Introdução à Informação Quântica

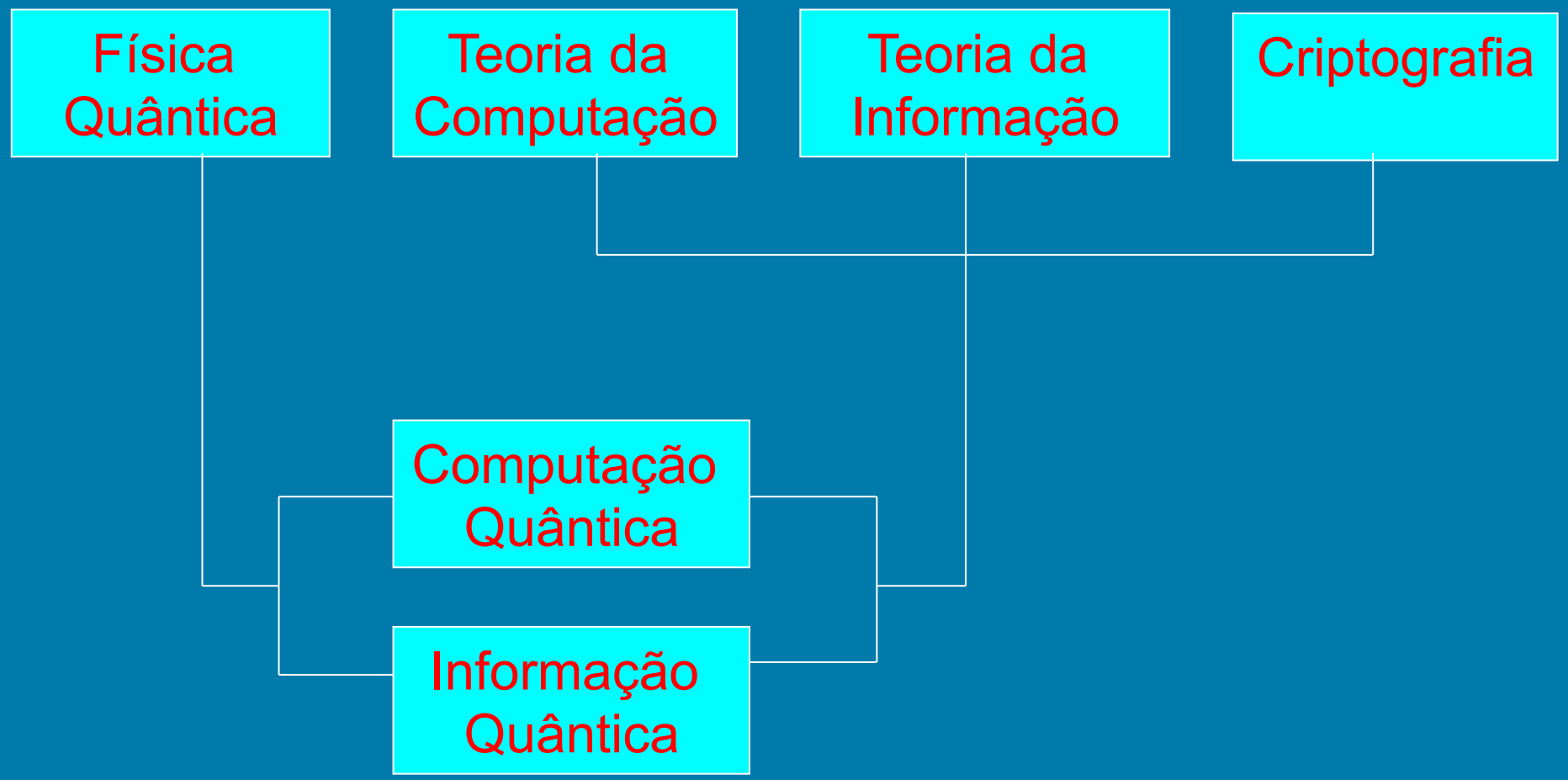
Amir O. Caldeira

IFGW-UNICAMP

Sumário da palestra

- Introdução; a evolução histórica das áreas que geraram a Informação Quântica.
- A Teoria Clássica da Informação.
- A Física Quântica: um exemplo
- A Informação Quântica.
- Comentários finais.

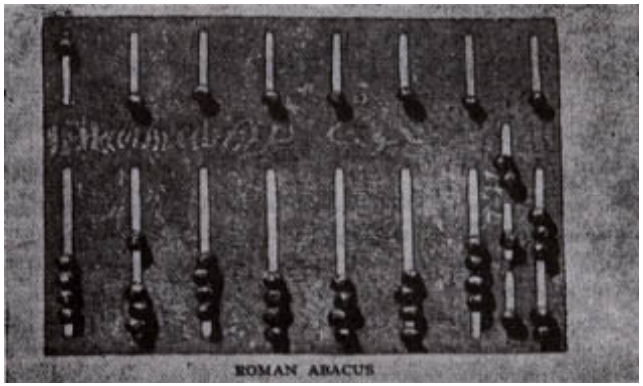
O desenvolvimento das diferentes áreas



A Teoria da Computação

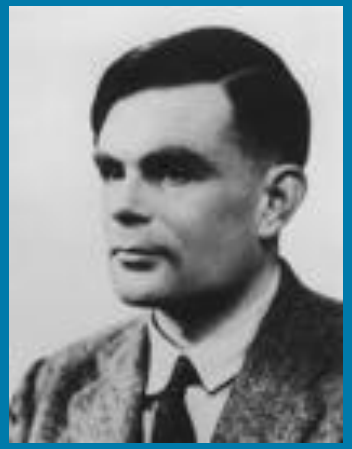
• Ábaco de areia inventado provavelmente na Babilônia em torno de 3000 a.C. Babilônios desenvolvem algoritmos de cálculo no período de Hammurabi (~ 1800 a.C).

• Ábacos gregos e romanos em torno de 400 a.C.

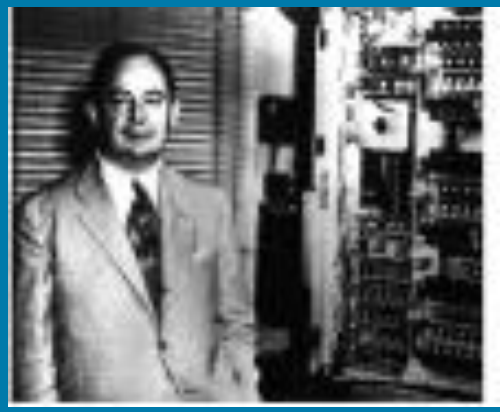


• Calculadoras mecânicas: Shickard, Pascal e Leibniz, e, posteriormente, réguas de cálculo (século XVII).

Desenvolvimento recente:

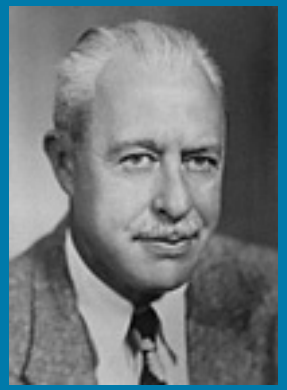


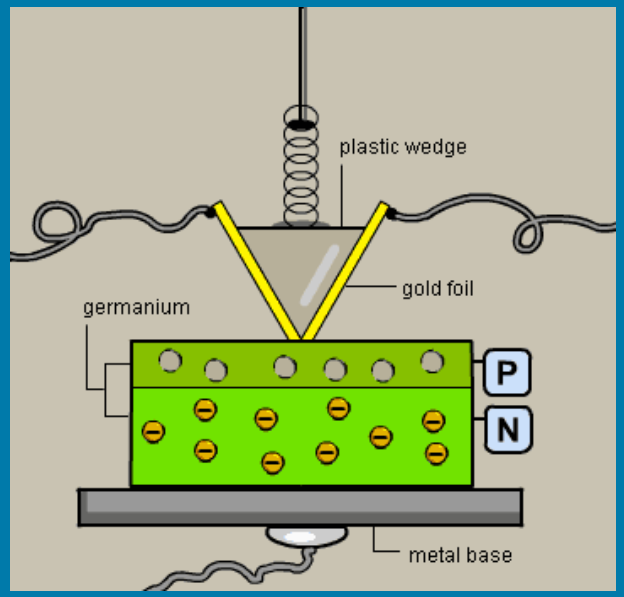
- Na década de 1930, Alan Turing desenvolve o conceito teórico de um computador programável; a máquina de Turing. “ Qualquer algoritmo pode ser eficientemente simulado em uma máquina de Turing”



- Pouco tempo depois John von Neumann desenvolve o modelo teórico de como implementar a máquina de Turing a partir de componentes eletrônicos

• “ Hardware” só teria impulso no final dos anos 40 após o desenvolvimento do transistor por Bardeen, Brattain e Shockley; Prêmio Nobel de Física de 1956



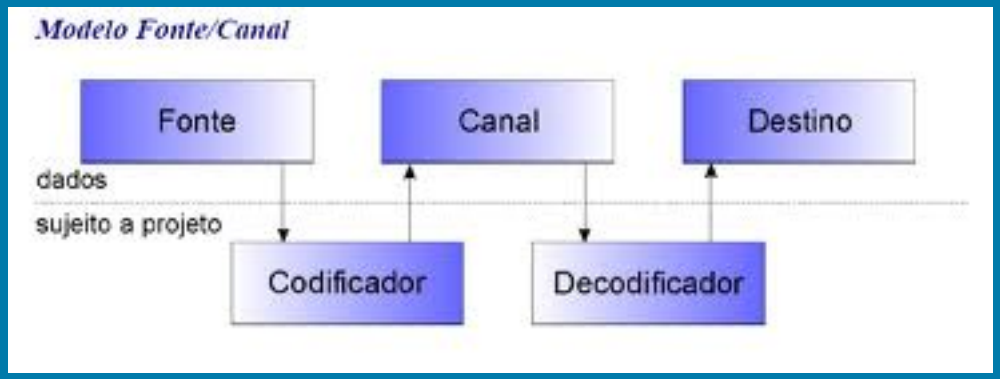


A Teoria da Informação

• Na década de 1940 Claude Shannon desenvolve matematicamente o conceito de informação. Quantificação do armazenamento e transmissão de informação. Codificação da informação em canais com e sem ruído e códigos de correção de erros.

Questões da teoria de informação

- Que recursos ou meios são necessários para a transmissão de informação através de canais de comunicação?

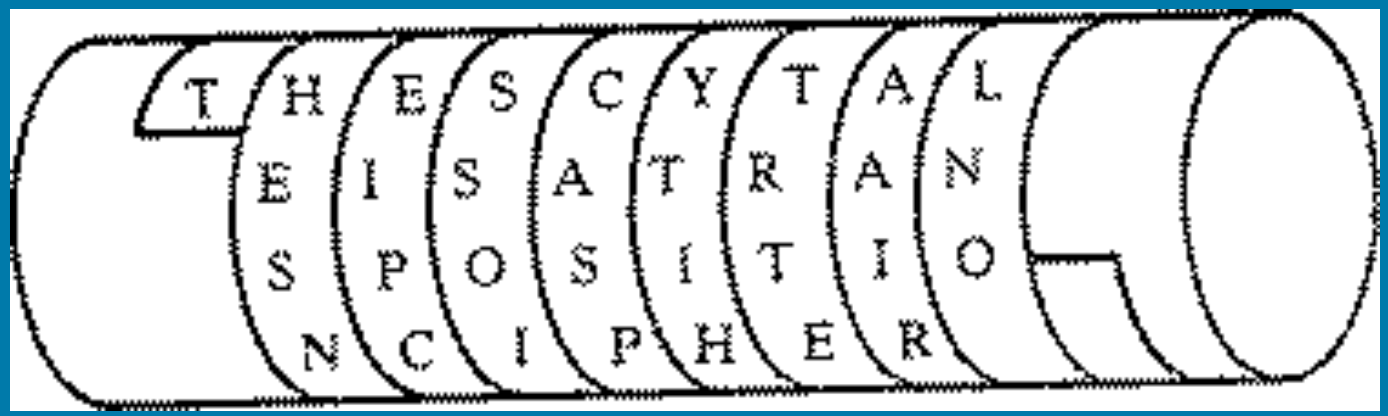


- Como esta informação pode ser protegida de influências externas (ruído) enquanto estiver sendo transmitida?

Criptografia

• Métodos de comunicação secreta foram desenvolvidos por inúmeras civilizações antigas na Mesopotâmia, Egito, Índia, China...

• Os espartanos desenvolveram a CÍTALA em torno de 400 a.C.



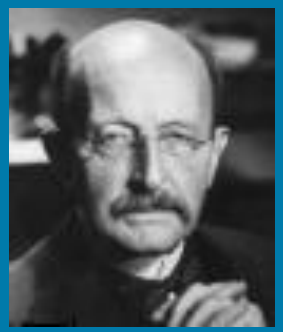
Desenvolvimento recente:

- Durante a segunda grande guerra ocorrem avanços significativos na criptografia ; Alan Turing e a equipe de Bletchley Park na Inglaterra quebram os códigos cifrados da ENIGMA (máquina de cifrar usada pelos alemães) ; desenvolvimento do primeiro computador digital, o COLOSSUS !

- Desenvolvimento de códigos criptográficos: sistemas criptográficos de chaves privadas ou públicas.

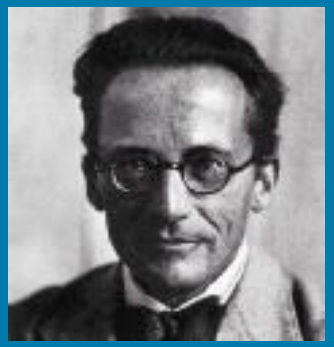
A Mecânica Quântica

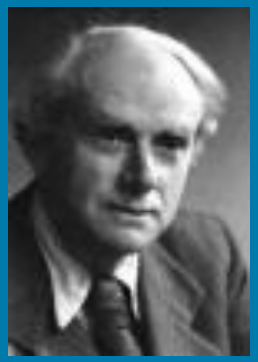
- Na virada do século XX a Física Clássica não consegue explicar diversos fenômenos observados experimentalmente.
- Hipóteses de Planck, Einstein, Bohr e de Broglie culminam com a criação de uma nova teoria na década de 20;



A Mecânica Quântica

- Um novo paradigma para as teorias físicas.
- Formulações complementares; Schrödinger & Heisenberg.
- A visão unificada de Dirac.
- O que é o sistema físico? A ênfase na observação; a teoria da medida. von Neumann.





Teoria Clássica da informação

- Envio de informação – letras, palavras, números – através de canais de comunicação que operam de acordo com as leis da física clássica.
- Codificação da informação : sistema binário (Leibniz)
- O sistema decimal

  $1120 = 1 \times 10^3 + 1 \times 10^2 + 2 \times 10^1 + 0 \times 10^0$

  $21 = 2 \times 10^1 + 1 \times 10^0$
- O sistema binário

  $21 = 16 + 4 + 1 = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 \Longrightarrow 10101$; representação alternativa para os números

Exemplo:

Deseja-se enviar mensagens com as 26 letras do alfabeto e alguns símbolos (pontuação e alguns outros)

⇩

40 elementos

⇩

a cada elemento corresponde um número; 1,2,...40

$$40 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$$
$$= 101000$$

⇩

Precisa-se de 6 dígitos por elemento e cada um deles = 0 ou 1. Diferentes codificações ⇨ maior eficiência na transmissão ou armazenamento.

dígito 0 ou 1 é o chamado **“ bit ”** de informação

- Por quê o sistema binário?

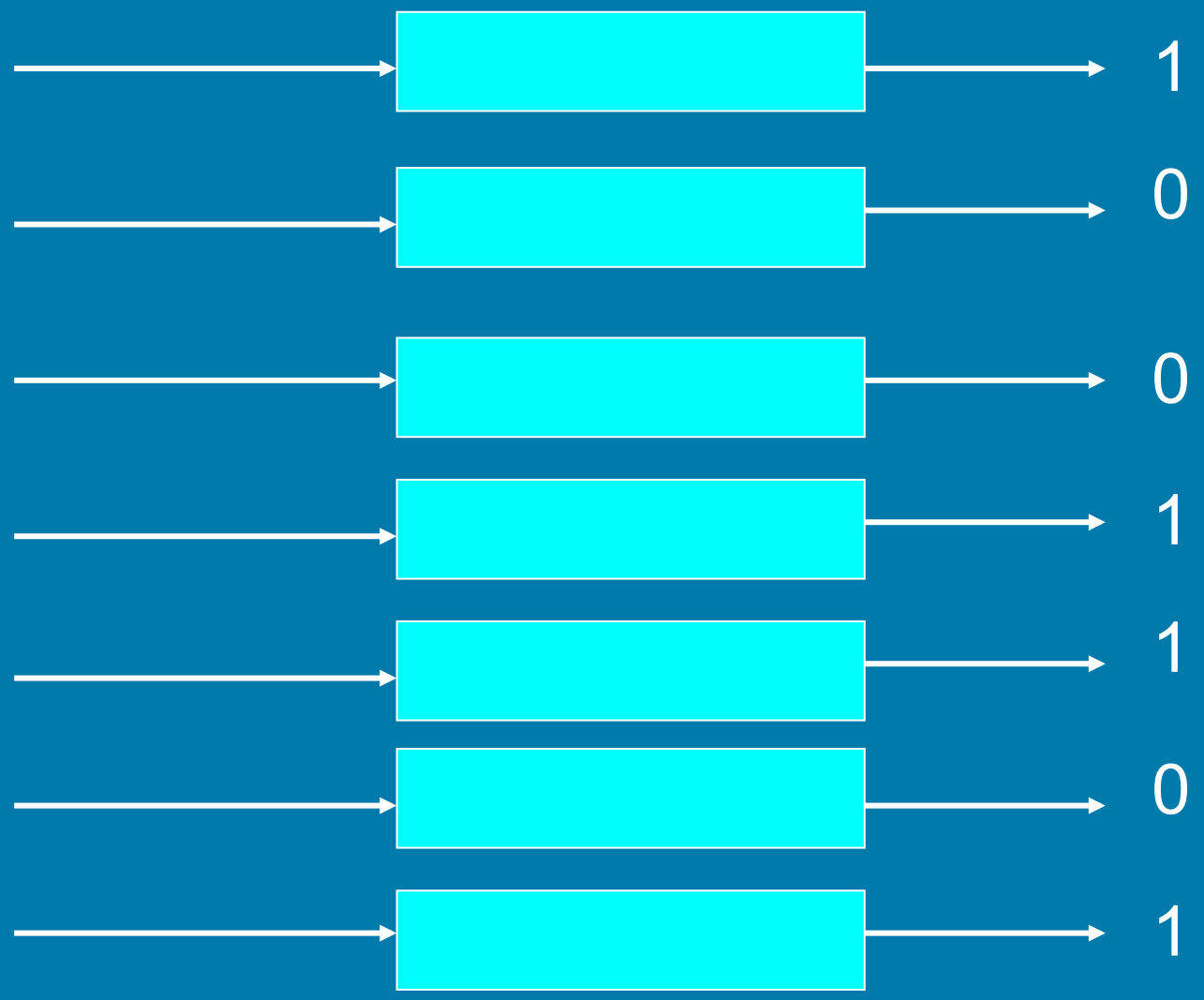
  Operacionalização: geração do bit

excitação → **Elemento Físico**

→ Determinada característica é ativada → 1

→ Não há ativação da característica em questão → 0

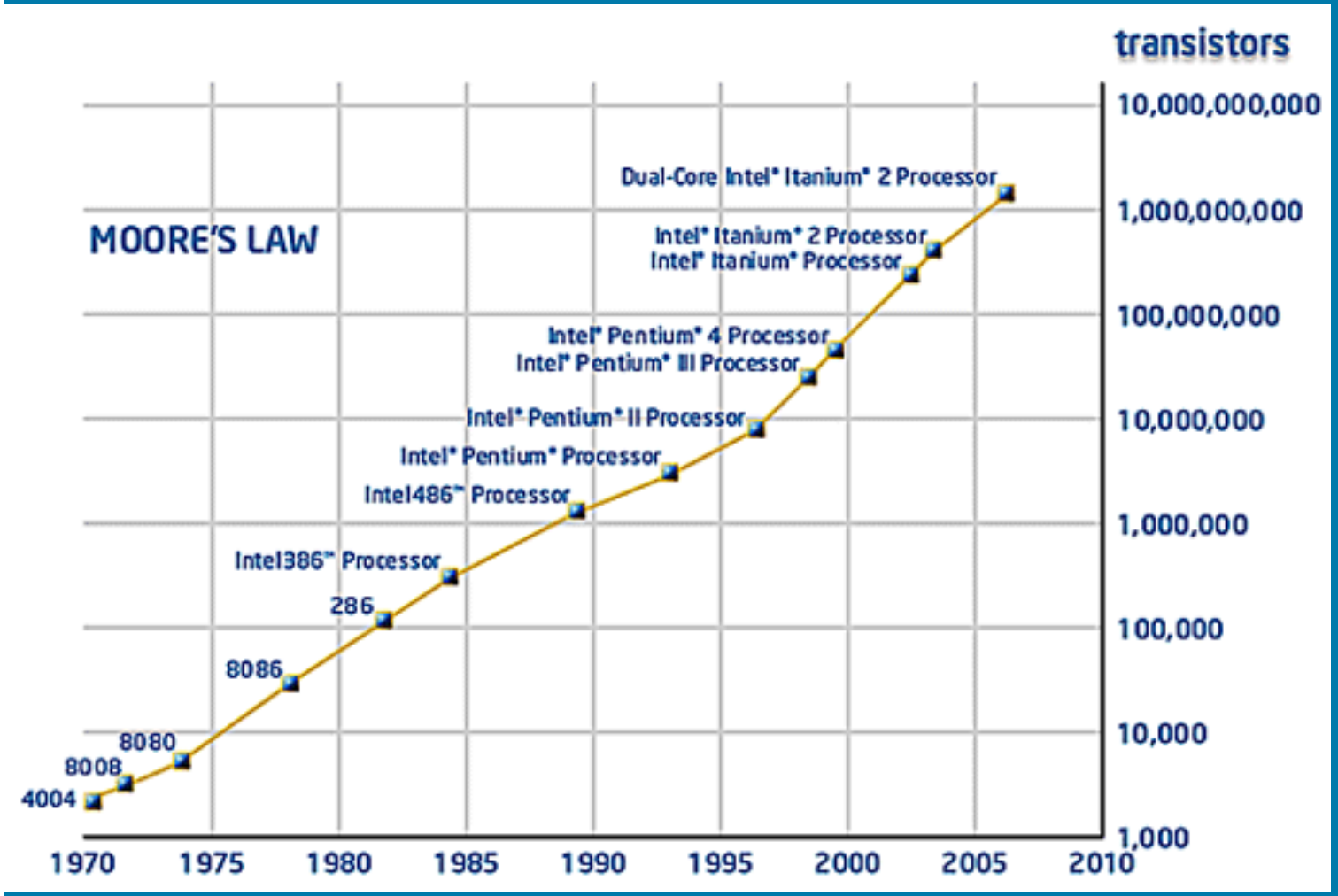
Se usarmos uma composição de elementos físicos como o anterior



• os bits são os elementos básicos na teoria clássica da informação, mas o elemento físico tende a ser cada vez menor para o melhor desempenho no armazenamento, transmissão e processamento da informação

↓

miniaturização



$1\,\text{Byte} = 8\,\text{bits}$

$1\text{KB} = 2^{10}\,\text{Bytes}$

$1\text{MB} = 2^{20}\,\text{Bytes}$

$1\text{GB} = 2^{30}\,\text{Bytes}$

$1\text{TB} = 2^{40}\,\text{Bytes}$

$1\text{PB} = 2^{50}\,\text{Bytes}$

$1\text{HB} = 2^{60}\,\text{Bytes}$

$1\text{ZB} = 2^{70}\,\text{Bytes}$

$1\text{YB} = 2^{80}\,\text{Bytes}$

$2^{10} \approx 10^{3}$

• tão pequenos que as leis da física clássica não mais se aplicam a eles ⇒ bits de sistemas regidos pela física quântica

“ q-bit ”

• Quem são e como se comportam ?
Para responder questões como estas precisamos de alguns conceitos novos.

A Mecânica Quântica

- O conjunto dos postulados

No nosso caso de interesse...

- Espaço de Hilbert bidimensional

Spin do elétron, polarização do fóton, sistemas de dois níveis em geral ;

$$\left|\phi^{(1)}\right\rangle = \left|\uparrow\right\rangle \quad ou \quad \left|\phi^{(0)}\right\rangle = \left|\downarrow\right\rangle$$

base associada aos valores 1 ou 0 do bit clássico.

Auto estados do observável

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Mas, em Mecânica Quântica existe o...

Princípio da superposição

$$\left|\phi^{(+)}\right\rangle = \frac{\left|\uparrow\right\rangle + \left|\downarrow\right\rangle}{\sqrt{2}} \quad ou \quad \left|\phi^{(-)}\right\rangle = \frac{\left|\uparrow\right\rangle - \left|\downarrow\right\rangle}{\sqrt{2}}$$

que são os auto - estados do operador

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Em geral

$$\left|\psi\right\rangle = \cos\theta\left|\uparrow\right\rangle + \sin\theta\left|\downarrow\right\rangle$$

Estado puro

N q-bits → espaço de Hilbert é um produto direto

$$\Xi_1 \otimes \Xi_2 \otimes \Xi_3 \otimes \ldots \otimes \Xi_N$$

$$\left|\psi\right\rangle = \left|\psi_1\right\rangle \otimes \left|\psi_2\right\rangle \otimes \ldots \otimes \left|\psi_N\right\rangle = \left|\psi_1, \psi_2, \ldots, \psi_N\right\rangle$$

é um produto direto de estados puros

Base do espaço

$$\left|\phi_{\{i_1, i_2, \ldots i_N\}}\right\rangle = \left|\phi_1^{(i_1)}, \phi_2^{(i_2)}, \ldots, \phi_N^{(i_N)}\right\rangle$$

Exemplo $\left|\uparrow_1, \uparrow_2, \ldots, \downarrow_N\right\rangle$

Forma genérica do estado

$$\left|\psi\right\rangle = \sum_{i_1, i_2, \ldots i_N = 0}^{1} c_{\{i_1, i_2, \ldots i_N\}} \left|\phi_1^{(i_1)}, \phi_2^{(i_2)}, \ldots, \phi_N^{(i_N)}\right\rangle$$

que em geral não é um produto direto !

→ Emaranhados

Exemplo em

$\Xi_1 \otimes \Xi_2$ →

$$\left|\psi\right\rangle = \frac{\left|\uparrow_1, \uparrow_2\right\rangle + \left|\downarrow_1, \downarrow_2\right\rangle}{\sqrt{2}}$$

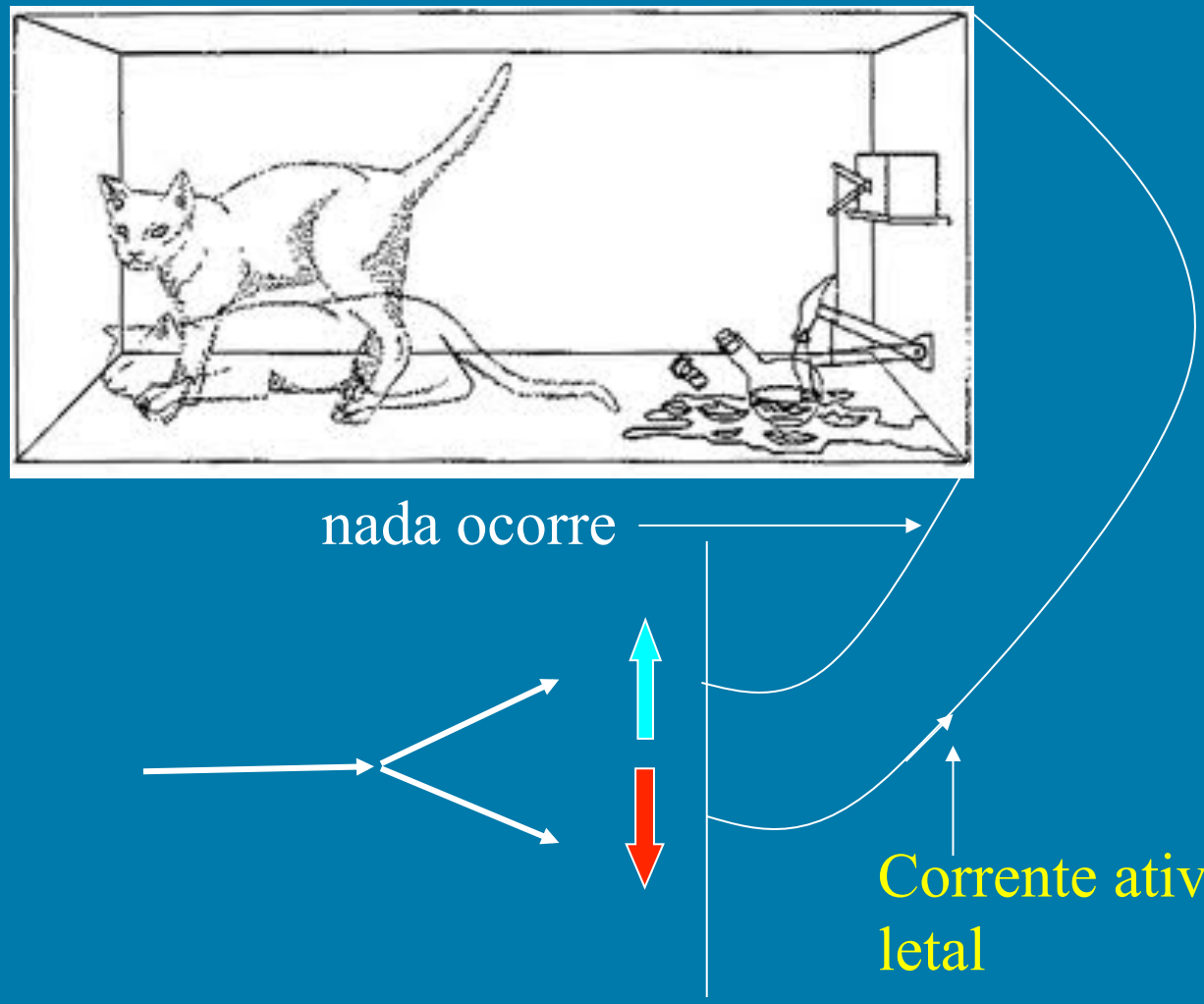
Emaranhados de N q-bits

$$|\psi\rangle = \frac{|\uparrow_1, \uparrow_2, \ldots, \uparrow_N\rangle + |\downarrow_1, \downarrow_2, \ldots, \downarrow_N\rangle}{\sqrt{2}}$$

Se N é macroscopicamente grande...

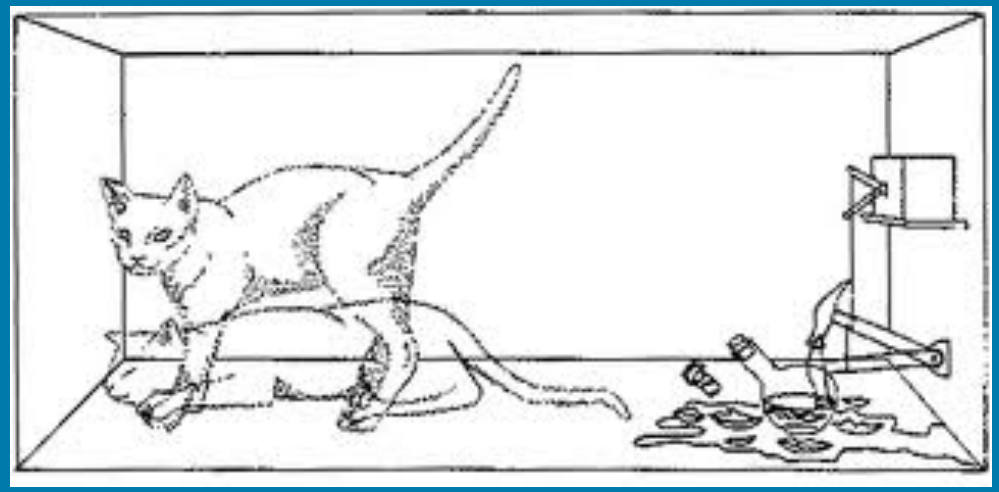
O gato de Schrödinger

O Gato de Schrödinger



O Gato de Schrödinger

O paradoxo



$$\underbrace{\uparrow\uparrow\uparrow\uparrow\cdots\uparrow}_{\text{gato vivo}} + \underbrace{\downarrow\downarrow\downarrow\downarrow\cdots\downarrow}_{\text{gato morto}}$$

Informação Quântica

Novamente queremos atuar em vários elementos físicos. Agora os elementos são quânticos

0 ou 1 $\longleftrightarrow$ $\left|\phi^{(1)}\right\rangle = \left|\uparrow\right\rangle \;\; ou \;\; \left|\phi^{(0)}\right\rangle = \left|\downarrow\right\rangle$

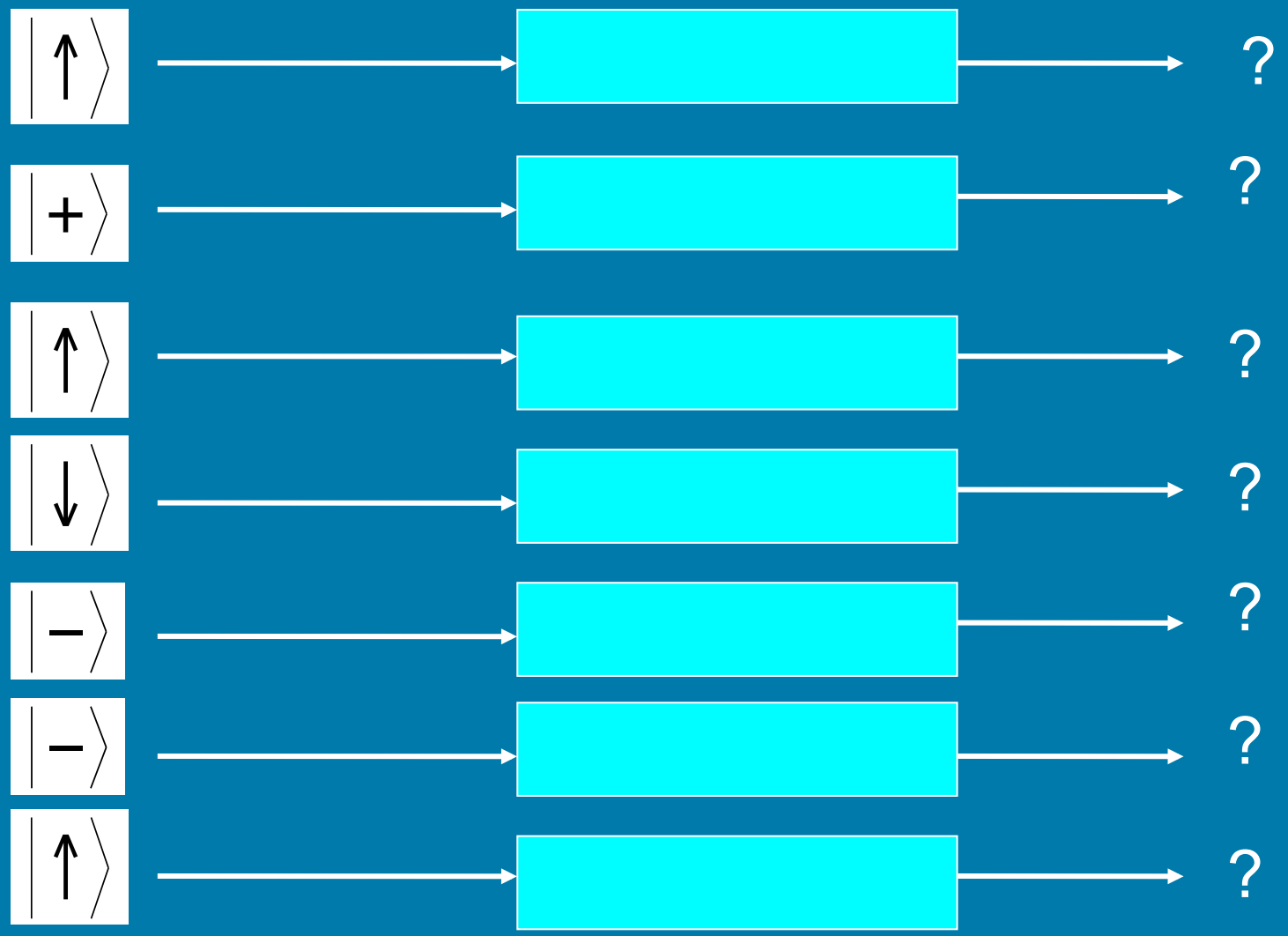
excitação $\longrightarrow$ Elemento Físico

Determinada característica é ativada $\longrightarrow$ $\left|\phi^{(1)}\right\rangle = \left|\uparrow\right\rangle$

Não há ativação da característica em questão $\longrightarrow$ $\left|\phi^{(0)}\right\rangle = \left|\downarrow\right\rangle$

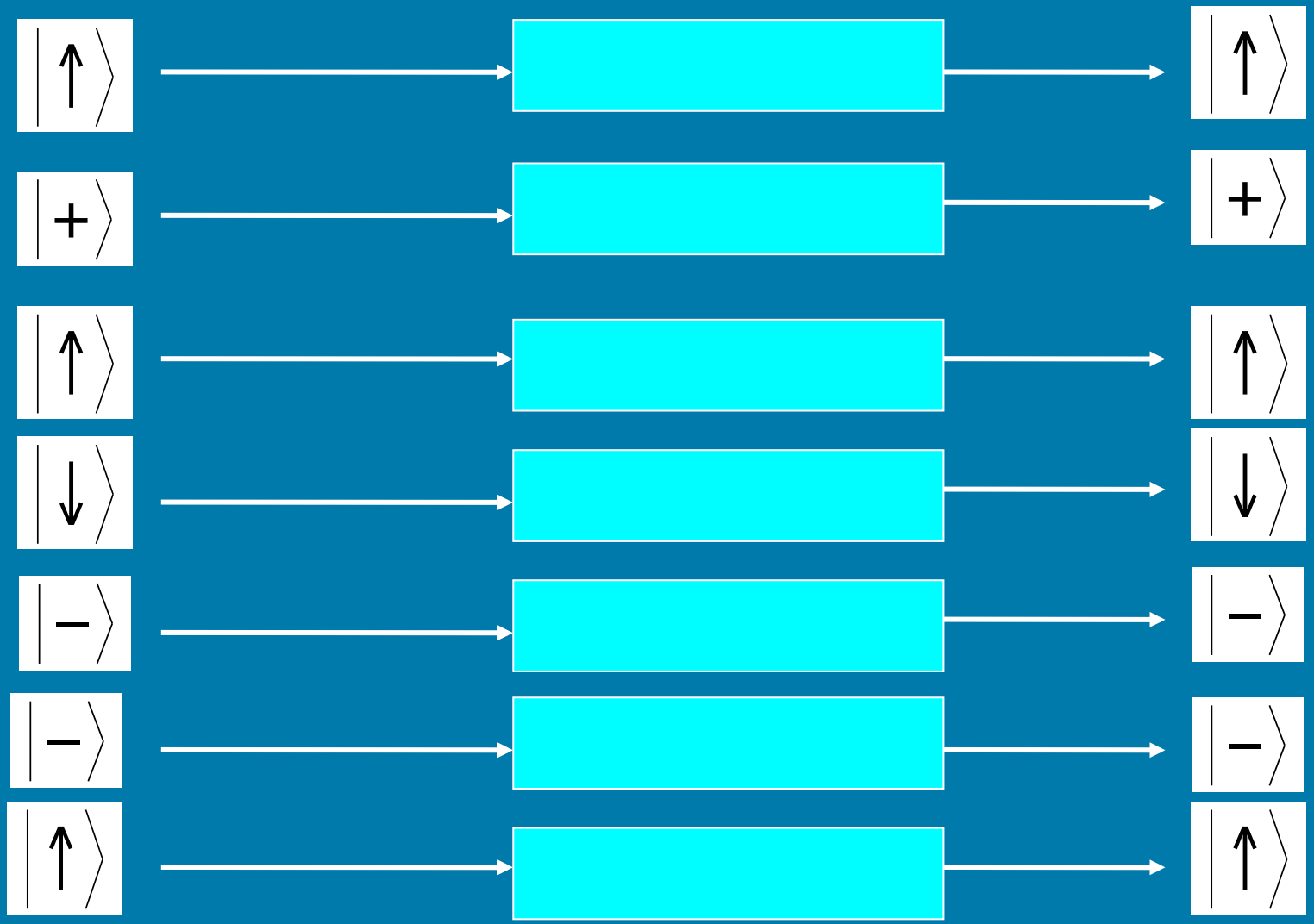
Stern-Gerlach

Q-bits podem ser preparados por inúmeros "magnetos" orientados para medir σ_x ou σ_z e, portanto, encarados como q-bits não-ortogonais



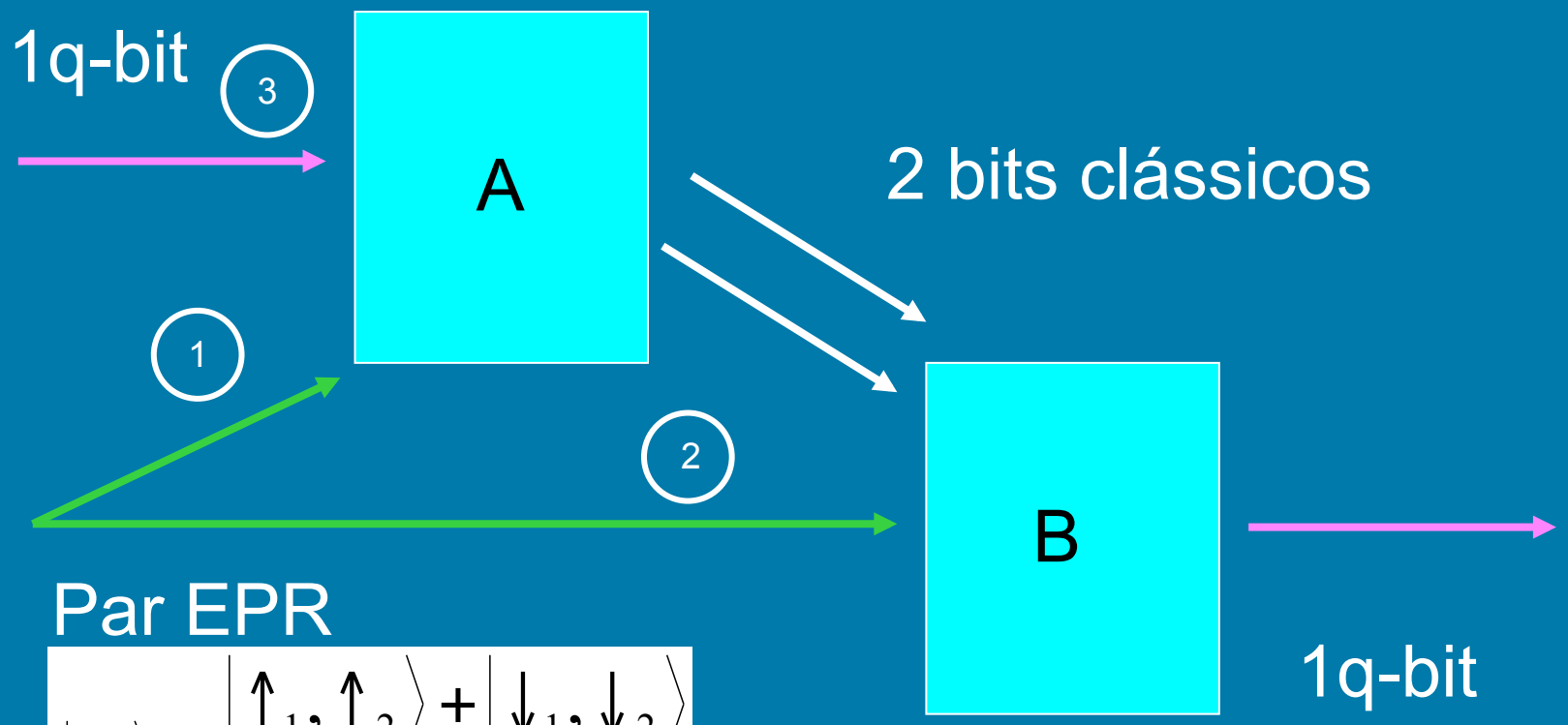
Comunicação de dados quânticos

A deseja enviar N q-bits para B: sem medir!!!



Teleportação

Comunicação sem medir os q-bits



Par EPR

$$|\psi\rangle = \frac{|\uparrow_1, \uparrow_2\rangle + |\downarrow_1, \downarrow_2\rangle}{\sqrt{2}}$$

Base de Bell para o par EPR

$$\left|\psi_{AB}^{(+)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|10\right\rangle_{AB} + \left|01\right\rangle_{AB}\right)$$

$$\left|\psi_{AB}^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|10\right\rangle_{AB} - \left|01\right\rangle_{AB}\right)$$

$$\left|\phi_{AB}^{(+)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|11\right\rangle_{AB} + \left|00\right\rangle_{AB}\right)$$

$$\left|\phi_{AB}^{(-)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|11\right\rangle_{AB} - \left|00\right\rangle_{AB}\right)$$

Emaranhamento com C

$$\left|\psi_C\right\rangle\left|\phi_{AB}^{(+)}\right\rangle = \left(a\left|0\right\rangle_C + b\left|1\right\rangle_C\right)\frac{1}{\sqrt{2}}\left(\left|11\right\rangle_{AB} + \left|00\right\rangle_{AB}\right)$$

$$\left|\psi_C\right\rangle\left|\phi_{AB}^{(+)}\right\rangle = \frac{1}{2}\left|\phi_{AC}^{(+)}\right\rangle\left|\psi_B\right\rangle + \frac{1}{2}\left|\psi_{AC}^{(+)}\right\rangle\sigma_x\left|\psi_B\right\rangle +$$

$$+\frac{1}{2}\left|\psi_{AC}^{(-)}\right\rangle(-i\sigma_y)\left|\psi_B\right\rangle + \frac{1}{2}\left|\phi_{AC}^{(-)}\right\rangle\sigma_z\left|\psi_B\right\rangle$$

A comunica classicamente (2 bits) a B o resultado de sua medida na base de Bell.
B através de transformações unitárias obtém o estado original!

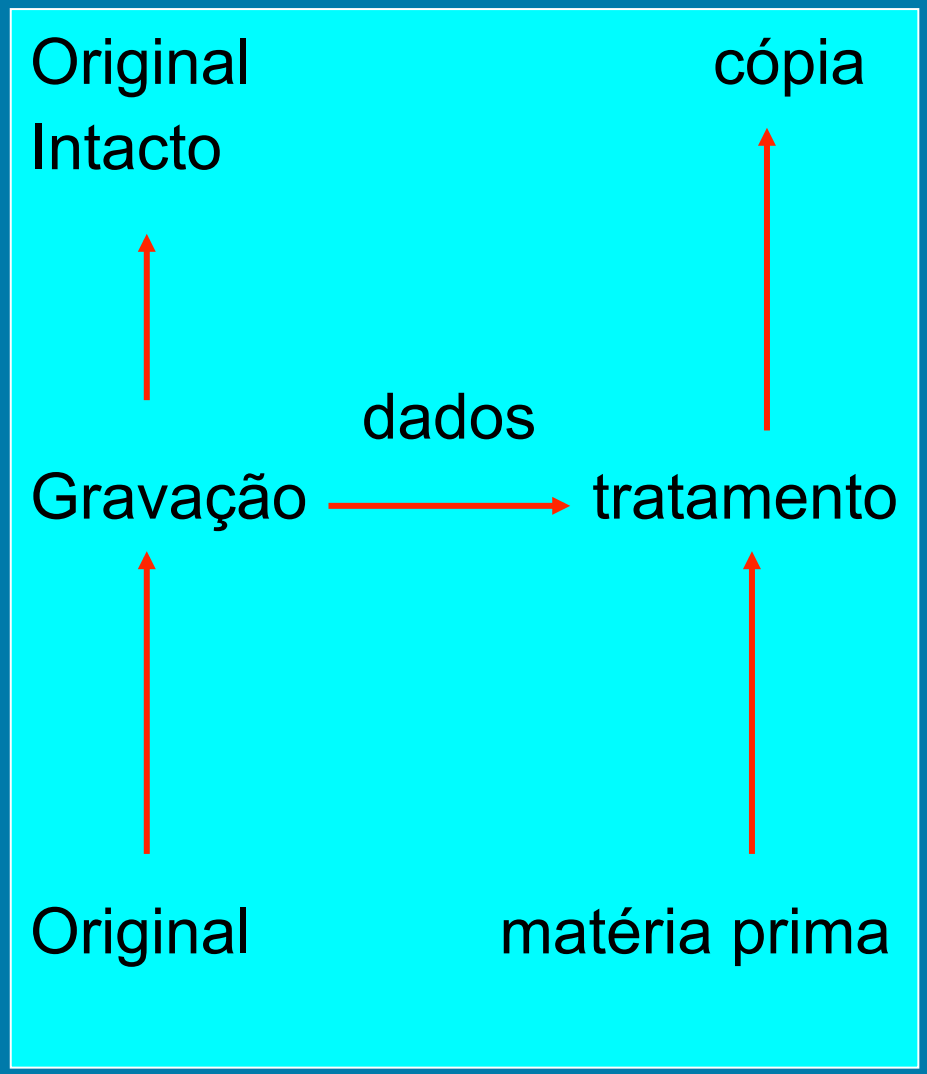
Determinação da característica do composto

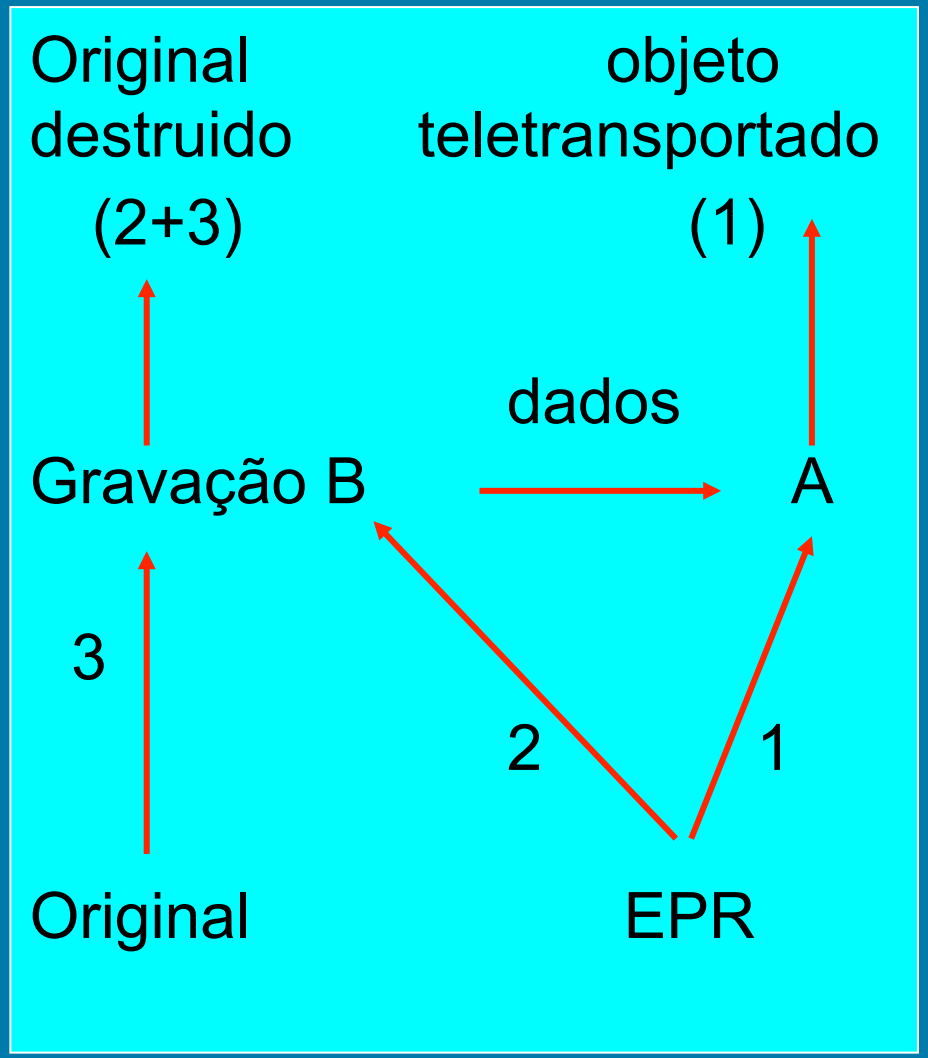
1 + 3 ⇒ a informação contida no objeto 3 desaparece!

⇓

Objetos quânticos não podem ser copiados (no – cloning)

Fax clássico X Teletransporte





Canais com ruído, decoerência e correção de erros

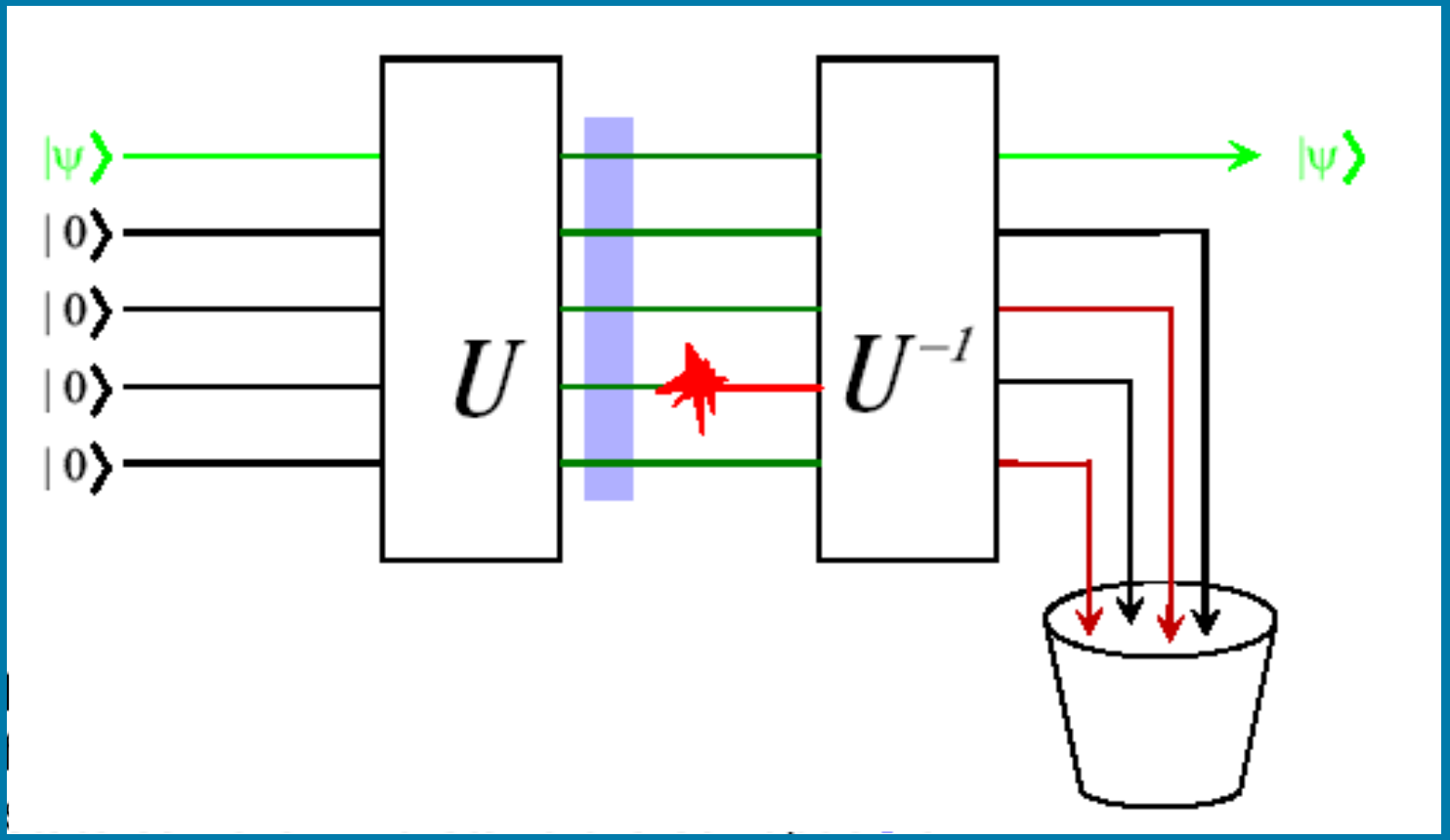
- Descrição do ruído em mecânica quântica: acoplamento com um meio externo, o reservatório

- Operador densidade representativo de uma mistura estatística = emaranhado (estado puro) do sistema composto

- Dinâmica irreversível do sub-sistema de interesse (N – q-bits) = evolução unitária do sistema composto

Correção de erro

Emaranhamento de um qubit com outros pode transportá-lo confiavelmente



Comentários gerais:

- Vimos como o uso de emaranhados em apenas 1 canal pode trazer resultados surpreendentes à teoria de comunicação.

- Importância grande em criptografia. Não – clonagem protege o envio de mensagens codificadas.

- Processamento de informação lado a lado com o desenvolvimento da computação quântica. Uma preocupação...quebra de senhas.

Avanço na implementação prática
destes conceitos

Manipulação individual de sistemas quânticos

- íons em armadilhas lineares
- fótons em cavidades ópticas
- spins em pontos quânticos
- fluxóides em dispositivos supercondutores
- NMR em moléculas

Comentários finais

• Informação + Computação Quântica; maior eficiência no armazenamento, processamento e transmissão da informação ⟷ paralelismo via emaranhamento.

• Influência do meio em processadores e canais quânticos de comunicação → decoerência → efeitos quânticos rapidamente destruidos. Códigos quânticos de correção de erros.

• Exploração de recursos de multi-canais quânticos ainda em desenvolvimento.

- Mais aplicações ?
- Problemas em aberto?
- Implementação em escala industrial ?

A área ainda está na sua infância e respostas a estas questões serão dadas nas próximas décadas !