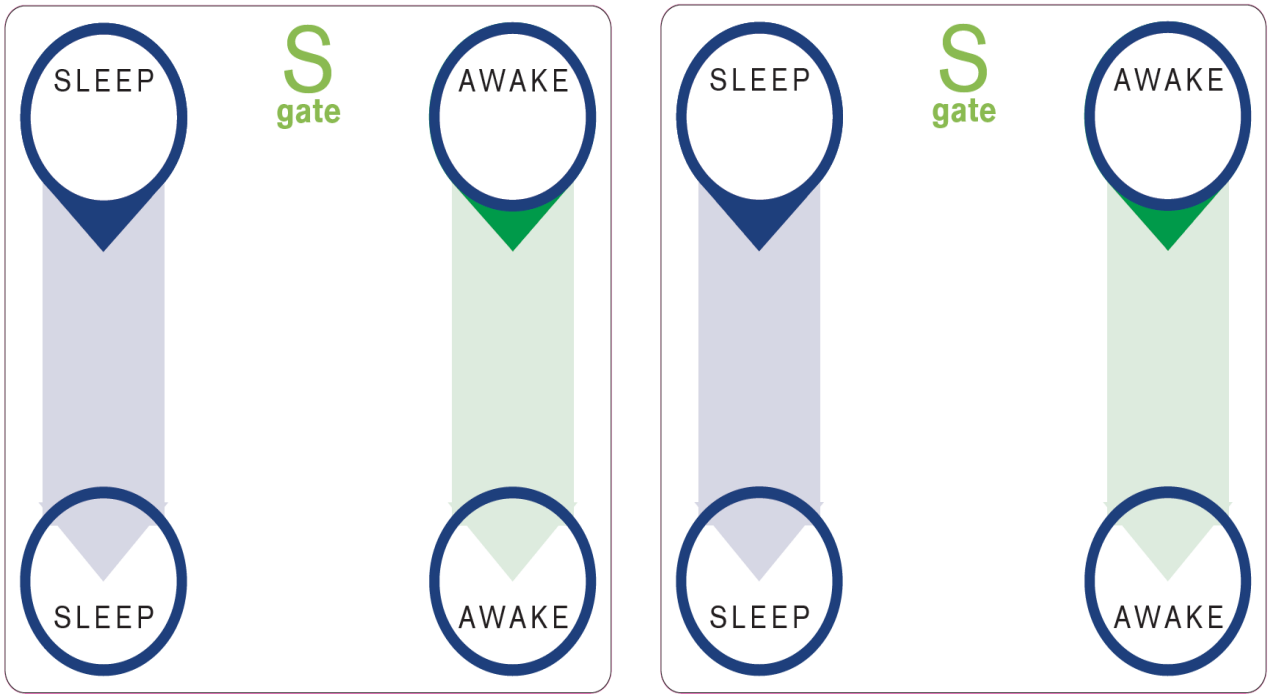
Esses gatos devem ser cortados em 16 fichas (vermelho/azul e amarelo/verde) e então dobrados e presos com fita adesiva de modo que um lado mostre vermelho e o outro lado mostre azul para 8 fichas e um lado mostre amarelo e o outro lado mostre verde para as outras 8 fichas.



Elas podem ser cortadas em 4 portas distintas (2 X e 2 Y).

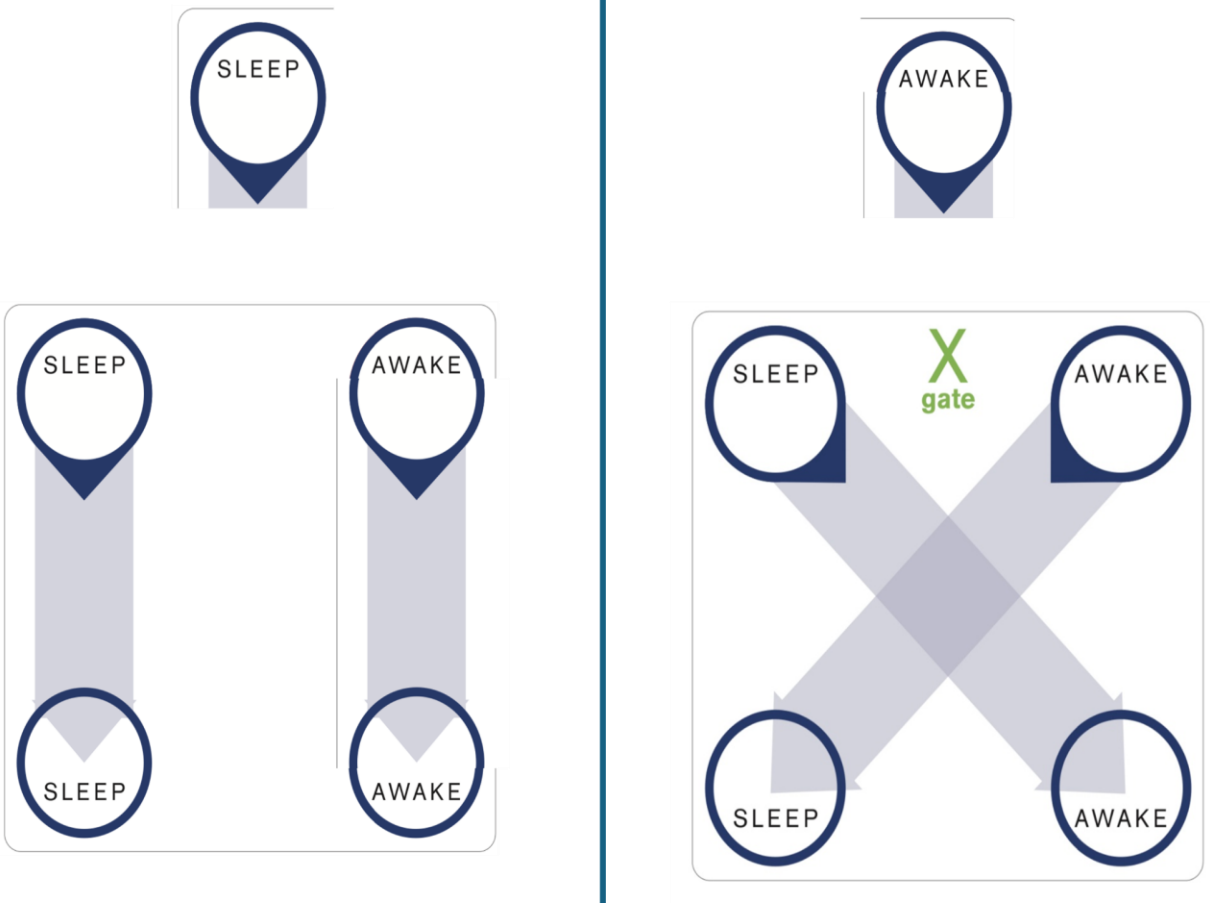


Elas podem ser cortadas em 4 portas distintas (2 Z e 2 H).

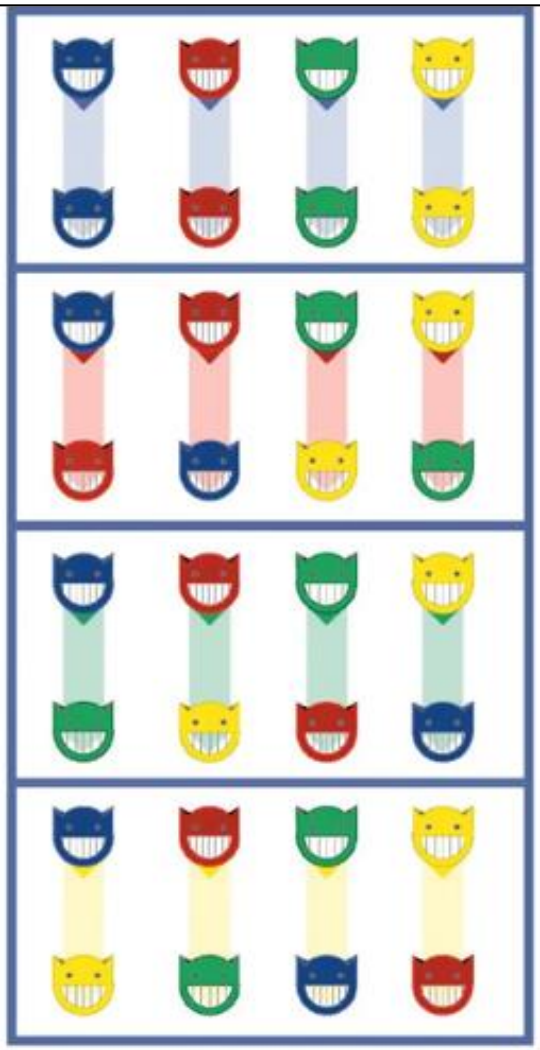


Eles podem ser cortados em 2 portas distintas (2 S).

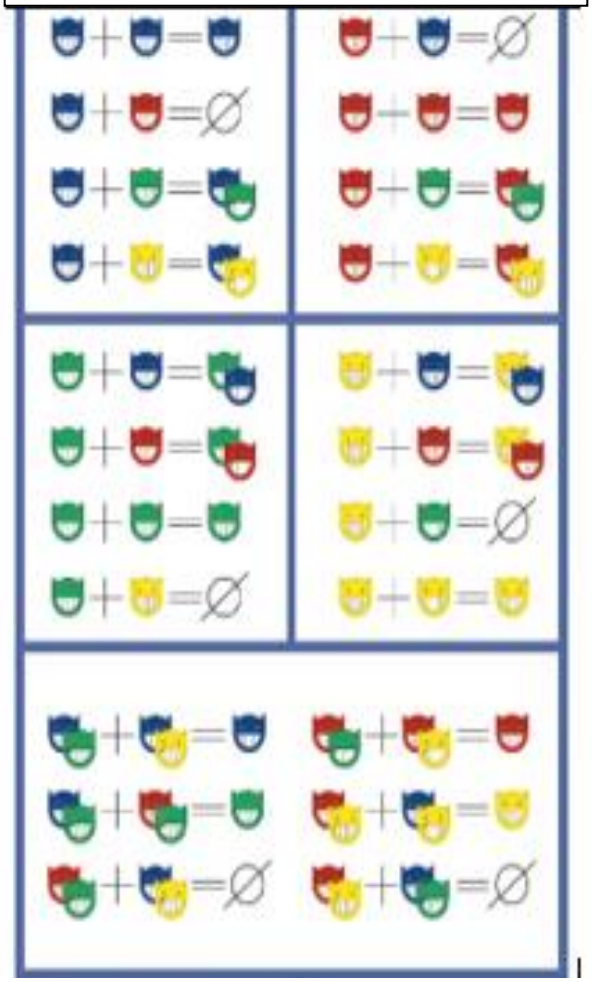
CNOT



mudanças de fase para caminhos de



interferência de qubits



4. Experimentos

Nota para professores:

Incentive a discussão aberta e as perguntas da turma ao apresentar os experimentos.

4.1. Parte I. Cara ou coroa quântica

4.1.1. *Questões pré-experimento*

1. O que significa um sistema quântico estar em estado de superposição? Como isso difere dos sistemas clássicos?
    a. *Resposta: Superposição significa que um sistema quântico (como uma partícula) existe em uma combinação de todos os estados possíveis simultaneamente, descritos por uma onda de probabilidade. Por exemplo, um elétron em um átomo não está em um único local, mas existe como uma "nuvem" de probabilidades, representada matematicamente por ondas sobrepostas. Isso não é apenas incerteza – é uma coexistência fundamental de estados até que sejam medidos.*

2. É possível saber o estado exato de um sistema quântico sem medi-lo? Por quê?
    a. *Resposta: Conhecer o estado sem medição é impossível. Antes da medição, o estado do sistema é uma superposição de probabilidades (por exemplo, a posição de um elétron ou o estado 0/1 de um qubit). A medição força o sistema a "escolher" um estado definido, destruindo a superposição.*

4.1.2. *Materiais*

- Moedas (de metal com dois lados distintos)
- Copos opacos

4.1.3. *Procedimento (trabalho em grupos de 2 a 4)*

1. Jogue uma moeda sobre uma mesa ou outra superfície dura e coloque o copo sobre ela, sem revelar se é cara ou coroa.

2. Preveja se a moeda é cara ou coroa.
3. Meça a moeda levantando o copo e registe os resultados.
4. Repita 20 vezes.

4.1.4. *Resultados*

Jogada de moeda	Cara ou coroa?
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	

4.1.5. *Perguntas pós-experimento*

1. Qual foi a porcentagem de vezes que você mediu cara? Coroa? Como isso variou na sua sala de aula?
    a. *Resposta: Isso pode variar. Os alunos devem calcular as porcentagens dividindo o número de caras pelo número total de lançamentos e multiplicando por 100.*

2. Como essas porcentagens se relacionam com a probabilidade esperada de cara ou coroa?
    a. *Resposta: A probabilidade esperada de cara é de 50%.*

3. O que você poderia fazer para que suas porcentagens medidas se aproximassem da probabilidade esperada de cara ou coroa?
    a. *<u>Resposta:</u> Para que as porcentagens medidas se aproximem da probabilidade esperada, você pode aumentar o número de lançamentos.*

4. Se considerarmos que a moeda representa um qubit, em que estado o qubit está quando está sob o copo antes da medição? E depois da medição?
    a. *<u>Resposta:</u> O qubit está em estado de superposição quando está sob o copo antes da medição (cara e coroa). Após a medição, o qubit fica cara ou coroa.*

5. Como colapsamos o estado de superposição da moeda?
    a. *<u>Resposta:</u> Nós "medimos" a moeda levantando o copo.*

4.2. Parte II. Criptografia Quântica

4.2.1. *<u>Contexto adicional</u>*

A distribuição quântica de chaves (QKD) é uma forma de trocar códigos criptográficos (chaves) com segurança usando a física quântica. Aqui, a luz é usada para transmitir informações entre duas partes. Imagine que Alice quer enviar uma mensagem para Bob, mas não quer que ninguém mais a leia. Alice envia a Bob um código secreto (uma chave) usando minúsculas partículas de luz chamadas fótons. Aqui está a reviravolta quântica: se alguém tentar escutar (como Eva), a pessoa perturbará os fótons, e Alice e Bob saberão. É como ter um sistema de alarme secreto para sua mensagem. Pense nas informações que você deseja manter seguras – mensagens telefônicas, senhas de contas bancárias e PINs. Todas essas são áreas em que a criptografia quântica pode ser útil!

Existem muitas maneiras pelas quais a criptografia quântica pode proteger nossas informações, mas e quanto às situações em que computadores quânticos estão sendo usados para tentar roubar nossas informações? Neste caso, usamos a física quântica para combater esses ataques. Especificamente, a criptografia pós-quântica (PQC) é um subcampo da criptografia quântica que desenvolve algoritmos para proteção contra computadores quânticos. À medida que os computadores quânticos se tornam mais poderosos, as formas como protegemos nossos dados actualmente podem não ser suficientes. A criptografia PQC foi projectada para ser super resistente a ataques, mesmo de computadores quânticos.

Nesta actividade, simularemos um protocolo de criptografia quântica – o protocolo BB84 – para enviar uma mensagem entre duas pessoas (Alice e Bob) que criará uma chave secreta que poderá ser usada no futuro para decodificar mensagens. No protocolo BB84 da vida real, fótons com polarizações diferentes são enviados através de um canal de comunicação usando filtros. Pense nisso como desenvolver um aperto de mão secreto com a luz! Polarização se refere à orientação das oscilações do fóton – pense nisso como a direção para a qual um fóton aponta seu campo eléctrico. Filtros são como pequenas portas que permitem a passagem apenas de fótons que oscilam em uma determinada direção. O receptor da mensagem usa filtros de polarização semelhantes para adivinhar em qual direção o remetente enviou os fótons. Após enviar uma longa sequência de fótons, Alice e Bob podem partilhar publicamente seus filtros para decidir quais bits manter (quando os filtros correspondem) e quais descartar (quando os filtros não correspondem) para sua chave secreta. Uma característica interessante desse protocolo é que ele possui detecção de escuta clandestina, pois qualquer tentativa de espionar os fótons os altera. Então, se Alice e Bob medirem uma taxa de erro (a taxa na qual seus filtros não correspondem) maior que a aleatória, eles podem supor que sua comunicação está sendo interceptada e não usam sua comunicação para formar sua chave secreta partilhada.

Como podemos simular o protocolo BB84? Precisaremos de algo para representar os fótons e como os filtramos. Aqui, usaremos dois tipos de balas embaladas: um tipo terá 0s ou 1s escritos e o outro tipo terá marcações vermelhas ou verdes. Alice selecionará uma de cada aleatoriamente para atribuir seu bit e cor de fóton e registar essas informações. Pense nesses dois descritores (bit e cor) juntos como uma analogia para a polarização do fóton. Alice então passará a bala de bit para Bob, e Bob selecionará aleatoriamente uma bala de cor para "visualizar" o bit. Bob registará as informações de bit e cor. Esse processo será repetido várias vezes para representar uma sequência de fótons passando pelo canal quântico. Então, Alice e Bob compararão publicamente suas informações de cor para os fótons. Se as cores corresponderem, eles mantêm os bits; caso contrário, eles descartam os bits.

4.2.2. *Perguntas pré-actividade*

1. O que é um filtro de polarização? Como ele é usado no protocolo BB84 para codificar e decodificar fótons?
    a. *Resposta: Filtros de polarização (como óculos de sol para luz) deixam passar apenas fótons alinhados com sua orientação. No BB84, Alice usa aleatoriamente um filtro para polarizar fótons, e Bob escolhe aleatoriamente um filtro para medir os fótons. Se o filtro de Bob*

corresponder ao de Alice, Bob tem o bit correcto. Caso contrário, o resultado é aleatório.

2. Que informações você registará sobre seus "fótons" nesta actividade? Por que essas informações são escolhidas aleatoriamente?
    a. *Resposta: Nesta actividade, você registará o bit "fóton" e a polarização (cor). O filtro de polarização (cor) é escolhido aleatoriamente para garantir que a chave permaneça secreta (a menos que um intruso corra o risco de ser pego).*

4.2.3. *Materiais*

- Doces embalados (ou pequenos pedaços de papel) (40 unidades no total por grupo)
- Baldes ou potes (2 por grupo)
- Canetas hidrográficas
- Fita adesiva colorida (vermelha e verde) (outras duas cores também podem ser usadas)

4.2.4. *Procedimento (trabalho em grupos de 2 a 4)*

1. Selecione uma pessoa do seu grupo para ser Alice e outra para ser Bob. Os outros membros do grupo podem actuar como assistentes de Alice e Bob e registar as informações sobre os "fótons" que são passados durante esta actividade.
2. Escreva 0 em 10 doces (ou pedaços de papel) e 1 em 10 doces (ou pedaços de papel) e coloque-os em um pote. Agite-os para garantir que estejam bem misturados.
3. Coloque fita vermelha em 10 doces (ou pedaços de papel) e fita verde em 10 doces (ou pedaços de papel) e coloque-os em um segundo pote. Agite-os para garantir que estejam bem misturados.
4. Alice seleciona um doce de cada pote aleatoriamente e regista as informações sobre o bit e a cor.
5. Alice passa o doce bit apenas para Bob.

6. Bob seleciona um doce do pote com cores diferentes e regista as informações sobre o bit (de Alice) e a cor (do pote).
7. Repita os passos 4 a 6 pelo menos 5 vezes e até 10 vezes.
8. Alice e Bob partilham publicamente as informações de cor dos "fótons". Se as cores coincidirem, eles mantêm as informações; caso contrário, descartam as informações.
9. Troquem de papéis no grupo e repitam os passos 4 a 8.

4.2.5. *Resultados*

Resultados de Alice

Fóton	Bit	Cor	Manter ou descartar?
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Resultados de Bob

Fóton	Bit	Cor	Manter ou descartar?
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

4.2.6. *Perguntas pós-actividade*

1. Descreva seus papéis como Alice e Bob.
    a. *Resposta: Alice codifica bits aleatórios como fótons polarizados e os envia para Bob. Bob mede fótons usando bases escolhidas aleatoriamente e, em seguida, reconcilia os resultados com Alice. Se houver um intruso (como Eva), essa pessoa tenta interceptar e medir fótons, inevitavelmente introduzindo erros que expõem sua presença.*

2. O que os doces e as informações contidas nos doces representam nesta actividade?
    a. *Resposta: Os doces representam bits (0 ou 1) e as cores (vermelho ou verde) representam a polarização do fóton.*

3. Qual foi a sua taxa de erro (qual a porcentagem de tempo que você teve para descartar seus fótons)? Como isso se relaciona com a chance aleatória que você teria de descartar seus fótons?
    a. *Resposta: A taxa de erro varia para cada grupo. A chance aleatória de Bob ter que descartar seu fóton é de 50%.*

4. Como a taxa de erro pode ser usada para determinar se alguém está espionando sua comunicação no protocolo BB84?
    a. *Resposta: Se a taxa de erro for maior que a chance aleatória, há uma possibilidade de que alguém esteja espionando a comunicação.*

4.3. Parte III. Portas de Computador Quântico

Este jogo nesta seção é baseado na actividade Salvar o Gato de Schrödinger do PhysicsQuest (American Physical Society).

4.3.1. *Contexto adicional*

As instruções que os computadores usam para realizar tarefas são chamadas de circuitos lógicos, e os blocos de construção desses circuitos são chamados de portas. O resultado da execução de qualquer circuito desse tipo em um computador clássico sempre terá apenas um de dois estados: Falso ou Verdadeiro. Podemos chamar esses estados do que quisermos, como Suspensão ou Acordado. O trabalho de um

programador de computador é construir circuitos que façam com que os estados mudem de forma a resolver um problema.

O jogo "Salve o Gato de Schrödinger" ensinará como a lógica dos sistemas mecânicos quânticos é fundamentalmente diferente da mecânica clássica. A primeira diferença fundamental é o uso da fase de um qubit, que é uma propriedade ondulatória que descreve o tempo da onda em relação a uma posição de referência. As portas dos computadores clássicos não afectam a fase do bit, mas muitas portas quânticas afectam. Isso significa que existem ferramentas adicionais para resolver problemas usando computadores quânticos.

A segunda diferença fundamental vem da interferência de bits, que se considerarmos os qubits como um objecto ondulatório é basicamente interferência de onda. A interferência de onda é a adição de duas ou mais ondas. A interferência é afectada pela fase da onda que representa o qubit. Uma onda pode começar na altura zero ou pode começar na sua altura máxima, ou pode começar em algum lugar entre os dois. Pode até ser negativa! Isso significa que quando duas ondas são adicionadas, o resultado pode variar. Por exemplo, as alturas máximas das ondas podem se alinhar, de modo que a adição resulta em uma altura maior. Isso é chamado de interferência construtiva. Ou a altura resultante pode ser zero se as ondas tiverem a mesma altura, mas uma começa no positivo e a outra no negativo. Isso é chamado de interferência destrutiva. A Figura 2 mostra exemplos de interferência de onda.

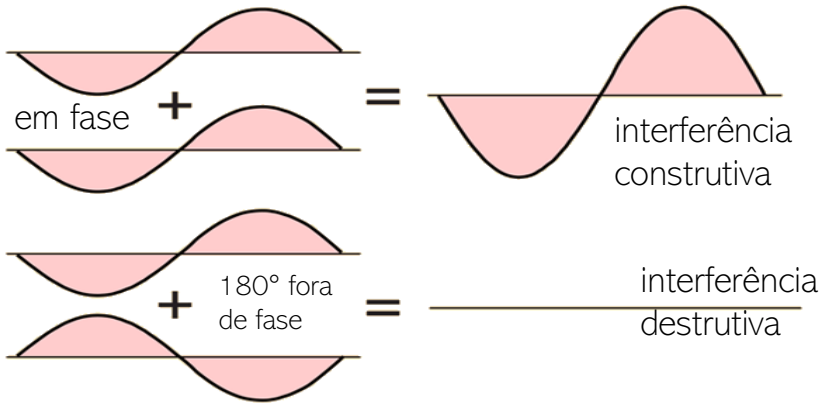


Figura 2. Interferência construtiva ocorre quando duas ondas se somam para gerar uma altura total maior (acima). Interferência destrutiva ocorre quando duas ondas fora de fase se somam para gerar uma onda com altura zero (abaixo). Na computação quântica, portas quânticas podem impactar a fase do qubit. Isso é exclusivo da computação quântica, pois portas clássicas não impactam a fase do bit. Esta foto, de autor desconhecido, está licenciada sob CC BY-NC.

A interferência de ondas desempenha um papel importante na porta quântica chamada porta de Hadamard. Como discutido anteriormente, essa porta coloca o qubit em um estado de superposição, o que significa que o bit está em dois ou mais estados ao mesmo tempo. Isso pode ser considerado como a capacidade de executar portas

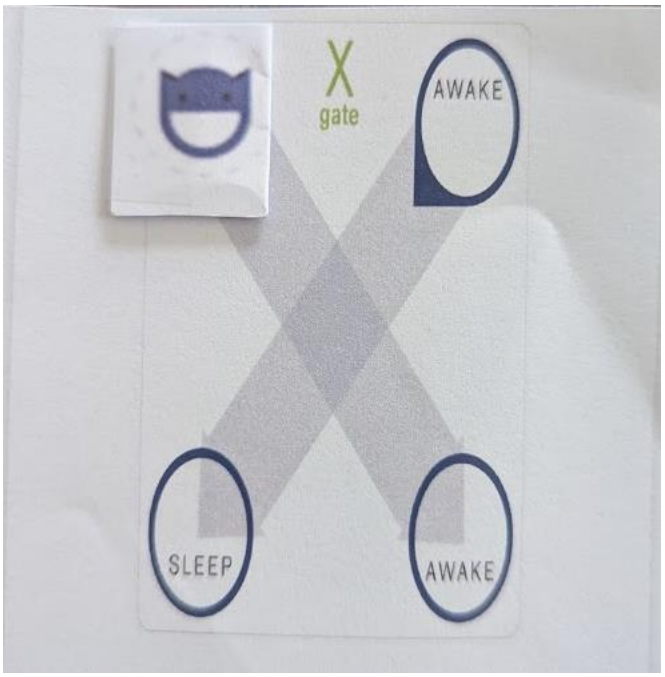
lógicas nos dois estados ao mesmo tempo, em vez de uma de cada vez em computadores clássicos. A superposição é uma propriedade que existe apenas em um estado quântico e, portanto, não pode ser usada em computadores clássicos. Para o propósito deste jogo, o estado zero (0) é o gato dormindo e o estado um (1) é o gato acordado. As fases do qubit são representadas por cores.

4.3.2. *Materiais (para cada grupo)*

- 8 tokens gato azul/gato vermelho para actuar como qubits
- 8 tokens gato amarelo/gato verde para actuar como qubits
- 2 portas X
- 2 portas Y
- 2 portas X
- 2 portas S
- 2 portas H
- 1 porta CNOT
- 1 tabela de mudança de fase de porta de qubit
- 1 tabela de interferência de qubit

4.3.3. *Procedimento e Análise (trabalho em grupos de 2 a 4)*

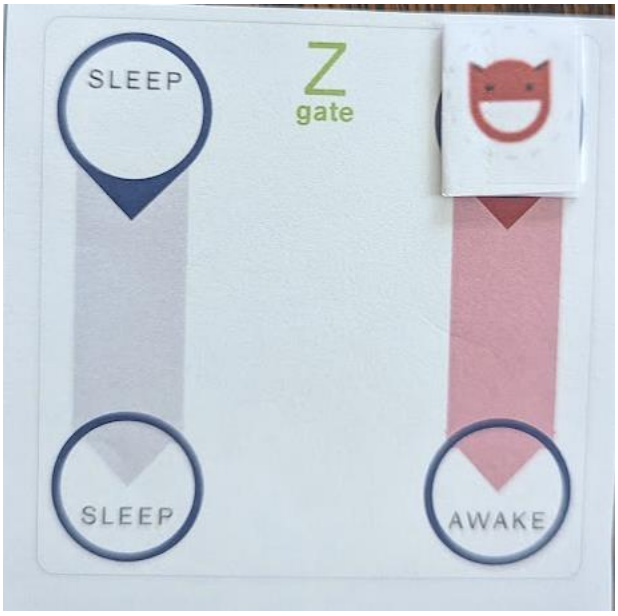
1. Organize seus QubitCats de acordo com a cor.
    a. *Nota para o professor: Pode valer a pena ajudar os alunos a se familiarizarem com as cores dos gatos, que representam as fases das ondas que eles representam, em oposição à cor dos caminhos, que pode alterar essas fases. Você pode pedir aos alunos que observem a tabela de Mudança de Fase e façam perguntas como "Como um gato vermelho pode ficar amarelo?" (RESPOSTA = seguir um caminho verde) ou "Como um gato verde pode permanecer verde?" (RESPOSTA = seguir um caminho azul).*
2. Coloque um portão X onde todos possam vê-lo. Seu primeiro desafio é acordar um gato azul. Coloque uma ficha de gato azul no círculo do Sono.



3. Observe que o caminho azul cruza para o lado Acordo do portão. Use sua tabela de mudança de fase do QubitCat para determinar se um gato azul viajando em um caminho azul muda de cor. Se a cor não mudar, coloque um gato azul no círculo Acordo. Se mudar, coloque a cor correta do gato no círculo. Registe este resultado em sua tabela.
    a. *Nota para o professor: Os alunos devem notar que o caminho azul não altera a cor (fase) do gato. Um gato azul adormecido se torna um gato azul acordado.*
4. Repita com os gatos vermelho, verde e amarelo no estado inicial de Sono. Registe os resultados para as outras cores.
    a. Você pode usar um portão X para acordar qualquer gato colorido?
        i. *Resposta: Sim. Os gatos permanecem da mesma cor e ficam acordados.*

5. Seu próximo desafio é transformar um gato vermelho acordado em um gato azul acordado.
    a. Você pode usar uma porta X para fazer isso?
        i. *Resposta: Não, o portão X não altera a cor (fase) do gato.*

6. Tentaremos outras portas. Desenhe a porta Z e coloque uma ficha de gato vermelho no círculo Acordo. Use sua tabela de mudança de fase do QubitCat para determinar o efeito do caminho vermelho em um gato vermelho acordado.



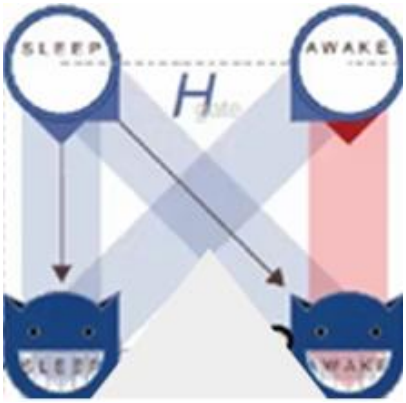
a. Você mudou a fase do gato vermelho acordado para um gato azul? Anote isso na sua tabela de resultados.
    i. *<u>Resposta:</u> Sim, o gato vermelho acordado se torna um gato azul acordado.*

b. Você consegue transformar um gato verde acordado em um gato amarelo acordado usando a porta Z? Anote isso na sua tabela de resultados.
    i. *<u>Resposta:</u> Sim, o gato verde acordado se torna um gato amarelo acordado. O estado do gato não muda, mas sua cor (fase) muda.*

7. Há mais duas portas para trabalhar, chamadas de porta Y e porta S. Experimente-as para ver qual delas transforma um gato vermelho adormecido em um gato amarelo acordado. Anote os resultados na sua tabela.
    a. *<u>Nota para o professor:</u> O gato vermelho adormecido se transforma em um gato amarelo acordado com uma porta Y. O vermelho adormecido permanece inalterado em uma porta S.*

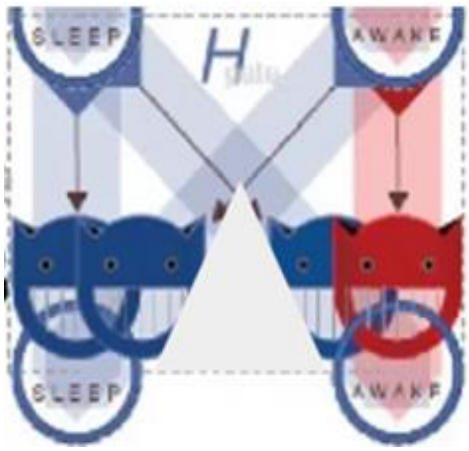
8. Há mais nas portas quânticas do que apenas essas quatro que você testou. Computadores quânticos também podem colocar qubits em superposição. Isso é chamado de preparação do estado. Computadores quânticos usam portas Hadamard (H) para isso. Desenhe sua porta H e trace os dois caminhos do Sono e os dois caminhos da Vigília. Procure por mudanças de fase em qualquer um dos caminhos. Comece um novo desafio colocando um único gato azul no círculo do Sono em uma porta H. Isso resultará em um gato em dois estados diferentes (Sono e Vigília), como mostrado na imagem abaixo. Observe que

ainda há apenas um único gato, mas ele está em um estado de superposição (Sono e Vigília), que você aprendeu em seu experimento anterior com as moedas.



9. Agora, quando aplicamos outra porta, temos ambos os estados para trabalhar. Use a superposição gato azul (dois tokens) como entrada para uma porta Z. Isso significa que você "aplica" uma porta Z e move o gato azul adormecido da porta H para o círculo de sono da porta Z, e também o gato azul acordado da porta H para o círculo de vigília da porta Z. Certifique-se de verificar as mudanças de fase ao aplicar a porta Z.
    a. *<u>Nota para o professor:</u> O gato azul adormecido no portão Z permanecerá como gato azul adormecido. O gato azul acordado se transformará em gato vermelho acordado.*

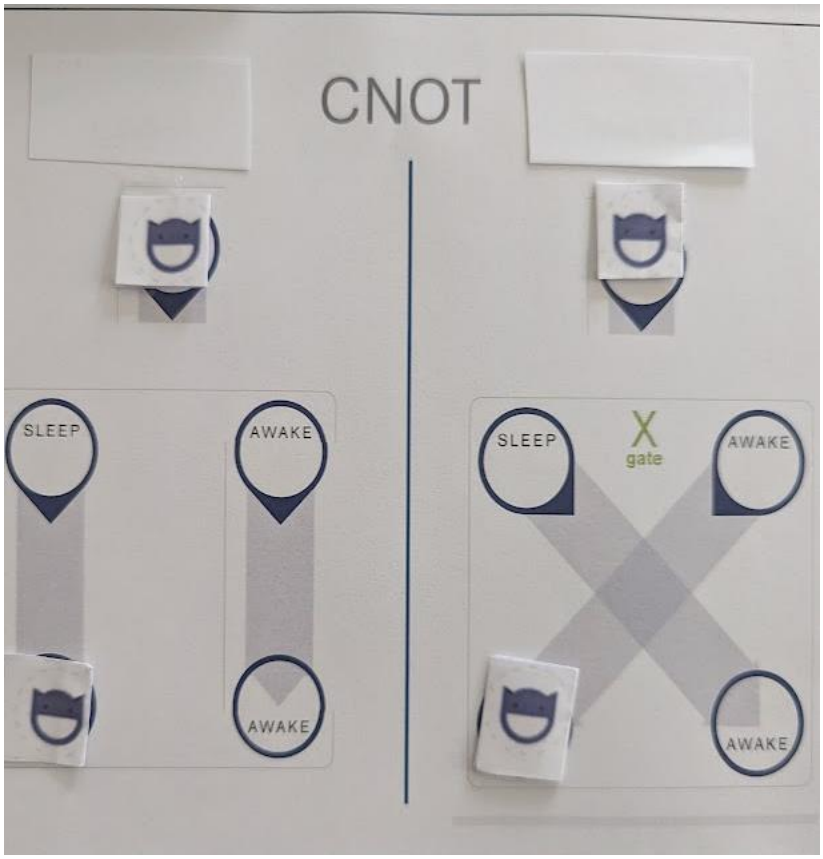
10. Para obter um resultado final, precisamos fazer uma medição aplicando uma segunda porta Hadamard (H). Ao contrário da primeira vez que usamos a porta H, agora há marcadores nos estados de vigília e sono. Isso resultará em quatro marcadores de gato na parte inferior da segunda porta Hadamard (H), sendo dois no círculo do Sono e dois no círculo da Vigília. Há um exemplo disso abaixo (embora não seja para este desafio).



11. Quando dois marcadores de gato ocupam o mesmo espaço, eles interferem um no outro e podem se anular. Quando usados corretamente, restará apenas um gato, pois o outro par interferirá e se anulará. Use sua tabela de interferência do QubitCat para determinar o resultado final do seu gato.
    a. Você acordou seu gato azul? Registe o resultado na tabela.
        i. <u>Resposta:</u> *O gato azul adormecido permanece azul e agora está em ambos os estados, Sono e Acordado. O gato vermelho acordado torna-se um gato vermelho adormecido e um gato azul acordado. Observando a tabela de interferência, vermelho + azul = zero, mas azul + azul = azul. Portanto, agora há apenas um gato azul acordado.*

12. Aqui vai outro desafio: comece com um gato vermelho dormindo. Aplique uma porta H e depois uma porta Y. Finalize fazendo uma medição aplicando a segunda porta H.
    a. Você tem um gato acordado?
        i. *<u>Resposta:</u> Sim, há um gato verde acordado. Agora, a interferência resulta em verde + verde = verde, e amarelo + verde = zero.*

13. Existe mais uma porta muito especial, exclusiva da computação quântica, chamada de porta CNOT. O "C" significa controlado, e são necessários dois qubits. O qubit na parte superior da porta é o bit de controle e o qubit de destino está na parte inferior da porta. Se o qubit de controle estiver no estado de suspensão, o qubit de destino segue o caminho à esquerda, começando no mesmo estado do qubit de controle (aqui, suspensão). Examine o caminho para ver se o qubit de destino sofreu uma mudança de estado. Se, em vez disso, o qubit de controle estiver no estado Acordado, o caminho à direita é seguido (novamente, o qubit alvo segue o caminho à direita no mesmo estado que o qubit de controle (aqui, Dormindo). Examine esse caminho e observe se o estado ou a fase do qubit alvo é alterado. Como você pode ver, o estado do qubit alvo depende do estado do qubit de controle. Este é um exemplo de entrelaçamento. O entrelaçamento é uma propriedade do sistema de dois qubits e é um fenômeno quântico único.
14. Preencha sua tabela de resultados para mostrar o estado de um gato azul acordado com um gato de controle acordado na porta CNOT. Repita com um gato azul adormecido e um gato de controle adormecido.
    a. *<u>Nota para o professor:</u> O bit de controle "Awake" faz com que o gato azul acordado se transforme em um gato azul adormecido. O bit de controle "Sleep" faz com que o gato azul adormecido permaneça o mesmo.*



4.3.4. *Resultados*

	Começando		Final	
Portão	Cor (fase)	Estado (bit)	Cor (fase)	Estado (bit)
X	Azul	Sono	*Azul*	*Acordado*
X	Vermelho	Sono	*Vermelho*	*Acordado*
X	Verde	Sono	*Verde*	*Acordado*
X	Amarelo	Sono	*Amarelo*	*Acordado*
Z	Vermelho	Acordado	*Azul*	*Acordado*
Z	Verde	Acordado	*Amarelo*	*Acordado*
Y	Vermelho	Sono	*Amarelo*	*Acordado*
S	Vermelho	Sono	*Vermelho*	*Sono*
HZH	Azul	Sono	*Azul*	*Acordado*
HYH	Vermelho	Sono	*Verde*	*Acordado*
CNOT (controle acordado)	Azul	Acordado	*Azul*	*Sono*
CNOT (controle do sono)	Azul	Sono	*Azul*	*Sono*

4.3.5. *Perguntas pós-actividade*

1. O que os gatos e suas cores representam neste jogo?
    a. *Resposta: Os gatos representam qubits, o modo Sono/Acordado representa o estado do qubit e as cores diferentes são fases diferentes.*

2. O que é interferência de ondas? Como isso se manifestou analogamente neste jogo?
    a. *Resposta: A interferência de ondas ocorre quando duas ou mais ondas estão no mesmo lugar ao mesmo tempo e se somam. Neste jogo, representamos a interferência de ondas quando a segunda porta H foi aplicada, o que resultou em dois gatos nas posições acordados e/ou dormindo.*

3. O que é superposição? Como isso se manifestou analogamente neste jogo?
    a. *Resposta: Superposição ocorre quando algo existe em vários estados ao mesmo tempo. Isso ficou evidente aqui quando aplicamos uma única porta H e um gato ficou acordado e dormindo ao mesmo tempo.*

4. O que é entrelaçamento? Como isso se manifestou analogamente neste jogo?
    a. *Resposta: Entrelaçamento ocorre quando duas coisas são interligadas de tal forma que se impactam, independentemente da distância entre elas. Isso apareceu neste jogo na porta CNOT, em que o bit de controle afectou o bit de destino.*

5. O que você gostou neste jogo?
    a. *Resposta: As respostas dos alunos variam.*

6. O que você achou desafiador neste jogo?
    a. *Resposta: As respostas dos alunos variam.*

5. Desafio de Design

O Desafio: Crie um desafio de mudança de QubitCat usando o jogo "Salve o Gato de Schrödinger".

Você praticou a transformação de gatos (qubits) de diferentes cores (fases) em diferentes estados e cores. Agora é a sua vez de criar um desafio para seus colegas. Primeiro, você escolherá seu gato e seu estado (sono ou acordado) e, em seguida, experimentará uma série de portas para mudar sua cor ou estado. Quando encontrar

uma que lhe agrade, escreva-a como um desafio para seus colegas: Pegue um gato (insira a cor) que esteja (sonolento/acordado) e transforme-o em um gato que esteja (insira a cor) (insira o estado).

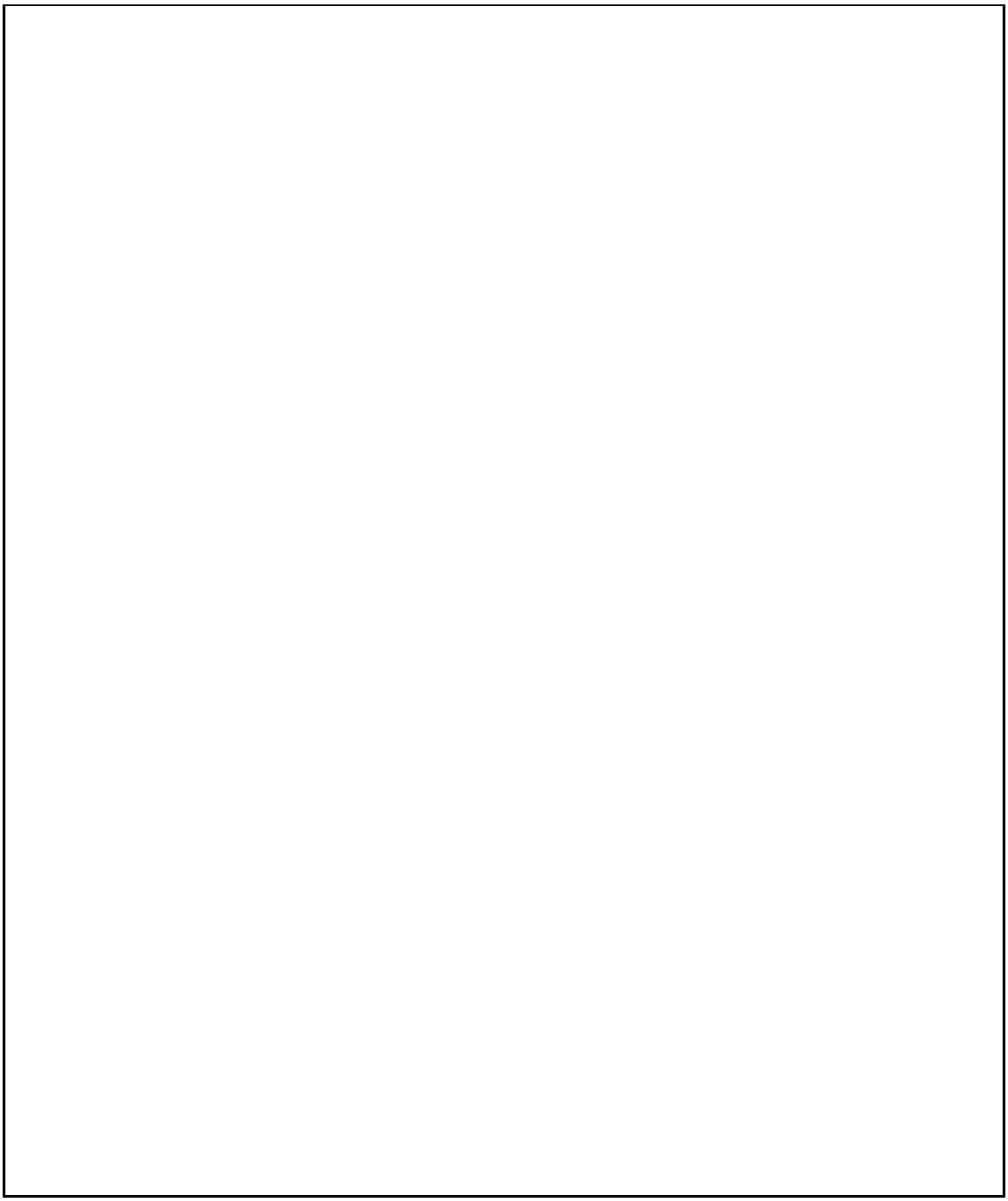
5.1 Questões de Design

1. Qual gato você escolherá como seu gato inicial? Ele está acordado ou dormindo?
2. Quais portões você usará inicialmente com seu gato para mudar sua cor ou estado? Pense em algumas opções e no que você prevê que acontecerá.

Nota para os professores: Incentive os alunos a escreverem suas ideias de brainstorming para ajudar a comunicar suas ideias entre si e para que você possa identificar quaisquer problemas. Haverá uma grande variação no que os alunos farão. Antes que os alunos troquem seus desafios, verifique se a resposta está correta. Se estiver incorreta, você pode dizer exatamente o que está errado ou simplesmente dizer que há um erro e deixar que eles decidam. Sua escolha dependerá de quão confortáveis os alunos estão trabalhando com as portas.

5.2 Esboço de Design

Esboce os designs da mudança do qubit do seu gato abaixo. Escreva o desafio da mudança usando: Pegue um gato (insira a cor) que está (dormindo/acordado) e transforme-o em um gato que está (insira a cor) (insira o estado).



6. Actividade suplementar: Computação quântica com Python e Qiskit

6.1 Informações Adicionais

A computação quântica é um novo paradigma da computação que utiliza os princípios da mecânica quântica para resolver problemas complexos intratáveis para computadores clássicos. Ao contrário dos computadores clássicos, que usam bits para representar informações como 0 ou 1, os computadores quânticos usam qubits, que podem existir em uma superposição de ambos os estados simultaneamente. Isso, juntamente com outros fenômenos quânticos, como entrelaçamento e interferência, permite que os computadores quânticos realizem certos cálculos muito mais rapidamente do que os computadores clássicos.

Em resumo, dois bits de um computador clássico podem estar em quatro estados possíveis (00, 01, 10 ou 11), mas apenas em um deles por vez. Isso limita o computador a processar uma entrada por vez (como tentar um corredor no labirinto). Em um computador quântico, dois qubits também podem representar exatamente os mesmos quatro estados (00, 01, 10 ou 11) ao mesmo tempo. A computação quântica é a ideia de que podemos usar essa quebra de regra quântica para processar informações de uma nova maneira — totalmente diferente de como os computadores comuns funcionam.

Para começar a programar computadores quânticos, você usará Python e Qiskit, uma estrutura de computação quântica de código aberto desenvolvida pela IBM. O Qiskit fornece ferramentas para criar, manipular e simular circuitos quânticos.

6.2 Procedimento

1. Antes de começar, você precisa instalar o Python, o Qiskit e o Jupyter Lab. Siga estes passos para configurar seu ambiente:
    a. Baixe o Python do site oficial (https://www.python.org/downloads/) e instale-o. Certifique-se de adicionar o Python ao PATH do seu sistema durante a instalação.
    b. Abra seu terminal ou prompt de comando.
    c. Use o pip, o instalador de pacotes do Python, para instalar o Qiskit (‘pip install qiskit’).
    d. Use o pip para instalar uma ferramenta de visualização do Qiskit (‘pip install pylatexenc’)

e. Use o pip (ou outro método: https://jupyter.org/install) para instalar o Jupyter Lab (‘pip install jupyterlab’)
f. Abra um interpretador Python digitando python no seu terminal. Importe os módulos do Qiskit para verificar a instalação (‘import qiskit’ e depois ‘print(qiskit.__version__)’).

2. Crie circuitos quânticos simples para gerar um estado de superposição e um estado de entrelaçamento, que é um conceito fundamental na computação quântica. Veja como fazer isso em um notebook Jupyter:
    a. Importe os pacotes Python necessários.
        i. *import qiskit as q*
        ii. *from qiskit import quantum_info as qi*
        iii. *from qiskit import QuantumCircuit*
    b. Instanciar a classe de circuito quântico.
        i. *qc = QuantumCircuit(2) # o argumento (2) representa 2 qubits com os quais vamos trabalhar*
        ii. *qc.draw(output = 'mpl')*
        iii. *state_0 = qi.Statevector(qc)*
        iv. *state_0.draw('bloch')*
    c. Aplique diferentes portas nesses qubits usando métodos diferentes, como x, h, etc.
        i. *qc.x(0) # x gate é aplicado no primeiro qubit*
        ii. *qc.h(1) # Portão Hadamard no segundo qubit*
        iii. *qc.draw(output = 'mpl')*
    d. Visualize a saída desses circuitos. (#para descobrir o vector de saída na saída do circuito. Vamos nomear o vetor de estado state_1)
        i. *state_1 = qi.Statevector(qc)*
        ii. *state_1.draw(output='bloch')*
    e. Aplique uma porta CNOT no primeiro qubit.
        i. *qc2 = QuantumCircuit(2)*
        ii. *qc2.x(0) # x gate no primeiro qubit ...*
        iii. *qc2.cx(0, 1) # Porta CNOT no primeiro qubit ...*
        iv. *qc2.draw(output = 'mpl')*
        v. *state_3 = qi.Statevector(qc2)*
        vi. *state_3.draw('bloch')*

7. Fontes

Histórico de computação quântica

- https://www.ibm.com/think/topics/quantum-cryptography
- https://risingwave.com/blog/beginners-guide-to-quantum-computing-for-dummies/
- https://www.youtube.com/watch?v=tsbCSkvHhMo

Protocolo BB84

- https://arxiv.org/pdf/2110.01402

“Save Schrodinger’s Cat” jogo

- https://www.youtube.com/watch?v=1OEqjGWOUhM&ab_channel=PhysicsCentral
- https://www.aps.org/learning-resources/save-schroedingers-cat