Projeto de Graduação

DEE DEPARTAMENTO DE ENGENHARIA ELÉTRICA

05/12/2011

QUBITS E ENTROPIA: UMA ABORDAGEM QUÂNTICA DA TEORIA DA INFORMAÇÃO

Gustavo Castro do Amaral

PUC RIO

Projeto de Graduação

DEPARTAMENTO
DE ENGENHARIA
ELÉTRICA

QUBITS E ENTROPIA: UMA ABORDAGEM QUÂNTICA DA TEORIA DA INFORMAÇÃO

Aluno: Gustavo Castro do Amaral

Orientador(es): Weiler Alves Finamore

Guilherme Penello Temporão

Trabalho apresentado com requisito parcial à conclusão do curso de Engenharia Elétrica na Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, Brasil.

Agradecimentos

Agradeço aos meus orientadores, pelas discussões e debates constantes sem as quais esse texto não teria sido possível.

Resumo

A Teoria da Informação clássica, criada por Claude Elwood Shannon na primeira metade do século XX, permitiu a evolução das técnicas de comunicação através de um mais profundo conhecimento das caracteristicas de um canal de comunicação, além da imprescindível noção de Entropia. Ao substituir o ferramental clássico, utilizado atualmente nas comunicações, pelo ferramental quântico, qual seria o tipo de evolução que isso introduziria nas técnicas de comunicação? Através da análise da teoria quântica à luz da problemática da Teoria da Informação, procura-se entender e utilizar esse ferramental, no intuito de construir uma visão mais rica e abrangente das comunicações.

Palavras-chave: Entropia; Informação; Quântico

DEE DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Qubits and Entropy: A Quantum Approach to Information Theory

Abstract

The Classic Information Theory, developed by Claude Elwood Shannon on the first half of the twentieth century, allowed the evolution of communications techniques by means of a more deep understanding of the characteristics of a communication channel, besides the indispensable notion of Entropy. When replacing the classic tools, used nowadays in communications, by the quantum tools, what would be the kind of evolution that this would bring to the communications techniques? Through the analysis of the quantum theory on the background of Information Theory, we seek to understand and use these tools, in the intention of building a broader and richer view over communications.

Keywords: Entropy; Information; Quantum

Sumário

1 Introdução

No dia a dia, falamos de informação como o conhecimento adquirido através das nossas percepções sensoriais. Contudo, o conceito de informação como definido por Shannon difere sutilmente da definição leiga. Segundo Shannon, informação é uma **quantidade** que pode ser **medida** e depende, apenas, da distribuição de probabilidades do sistema que estamos observando. Em última análise, a informação nos diz quão surpresos ficamos quando um determinado evento ocorre. Sendo assim, quanto menos provável a ocorrência do evento for, mais surpresos ficaremos, o que significa que teremos absorvido mais informação.

Tomemos o lançamento de uma moeda como exemplo. Estamos interessados em um evento simples, a moeda ser cara ou coroa. Se a moeda for justa, ou seja, não possua defeitos nem tenha sido construída de forma que dê um resultado com maior probabilidade que outro, podemos dizer que a probabilidade do evento ser cara ou coroa é a mesma. Como dito anteriormente, a informação é **mensurável** e **quantificável** e depende apenas da distribuição de probabilidades, sendo assim, calculemos a informação que podemos absorver dessa experiência.

2 Teoria da Informação

O conceito de "informação que podemos absorver através de uma experiência", ou de reservatório de informação, já fora levado em consideração por Shannon. Essa entidade foi chamada por ele de **Entropia** e, como na entropia da termodinâmica, leva em consideração todas as possíveis configurações de um determinado sistema. Ao contrário, no entanto, da entropia da termodinâmica, a Entropia de Shannon está preocupada em contar, na base binária, o número de estados possiveis do sistema, fazendo de sua unidade o bit. O conceito por trás desse reservatório de informação, apesar de parecer extremamente complicado, é simples: quantos bits são necessários para representar todos os estados possíveis de um sistema.

Como "bit"é um nome que pode se referir tanto à unidade da Entropia de Shannon quanto à unidade da base binária, ao longo do texto, sempre que nos referirmos à informação, usaremos o nome "shannon"para identificar a unidade de Entropia. A diferença entre um bit e um shannon é que o primeiro pode assumir valores, '0' e '1', enquanto o segundo pode assumir qualquer valor real entre 0 e 1. Uma mensagem, por exemplo, que possua um determinado número de bits, não carrega, necessariamente, essa mesma quantidade de informação, ou mesmo número de shannons, já que podem haver bits redundantes que não influenciam na entropia.

O exemplo de uma mensagem digital, composta por bits, é um ótimo recurso para o entendimento claro da distinção entre os dois conceitos. Digamos que um transmissor pode enviar uma mensagem a um receptor que diz respeito ao estado em que se encontra um sistema que pode assumir 16 diferentes estados com igual probabilidade. Cada mensagem possuirá 4 shannons, mas não necessariamente é composta por 4 bits, já que podemos introduzir bits para controle e detecção de erros que não carregam informação a respeito do estado do sistema. Tomando o mesmo exemplo, mas assumindo agora que são 12 os possíveis estados do sistema, a mensagem carregará 3.58 shannons. Mesmo sem bits de detecção e correção de erros, o número mínimo de bits enviados pela mensagem é 4.

Olhando para o experimento da moeda com outros olhos, concluímos rapidamente que é necessário apenas um shannon para representar seu reservatório de informação. Já que a moeda pode assumir dois estados diferentes, podemos relacionar o estado "cara"ao valor '0' e o estado "coroa"ao valor '1', que são possíveis estados de um bit. Observando o bit que guarda o resultado final podemos dizer se o resultado do lançamento foi cara ou coroa. Usando a fórmula de Shannon para a entropia da fonte, podemos confirmar essa suposição:

$$H = -\sum_{i=1}^{N} P(x = X_i) \times \log_2(P(x = X_i)) \tag{1}$$

É fácil ver que, por termos apenas dois eventos diferentes (cara ou coroa), $N = 2$ e, pelo fato das probabilidades serem iguais, $P(x = X_i) = \frac{1}{2}$, sendo X_1 o evento da moeda ser "cara"(bit com valor '0') e X_2 o evento da moeda ser "coroa"(bit com valor '1'). Dessa forma, ao calcular a entropia da fonte, ou seja, a quantidade de informação que podemos absorver desse experimento, encontramos o seguinte resultado, já esperado:

$$H = -\frac{1}{2} \times \log_2\left(\frac{1}{2}\right) - \frac{1}{2} \times \log_2\left(\frac{1}{2}\right) = 1 \tag{2}$$

Acabamos de descobrir, então, que a informação contida em um experimento de lançar uma moeda é um shannon. Pensemos agora na estrutura complexa da moeda enquanto um sólido. Ela é composta por uma infinidade de átomos e, portanto, prótons, elétrons e nêutrons. Para que o experimento da moeda se torne mensurável macroscopicamente (observável a olho nu), é necessário que uma infinidade dessas subpartículas microscópicas assuma um determinado

estado. O que dizer, então, de toda essa informação armazenada microscopicamente à qual não temos acesso? Digamos, apenas, que a Entropia de Shannon quando calculada para eventos macroscópicos, nos dá como resultado a quantidade de informação que podemos absorver macroscopicamente, renegando toda a informação armezenada a nível subatômico.

Através do estudo da mecânica quântica, isto é, do comportamento das partículas microscópicas, torna-se possível ter acesso aos seus possíveis estados quânticos. Com isso, transformamos um elétron, por exemplo, em uma moeda, podendo realizar a experiência para determinar seu estado e absorver bits de informação. Apesar de parecer uma grande vantagem, caso trocar o universo clássico pelo quântico fosse apenas transformar um elétron em uma moeda, isso se resumiria a possuir uma grande quantidade de moedas. As propriedades quânticas das subpartículas, no entanto, mostram que as vantagens vão muito além disso.

Como, então, conseguimos determinar os estados de um sistema quântico e como, em última análise, fazemos uso do reservatório de informação contido nesses sistemas? Primeiramente, é necessário traçar um paralelo entre os dois mundos, de forma que possamos aplicar toda a teoria bem fundamentada dos processos macroscópicos sobre os quânticos de maneira consistente.

3 Entidades dos Sistemas de Comunicação

Ao estudar um sistema de comunicações, seja ele clássico ou quântico, é necessário identificar os protagonistas. Como, em um primeiro momento, pode ser pouco intuitiva a conexão entre os dois tipos de sistema, através da descrição das entidades envolvidas, procuramos traçar um paralelo entre as duas. Veremos que o ponto divergente é o processo de medição, que, apesar de parecer um detalhe, distingue completamente o universo clássico do quântico do ponto de vista da informação.

Entidades Clássicas

A medição de um estado clássico é uma tarefa razoavelmente simples, já que a energia do objeto de estudo é ordens de grandeza superior à energia das partículas que possibilitam medi-lo. Por exemplo uma moeda e o fóton que "usamos"para medir (ou observar) a face que está virada para cima. A medição é possível através dessa partícula de luz, que é refletida pela face da moeda e chega aos nossos olhos e que não afeta o estado da moeda ao fazê-lo.

Através da repetição do experimento repetidas vezes determinamos, cada vez com mais precisão, as distribuições de probabilidade que regem os resultado possíveis do evento. De posse dessas distribuições, podemos calcular a entropia, ou seja, a quantidade de informação contida na medição da face de uma moeda. Notamos, portanto, que a medição clássica desacopla as informações sobre o objeto da medição e os meios para obtê-la.

1. **Fonte:** Processo aleatório que produz símbolos de um alfabeto conhecido com uma determinada distribuição de probabilidade. A quantidade de informação produzida pela fonte pode ser encontrada através do cálculo da sua entropia.

2. **Símbolo:** Elemento de um alfabeto conhecido cujo valor pode ser determinado através de uma medição.

3. **Alfabeto:** Conjunto conhecido de símbolos que podem ser gerados por uma fonte.

4. **Informação:** O quão surpreso ficamos com o resultado da medição.

5. **Entropia de Shannon:** Quantidade de informação que pode ser extraída de um sistema clássico.

Entidades Quânticas

É importante comentar que a obtenção de informação envolve, necessariamente, um processo de medição de um estado previamente desconhecido. Na mecânica quântica, a palavra "medição", ao contrário do caso clássico, deve ser tratada com certo cuidado. Para medir o estado de uma moeda macroscopicamente, basta olhar para a moeda sobre a mesa. Esse processo, como já foi dito, envolve captar os fótons que "batem"na face da moeda que está virada para cima e que chegam aos nossos olhos. Os fótons que batem na moeda, contudo, não possuem energia suficiente para fazer com que a moeda mude de estado quando colidem com ela porque a moeda possui energia incrivelmente maior que a de um fóton. Sendo assim, ao realizar a medição macroscópica da moeda podemos desconsiderar a interação da moeda com o fóton que usamos para medi-la admitindo que o estado da moeda não será alterado por esse processo.

Quando tratamos de um experimento quântico, as coisas ficam mais complicadas porque essa suposição não pode mais ser levada em consideração, já que as partículas sobre as quais interagimos passam a ter energia comparável à das partículas com as quais fazemos a medição!

Se fosse possível ver um elétron a olho nu (o que não é) deveríamos captar fótons que são refletidos pelo elétron que queremos observar. No instante que esse fóton interage com o elétron, contudo, ele afeta suas propriedades fazendo com que o que enxergamos não seja mais o estado no qual o elétron se encontrava antes da interação, mas um novo estado, produto da interação do estado anterior com o fóton de medida. Ao contrário da moeda, que permanece inalterada depois de colidir com o fóton, o estado do elétron é modificado.

A medição, portanto, é o grande dilema da mecânica quântica, já que ela própria se sabota, no sentido que, ao realizá-la, o resultado torna-se, automaticamente, diferente daquilo que se procurava no primeiro momento. As entidades quânticas sao definidas com base nesse dilema, donde podemos destacar duas noções primitivas. A primeira delas, a preparação, é como uma receita em um livro de culinária: descreve o passo-a-passo da montagem do experimento. As regras de uma preparação deveriam ser inambíguas, ou seja, completamente reproduzíveis em diferente ambientes. A outra noção primitiva, o teste, começa como uma preparação, mas envolve um estágio a mais, no qual informação não disponível previamente pelo preparador (ou pesquisador) é absorvida em uma medição. O objetivo de um teste é definir o estado quântico de uma partícula, isto é, determinar, quando o número de repetições tender a infinito, todos os resultados possíveis para um grupo de preparações idênticas. A idéia, portanto, é a mesma de eventos clássicos, levando em conta, nesse caso, o dilema básico da medição na mecânica quântica. Vejamos as entidades relacionadas a uma medição quântica.

1. **Estado Quântico:** Probabilidades de todos os possíveis resultados de todos os testes concebíveis (sobre cada um dos graus de liberdade). Indica a distribuição de probabilidades dos resultados possiveis de uma medição.

2. **Grau de Liberdade:** Característica física de uma partícula quântica que pode ser medida.

3. **Parâmetro Físico Observável:** Definição do Grau de Liberdade que se procura detectar ao realizar uma medição.

4. **Entropia de Von Neumann:** Grau de descorrelação de um sistema quântico.

5. **Entropia de Shannon:** Incerteza sobre a informação clássica codificada no sistema quântico.

Após elencar as entidades presentes nos sistemas quânticos e clássicos, é possivel notar uma grande semelhança entre, por exemplo, o conceito de **Fonte** e de **Estado Quântico**, já que ambas possuem reservatório de informações, isto é, estados que podem ser medidos com uma determinada distribuição de probabilidades. São entidades, portanto, que possuem entropia, das quais podemos absorver informação. Além disso, os conceitos de **Símbolo** e **Grau de Liberdade** são bastante semelhantes, por serem as características detectáveis em uma medição e por fazerem parte de um conjunto restrito e conhecido. No caso clássico, um **Alfabeto** e no caso quântico, um **Parâmetro Físico Observável**.

Um comentário torna-se essencial em relação às duas diferentes definições de entropia. Enquanto a entropia de Shannon utiliza distribuições de probabilidade para o cálculo da informação armazenada em um sistema, a entropia de Von Neumann substitui as distribuições de probabilidade por operadores de densidade, entidades matemáticas presentes na teoria quântica. Esses operadores em sua forma diagonalizada são equivalentes às distribuições de probabilidade clássica, de forma que as duas entropias (de Von Neumann e Shannon) se equivalem. Contudo, há uma diferença que faz da entropia de Von Neumann uma quantidade mais palpável do ponto de vista quântico, a **fidelidade**.

A fidelidade é um conceito simples de ser compreendido. Ela nos indica a probabilidade de, dada uma medida sobre dois estados, haver uma confusão entre eles não sendo possivel distinguir entre os dois. sistemas clássicos são completamente distinguíveis, mas o mesmo não acontece com sistemas quânticos. Estados completamente distinguíveis apresentam mínima fidelidade (o cálculo da entropia de Von Neumann para um sistema de dois estados totalmente distinguívies seria zero), enquanto estados completamente misturados e indistinguíveis apresentam máxima fidelidade (o cálculo da entropia de Von Neumann para um sistema de dois estados completamente indistinguíveis seria 1). Vemos, portanto, que para o cálculo da entropia baseada numa distribuição de probabilidades, as duas entropis se equivalem, mas quando tratamos de um sistema de partículas, a entropia de Von Neumann introduz um conceito a mais. Uma vez expostas as relações entre entidades, é possivel ir mais a fundo na discussão. Se as semelhanças são tantas, porque não usar, simplesmente, os sistemas quânticos e usufruir do seu número infinito de "moedas"? Basicamente porque é muito mais difícil lidar com esse tipo de sistema, como já vimos em relação à medição. É fácil visualizar essa idéia ao imaginar como lançaríamos um elétron no ar e como mediríamos seu estado, "cara"ou "coroa". Por isso, é necessário tratar da física subatômica, ou seja, da mecânica quântica. E é justamente quando entram em cena os bits quânticos, ou Qubits.

4 Bits e Qubits

Informação é uma quantidade mensurável e tem como unidade o shannon. Isso faria da informação absorvida de um sistema quântico um shannon quântico? Apesar de incorrermos facilmente nesse erro por conta do nome "Qubits"(Quantum Bits), o Qubit não é a unidade de informação de um sistema quântico. Ele é, na verdade, a expressão de um sistema quântico em termos de um grau de liberdade com sua devida distribuição de probabilidades. O shannon, portanto, continua sendo a unidade de informação em um sistema quântico. Mesmo assim, o Qubit exerce papel fundamental no estudo da Teoria da Informação Quântica e, para entendê-lo melhor, é necessário rever certos aspectos dessa teoria.

Em 1926, Erwin Rudolf Josef Alexander Shcrödinger propôs uma equação que seria capaz de determinar o comportamento de uma partícula subatômica. A equação, ao invés de tratar tais entidades como partículas, as trata como ondas. Mais precisamente, como uma **Função de Onda**. Apesar de não possuir significado físico, a função de onda de, por exemplo, um elétron, está intimamente associada à distribuição de probabilidades dos possiveis estados desse elétron. Em última análise, o módulo ao quadrado da função de onda é a função distribuição de probabilidade do elétron.

Apesar de ser um conceito extremamente difícil de assimilar, a idéia por trás dele é a seguinte: uma entidade quântica tem seu comportamente ditado por uma onda de probabilidade que se extende por todo o espaço. Diz-se que essa entidade está em uma **Superposição de Estados** porque pode se manifestar sobre qualquer forma desde que sua onda de probabilidade seja não-nula no que diz respeito a essa manifestação. Digamos, portanto, que a posição de um elétron é descrita como uma onda de probabilidade que é não-nula tanto em um laboratório de pesquisas na Terra quanto em Marte. Mesmo que seja muito pequena, há uma chance desse elétron se manifestar em Marte e, para todos os efeitos, até que ele seja medido, ele está em ambos os lugares ao mesmo tempo.

Pelo fato das entidades quânticas possuírem várias características e vários estados possíveis para cada uma dessas características (velocidade, posição, spin, etc..) é que a **Medição** se torna um fator tão importante. Ao definir um **Grau de Liberdade** decidimos que tipo de **Parâmetro Físico Observável** de uma entidade quântica queremos detectar. Felizmente, esses parâmetros físicos observáveis são um tipo especial de parâmetro, o que torna possivel representar todo o comportamento das entidades quânticas em função deles. Mais precisamente, eles são auto-vetores associados aos operadores de medição em um espaço de Hilbert (que, para todos efeitos, é um espaço vetorial especial). Apesar de matematicamente complexo, o conceito por trás dessa idéia é simples. Voltemos a imaginar a moeda que foi lançada há pouco. Apesar de podermos descrever várias distribuições de probabilidade relacionadas ao evento de lançá-la, por exemplo o lugar onde a moeda vai pousar ou quantas voltas completas vai descrever no ar antes disso, retratamos o evento todo, englobando todas as outras distribuições de probabilidade, como "face para cima"ou "face para baixo".

O mesmo acontece com um sistema quântico. Seu comportamento pode ser descrito como vários eventos de probabilidade, mas escolhemos (ao escolher um grau de liberdade) aquele que nos interessa. Vamos tomar um exemplo simples de uma partícula quântica. Imagine um Qubit que descreva o comportamento de um fóton em função da sua polarização (uma das características possíveis dessa entidade), onde $|H\rangle$ é o auto-vetor que define a polarização horizontal e $|V\rangle$ é o auto-vetor que define a polarização vertical. Um estado genérico desse fóton, ou seja, o Qubit associado a esse fóton nessa base de medidas, pode ser escrito da seguinte maneira:

$$|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle \tag{3}$$

Os coeficientes α e β que multiplicam cada um dos auto-vetores dizem respeito às probabilidades do fóton ser detectado com uma polarização vertical ou com uma polarização horizontal. Até que esse fóton seja medido usando um discriminador de polarização e detectores, ele está numa superposição de estados, ou seja, ele está tanto polarizado horizontalmente quanto verticalmente. Assim que ele é medido, ele colapsa para os estados $|H\rangle$ ou $|V\rangle$ com probabilidade α^2 e β^2, respectivamente. Como já fora dito, a probabilidade está relacionada ao módulo ao quadrado desses coeficientes.

Uma observação torna-se necessária a essa altura. O Qubit relacionado ao estado de polarização do fóton acima tem grande similaridade com o estado da moeda que foi lançada há pouco tempo. Se fosse possível escrever o estado dessa moeda antes da medida ser realizada na mesma notação da mecânica quântica (se a moeda pudesse ser descrita como uma função de onda), provavelmente teríamos algo como a expressão a seguir:

$$|\psi_{moeda}\rangle = \left(\frac{1}{\sqrt{2}}\right)|cara\rangle + \left(\frac{1}{\sqrt{2}}\right)|coroa\rangle \tag{4}$$

Já que a probabilidade da moeda assumir cada um dos estados é 1/2, sua suposta função de onda deveria possuir coeficientes que são a raiz quadrada dessa probabilidade. Comparando α e β com os coeficientes $\left(\frac{1}{\sqrt{2}}\right)$ torna-se claro o paralelo muito forte entre ambos os eventos. Sabemos, contudo, que a moeda é uma entidade clássica e que, portanto, não é descrita como uma função de onda.

Uma diferença importantíssima que pode ser citada é que, no caso do fóton, podemos trocar a base na qual escolhemos fazer a medição do grau de liberdade e encontrar resultados completamente diferentes do ponto de vista probabilístico enquanto no caso da moeda só possuímos uma base possivel. Uma nova base para a medição do fóton seria, ao invés da base $|H\rangle$ e $|V\rangle$, a base $|+45^o\rangle$ e $|-45^o\rangle$. Esse caso é interessante porque uma fonte que produza fótons polarizados a $+45^o$, tem probabilidade igual de ser medida como $|H\rangle$ e $|V\rangle$, ou seja $\frac{1}{2}$, e probabilidade 1 de ser medida como $|+45^o\rangle$. Ao trocar a base de medida, mudamos completamente o resultado da medição. No caso da moeda, a única base possível é "cara"e "coroa".

5 Teoria da Informação Quântica

Imaginemos, portanto, um fóton, ou qualquer outra partícula quântica. A partir desse momento podemos considerá-lo, para fins de simplicidade, como uma moeda muito especial, cujo comportamento é descrito através de uma função de onda. Além disso, os métodos convencionais de medição não se aplicam a essa moeda quântica, sendo necessário utilizar técnicas mais complexas para a detecção dos seus estados. Uma vez dito isso, as propriedades da mecânica quântica passam a valer e podem ser exploradas.

Analisemos, portanto, o algoritmo de Deutsch, um exemplo interessante das melhorias associadas à aplicação de todo o enfoque quântico na teoria da informação.

Algoritmo de Deutsch

Para entender o **Algoritmo de Deutsch** e suas aplicabilidades, é necessário realizar um experimento clássico. Imaginemos uma caixa preta que implementa uma função sobre um número binário na sua entrada. As possiveis operações sobre um número binário são apenas quatro e estão descritas a seguir:

1. *Identidade*: O número binário na entrada será mantido na saída. Logo, o número '1' na entrada produzirá o número '1' na saída enquanto o número '0' na entrada produzirá o número '0' na saída.

2. *Negação*: O número binário na entrada será negado para produzir a saída. Logo, o número '1' na entrada produzirá o número '0' na saída enquanto o número '0' na entrada produzirá o número '1' na saída.

3. *Constante '1'*: Qualquer número binário na entrada produzirá o número '1' na saída.

4. *Constante '0'*: Qualquer número binário na entrada produzirá o número '0' na saida.

Diz-se que uma sequência binária é balanceada quando possui uma quantidade de '0's igual a de '1's. Aplicando essa sequência balanceada sobre a caixa preta que acabamos de definir (repare que a caixa é preta porque não sabemos qual das quatro operações ela implementa) obteremos uma sequência binária de saída. Caso a caixa esteja implementando uma das duas primeiras funções possíveis, a sequência de saída permanecerá sendo balanceada, ou seja, com mesmo número de '0's e '1's. No entanto, se a caixa implementar uma das duas últimas funções possíveis, a sequência de saída não será mais balanceada, possuirá uma maior quantidade de '1's ou de '0's. Podemos dizer que há, portanto, dois grupos de função, que chamaremos de *Balanceada* e *Não-Balanceada*.

O experimento é simples. Queremos saber qual dos dois grupos de função é implementado. Uma possível abordagem seria criar uma sequência balanceada bem grande de bits, aplicá-la sobre a caixa e analisar a saída, contando os números de '0's e '1's. Contudo, já conhecemos a Teoria da Informação de Shannon e podemos aplicá-la para otimizar o experimento. Repare que a informação que queremos absorver está contida em apenas um bit, ou seja, são dois os estados possíveis do sistema que procuramos medir. Se calcularmos a entropia desse sistema, podemos saber que fração de bit absorvemos por medição e estipular quantas medições são necessárias para absorvermos o bit que nos interessa, ou seja, que nos dará a informação que procuramos sobre o sistema. Algumas coisas interessantes acontecem ao proceder dessa maneira, vejamos.

Assumimos, novamente como no caso da moeda, que a caixa é "honesta"e implementa cada uma das funções com igual probabilidade. Após algumas poucas contas de probabilidade, é possível calcular exatamente a informação contida no bit da primeira medição. A seguir

podemos ver o passo-a-passo que nos leva ao resultado final. A variável f que aparece no desenvolvimento é à variável aleatória que descreve qual função a caixa implementa. Ela é essencial já que a saída depende diretamente dessa função.

$$H = -\sum_{i=1}^{N} P(x = X_i) \log_2(P(x = X_i)) \tag{5}$$

$$X_1 = \text{‘1’} \; ; \; X_2 = \text{‘0’}$$
$$f_1 = \textit{Constante ‘1’} \; ; \; f_2 = \textit{Constante ‘0’} \; ; \; f_3 = \textit{Identidade} \; ; \; f_4 = \textit{Negação}$$

$$P(x = X_1) = P(x = X_1|f = f_1) \times P(f = f_1) + P(x = X_1|f = f_2) \times P(f = f_2) +$$
$$P(x = X_1|f = f_3) \times P(f = f_3) + P(x = X_1|f = f_4) \times P(f = f_4) \tag{6}$$
$$P(x = X_1) = 1 \times \frac{1}{4} + 0 \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4} = \frac{1}{2} \tag{7}$$
$$P(x = X_2) = P(x = X_2|f = f_1) \times P(f = f_1) + P(x = X_2|f = f_2) \times P(f = f_2) +$$
$$P(x = X_2|f = f_3) \times P(f = f_3) + P(x = X_2|f = f_4) \times P(f = f_4) \tag{8}$$
$$P(x = X_2) = 0 \times \frac{1}{4} + 1 \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4} = \frac{1}{2} \tag{9}$$
$$H = -\frac{1}{2} \times \log_2\left(\frac{1}{2}\right) - \frac{1}{2} \times \log_2\left(\frac{1}{2}\right) = 1 \tag{10}$$

Acabamos de descobrir que a entropia dessa fonte é 1. Isso significa que, ao realizar uma medição sobre um dos simbolos na sua saída, absorvemos um bit de informação. Aparentemente, esse é o melhor caso que se podia esperar, ou seja, com apenas uma medição (que é o menor número de medições possível) absorveremos um bit de informação, que é exatamente o que precisávamos para determinar o tipo de função que a caixa implementa. Apesar do raciocínio estar certo, o problema é ligeiramente mais complexo.

É necessário entender que o bit de informação que absorvemos na primeira medição reduz a incerteza quanto a qual função a caixa implementa mas não quanto a ela ser balanceada ou constante, isto é, nos envia um bit de informação que não nos é útil. No caso de, por exemplo, termos entrado com o número ‘1’ no sistema e obtido o número ‘1’ na saída, sabemos que a função implementada é ou *Identidade*, ou *Constante ‘1’*. Apesar de termos absorvido um bit de informação, continuamos com a mesma dúvida, agora sobre duas funções ao invés de quatro. É fácil de ver que as quatro combinações de entradas e saídas possíveis para 1 bit restringirão a função implementada para um grupo que contém uma função balanceada e uma função constante, o que não resolve o nosso problema. A seguir encontram-se os resultados possíveis para diferentes entradas e saídas:

1. $\textit{Entrada}_1$ = *‘1’ e* $\textit{Saída}_1$ = *‘1’*: A caixa implementa a função Identidade ou a função Constante ‘1’.

2. $\textit{Entrada}_1$ = *‘1’ e* $\textit{Saída}_1$ = *‘0’*: A caixa implementa a função Negação ou a função Constante ‘0’.

3. $\textit{Entrada}_1$ = *‘0’ e* $\textit{Saída}_1$ = *‘1’*: A caixa implementa a função Negação ou a função Constante ‘1’.

4. $\textit{Entrada}_1$ = *‘0’ e* $\textit{Saída}_1$ = *‘0’*: A caixa implementa a função Identidade ou a função Constante ‘0’.

Já que não possuímos a informação necessária para resolver o problema, é necessário aplicar mais uma entrada no sistema e medir sua saída. Repare que caso apliquemos a mesma entrada novamente, não ganharemos nenhuma informação continuaríamos na mesma situação, o que não seria vantajoso. Sendo assim, aplicaremos uma entrada diferente do primeiro caso. Vamos, então, calcular a quantidade de informação contida no segundo bit lembrando que já realizamos a primeira medida. A variável aleatória y_1 está associada com o evento de medida da saida do primeiro experimento.

$$H = -\sum_{i=1}^{N} P(x = X_i) \times \log_2(P(x = X_i)) \tag{11}$$

$$X_1 = \text{‘1’} \; ; \; X_2 = \text{‘0’}$$

$$f_1 = \textit{Constante ‘1’} \; ; \; f_2 = \textit{Constante ‘0’} \; ; \; f_3 = \textit{Identidade} \; ; \; f_4 = \textit{Negação}$$

$$P(x = X_1) = P(x = X_1|y_1 = X_2) \times P(y_1 = X_2) +$$

$$P(x = X_1|y_1 = X_2) \times P(y_1 = X_2) \tag{12}$$

Expandimos os termos de probabilidade condicional em relação às funções implementadas pela caixa preta. Temos, portanto, dois termos.
O primeiro será:

$$\begin{aligned} P(x = X_1|y_1 = X_1) = {} & P(x = X_1|f = f_1|y_1 = X_1) \times P(f = f_1|y_1 = X_1) + \\ & P(x = X_1|f = f_2|y_1 = X_1) \times P(f = f_2|y_1 = X_1) + \\ & P(x = X_1|f = f_3|y_1 = X_1) \times P(f = f_3|y_1 = X_1) + \\ & P(x = X_1|f = f_4|y_1 = X_1) \times P(f = f_4|y_1 = X_1) \end{aligned} \tag{13}$$

E o segundo será:

$$\begin{aligned} P(x = X_1|y_1 = X_2) = {} & P(x = X_1|f = f_1|y_1 = X_2) \times P(f = f_1|y_1 = X_2) + \\ & P(x = X_1|f = f_2|y_1 = X_2) \times P(f = f_2|y_1 = X_2) + \\ & P(x = X_1|f = f_3|y_1 = X_2) \times P(f = f_3|y_1 = X_2) + \\ & P(x = X_1|f = f_4|y_1 = X_2) \times P(f = f_4|y_1 = X_2) \end{aligned} \tag{14}$$

$$\begin{aligned} P(x = X_1) = {} & \frac{1}{2} \times \left(1 \times \frac{1}{2} + 0 \times 0 + \frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4}\right) + \\ & \frac{1}{2} \times \left(1 \times 0 + 0 \times 1 + \frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4}\right) = \frac{1}{2} \end{aligned} \tag{15}$$

É fácil ver que o cálculo de $P(x = X_2)$ terá o mesmo resultado. Sendo assim, chegamos à entropia da segunda medição.

$$H = -\frac{1}{2}\log_2\left(\frac{1}{2}\right) - \frac{1}{2}\log_2\left(\frac{1}{2}\right) = 1 \tag{16}$$

Aliando esta medição à primeira, podemos acabar com a dúvida a qual o problema se reduzira e afirmar, com certeza, se a função implementada é balanceada ou constante. O mais interessante, no entanto, é que, com esses dois bits, podemos afirmar mais do que apenas a que grupo a função pertence, mas também que função é essa.

Podemos concluir, deste experimento clássico, que o bit referente à informação *Balanceada/Constante* está embutido nos dois bits que definem qual função é implementada. Contudo, esse bit não pode ser extraído de forma independente. Para todos os efeitos, portanto, são necessárias duas medições para chegar ao resultado do problema.

Vamos, agora, para a implementação quântica desse mesmo problema. Para isso, é necessário falar rapidamente sobre o já mencionado espaço de Hilbert, já que as operações e os vetores (onde $|H\rangle$ seria um exemplo de vetor) são definidos neste espaço.

O espaço de Hilbert é uma espaço vetorial onde se define um produto interno. Isso significa que estados quânticos podem ser representados nesse espaço vetorial como vetores e as operações sobre esses estados como transformações lineares, ou seja, matrizes.

Exemplos de vetores e transformações no espaço de Hilbert são os auto-vetores associados à uma medição genérica e a matriz da transformação de Hadamard:

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad ; \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \quad ; \quad \mathbf{H} = \frac{1}{\sqrt{2}} \times \begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \tag{17}$$

Essas serão as únicas ferramentas utilizadas, além, é claro, da implementação quântica da caixa preta. Apesar de pouco intuitiva, a implementação é a seguinte:

$$f : |x\rangle\,|y\rangle \to |x\rangle\,|f(x) \oplus y\rangle \tag{18}$$

A configuração geral do experimento será:

- Passo 1: Criação de um estado de 2 Qubits.
- Passo 2: Aplicação da Transformação de Hadamard sobre os 2 Qubits de entrada.
- Passo 3: Aplicação da caixa preta quântica sobre o resultado do passo anterior.
- Passo 4: Aplicação da Transformação de Hadamard sobre o resultado do passo anterior.
- Passo 5: Medição do resultado final.

Vejamos como esse processo todo é desenvolvido.

$$|x\rangle\,|y\rangle \to \mathbf{H} \tag{19}$$

$$\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} \times \frac{1}{\sqrt{2}} \times \begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = \frac{1}{2} \times \begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{2} \times (|0\rangle + |1\rangle)\,(|0\rangle - |1\rangle) \tag{20}$$

$$\frac{1}{2} \times (|0\rangle + |1\rangle)\,(|0\rangle - |1\rangle) \to f \tag{21}$$

$$\frac{1}{2} \times (|0\rangle\,|f(0) \oplus 0\rangle + |1\rangle\,|f(1) \oplus 0\rangle - |0\rangle\,|f(0) \oplus 1\rangle - |1\rangle\,|f(1) \oplus 1\rangle) \tag{22}$$

$$\frac{1}{2} \times \left((-1)^{f(0)}\,(|0\rangle - |1\rangle) + (-1)^{f(1)}\,(|0\rangle - |1\rangle)\right) \tag{23}$$

Esse estado também pode ser escrito de outra forma, que permite identificar uma fase global que pode ser desconsiderada:

$$\frac{1}{2} \times \left(\underbrace{(-1)^{f(0)}}_{f_{ase\,global}} \left(|0\rangle + (-1)^{f(0)\oplus f(1)} |1\rangle \right) (|0\rangle - |1\rangle) \right) \tag{24}$$

Ignoramos, também, o Qubit da direita, que não carrega informação sobre o sistema. Ele é chamado de "Decoy"e não será medido. Obtemos o estado de saída da caixa preta sobre o qual aplicaremos Hadamard novamente:

$$\frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{f(0)\oplus f(1)} |1\rangle \right) = \frac{1}{\sqrt{2}} \times \begin{pmatrix} 1 \\ (-1^{f(0)\oplus f(1)}) \end{pmatrix} \rightarrow \mathbf{H} \tag{25}$$

$$\frac{1}{\sqrt{2}} \times \begin{pmatrix} 1 \\ (-1^{f(0)\oplus f(1)}) \end{pmatrix} \times \frac{1}{\sqrt{2}} \times \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 + (-1)^{f(0)\oplus f(1)} \\ 1 - (-1)^{f(0)\oplus f(1)} \end{pmatrix} \tag{26}$$

É fácil de ver que a probabilidade de medir o estado $|0\rangle$ será 1 se e somente se a operação $f(0) \oplus f(1)$ for igual a 0, o que significa que a função é constante. Enquanto isso, a probabilidade de medir o estado $|1\rangle$ será 1 se e somente se a operação $f(0) \oplus f(1)$ for igual a 1, o que significa que a função é balanceada.

Observe que foi necessária apenas uma medida para chegar a essa conclusão, já que o estado "Decoy"não foi medido. Calculemos, portanto, a quantidade de informação contida no Qubit medido na saída:

$$H = -\sum_{i=1}^{N} P(x = X_i) \times \log_2(P(x = X_i)) \tag{27}$$

$$\frac{1}{2} \begin{pmatrix} 1 + (-1)^{f(0)\oplus f(1)} \\ 1 - (-1)^{f(0)\oplus f(1)} \end{pmatrix} = \frac{1}{2} \left(\left(1 + (-1)^{f(0)\oplus f(1)} \right) |0\rangle + \left(1 - (-1)^{f(0)\oplus f(1)} \right) |1\rangle \right) \tag{28}$$

$$a = f(0) \oplus f(1) \tag{29}$$

$$P(x = |0\rangle) = P(x = |0\rangle \, | a = 0) \times P(a = 0) + P(x = |0\rangle \, | a = 1) \times P(a = 1) \tag{30}$$

$$P(x = |0\rangle \, | a = 0) = \left(\frac{1}{2} \left(1 + (-1)^0 \right) \right)^2 = 1 \tag{31}$$

$$P(x = |0\rangle \, | a = 1) = \left(\frac{1}{2} \left(1 + (-1)^1 \right) \right)^2 = 0 \tag{32}$$

$$P(x = |1\rangle \, | a = 0) = \left(\frac{1}{2} \left(1 - (-1)^0 \right) \right)^2 = 0 \tag{33}$$

$$P(x = |1\rangle \, | a = 1) = \left(\frac{1}{2} \left(1 - (-1)^1 \right) \right)^2 = 1 \tag{34}$$

$$H = -\frac{1}{2} \log_2 \left(\frac{1}{2} \right) - \frac{1}{2} \log_2 \left(\frac{1}{2} \right) = 1 \tag{35}$$

Algumas observações se fazem necessárias. O Qubit que chamamos de "Decoy", apesar de não ser medido, tem papel fundamental na interação do sistema com o estado de entrada, sem

ele não seria possível obter uma resposta desse tipo com apenas uma medição. O nome, que poderia ser traduzido como "isca", reflete exatamente essa idéia, ou seja, um elemento que será introduzido no sistema mas sob o qual não se realizarão medições.

O fato da quantidade de informação absorvida através da medição do estado de saída ser 1 bit não chama atenção, já que chegáramos a essa conclusão anteriormente. Contudo, o fato desse bit de informação dizer respeito exatamente à informação que procurávamos é formidável já que esse bit era inacessível classicamente.

6 Conclusão

A abordagem quântica do problema proposto e seu desenrolamento revela duas conclusões, ambas bastante interessantes. A primeira, mais prática, nos diz que o método quântico para a determinação da resposta melhora o desempenho do sistema numa taxa de 2 para 1, ou seja, realiza apenas uma medida enquanto, classicamente, seriam necessárias duas.

A segunda, mais subjetiva, nos diz que a interação entre os Qubits e a estrutura quântica do sistema (as adaptações pelas quais o sistema passou para que pudesse ser realizado quanticamente) é capaz de produzir uma informação outrora inacessível pelos métodos clássicos. Em outras palavras, o sistema clássico não acessa o bit de informação relacionado à natureza da função ser *Balanceada/Constante*, mas ele está lá para ser acessado pelo sistema quântico. Daí, tiramos que o plano de fundo quântico nos permite perscrutar interações muito mais ricas no intuito de aumentar a quantidade de informação disponível.

Referências

[1] Vlatko Vedral: *Introduction to Quantum Information Science*, Oxford University Press
Vol. 1 Year 2006

[2] Asher Peres: *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers
Vol. 72 Year 1995

[3] Michael A. Nielsen and Isaac L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press
Vol. 1 Year 2000