Revista Brasileira de Ensino de Física, vol. 43, e20210088 (2021)
www.scielo.br/rbef
DOI: https://doi.org/10.1590/1806-9126-RBEF-2021-0088

Artigos Gerais

O isomorfismo inesperado entre um sistema de bilhar e um algoritmo quântico

The unexpected isomorphism between a billiard system and a quantum algorithm

Vitor Lucas O. Sena*[1], Diogo O. Soares-Pinto[1]

[1]Universidade de São Paulo, Instituto de Física de São Carlos, São Carlos, SP, Brasil.

Recebido em 08 de março de 2021. Revisado em 09 de junho de 2021. Aceito em 14 de junho de 2021.

O matemático Gregory Galperin desenvolveu, em seu artigo "Playing Pool with π", um incrível método para calcular os dígitos do número π, com precisão arbitrária, fazendo uso de um sistema elementar da Física em Mecânica Clássica: colisões elásticas em uma dimensão. Inspirado no trabalho de Galperin, Adam Brown demonstrou que existe um isomorfismo entre o sistema físico usado por Galperin e um famoso algoritmo quântico de busca: o algoritmo de Grover. O presente projeto visa entender o porquê desse isomorfismo. Desenvolvemos os resultados de forma original demonstrando, explicitamente, como o isomorfismo entre esses dois sistemas surge a partir de seus espaços de configuração.
Palavras-chave: Colisões elásticas, espaços de configuração, Computação Quântica, algoritmo de Grover.

The mathematician Gregory Galperin developed in his article "Playing Pool with π", an incredible method for calculating the digits of the number π with an arbitrary precision, making use of an elementary system of Physics in Classical Mechanics: elastic collisions in one dimension. Inspired by Galperin's work, Adam Brown demonstrated that there is an isomorphism between the physical system used by Galperin and the famous quantum search algorithm: Grover's algorithm. The present project aims to understand the reason for this isomorphism. We develop the results in an original way explicitly demonstrating how the isomorphism between these two systems arises from their configuration spaces.
Keywords: Elastic colisions, configuration spaces, Quantum Computing, Grover's algorithm.

1. Introdução

O biólogo Magnus Equist, ao estudar como nós, humanos, identificamos beleza nas coisas constatou que essa habilidade está fortemente ligada ao nosso reconhecimento de padrões [1], o que em Matemática associamos a simetria. Daí, emerge uma das nossas capacidades mais poderosas nas ciências: a de conseguirmos enxergar em coisas a priori distantes relações que as conectam intimamente. Nesse sentido, a Física e a Matemática podem vir a nos inspirar de maneiras surpreendentes. A riqueza de aprendizado, conhecimento e fascínio que surgem disso, suscitam a concepção da ciência como não somente útil, mas intrinsecamente bela. O nosso trabalho visa estudar a não tão óbvia relação entre um sistema simples de bilhar clássico, um algoritmo quântico de busca e o número π.

O número π é, provavelmente, o número irracional mais importante da Matemática[1] e obtê-lo sempre foi um desafio. Matemáticos desenvolveram métodos da Aritmética (e.g. séries geométricas) à Computação (e.g. método de Monte Carlo) para calcular esse número, e também alguns bem curiosos como o método das agulhas de Buffon [2]. Entretanto, aquele descrito na Sec. 2 deste trabalho é um dos menos ortodoxos dentre todos esses. Tal método foi desenvolvido pelo matemático Galperin [3] utilizando um sistema bastante familiar para qualquer físico: duas bolas colidindo elasticamente entre si e com uma parede, também conhecido por pesquisadores de sistemas dinâmicos como um problema de bilhar.

A. B. Katok, coloquialmente, disse que os problemas de bilhar são uma espécie de playground para físicos e matemáticos. Nós podemos entender essa afirmação de um ponto de vista lúdico - que não deixa de estar correto, ou de um ponto de vista mais sério, entendendo que ele se referenciou a esse tipo de sistema como um "solo de testes" para hipóteses, conjecturas e relações [4]. Foi nessa brincadeira que Galperin concluiu que, desse problema unidimensional de colisões, poderia-se aferir os dígitos de π, com uma precisão arbitrária, simplesmente contando o número de colisões no sistema.

Como se não bastasse esse desdobramento bastante exótico, o físico Adam Brown propôs um isomorfismo entre esse sistema de bilhar e o algoritmo quântico de busca [5]. O que nós fizemos, portanto, foi concatenar todos esses assuntos num só lugar. Inspirados no trabalho [6], derivamos o resultado que comprova como o número π surge a partir do sistema de bilhar definido

* Endereço de correspondência: vitorlucasena@gmail.com
[1] Discutivelmente, o número de Euler (e) divide o pódio com ele.

por Galperin; demonstramos, com uma análise original, como funciona o algoritmo de Grover; e, ao final, traçamos discussões a respeito de ambos os sistemas, apresentando, dentre outras coisas, uma proposta de revisão a um dos resultado obtidos por Adam Brown.

2. Bolas de bilhar

Um sistema de bilhar é um sistema de partículas, numa região limitada, colidindo entre si e com as fronteiras dessa região. Esse nome é, de fato, inspirado no famoso jogo de bilhar de mesas retangulares, mas pode-se elaborar tal sistema de maneira mais abstrata, variando-se a dimensão e forma dessa "mesa" e a quantidade e tipo de bolas em jogo.

2.1. Sistema unidimensional de colisões elásticas

O sistema tratado aqui será unidimensional. Ele se constitui de duas bolas diferentes, uma com massa M e outra com massa m, em que $M \geq m$; e de uma parede que considera-se ter massa infinita. Para facilitar a comunicação, iremos nos referir às bolas como "bola M" e "bola m", respectivamente.

Embora na Figura 1 as bolas possuam dimensão, isso é apenas ilustrativo - consideremo-las partículas pontuais. Todas as colisões são perfeitamente elásticas, o sistema como um todo encontra-se em repouso a partir de um referencial inercial e não existe qualquer tipo de atrito ou dissipação no problema [7]. O sentido positivo das velocidades é da esquerda para a direita. Por mais simplificada que essa construção possa parecer, ela será suficiente para depreender de tudo que precisamos.

Num primeiro momento, o nosso objetivo é identificar como esse sistema se relaciona com o número π. Galperin abordou tal problema[2] num artigo que veio a público em 2003 [3], no qual ele respondeu a seguinte pergunta: dadas duas bolas inicialmente sem velocidade, como as ilustradas na Figura 1, ao ser concedida uma velocidade inicial positiva v à bola M, qual o número de colisões máximo que este sistema terá? Ele concluiu que

$$k \equiv \#\text{colisões} = \left\lfloor \pi \sqrt{\frac{M}{m}} \right\rfloor \tag{1}$$

onde # denota *número* e $\lfloor a \rfloor$ denota *o maior inteiro menor que a*.

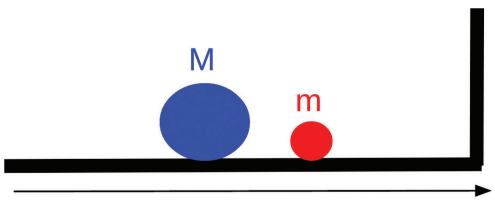


Figura 1: Sistema de bilhar 1D de dois corpos.

[2] Veja também as Refs. [8, 9] para mais detalhes.

Veja desse resultado que se, por exemplo, $M/m = 100^d$, sendo d um número natural[3], o número de colisões no sistema será os dígitos de π, sem a vírgula, até a d-ésima casa decimal. Dedicaremo-nos a provar o resultado da Eq. (1) ao longo de todo o resto da Sec. 2.

2.2. Evolução do sistema de bilhar

Como construído, o sistema envolve dois corpos movendo-se linearmente no espaço, livres para colidir entre si e com uma parede. Essa construção é completamente clássica e, como as colisões são perfeitamente elásticas, duas leis de conservação básicas devem ser respeitadas, a de energia e a de momento linear[4]

$$\frac{1}{2}Mv^2 + \frac{1}{2}mu^2 = E = \text{constante}, \tag{2}$$

$$Mv + mu = p(t), \tag{3}$$

em que v é a velocidade da bola M, e u, a velocidade da bola m. O fato de o momento linear ser dependente do tempo será explorado, com algum detalhe, na Sec. 4.2. Por ora, busquemos modelar o comportamento do sistema.

No espaço de configuração das velocidades, a equação da energia configura uma elipse, mas guiados pela busca de simplicidade, é conveniente projetá-la numa circunferência; como ilustrada na Figura 2, a seguinte mudança de coordenadas vem a calhar: $y = \sqrt{m}u$, $x = \sqrt{M}v$. Com essa parametrização, as leis de conservação tornam-se

$$\frac{1}{2}(x^2 + y^2) = \text{constante}, \tag{4}$$

$$y = \tilde{p}(t) - \sqrt{\frac{M}{m}}x, \tag{5}$$

onde $\tilde{p}(t) \equiv p(t)/\sqrt{m}$.

Os estados de velocidades acessíveis ao sistema estão sobre a circunferência, cujo comprimento é fixo para uma dada energia, como visto na Eq. (2). Inicialmente, a bola de massa M move-se com uma velocidade v constante em direção à bola de massa m, que se encontra com velocidade nula. O ponto sobre a circunferência na Figura 3 representa o estado do sistema no plano xy.

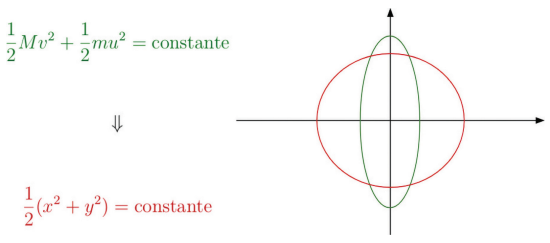


Figura 2: Mudança de coordenadas $y = \sqrt{m}u$, $x = \sqrt{M}v$.

[3] Considere 0 um número natural.

[4] A lei descrita na Eq. (3) não é uma *lei de conservação* stricto sensu, uma vez que, na prática, o momento linear total $p(t)$ varia com o tempo, mas nos permitiremos usar essa terminologia por praticidade. Esse detalhe é melhor discutido na Sec. 4.2.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2021-0088

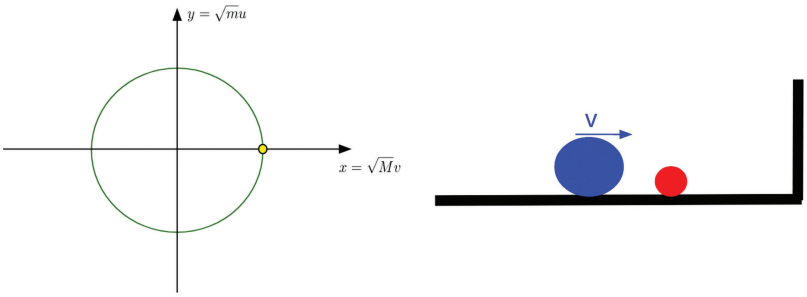


Figura 3: Estado inicial do sistema ($t = t_0$).

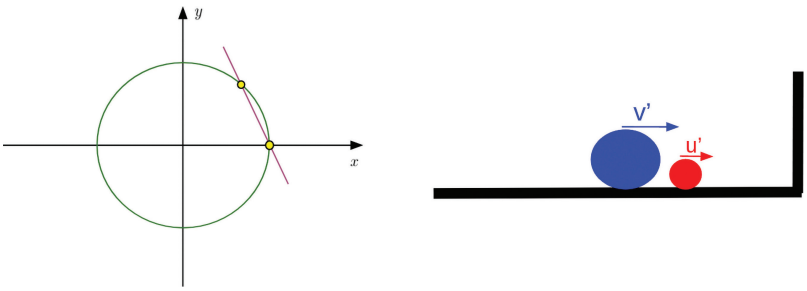


Figura 4: Sistema após a primeira colisão ($t = t_1$).

Sendo a velocidade das bolas, após a colisão, v' e u', pela conservação de energia, temos:

$$\frac{1}{2}Mv^2 + \frac{1}{2}mu^2 = \frac{1}{2}M(v')^2 + \frac{1}{2}m(u')^2,$$

e pela conservação do momento linear, temos:

$$Mv + mu = Mv' + mu'.$$

A solução desse sistema para u' e v' é

$$u' = \left(\frac{m-M}{M+m}\right)u + \left(\frac{2M}{M+m}\right)v, \tag{6}$$

$$v' = \left(\frac{2m}{M+m}\right)u + \left(\frac{M-m}{M+m}\right)v, \tag{7}$$

ou, na forma matricial, com $r \equiv M/m$

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \underbrace{\begin{pmatrix} \left(\frac{1-r}{1+r}\right) & \left(\frac{2r}{1+r}\right) \\ \left(\frac{2}{1+r}\right) & -\left(\frac{1-r}{1+r}\right) \end{pmatrix}}_{\equiv R(r)} \begin{pmatrix} u \\ v \end{pmatrix},$$

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = R(r) \begin{pmatrix} u \\ v \end{pmatrix}. \tag{8}$$

A operação $R(r)$ na Eq. (8), assim, representa a colisão das bolas uma com a outra no sistema físico. Após a primeira colisão, ambas estarão movendo-se para a direita (Figura 4 à direita). Devido ao vínculo da energia, o ponto que representa o estado do sistema no espaço de configuração deverá continuar sobre a circunferência, mas onde exatamente? Bem, basta nos lembrarmos do vínculo do momento linear, que, no plano xy, é dado pela reta da Eq. (5).

Colisões entre as bolas deixam o momento total $\tilde{p}(t)$ inalterado, isto é, $\tilde{p}(t_0) = \tilde{p}(t_1)$. Portanto, o próximo ponto deve estar sobre a mesma reta que o primeiro. Tendo o coeficiente angular fixado, resta-nos uma única alternativa (Figura 4 à esquerda).

Já que $M \geq m$, constata-se que $u' > v'$, de forma que a próxima colisão da bola m certamente será com a parede[5]. Como estamos considerando uma parede de massa infinita, o momento linear da bola m inverterá seu sentido, passando de mu' para $-mu'$, o que também altera o valor do momento linear total do sistema, i.e., $\tilde{p}(t_1) \neq \tilde{p}(t_2)$. Algebricamente, temos

$$\begin{pmatrix} u'' \\ v'' \end{pmatrix} = \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}}_{\equiv S} \begin{pmatrix} u' \\ v' \end{pmatrix},$$

$$\begin{pmatrix} u'' \\ v'' \end{pmatrix} = S \begin{pmatrix} u' \\ v' \end{pmatrix}. \tag{9}$$

A operação S na Eq. (9) representa uma colisão da bola m com a parede. No espaço de configuração, isso se traduz numa reflexão do estado sobre o eixo x, conforme mostrado na Figura 5.

Assim,

$$\begin{pmatrix} u^{(j)} \\ v^{(j)} \end{pmatrix} = SR(r) \begin{pmatrix} u^{(j-2)} \\ v^{(j-2)} \end{pmatrix},$$

[5] Para ver que $u' > v'$, subtrai-se as Eqs. (6) e (7), respectivamente; assim: $u' - v' = v - u > 0 \Rightarrow u' > v'$.

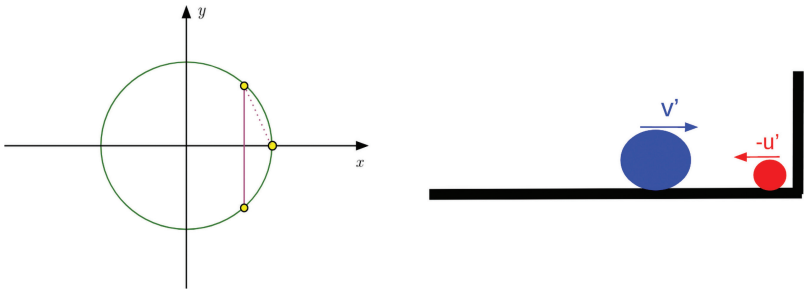


Figura 5: Sistema após a primeira colisão da bola m com a parede ($t = t_2$).

Esses são os dois únicos tipos de colisão possíveis nesse sistema: da bola M com a bola m e da bola m com a parede. Note que, na próxima colisão bola-bola, a trajetória no espaço de configuração será descrita por uma outra reta com o mesmo coeficiente angular da primeira, mas deslocada um pouco à esquerda, justamente pela variação no momento linear total do sistema que aconteceu na colisão bola-parede (vide Eq. (5)). Dessa forma, a evolução do sistema pode ser descrita por sucessivas aplicações de $R(r)$ e S no estado inicial

$$\begin{pmatrix} u^{(j)} \\ v^{(j)} \end{pmatrix} = SR(r)SR(r)...SR(r)SR(r) \begin{pmatrix} u^{(0)} \\ v^{(0)} \end{pmatrix} \qquad (10)$$

até o ponto em que $u^{(j)}$ e $v^{(j)}$ sejam ambos negativos (bolas indo para a esquerda no espaço real) e $|v^{(j)}| > |u^{(j)}|$, garantindo-nos que não haverá mais nenhum tipo de colisão no sistema. Chamaremos esse estado de *estado terminal*.

2.3. Contagem das colisões

A construção da Sec. 2.2 deve nos levar ao número de colisões k dado na Eq. (1). Como os pontos na Figura 6 representam os estados assumidos pelo sistema, a quantidade deles menos 1 (da configuração inicial) nos dá o número de colisões totais que ocorreram.

$$\#\text{estados} - 1 = \#\text{colisões} = \#\text{arcos sobre } \theta \qquad (11)$$

As retas transversais possuem o mesmo coeficiente angular, são paralelas entre si; assim como as verticais, obviamente. Logo, o ângulo formado entre essas retas é sempre o mesmo (θ), tais quais os arcos de circunferência que eles subtêm, conforme ilustrado na Figura 6. Dada a relação da Eq. (11), podemos contar o número de colisões a partir do número de arcos subtendidos por θ. Como é mais fácil trabalhar com ângulos a partir do centro da circunferência, faremos uso do Teorema do ângulo inscrito, ilustrado na Fig 7.

Teorema 1 (Teorema do ângulo inscrito)**.** *Numa circunferência, a medida do ângulo central é igual ao dobro da medida do ângulo inscrito que subtende o mesmo arco.*

Isso significa que, a cada colisão, cobre-se na circunferência do espaço de configuração um arco proporcional

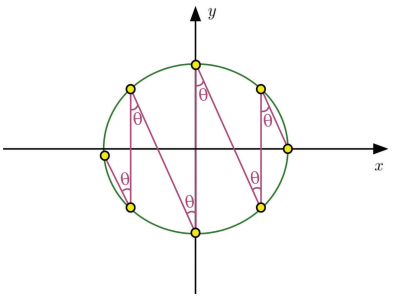


Figura 6: Ângulo formado entre as retas da Eq. (5) e a vertical.

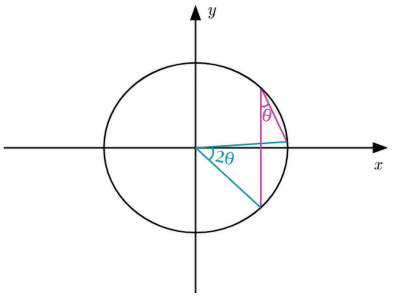


Figura 7: Ilustração do Teorema do ângulo inscrito para o nosso caso.

a 2θ, conforme vimos nas Figs. 4 e 5. Uma vez que a bola de massa M passa a ter uma velocidade negativa (estados passem ao segundo e terceiro quadrante no espaço de configuração), ela não pode voltar a ter sua velocidade aumentada positivamente, pois, nem a parede, nem a bola m podem contribuir para tal acréscimo, já que estão sempre à direita da bola M. Em outras palavras, no espaço de configuração, o estado só pode caminhar da direita para a esquerda, sempre cobrindo novos arcos correspondentes a 2θ.

Então há um limite para a evolução do sistema – ele deve chegar, em algum momento, num estado terminal, já que o comprimento da circunferência é finito. A razão para isso é puramente geométrica e nos trará justamente a resposta da nossa pergunta: quantas colisões teremos no sistema até que ele alcance o estado terminal? Equivalentemente, quantos arcos proporcionais a 2θ podemos somar antes que o valor dessa soma supere 2π

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2021-0088

(comprimento da circunferência)?

$$2\theta + 2\theta + \cdots + 2\theta < 2\pi \;\Rightarrow\; k\theta < \pi. \tag{12}$$

Por exemplo, se θ fosse 0.01, $k = 314$ respeitaria a inequação (12), já $k = 315$ a violaria. O número de colisões do sistema será, portanto, o maior k que não viola essa desigualdade.

O cálculo de θ é simples, basta lembrar (vide Eq. (5)) que o coeficiente angular da reta transversal à circunferência é $-\sqrt{\frac{M}{m}}$. Sendo θ o ângulo de referência,

$$\tan\theta = -\frac{1}{\text{coef ang}} \;\Rightarrow\; \tan\theta = \sqrt{\frac{m}{M}} \;\Rightarrow$$
$$\Rightarrow\; \theta = \arctan\sqrt{\frac{m}{M}}. \tag{13}$$

Perceba que, à medida que M aumenta, a aproximação $\arctan x \approx x$ melhora cada vez mais. Uma maneira de justificar algebricamente essa aproximação é pela expansão de Taylor do $\arctan x$,

$$\arctan x = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 + \ldots \;\Rightarrow\; \arctan x = x - O(x^3),$$

significando que quando $x \ll 1$ haverá apenas um erro de ordem cúbica à aproximação.

Assim, dado que k é o número de colisões que acontecem no sistema, uma vez que $\theta = \arctan\sqrt{m/M} \approx \sqrt{m/M}$, temos

$$k\sqrt{\frac{m}{M}} < \pi,$$

ou seja, o maior k que não viola essa desigualdade, de fato, é descrito pela Eq. (1). Para o caso especial em que $M/m = 100^d$, encontra-se $k\left(\frac{1}{10}\right)^d < \pi$. O maior inteiro k que não satura esta desigualdade será igual aos dígitos de π até a d-ésima casa decimal, como queríamos demonstrar.

3. Algoritmos quânticos

Um algoritmo é uma sequência finita de ações executáveis que visam chegar à solução de um determinado tipo de problema [10], sendo os algoritmos quânticos aqueles que se utilizam de princípios da teoria quântica para chegar a essa resposta. Esta definição é geral, aqui, no entanto, ateremo-nos a um problema específico: realizar uma busca numa base de dados aleatória. Por exemplo, imagine que gostaríamos de encontrar o caminho mais curto entre duas cidades A e B. Um algoritmo para encontrá-lo seria: percorrer todas as N rotas possíveis, enquanto armazena-se numa memória as distâncias de cada uma delas para, ao fim, compará-las e determinar a mais curta. Essa descrição bem ilustra que um algoritmo clássico leva, invariavelmente, algo da ordem de N iterações ($\mathcal{O}(N)$) para encontrar o caminho ótimo entre A e B. No entanto, existe um algoritmo quântico, idealizado por Lov Grover [11], que se propõe a solucionar este problema em $\mathcal{O}(\sqrt{N})$ iterações.

O potencial do algoritmo de Grover (como este é conhecido) em solucionar problemas de busca com uma aceleração quadrática se comparado ao seu equivalente clássico, torna-o digno da nossa atenção. Vejamos como esta melhora é possível.

3.1. O algoritmo de Grover

Dentre as várias maneiras de se fazer Computação Quântica [10, 12], fundamentaremos a análise a seguir num modelo bastante simples: um vetor $|\psi\rangle$, que encapsula um certo estado inicial, terá sua evolução dada por aplicações sucessivas de operadores unitários U_i sobre ele até que chegue num estado final $|\psi_k\rangle$; ou seja, $|\psi_k\rangle = U_k \ldots U_1 |\psi\rangle$. Os vetores $|\psi\rangle$ pertencem a um espaço de Hilbert de dimensão N, e U_i são operadores associados a esse espaço.

O problema de busca pode ser definido assim: numa base de dados ($\mathbb{X}$) de N elementos, queremos encontrar n dos quais são soluções do nosso problema. Claramente, $n \leq N$. Se a solução for única, $n = 1$. Para sermos o mais democráticos possível, digamos que o nosso estado inicial, representando os elementos do conjunto $\mathbb{X}$, é uma superposição igualmente balanceada nas amplitudes de probabilidade de todos os possíveis estados $\{|x\rangle\}$, que formam uma base ortonormal. Cada estado dessa base mapeia um único elemento do conjunto de busca. Assim,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{14}$$

Grover propôs que atuação iterativa de dois operadores é suficiente para resolver esse problema. O primeiro operador é chamado de *oráculo*. Digamos que a solução do nosso problema seja descrita por $|s\rangle$, o que o oráculo faz é inverter a amplitude de probabilidade deste estado dentro de $|\psi\rangle$. Sendo I a identidade, o operador que descreve essa ação é

$$U_s \equiv I - 2\,|s\rangle\,\langle s|. \tag{15}$$

A segunda operação é a chamada *inversão em torno da média*. Ficará claro o porquê desse nome na Sec. 3.2, mas – por enquanto – vamos nos ater a sua forma operacional

$$U_\psi^\perp \equiv 2\,|\psi\rangle\,\langle\psi| - I. \tag{16}$$

Existe uma bela e interessante razão para usarmos esses operadores: eles garantem que o algoritmo de Grover seja ótimo em solucionar o problema de busca, isto é, que nenhum outro algoritmo quântico possa superá-lo em eficiência, conforme provado por Grover [11]. Para nossos propósitos, você pode imaginá-los apenas como "operações espertas" que Grover formulou para resolver o problema de busca, o que não deixa de ser verdade.

Ainda assim, é válido perguntarmo-nos aqui se o uso das operações descritas nas Eqs. (15) e (16) é honesto, em especial essa primeira. A formulação da teoria quântica pressupõe que nós não tenhamos total acesso ao estado com o qual estamos lidando, a menos que performemos uma medição sobre ele. No entanto, uma das vantagens de uma computação quântica é a de podermos manipular esses estados mesmo sem necessariamente medi-los. Nós não precisamos conhecer $|s\rangle$ para sermos capazes de construir o oráculo.

O uso de oráculos é razoavelmente comum em Ciência da Computação. Tentemos entender seu uso com o exemplo prático apresentado na Ref. [10] sobre fatoração de números. Considere um número m cujos fatores primos, a priori desconhecidos, são p e q. Naturalmente, se soubermos um dos fatores teremos o outro de maneira direta, pois $p = m/q$ e $q = m/p$. É possível imaginar esse problema como um problema de busca: numa base de dados (conjunto dos números naturais de 2 até $\sqrt{m}$) queremos encontrar um dos fatores primos de m, digamos q. Mesmo sem conhecer q, podemos, dado um número qualquer g, testar se g é ou não um fator de m simplesmente checando se m/g é um número natural. Em outras palavras, reconhecer se g é ou não fator de m é completamente factível mesmo que não conheçamos os fatores p e q. O que a operação dada na Eq. (15) faz é algo parecido; ela testa todos os estados da base que constitui $|\psi\rangle$ e apenas identifica o estado $|s\rangle$ multiplicando a sua amplitude de probabilidade por -1. Em suma, é possível atestar a existência da solução de um certo problema sem necessariamente precisar conhecê-la.[6]

Para que fique mais explícito o funcionamento do algoritmo de Grover, façamos o exemplo de $N = 8$. Classicamente, esperaríamos, em média, $N/2 \sim 4$ iterações até que a solução fosse encontrada [10]; quanticamente, esperaríamos $\sim \sqrt{N} \sim 2$, isto é, apenas duas iterações![7] Façamos o cálculo do caso quântico. A Eq. (14) para $N = 8$ resulta no estado

$$\begin{aligned} |\psi\rangle \;=\; & \frac{1}{\sqrt{8}}|0\rangle + \frac{1}{\sqrt{8}}|1\rangle + \frac{1}{\sqrt{8}}|2\rangle + \frac{1}{\sqrt{8}}|3\rangle \\ & + \frac{1}{\sqrt{8}}|4\rangle + \frac{1}{\sqrt{8}}|5\rangle + \frac{1}{\sqrt{8}}|6\rangle + \frac{1}{\sqrt{8}}|7\rangle\,, \end{aligned}$$

retratado esquematicamente na Figura 8.
Busquemos, por exemplo, o valor $|s\rangle = |3\rangle$. Pela Eq. (15), vê-se que $U_s = I - 2\,|3\rangle\langle 3|$, e então

$$\begin{aligned} U_s|\psi\rangle \;=\; & \frac{1}{2\sqrt{2}}|0\rangle + \frac{1}{2\sqrt{2}}|1\rangle + \frac{1}{2\sqrt{2}}|2\rangle - \frac{1}{2\sqrt{2}}|3\rangle \\ & + \frac{1}{2\sqrt{2}}|4\rangle + \frac{1}{2\sqrt{2}}|5\rangle + \frac{1}{2\sqrt{2}}|6\rangle + \frac{1}{2\sqrt{2}}|7\rangle \end{aligned}$$

[6] Caso seja de seu interesse um aprofundamento no tema, deixamos como sugestão as Refs. [13], [14] e [15], que discutem a construção do algoritmo de Grover com bastante didática e exemplos práticos.
[7] Você pode argumentar (com razão) que $\sqrt{8}$ é muito mais próximo de 3 do que é de 2. No entanto, mostraremos na seção seguinte que o algoritmo de Grover retorna a solução com boa precisão para $\approx \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$.

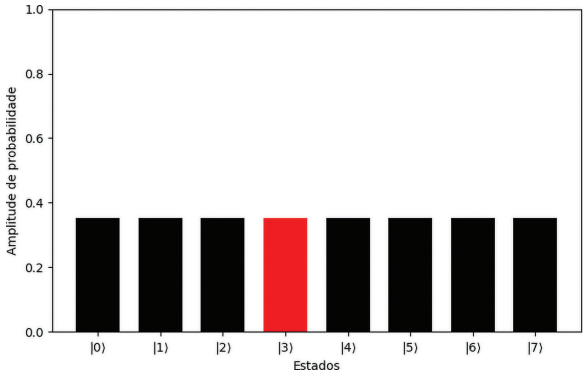


Figura 8: Estado inicial do algoritmo de Grover para $N = 8$.

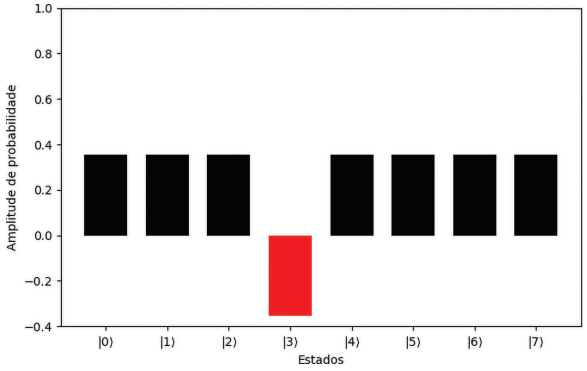


Figura 9: Estado após a primeira aplicação de U_s.

$$U_s|\psi\rangle = |\psi\rangle - \frac{2}{2\sqrt{2}}|3\rangle\,.$$

Estado este representado na Figura 9.

A próxima operação é $U_\psi^\perp$, definida na Eq. (16),

$$\begin{aligned} U_\psi^\perp U_s|\psi\rangle \;&=\; [2\,|\psi\rangle\langle\psi| - I]\left[|\psi\rangle - \frac{2}{2\sqrt{2}}|3\rangle\right] \\ &=\; 2|\psi\rangle\langle\psi|\psi\rangle - \frac{4}{2\sqrt{2}}|\psi\rangle\underbrace{\langle\psi|3\rangle}_{1/\sqrt{8}} - |\psi\rangle + \frac{2}{2\sqrt{2}}|3\rangle \\ &=\; \frac{1}{2}|\psi\rangle + \frac{1}{\sqrt{2}}|3\rangle. \end{aligned}$$

Mas note que $|\psi\rangle$ possui uma componente $|3\rangle$. Escrevendo a Eq. (14) para $N = 8$ e separando essa componente, temos o estado

$$U_\psi^\perp U_s|\psi\rangle \;=\; \frac{1}{2}\left(\frac{1}{2\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle\right) + \frac{1}{4\sqrt{2}}|3\rangle + \frac{1}{\sqrt{2}}|3\rangle\,,$$

$$U_\psi^\perp U_s|\psi\rangle \;=\; \frac{1}{4\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle + \frac{5}{4\sqrt{2}}|3\rangle\,,$$

representado na Figura 10.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2021-0088

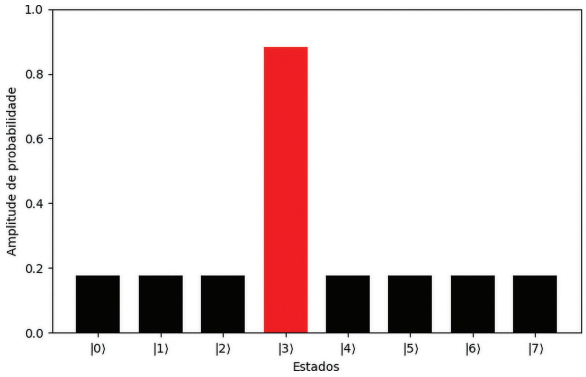


Figura 10: Estado após a primeira aplicação de $U_\psi^\perp$.

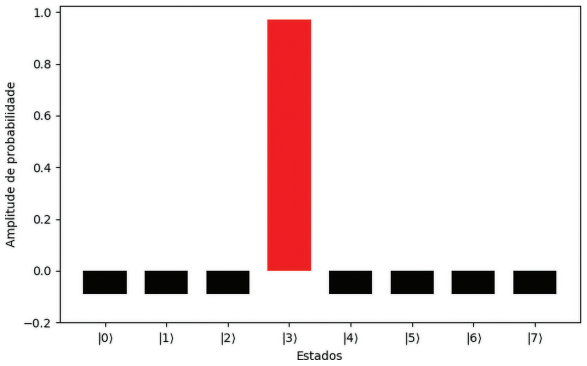


Figura 11: Estado após a segunda iteração de Grover.

Essas duas operações, nessa ordem, formam o que chamamos de *iteração de Grover* (G), de maneira que $G \equiv U_\psi^\perp U_s$. Uma vez ilustrada a amplificação da probabilidade de obter o estado desejado, faremos os cálculos da segunda iteração de Grover com menos detalhes. As etapas são as mesmas, primeiro, atua-se o oráculo

$$U_s G\left|\psi\right\rangle = \frac{1}{4\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{4}\left|x\right\rangle - \frac{5}{4\sqrt{2}}\left|3\right\rangle$$

e, em seguida, a inversão em torno da média

$$U_\psi^\perp U_s G\left|\psi\right\rangle = -\frac{1}{8\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{4}\left|x\right\rangle + \frac{11}{8\sqrt{2}}\left|3\right\rangle$$

$$\begin{aligned} G^2\left|\psi\right\rangle = &-\frac{1}{8\sqrt{2}}\left|0\right\rangle - \frac{1}{8\sqrt{2}}\left|1\right\rangle - \frac{1}{8\sqrt{2}}\left|2\right\rangle + \frac{11}{8\sqrt{2}}\left|3\right\rangle \\ &- \frac{1}{8\sqrt{2}}\left|4\right\rangle - \frac{1}{8\sqrt{2}}\left|5\right\rangle - \frac{1}{8\sqrt{2}}\left|6\right\rangle - \frac{1}{8\sqrt{2}}\left|7\right\rangle . \end{aligned}$$

Se medirmos o estado $G^2\left|\psi\right\rangle$ (ilustrado esquematicamente na Figura 11), obteríamos o elemento $\left|3\right\rangle$ com probabilidade $\left|\frac{11}{8\sqrt{2}}\right|^2 = 121/128 \approx 94,5\%$. Mesmo para poucos q-bits[8], o algoritmo de Grover responde corretamente à busca com boa margem, a probabilidade de acerto é 17 vezes maior que a de erro, e a precisão de acerto só melhora à medida que aumentamos N.

3.2. Uma análise geométrica

Voltemo-nos agora ao nosso objetivo central: encontrar o isomorfismo entre o sistema de bilhar e o algoritmo de Grover. Simularemos uma busca numa base de dados $\mathbb{X}$ com N elementos, o estado da Eq. (14) encapsula essa base de dados. Para facilitar nossa análise, consideraremos dois subconjuntos: $\mathbb{S}$, com n elementos (as *soluções* da busca), e $\mathbb{W}$, com $N-n$ elementos (*não-soluções* da busca), tal que $\mathbb{X} = \mathbb{S}\cup\mathbb{W}$. Respeitando a normalização, define-se os estados que representam uma superposição dos elementos de $\mathbb{S}$ e $\mathbb{W}$, respectivamente.

$$\left|s\right\rangle \equiv \frac{1}{\sqrt{n}}\sum_{x\in\mathbb{S}}\left|x\right\rangle ; \tag{17}$$

$$\left|w\right\rangle \equiv \frac{1}{\sqrt{N-n}}\sum_{x\in\mathbb{W}}\left|x\right\rangle . \tag{18}$$

Usando estes resultados na Eq. (14), temos

$$\left|\psi\right\rangle = \sqrt{\frac{n}{N}}\left|s\right\rangle + \sqrt{\frac{N-n}{N}}\left|w\right\rangle . \tag{19}$$

Inspirados no desenvolvimento feito na Ref. [12], descreveremos as amplitudes de probabilidade em termos de um ângulo θ

$$\sin\theta \equiv \sqrt{\frac{n}{N}}, \tag{20}$$

de maneira que

$$\left|\psi\right\rangle = \sin\theta\left|s\right\rangle + \cos\theta\left|w\right\rangle . \tag{21}$$

Para nos auxiliar nas contas, construiremos um vetor ortogonal $\left|\phi\right\rangle$ a $\left|\psi\right\rangle$, dado por

$$\left|\phi\right\rangle = \cos\theta\left|s\right\rangle - \sin\theta\left|w\right\rangle . \tag{22}$$

Também nos ajudará definir um espaço de coordenadas ortonormal em $\left|w\right\rangle$ e $\left|s\right\rangle$. Nesse espaço, podemos delinear uma circunferência de raio unitário fazendo alusão ao fato de a probabilidade estar normalizada a 1. Isso implica que qualquer vetor de estado nesse espaço deve estar restrito a tal circunferência. Na Figura 12, ilustra-se o espaço de configuração que descreve esse sistema.

Perceba das Eqs. (21) e (22), que $\{\left|\psi\right\rangle, \left|\phi\right\rangle\}$ também forma uma base ortonormal, de maneira que podemos

[8] O q-bit é a unidade básica de informação quântica, tal qual o bit é a unidade básica de informação clássica. Os q-bits formam uma base num espaço de Hilbert e nos permitem descrever, por exemplo, um estado genérico de 1 q-bit como uma superposição do tipo $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$, em que $|\alpha|^2 + |\beta|^2 = 1$.

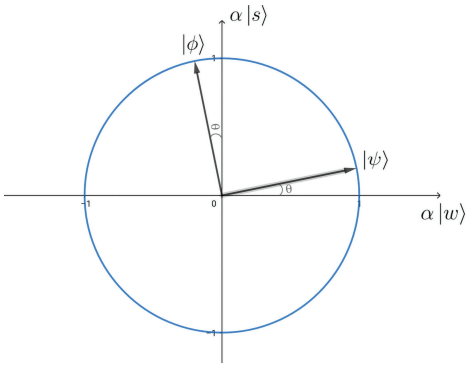


Figura 12: Gráfico do estado inicial no algoritmo de Grover. Nos eixos, α é uma constante maior que um ($\alpha > 1$) posta apenas para melhorar a escala do gráfico.

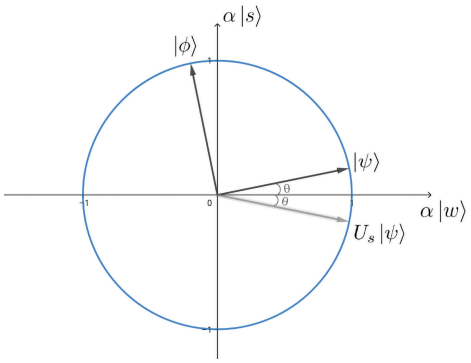


Figura 13: Primeira aplicação de U_s sobre o estado inicial.

alternar nossa descrição entre esta e a base $\{|w\rangle, |s\rangle\}$, visto que

$$|w\rangle = \cos\theta\,|\psi\rangle - \sin\theta\,|\phi\rangle\,; \tag{23}$$

$$|s\rangle = \sin\theta\,|\psi\rangle + \cos\theta\,|\phi\rangle\,. \tag{24}$$

Usaremos esse "truque" de alternar entre as bases para facilitar as contas. Lembre-se, o que nos interessa é saber como $|\psi\rangle$ evolui. Vejamos o que acontece em cada etapa do algoritmo. Primeiro, na aplicação de U_s:

$$U_s\,|\psi\rangle = -\sin\theta\,|s\rangle + \cos\theta\,|w\rangle = \cos(2\theta)\,|\psi\rangle - \sin(2\theta)\,|\phi\rangle\,.$$

Na Figura 13, vê-se que, no espaço de estados, U_s faz uma reflexão em torno do eixo $|w\rangle$. Se nós olharmos para as definições dos operadores nas Eqs. (15) e (16) e comparámo-los, fica claro que, na base $\{|\psi\rangle, |\phi\rangle\}$, $U_\psi^\perp$ faz uma reflexão em torno de $|\psi\rangle$, por isso o nome "inversão em torno da média". Assim, quando calculamos $U_\psi^\perp U_s\,|\psi\rangle$, obtemos (esquema na Figura 14)

$$\begin{aligned} U_\psi^\perp U_s\,|\psi\rangle &= \cos(2\theta)\,|\psi\rangle + \sin(2\theta)\,|\phi\rangle \\ &= \sin(3\theta)\,|s\rangle + \cos(3\theta)\,|w\rangle \end{aligned}$$

A combinação dessas duas reflexões é uma rotação. Assim, podemos induzir que cada iteração de Grover

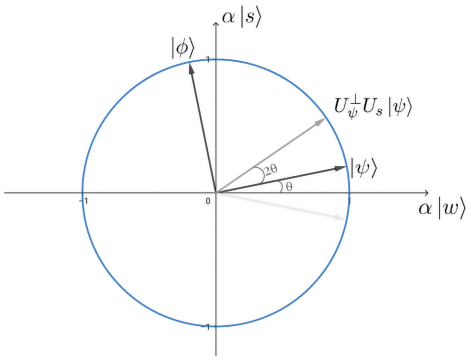


Figura 14: Aplicação de $U_\psi^\perp$ sobre o estado $U_s\,|\psi\rangle$. Final da primeira iteração de Grover.

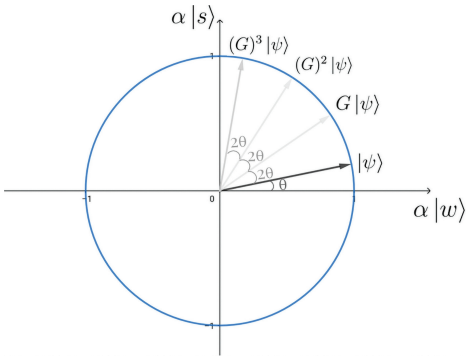


Figura 15: Iterações de Grover para $k = 3$.

rotaciona em 2θ o vetor de estado. Destarte, a forma geral do estado após k iterações de Grover é

$$(U_\psi^\perp U_s)^k\,|\psi\rangle = \cos(2k\theta)\,|\psi\rangle + \sin(2k\theta)\,|\phi\rangle\,; \tag{25}$$

$$(G)^k\,|\psi\rangle = \sin((2k+1)\theta)\,|s\rangle + \cos((2k+1)\theta)\,|w\rangle\,. \tag{26}$$

O objetivo do algoritmo é fazer com que o estado inicial tenda o tanto quanto possível à solução, ou seja, queremos $(G)^k\,|\psi\rangle \to |s\rangle$. O menor k que faz isso é aquele que torna o seno na Eq. (26) o mais próximo possível de 1, por isso, é necessário impor o vínculo $(2k+1)\theta \to \frac{\pi}{2}$. Assim,

$$(2k+1)\theta \leq \frac{\pi}{2} \;\Rightarrow\; k \leq \frac{\pi}{4\theta} - \frac{1}{2} \leq \frac{\pi}{4}\frac{1}{\arcsin\sqrt{\frac{n}{N}}} - \frac{1}{2}. \tag{27}$$

Como sabemos, para $x > 0$, temos $\frac{1}{x} \geq \frac{1}{\arcsin x}$, que tende à igualdade para x pequeno. Assim, o maior k que não viola a desigualdade (27) também é

$$k = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{n}} - \frac{1}{2} \right\rfloor. \tag{28}$$

Limitamos k inferiormente pela razão lógica de que queremos nos aproximar ao máximo da solução, mas sem correr o risco de passar dela. Assim, as iterações de Grover para um caso em que $k = 3$ funcionam como ilustrado na Figura 15.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2021-0088

4. O Isomorfismo de fato

Discutamos as simetrias e alguns detalhes importantes de ambos os sistemas fazendo as considerações necessárias.

4.1. O bilhar de Grover

Mapeemos o problema de bilhar no algoritmo de Grover e tentemos enxergar o isomorfismo entre eles de forma nítida. Algumas diferenças surgem de como lemos o problema, por exemplo, o algoritmo de Grover não conta a primeira colisão, mas começa a partir dela. Outra distinção está no método de contagem, já que as iterações de Grover correspondem a duas colisões simultâneas. Se ao invés disso contássemos o número de operações unitárias U_s e $U_\psi^\perp$ mais a condição inicial no algoritmo, teríamos $\tilde{k} \equiv 2k+1$ na Eq. (26). Assim $\tilde{k}\theta \to \frac{\pi}{2}$ e, portanto

$$\tilde{k} = \left\lfloor \frac{\pi}{2}\sqrt{\frac{N}{n}} \right\rfloor, \tag{29}$$

com $\tilde{k}$ sendo o número total de estados durante todo o processo. Note a semelhança da Eq. (29) com a Eq. (1). A diferença desse fator 1/2 vem do fato de, no algoritmo de Grover, percorrermos apenas metade do espaço de estados. Se modelássemos o número de operações no algoritmo de Grover pelas colisões no sistema de bilhar, deveríamos parar no momento em que a bola M transferisse toda a sua energia para a bola m, ou seja, na iminência de o sinal da velocidade da bola M se tornar negativo. Isso corresponde exatamente a percorrer metade do espaço de configuração, daí o fator 1/2. Veja que não há problema em parar em metade do espaço de configuração porque o critério de parada no algoritmo de Grover não é consequente, mas impositivo. Ilustra-se na Figura 16 a evolução dos dois espaços de fase pelo sistema de bolas de bilhar.

Analisando os detalhes dessa relação, conseguimos construir um isomorfismo entre cada entidade física dos dois sistemas, como mostrado na Tab. 1.

4.2. Discussões

- **Momento linear total variável**

Quando consideramos, na elaboração do sistema de bilhar (Sec. 2.1), que a parede tem massa infinita, ela acaba por funcionar como uma "sorvedouro de momento linear" do sistema, uma vez que, a cada colisão bola-parede, o momento linear total diminui. Veja que "aumentar" ou "diminuir" aqui depende apenas de uma convenção. Se o sentido de orientação do sistema fosse invertido, a parede seria uma "fonte de momento linear", o que não mudaria o problema como um todo – o que interessa é a variação do momento linear total em módulo.

- **Critério de parada**

Pode não ser tão óbvio que o sistema de bilhar vá chegar a um estado terminal, como foi afirmado na Sec. 2.2. A princípio, existem três possibilidades: (1) a velocidade da bola M é sempre positiva e a bola m oscila, indefinidamente, entre a bola M e a parede; (2) o sistema evolui até que a bola M passe a ter velocidade negativa, enquanto a bola m continua oscilando entre ela e a parede, infinitamente; (3) o sistema chega a um estado terminal em que $v^{(j)}$ e $u^{(j)}$ são ambas negativas e $|v^{(j)}| > |u^{(j)}|$, garantindo que elas não vão mais se tocar.

As situações (1) e (2) implicam um número infinito de colisões, enquanto (3), um número finito. Para nossa análise, usemos nas Eqs. (2) e (3), $r = M/m$, $\tilde{E} = 2E/m$ e $\tilde{p} = p(t)/m$,

$$u^2 + rv^2 = \tilde{E} \quad u + rv = \tilde{p}$$

A solução deste sistema para u e v é

$$u = \frac{\tilde{p} \pm \sqrt{r(\tilde{E}r + \tilde{E} - \tilde{p}^2)}}{r+1} \quad v = \frac{r\tilde{p} \pm \sqrt{r(\tilde{E}r + \tilde{E} - \tilde{p}^2)}}{r(r+1)}$$

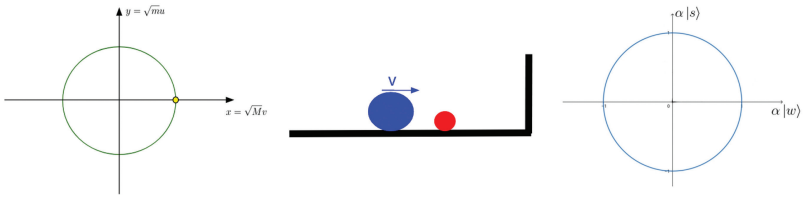
Como as velocidades devem ser valores reais, há um limite para o quanto $\tilde{p}$ pode aumentar: $\tilde{p}^2 \leq \tilde{E}(r+1) \Rightarrow |p| \leq \sqrt{2E(M+m)}$. Este resultado descarta a possibilidade (1), pois, para que ela fosse verdade, a bola m teria sua velocidade, em módulo, aumentada a passos cada vez maiores, fazendo o momento linear total do sistema, também em módulo, aumentar indefinidamente.

Embora (2) não possa ser descartada apenas com esse argumento ($|p|$ poderia tender assintoticamente ao seu limite superior), já sabemos com certeza que o sinal da velocidade da bola M irá inverter em algum momento, ou seja, o estado vai passar para o lado esquerdo do espaço de configuração. Daí podemos facilmente usar o argumento já apresentado na Seção 2.3 de que, dado que o sistema evolui a rotações de 2θ no espaço de configuração, como o comprimento da circunferência é finito, o número de colisões também deve ser finito. Isso exclui a possibilidade (2). Logo, o sistema evoluirá segundo (3). No algoritmo de Grover, o critério de parada é imposto. Nós *escolhemos* parar a evolução do sistema após um número específico de iterações.

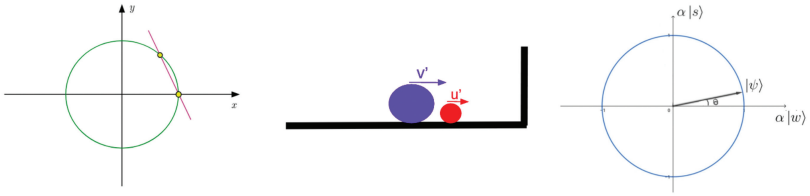
- **Aproximações espúrias?**

As conclusões tanto para o número de colisões do problema de bilhar, quanto para o número de iterações do algoritmo de Grover, baseiam-se em aproximações. No primeiro caso, que $\arctan x \approx x$ e, no segundo caso, que $\arcsin x \approx x$, em ambos considerando x pequeno.

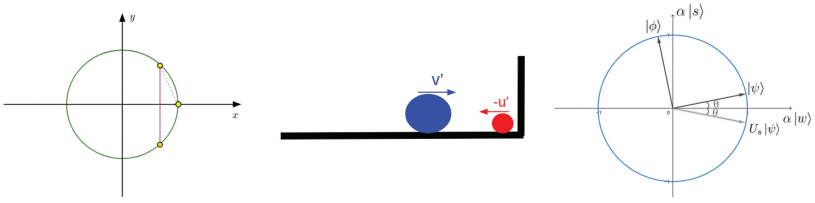
Não obstante essas aproximações pareçam bastante razoáveis, o problema aqui não é tão simples. Isso, porque nós estamos lidando com truncamentos da parte inteira de números reais, assim, uma pequena flutuação numa longínqua casa decimal é suficiente para alterar o nosso resultado. Uma vez que essas aproximações



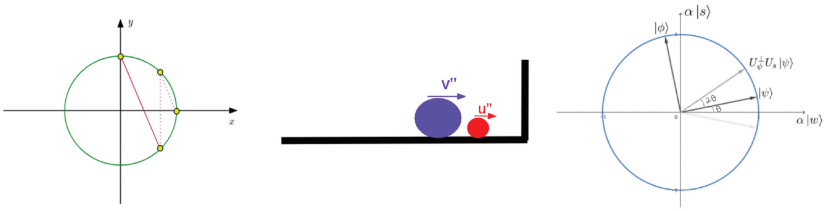
(a)Estado inicial. Não aparece no algorítimo de Grover.



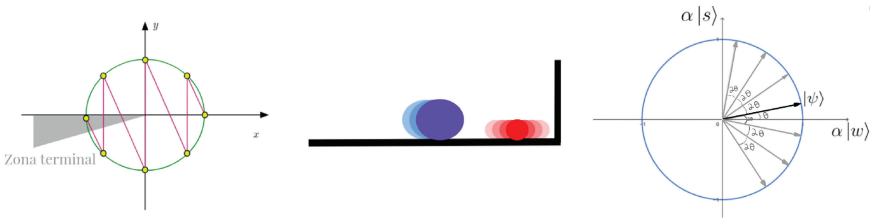
(b)Primeira colisão



(c)Segunda colisão, reflexão na parede.



(d)Terceira colisão geral, segunda entre as bolas.



(e)Evolução genérica do sistema.

Figura 16: Comparação entre os espaços de configuração sob a perspectiva do problema de bilhar.

Tabela 1: Mapa do isomorfismo entre o sistema de bilhar e o algoritmo de Grover.

Problema de bilhar	Algoritmo de Grover
Massa da bola maior: M	Número de elementos na base de dados: N
Massa da bola menor: m	Número de soluções na base de dados: n
Colisão entre as bolas: operação $R(r)$	Inversão em torno da média $U_\psi^\perp$
Colisão bola m – parede: operação S	Oráculo U_s
Alternância entre colisão bola-bola e bola-parede	Alternância entre U_s e $U_\psi^\perp$
Conservação da energia cinética	Conservação da probabilidade
Conservação do espaço de configuração	Unitariedade das operações
Movimento puramente horizontal	Funções de onda puramente reais
Ordem das colisões importa	U_s e $U_\psi^\perp$ não comutam

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2021-0088

sejam boas, as flutuações advindas desse truncamento não diferirão por mais que 1 do resultado "exato". Mas isso ainda nos é um problema, pois se o nosso objetivo é contar exatamente o número de colisões (ou iterações) do sistema, errar por ± 1 significa errar completamente!

Consideremos $M/m = N/n = 100^d$ (com $d \neq 0$). Para garantir nosso acerto, devemos assegurar que as relações das Eqs. (30) e (31) sejam verdadeiras,

$$\left\lfloor \frac{\pi}{\arctan\left(10^{-d}\right)} \right\rfloor = \left\lfloor \frac{\pi}{10^{-d}} \right\rfloor; \tag{30}$$

$$\left\lfloor \frac{\pi}{2} \frac{1}{\arcsin\left(10^{-d}\right)} \right\rfloor = \left\lfloor \frac{\pi}{2} \frac{1}{10^{-d}} \right\rfloor. \tag{31}$$

Assim como Galerin, somos fortemente inclinados a acreditar que estas relações são verdadeiras, embora não sejamos capazes de prová-las. Este é um problema ainda em aberto na matemática e, segundo Galperin, a melhor referência para tentar entendê-lo é a do matemático Alfred van der Poorten, que pode ser encontrada na Ref. [16].

No entanto, a crença nos resultados dado nas Eqs. (30) e (31) não é cega. Ela se fundamenta nos resultados dado nas Eqs. (32) e (33), que são passíveis de prova, como as feitas na Ref. [3].

$$\left\lfloor \frac{\sqrt{2}}{\arctan\left(10^{-d}\right)} \right\rfloor = \left\lfloor \frac{\sqrt{2}}{10^{-d}} \right\rfloor; \tag{32}$$

$$\left\lfloor \frac{\pi}{\arctan\left(1/d\right)} \right\rfloor = \left\lfloor \frac{\pi}{1/d} \right\rfloor. \tag{33}$$

A extensão destes para arcsin pode ser feita seguindo os mesmos passos lógicos na prova de Galperin. Ainda que isso não seja satisfatório para fazer-nos confiar nos resultados das Eqs. (30) e (31), aqui vai um argumento derradeiro: neste caso, as aproximações $\arctan x \approx x$ e $\arcsin x \approx x$ *podem* ser um problema se dentre os $2d$ primeiros dígitos de π nós tivermos uma cadeia de d números 9 em sequência [3], o que parece ser uma coisa bastante difícil de acontecer. Por exemplo, nos primeiros 100 milhões de dígitos de π, a maior cadeia de 9s que aparece tem tamanho oito, mas precisaríamos de uma cadeia de tamanho 50 milhões para possivelmente violar as igualdades nas Eqs. (30) e (31), o que soa bastante improvável de acontecer [3, 6].

Essa área em si envolve tantos conceitos complexos e pode desenrolar tantas discussões que mereceria um trabalho completo apenas dedicado a ela.

- **Revisão**

Em seu artigo [5], Adam Brown utilizou como fórmula de contagem das iterações de Grover, no caso de $n = 1$, a relação: $\left\lfloor \frac{\pi}{4}\sqrt{N-1} \right\rfloor$, que difere da que nós encontramos na Eq. (28) por um fator 1/2, o qual nós consideramos ser relevante. Como discutimos na Sec. 4.1, esse fator equivale a começar a contagem a partir de uma primeira (semi-)colisão no sistema de bilhar, e isso faz diferença na contagem final. Isso porque, ainda que para valores de N grande, as partes $\left\lfloor \frac{\pi}{4}\sqrt{N-1} \right\rfloor$ e $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ das nossas expressões equivalham, se o número real dentro de $\lfloor\ \rfloor$ tiver o primeiro dígito após a vírgula menor ou igual 4, o resultado final das contagens nossa e do Brown diferirá. Por exemplo, consideremos o caso $N = 100^3$, em que as nossas expressões, desconsiderando o fator 1/2, sejam equivalentes,

$$\left\lfloor \frac{\pi}{4}\sqrt{100^3 - 1} \right\rfloor = \left\lfloor \frac{\pi}{4}\sqrt{100^3} \right\rfloor = \lfloor 785, 4\ldots \rfloor = 785.$$

Subtrair 1/2 desse valor, muda-o para $\lfloor 784, 9\ldots \rfloor = 784$, alterando o resultado da contagem.

5. Conclusão

O método de bilhar não é nem de longe o melhor para se calcular π. Ele não só assume condições extremamente idealizadas, tornando-o fisicamente impraticável, como leva tempos absurdos para ser processado num computador por um algoritmo iterativo. Da mesma forma, não seria nada prático processar o algoritmo de Grover utilizando esse sistema. Ainda assim, é encantador como de um problema aparentemente tão simples, consegue-se desdobrar discussões tão profundas, de algoritmos quânticos a teoria de números. Como disse Adam Brown: "Utilizar esse sistema de bilhar para processar o algoritmo de Grover não seria nem fácil e nem útil, mas seria um jeito pitoresco de procurar π em meio aos $|\psi\rangle$" [5].

6. Agradecimentos

D.O.S.P. agradece o suporte financeiro das agências de financiamento CNPq (projeto número 307028/2019-4) e FAPESP (projeto número 2017/03727-0) e do Instituto Nacional de Ciência e Tecnologia em Informação Quântica [CNPq INCT-IQ (465469/2014-0)]. V.L.O.S. agradece aos seus colegas Yuri P. Asnis, Matheus F. S. Lemes e Jallon F. Rocha, pelas valiosas conversas e sugestões que ajudaram a construir este trabalho; e também à Maria Eliane de Oliveira, pela revisão do texto. Os autores também são gratos a Adam R. Brown, por ter proposto originalmente o isomorfismo discutido neste artigo e por responder a nossos contatos sempre com atenção e cordialidade.

Referências

[1] M. Enquist e A. Arak, Nature **372**, 169 (1994).

[2] E.W. Weisstein, *Buffon's Needle Problem*, disponível em: https://mathworld.wolfram.com/BuffonsNeedleProblem.html.

[3] G. Galperin, Regular and Chaotic Dynamics **8**, 375 (2003).

[4] A. Katok, London Math. Soc. Lecture Notes **321**, 216 (2005).

[5] A.R. Brown, Quantum **4**, 357 (2020).

[6] https://www.youtube.com/watch?v=HEfHFsfGXjs, acessado em: 13/12/2020.
[7] H.M. Nussenzveig, *Curso de Física Básica: Mecânica* (Editora Blutcher, São Paulo, 1998), v. 1.
[8] M.Z. Rafat e D. Dobie, arXiv:1901.06260 (2019).
[9] X.M. Aretxabaleta, M. Gonchenko, N.L. Harshman, S.G. Jackson, M. Olshanii e G.E. Astrakharchik, arXiv:1712.06698 (2020).
[10] M.A. Nielsen e I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2010), 10ª ed.
[11] L.K. Grover, em: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (Pennsylvania, 1996).
[12] P. Kaye, R. Laflamme e M. Mosca. *An introduction to quantum computing* (Oxford University Press, Oxford 2007).
[13] D. Reitzner e M. Ziman, European Physical Journal Plus **129**, 128. (2014).
[14] *Grover's Algorithm*, disponível em: https://qiskit.org/textbook/ch-algorithms/grover.html, acessado em: 23/04/2021.
[15] F. Song, arXiv:1709.01236 (2017).
[16] A. Van Der Poorten e R. Apéry, The Mathematical Intelligencer **1**, 195 (1979).