O que vem a ser computação quântica?

Encontro Regional de Ciências

Roberto Imbuzeiro Oliveira (IMPA)

Rio de Janeiro, 02/08/2012

Computação quântica?

- Por que isso pode ser útil?

Computação quântica?

- Por que isso pode ser útil?
- O que há de diferente com relação à computação usual?

Computação quântica?

- Por que isso pode ser útil?
- O que há de diferente com relação à computação usual?
- O que há de matemática nisto?

O gato e os escravos de Schödinger

O gato de Schrödinger

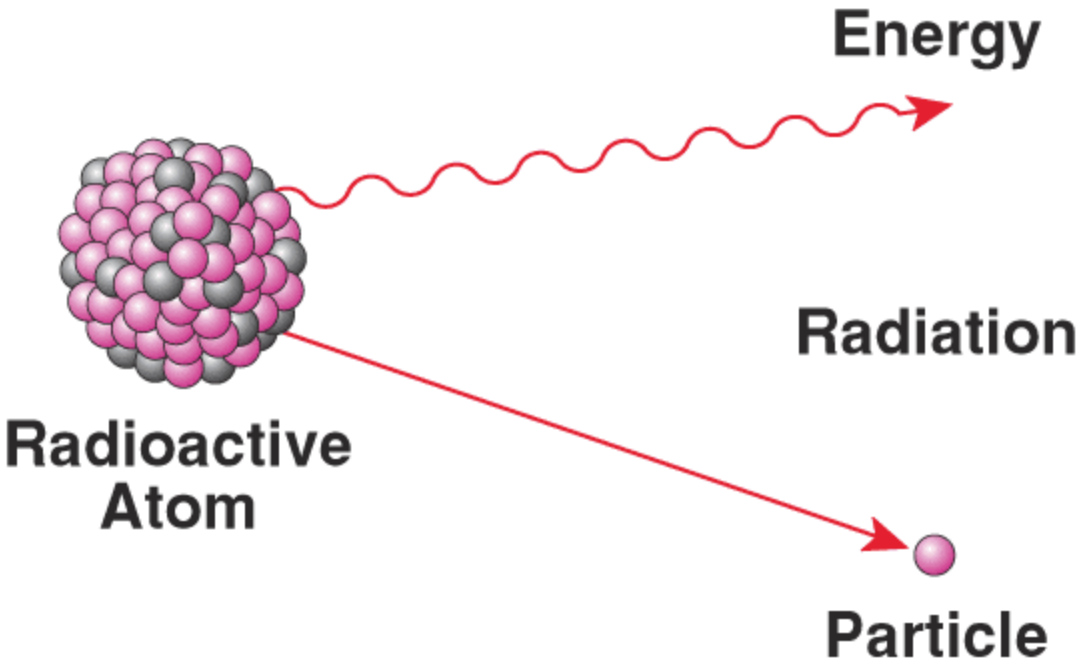
- A Mecânica Quântica nos diz que certas perguntas sobre o estado de um sistema físico não têm resposta definida até o momento em que se observa o sistema.

O gato de Schrödinger

- A Mecânica Quântica nos diz que certas perguntas sobre o estado de um sistema físico não têm resposta definida até o momento em que se observa o sistema.
- Ou seja, um sistema pode existir numa superposição de estados possíveis.

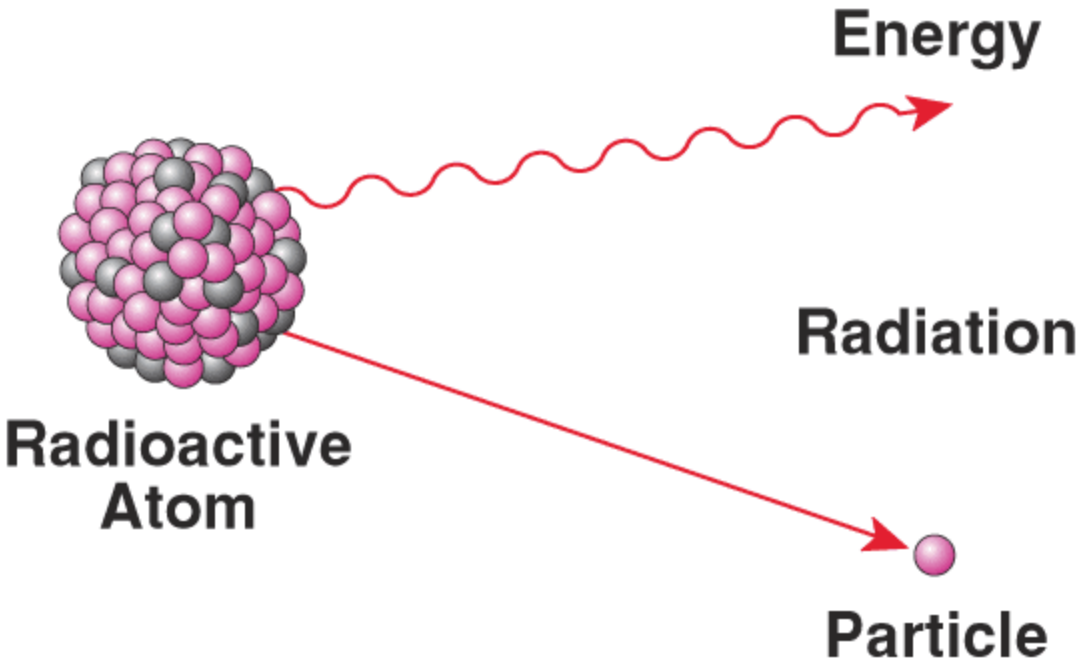
O gato de Schrödinger

- Imagine por exemplo um átomo de material radioativo.



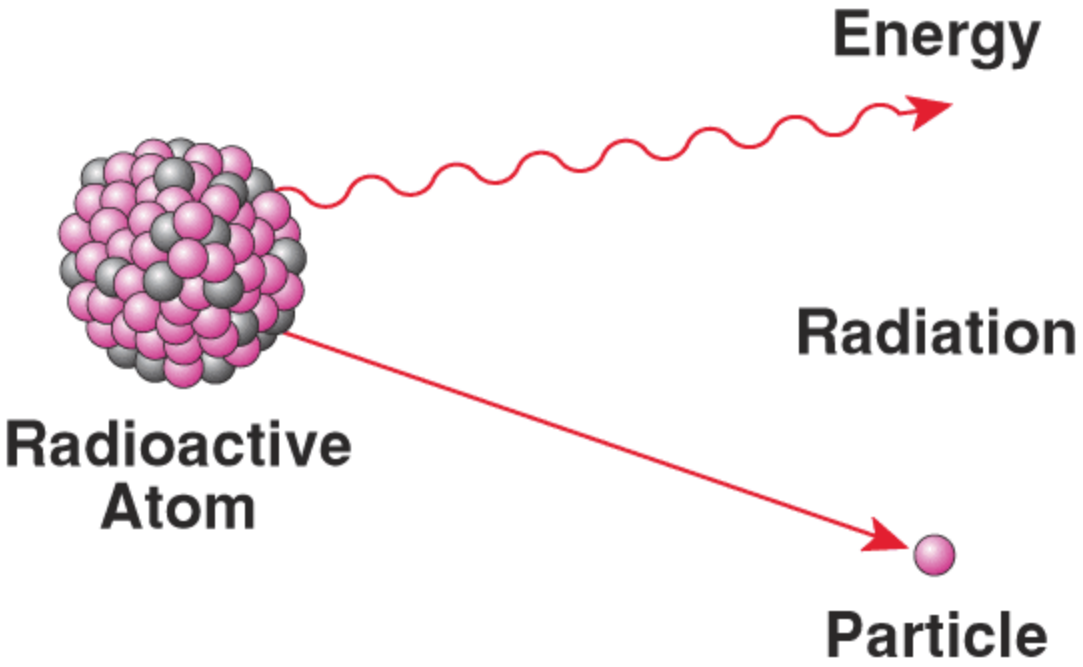
O gato de Schrödinger

- Será que ele emitiu radiação no último minuto?



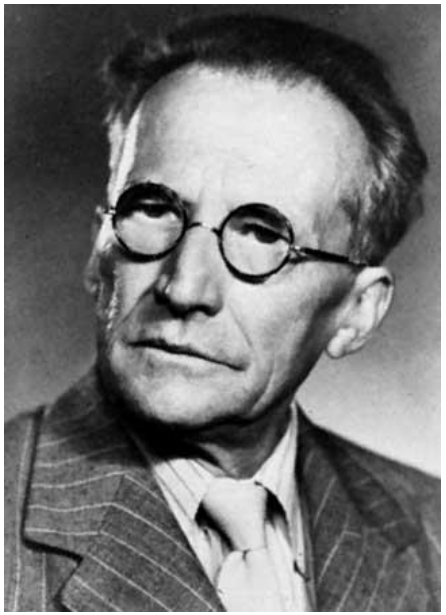
O gato de Schrödinger

- Segundo uma interpretação da MQ, <u>não faz sentido</u> perguntar isso sem medir.



O gato de Schrödinger

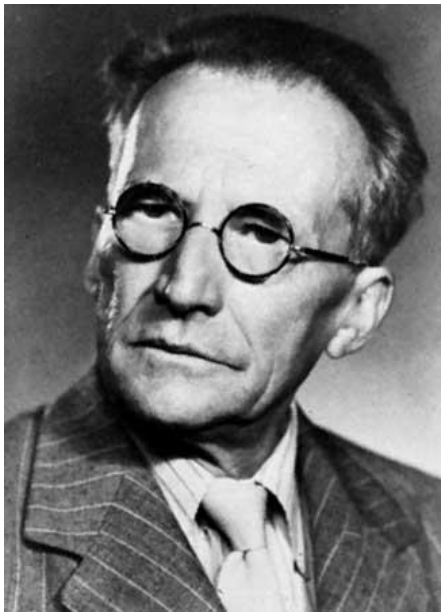
- Quando soube disso, Schrödinger ficou perplexo.



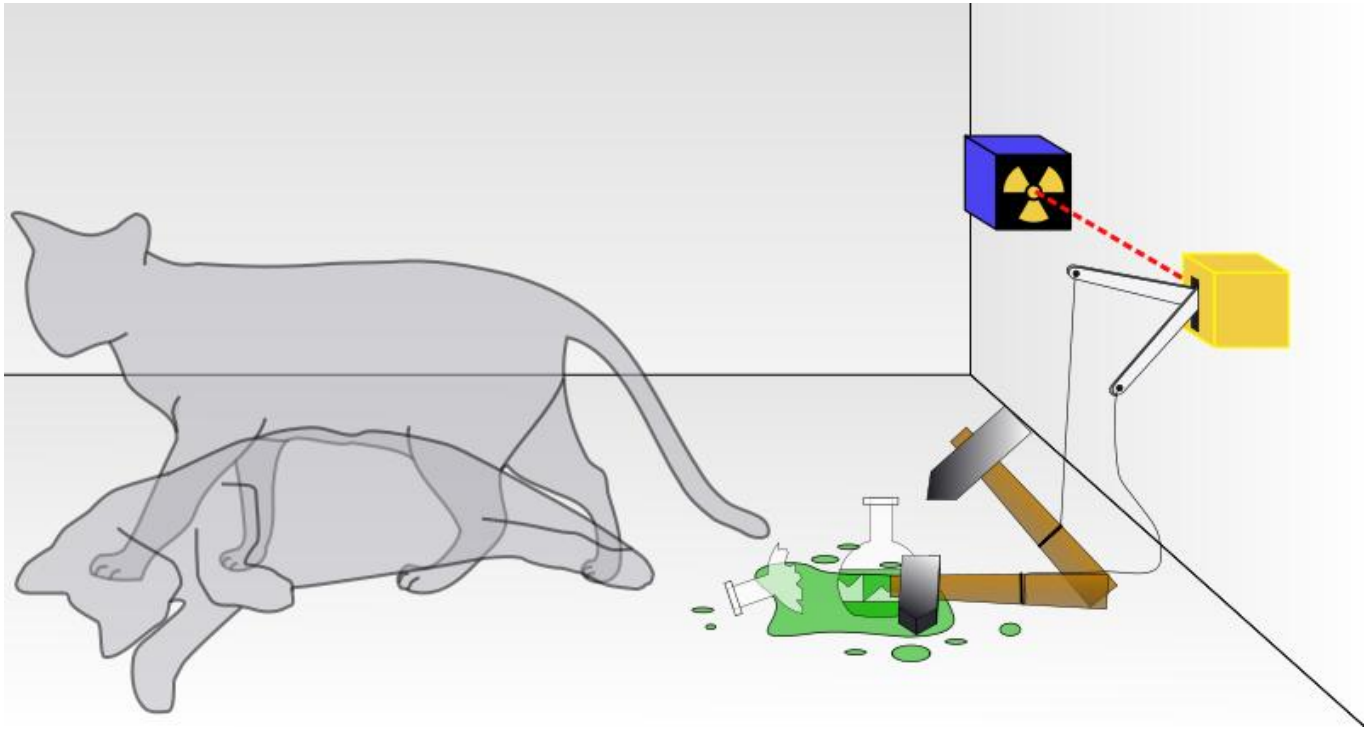
O gato de Schrödinger

- Quando soube disso, Schrödinger ficou perplexo.

  Ele notou que isto sugeria fenômenos estranhos.

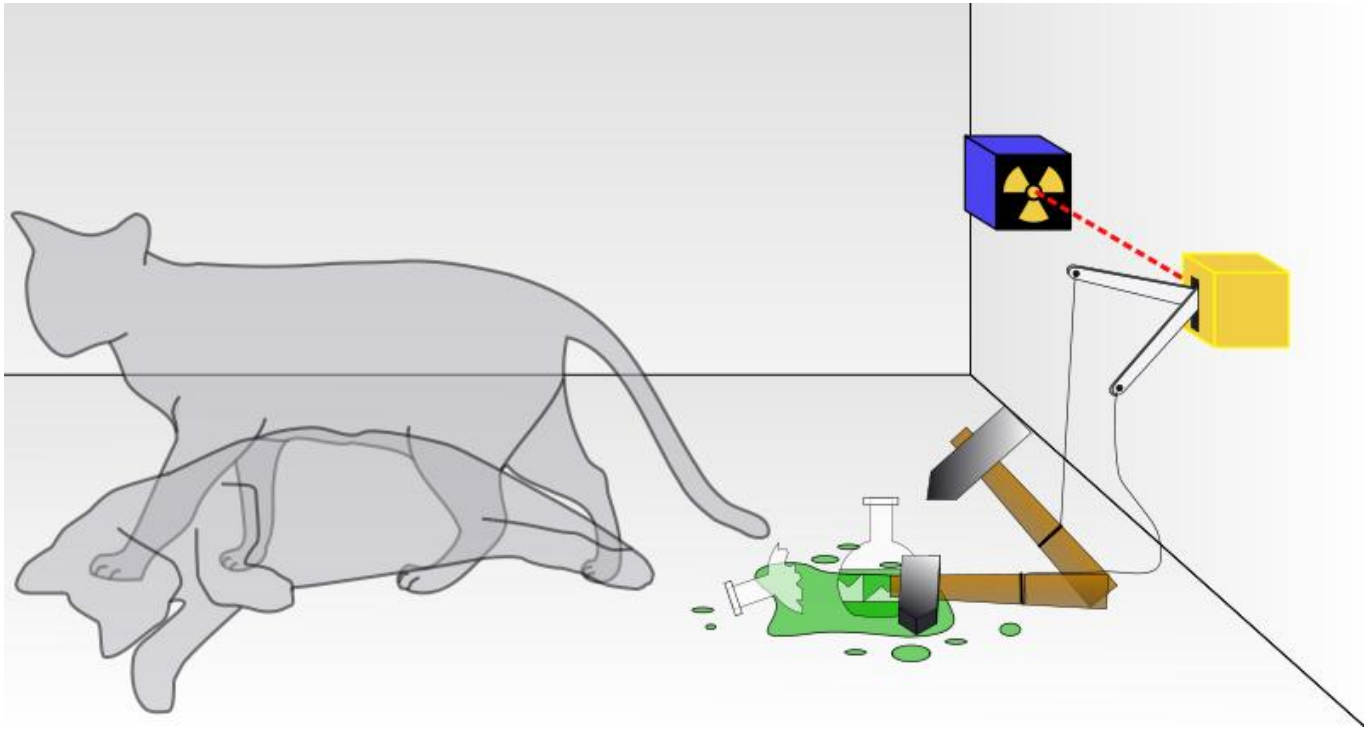


O gato de Schrödinger



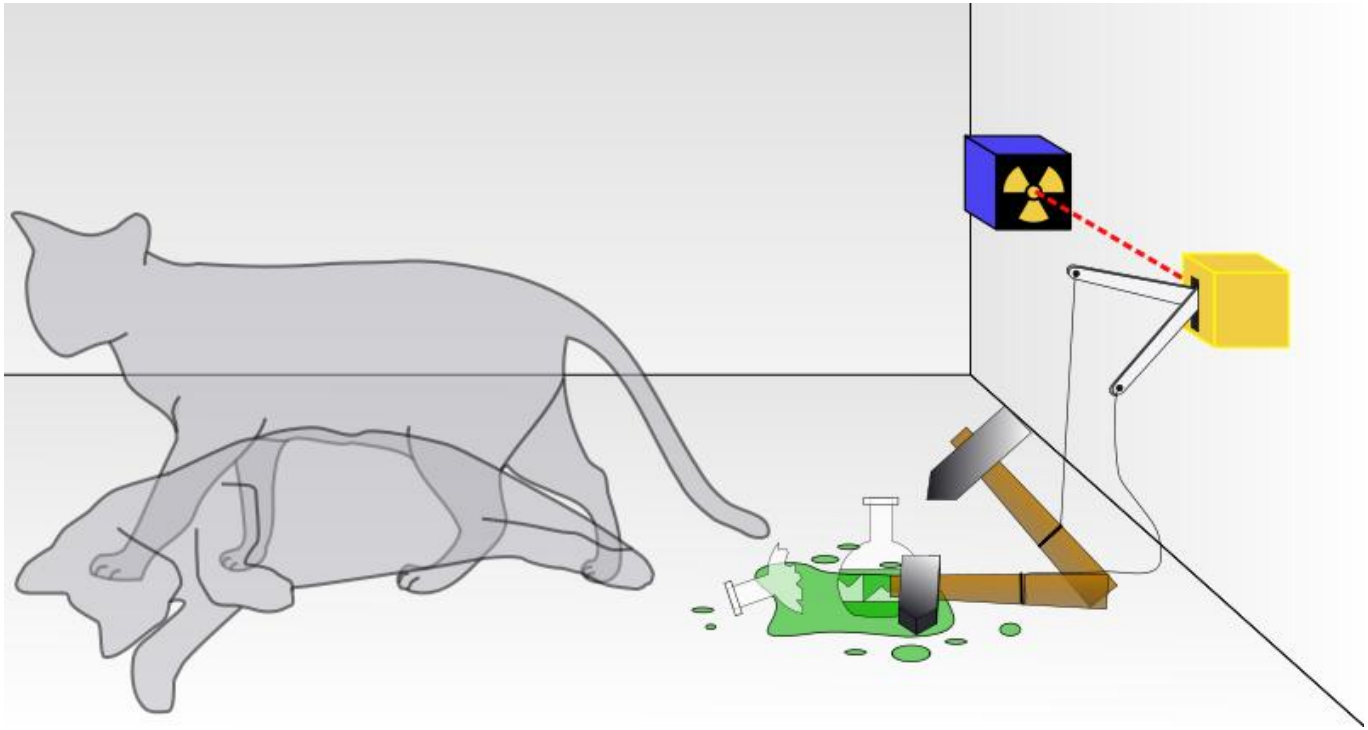
- E se ligamos um contador Geiger a um dispositivo que envenena um gato?

O gato de Schrödinger



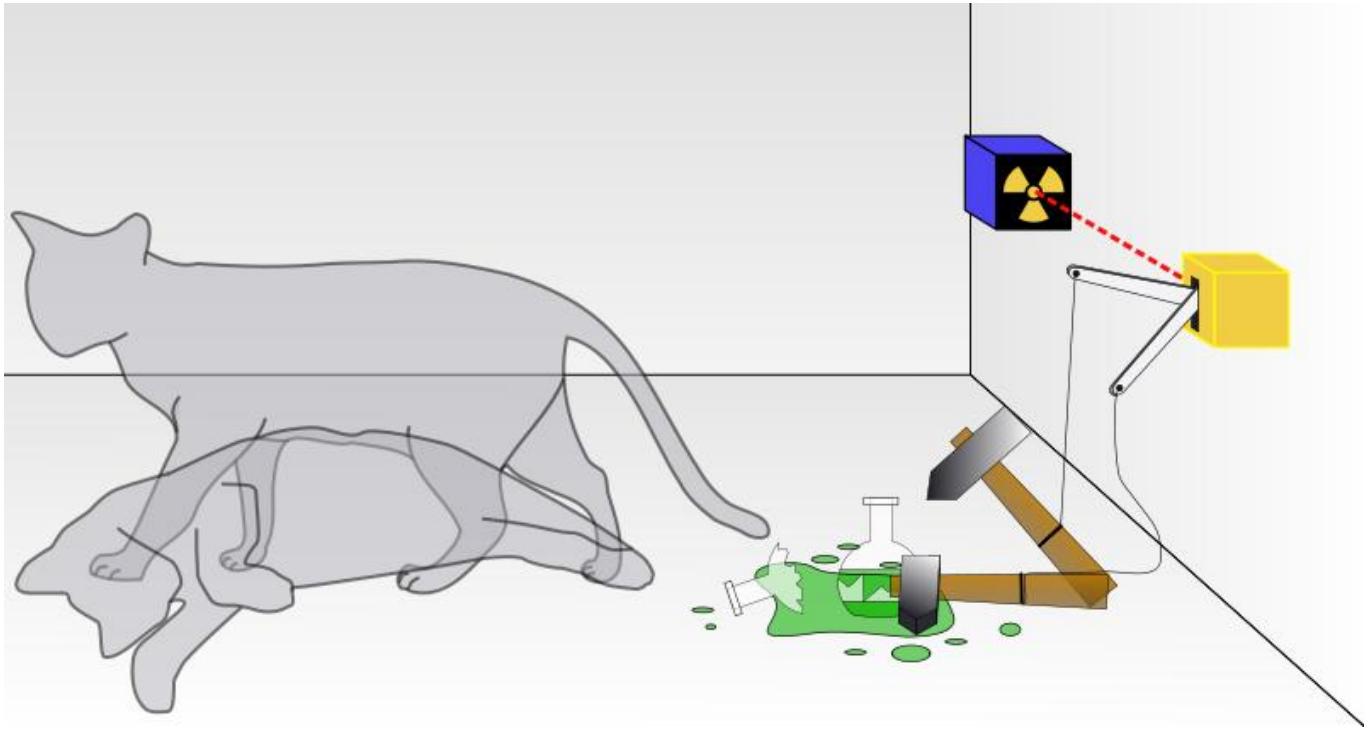
- O gato morre se sai radiação, fica vivo se não sai.

O gato de Schrödinger



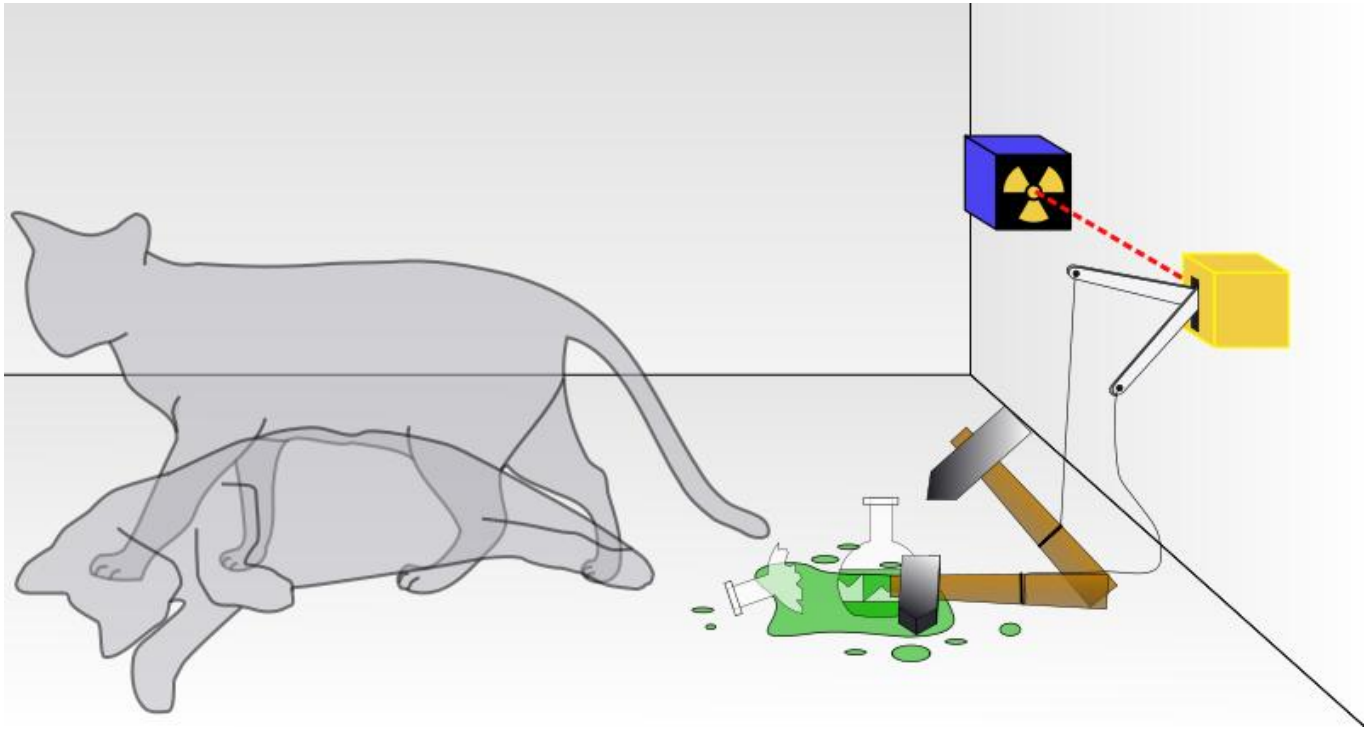
- Afinal, ele está vivo ou não está? Será que esta pergunta não faz sentido?

O gato de Schrödinger



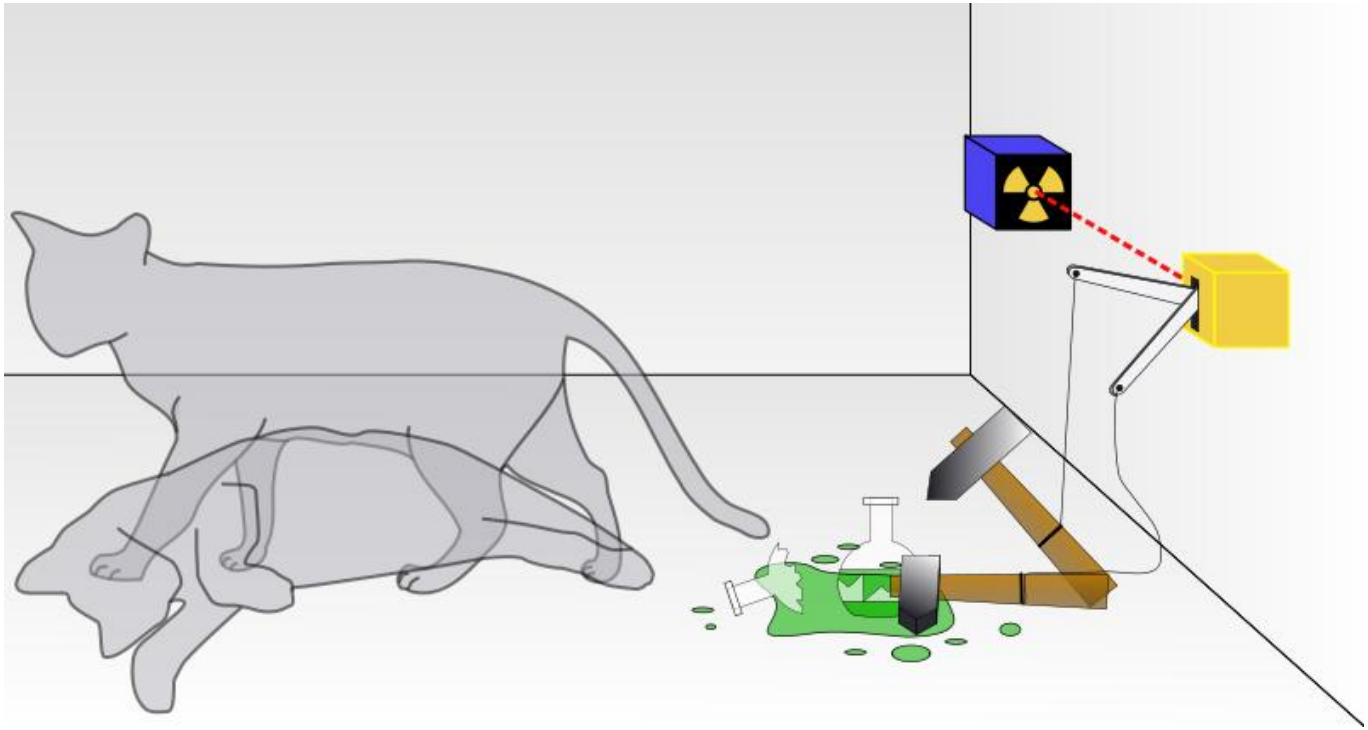
- Note: há uma resposta definida depois que se olha pro gato. Mas e antes?

O gato de Schrödinger



- Será que o gato está vivo e morto ao mesmo tempo?

O gato de Schrödinger



- Será que ele pode ir ao cartório prá mim e fazer o jantar ao mesmo tempo?

O escravo de Schrödinger

- Um só escravo acha um objeto numa destas gavetas em pouco tempo.

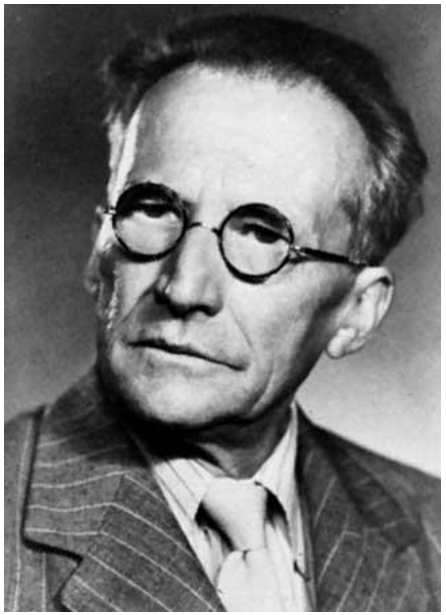
O escravo de Schrödinger

- Use vários átomos.

  Dependendo de

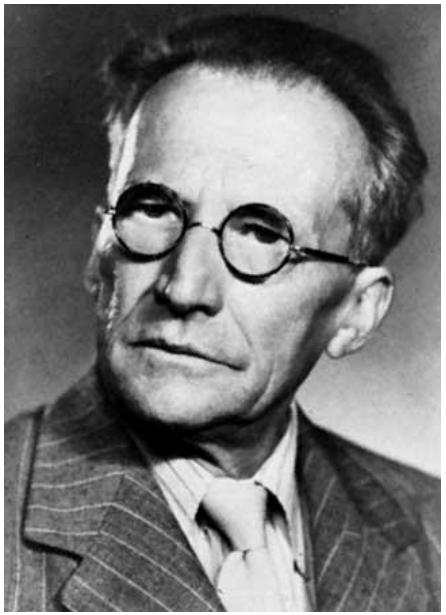
  quais emitem radiação, o escravo procura

  em uma gaveta...



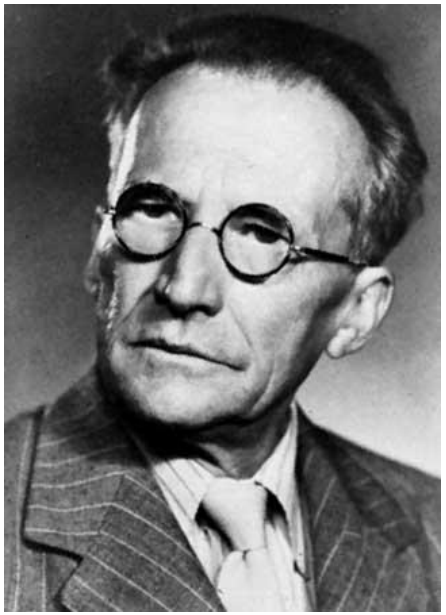
O escravo de Schrödinger

- Se o gato está vivo e morto, o escravo procura em todas as gavetas ao mesmo tempo!



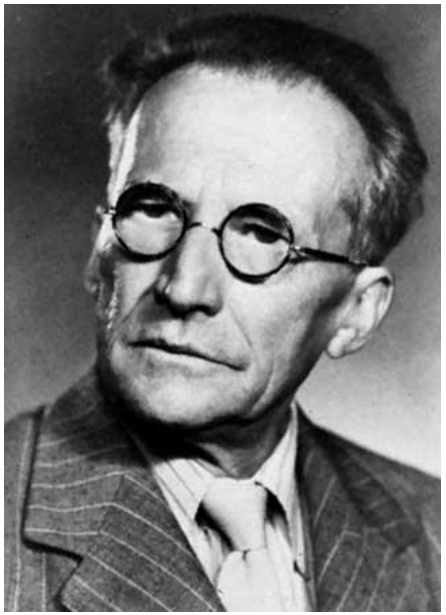
O escravo de Schrödinger

- Num computador, isso nos dá um jeito de achar dados muito rapidamente num banco de dados!



O problema

- As coisas só acontecem ao mesmo tempo até observarmos o sistema. Aí ou vemos um escravo feliz (pouco provável), ou não...



Conclusão desta parte

- Fenômenos quânticos geram superposições de estados que podem em princípio ser ampliados para efeitos macroscópicos.

Conclusão desta parte

- Fenômenos quânticos geram superposições de estados que podem em princípio ser ampliados para efeitos macroscópicos.
- Em algum sentido, várias coisas acontecem ao mesmo tempo...

Conclusão desta parte

- Fenômenos quânticos geram superposições de estados que podem em princípio ser ampliados para efeitos macroscópicos.
- Em algum sentido, várias coisas acontecem ao mesmo tempo...
- ... Mas só até olharmos para ver o que aconteceu!

O experimento das duas fendas

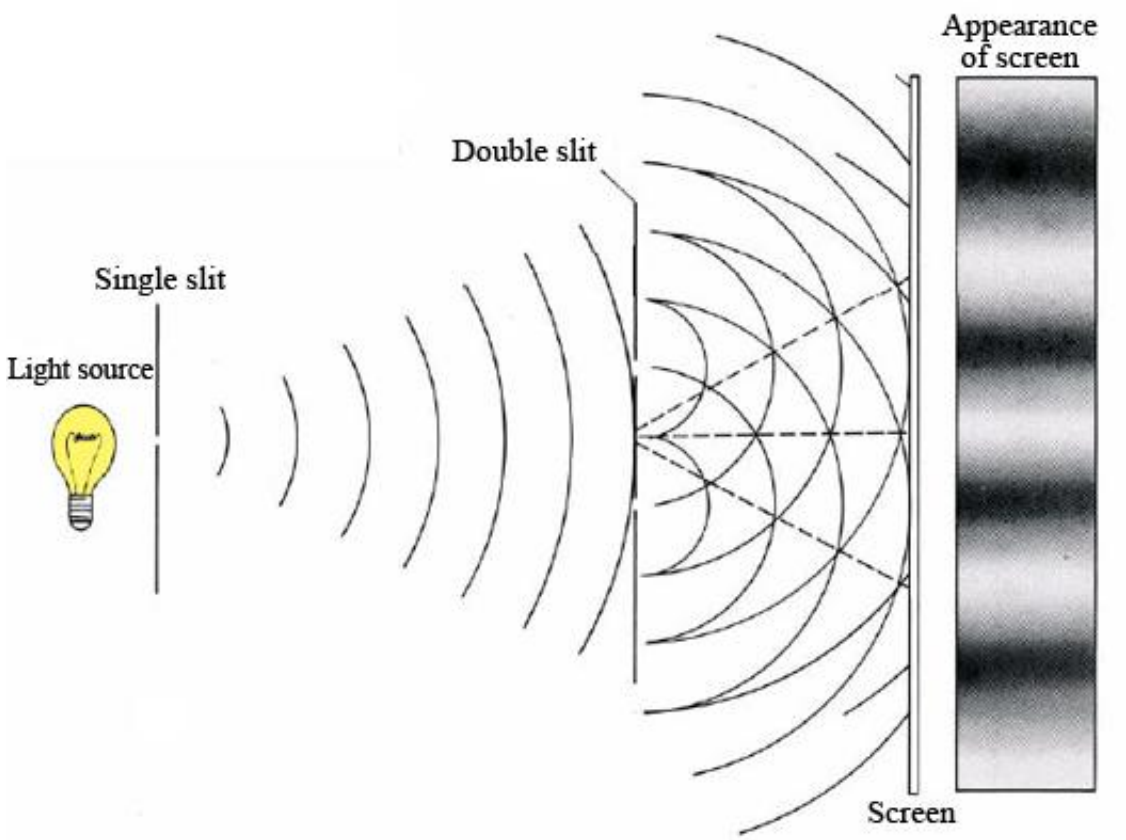
Duas fendas?

- Este experimento mostra que diferentes possibilidades em superposição podem cancelar ou reforçar umas às outras.

Duas fendas?

- Este experimento mostra que diferentes possibilidades em superposição podem cancelar ou reforçar umas às outras.
- Isto será útil no caso dos escravos, para reforçar o bom comportamento.

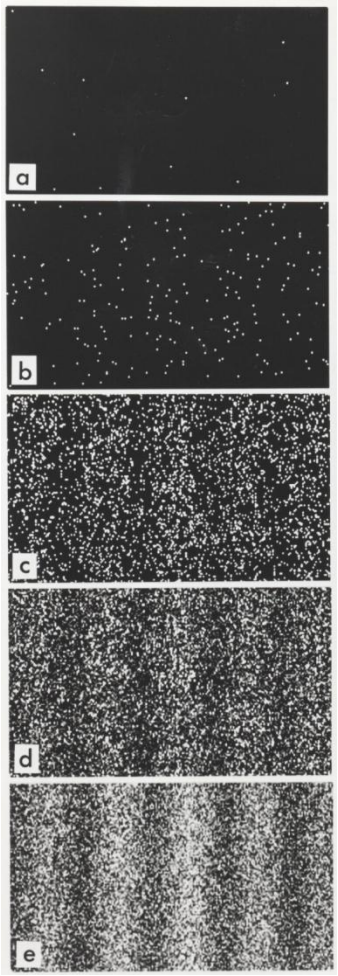
As duas fendas de Young



- A luz se comporta como onda. Ondas podem se cancelar ou se reforçar.

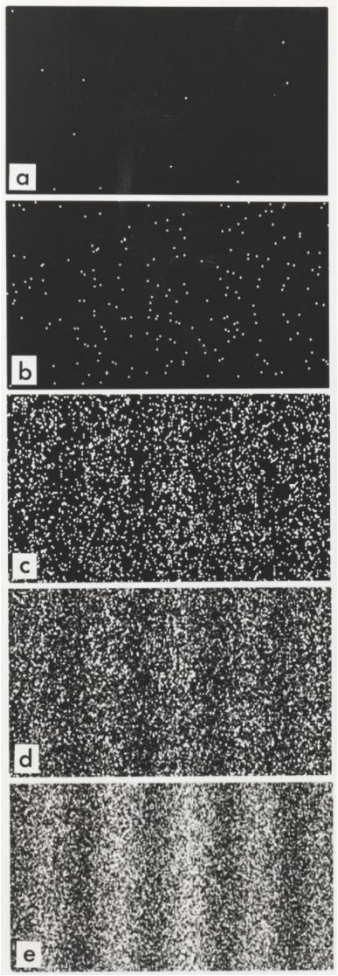
As duas fendas de Young

- Um único fóton se comporta como uma onda.Sua probabilidade de parar num ponto depende das duas trajetórias possíveis (duas fendas)

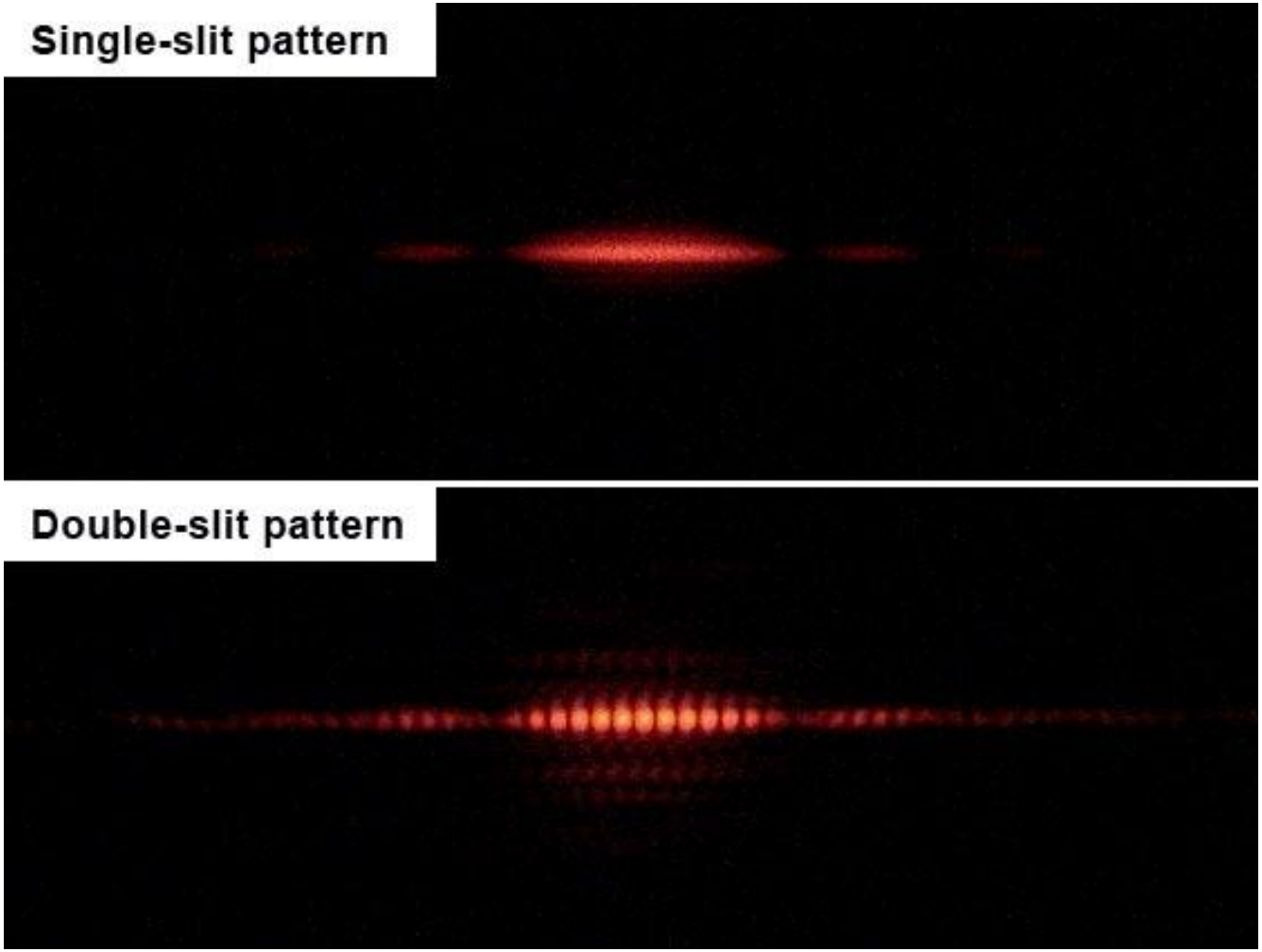


As duas fendas de Young

- Isto porque as diferentes possibilidades em superposição se cancelam e se reforçam umas às outras.



Uma vs. duas fendas



O que está acontecendo?

- Em toda a MQ o estado de um sistema é descrito por sua função de onda, que descreve a superposição de estados correspondente.

O que está acontecendo?

- Em toda a MQ o estado de um sistema é descrito por sua função de onda, que descreve a superposição de estados correspondente.
- Ao contrário de probabilidades, ondas podem se somar e se subtrair.

O que está acontecendo?

- Em toda a MQ o estado de um sistema é descrito por sua função de onda, que descreve a superposição de estados correspondente.
- Ao contrário de probabilidades, ondas podem se somar e se subtrair.
- No entanto, quando algo é medido, a onda quântica “colapsa” probabilisticamente em algo definido.

Voltando ao escravo

- O problema do escravo de Schrödinger é que ele fazia coisas em superposição, mas, quando medido, só revelava uma das possibilidades (geralmente a errada).

Voltando ao escravo

- O problema do escravo de Schrödinger é que ele fazia coisas em superposição, mas, quando medido, só revelava uma das possibilidades (geralmente a errada).
- No entanto, se a sua função de onda fizer uma “coreografia” antes de ser medida, talvez possamos reforçar o comportamento bom.

O algoritmo de Grover para busca

O que é um algoritmo?

- Tradicionalmente, é uma maneira metódica, baseada em regras bem definidas, de se resolver um problema.

O que é um algoritmo?

- Tradicionalmente, é uma maneira metódica, baseada em regras bem definidas, de se resolver um problema.
- Exemplo: algoritmo para a divisão (de Euclides).

O que é um algoritmo?

- Tradicionalmente, é uma maneira metódica, baseada em regras bem definidas, de se resolver um problema.
- Exemplo: algoritmo para a divisão (de Euclides).
- Não-exemplo: “eu sei fazer, mas não sei explicar”.

A evolução dos algoritmos

- Primeiro: papel e lápis (ou ábaco).

A evolução dos algoritmos

- Primeiro: papel e lápis (ou ábaco).
- Século XX: máquinas podem executar algoritmos (computação).

A evolução dos algoritmos

- Primeiro: papel e lápis (ou ábaco).
- Século XX: máquinas podem executar algoritmos (computação).
- Século XXI (?): dispositivos quânticos podem executar algoritmos.

Por que algos.quânticos?

- Necessidade tecnológica: limites físicos da Lei de Moore.

Por que algos.quânticos?

- Necessidade tecnológica: limites físicos da Lei de Moore.
- Possibilidades novas de eficiência!

Exemplo: fatoração

- A criptografia usada na segurança de compras online (RSA) é baseada na imensa dificuldade que se tem para achar os fatores primos de um número muito grande.

Exemplo: fatoração

- A criptografia usada na segurança de compras online (RSA) é baseada na imensa dificuldade que se tem para achar os fatores primos de um número muito grande.

- Algoritmo quântico de Shor poderá fazer isto rapidamente.

Muitos outros exemplos

- Problemas matemáticos que têm a ver com simetrias.
- Problemas físicos e químicos: simulação de sistemas complexos.
- Problemas fundamentas de computação

O algoritmo de Grover…

- … acha um item em escondido em uma das N gavetas em tempo ~ √N.

Ideia básica

- Use fendas escolhidas de maneira esperta.

Como funciona

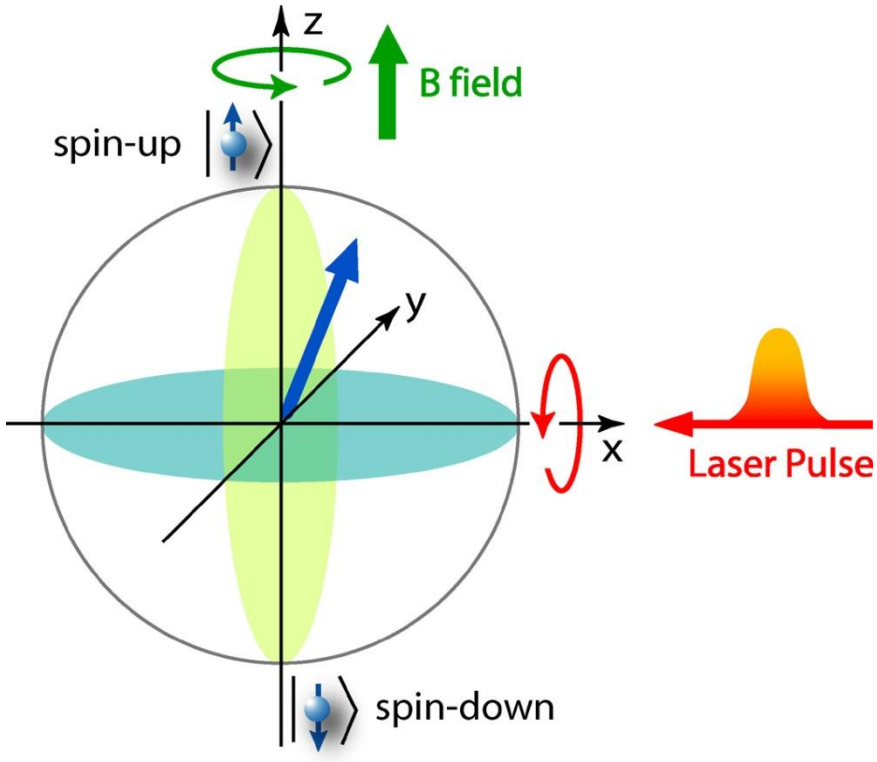
- Lembre que um sistema quântico é descrito por uma função de onda. Ela atribui a cada possibilidade em superposição um número complexo (amplitude).

Como funciona

- Lembre que um sistema quântico é descrito por uma função de onda. Ela atribui a cada possibilidade em superposição um número complexo (amplitude).
- Vamos fazer uma coreografia para as amplitudes e depois medir o sistema.

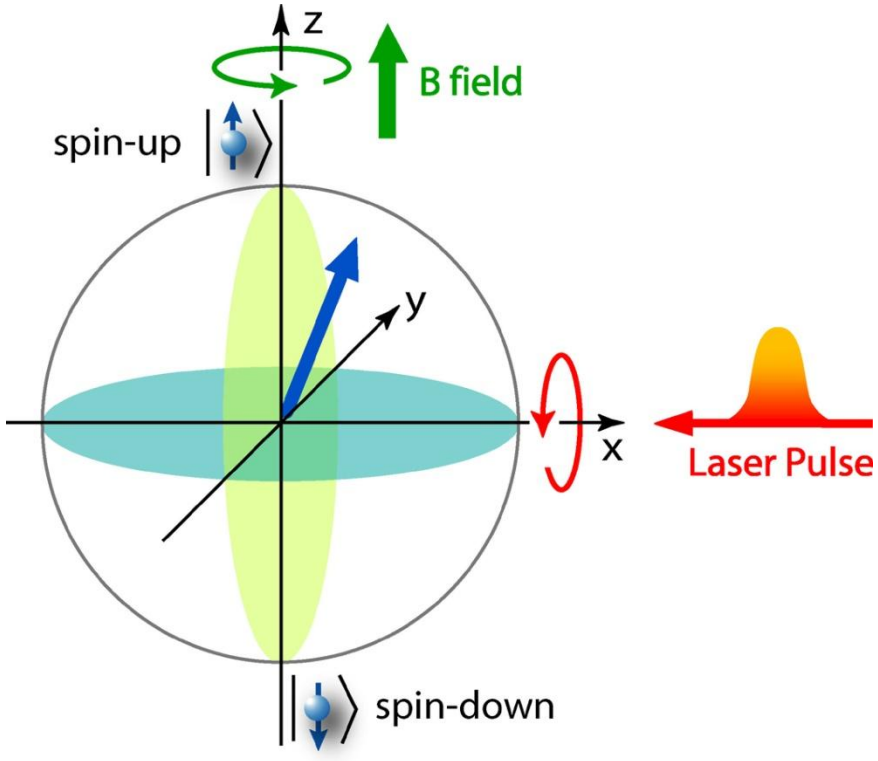
Ondas e vetores

- Você pode pensar na função de onda como um vetor: uma “setinha” num espaço de dimensão muito alta.



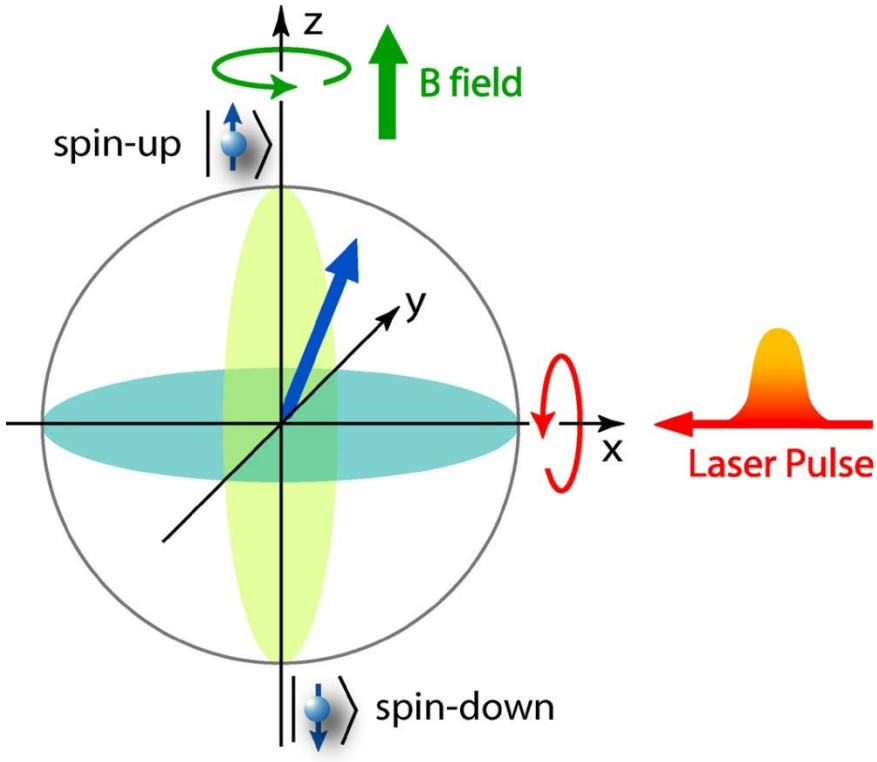
Ondas e vetores

- Algumas direções correspondem ao escravo apontar para uma gaveta; as outras são as superposições.



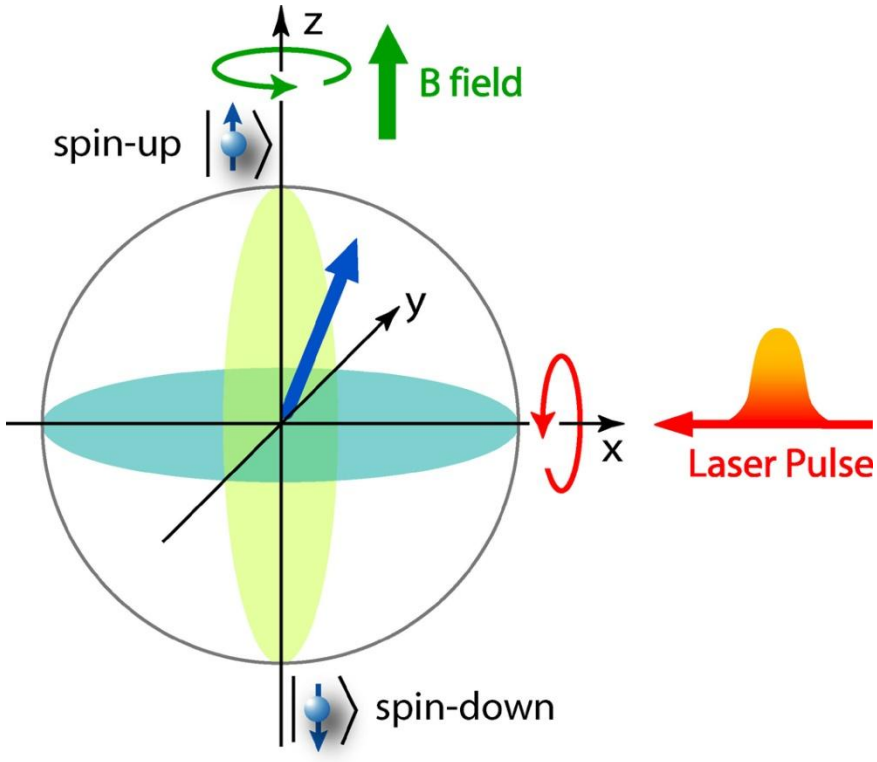
Evolução do sistema

- Grover achou uma sequencia de rotações e reflexões que faz o vetor apontar para a gaveta certa.



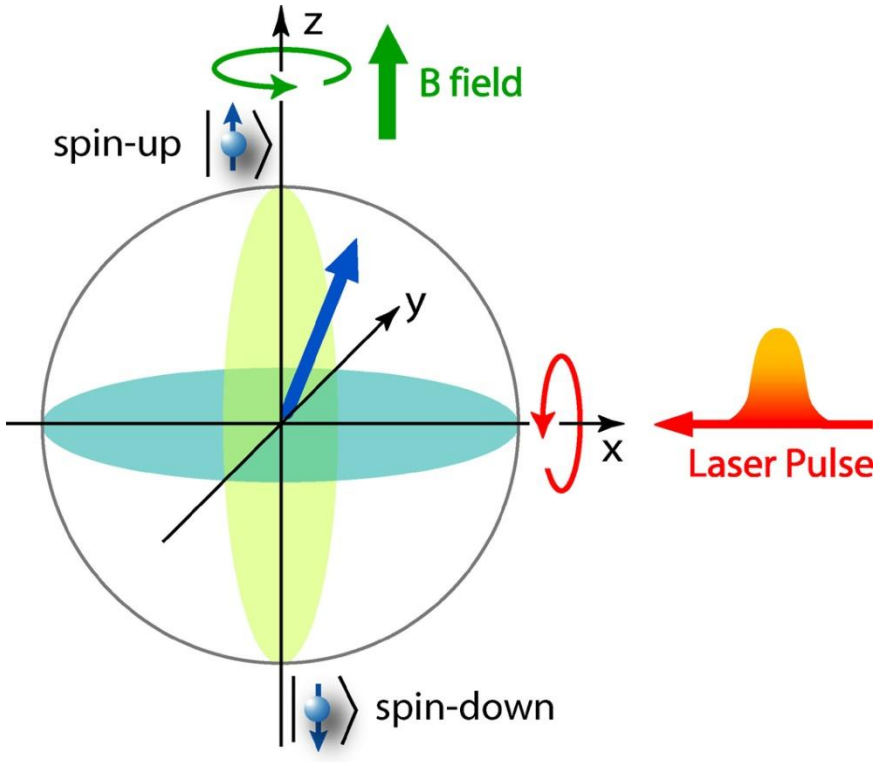
Evolução do sistema

- Tudo isto pode ser implantado em sistemas baseados em lasers, além de várias outras alternativas.



Evolução do sistema

- Infelizmente, ainda é muito difícil implantar isto em grande escala.



Não há computadores quânticos?

Computadores quânticos?

- Já se conseguiu fatorar 15 e catar itens em 4 gavetas. Isto com muito custo!

Computadores quânticos?

- Já se conseguiu fatorar 15 e catar itens em 4 gavetas. Isto com muito custo!
- Dificuldade: fazer os fenômenos quânticos resistirem à sua tendência de se “classicarem” (descoerência).

Computadores quânticos?

- Já se conseguiu fatorar 15 e catar itens em 4 gavetas. Isto com muito custo!
- Dificuldade: fazer os fenômenos quânticos resistirem à sua tendência de se “classicarem” (descoerência).
- Se esta tendência não existisse, talvez já tivéssemos visto gatos morto-vivos por aí.

O que há de matemática nisto?

Matemática da MQ

- Paralelamente à MQ, foram desenvolvidas várias ferramentas matemáticas para analisá-la, como a Análise Funcional (funções são vetores) e a Teoria de Representações de Grupos (estudo abstrato de simetrias).

Matemática da MQ

- O que acabamos de ver sobre Grover mostrou que um algoritmo quântico pode (e deve!) ser encarado como um problema geométrico, ainda que a geometria seja em dimensão muito alta.

Matemática da MQ

- Compreender este e outros algoritmos quânticos envolve uma dose razoável de matemática.

Matemática da MQ

- Compreender este e outros algoritmos quânticos envolve uma dose razoável de matemática.
- Entender as possibilidades e limitações da Computação Quântica requer muito mais matemática. Uma boa parte dela ainda não foi criada...

Exemplo: correção de erros

- Manter um computador quântico funcionando envolve a correção ativa de erros causados pela interação com o ambiente.

Exemplo: correção de erros

- Manter um computador quântico funcionando envolve a correção ativa de erros causados pela interação com o ambiente.
- A matemática envolvida nesta correção de erros vai desde a Combinatória até a Geometria Algébrica.

Muito obrigado!