A modalidade quântica do conhecimento
Jogos e decisão

Rui Vilela Mendes

UTL e GFM

11-01-2005

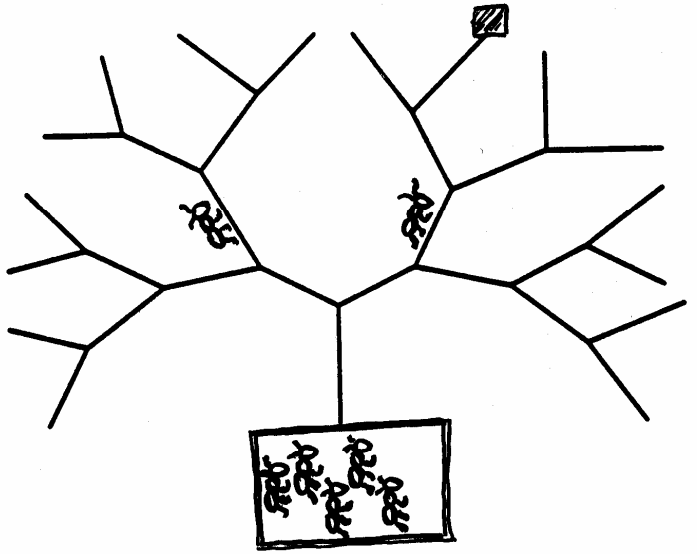
1. Uma noção operacional de “conhecimento”
2. Formalização do processo de observação. A algebra da medida
3. Codificações. O espaço de Hilbert como codificação da incompatibilidade
4. Algumas consequências da modalidade quântica. Sobreposição e entrelaçamento
5. Observáveis não-compatíveis na Natureza
6. Jogos. Equilíbro de Nash e jogos quânticos
7. Um enquadramento computacional para problemas de decisão

1. Uma noção operacional de conhecimento

- "Conhecimento" = { *Capacidade de prever o resultado duma acção* }
- { *Capacidade de prever o resultado duma acção* } $\Leftarrow$ { Regras + consequências }
- A natureza dinâmica (temporal) do conhecimento humano !
- {Aquisição de conhecimento} = {1. Perguntas
  2. Registo das respostas
  3. Compressão da informação}

As formigas e a compressão da informação

- (Reznikova e Ryabko)



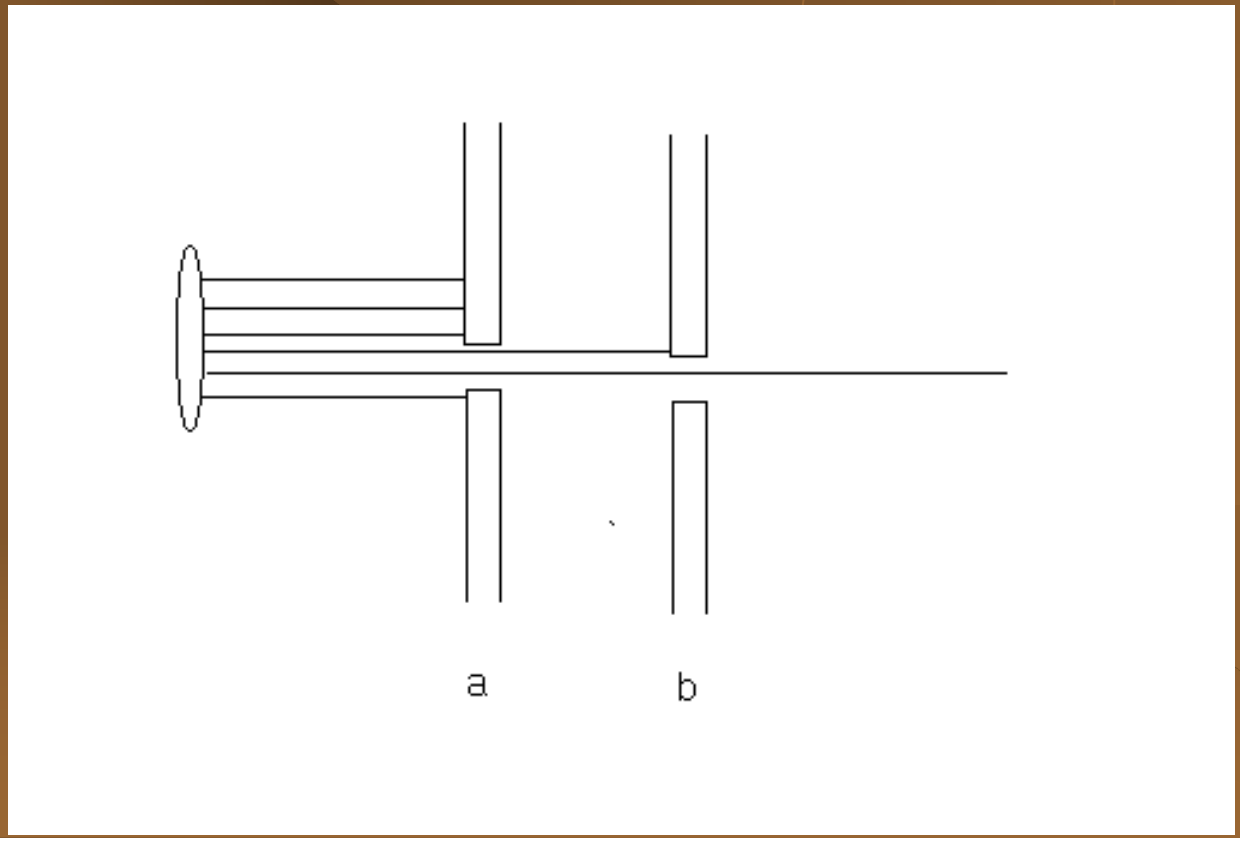
No.	SEQUENCE OF TURNS TO SYRUP	MEAN TIME SEC.	SAMPLE STANDARD DEVIATION	NUMBER OF TESTS
1	LLL	72	8	18
2	RRR	75	5	15
3	LLLLLL	84	6	9
4	RRRRR	78	8	10
5	LLLLL	90	9	8
6	RRRRRR	88	9	5
7	LRLRLR	130	11	4
8	RLRLRL	135	9	8
9	LLR	69	4	12
10	LRLL	100	11	10
11	RLLLR	120	9	6
12	RRLRL	150	16	8
13	RLRRRL	180	20	6
14	RRLRRR	220	15	7
15	LRLLRL	200	18	5

1. Uma noção operacional de conhecimento

- "Conhecimento" = { *Capacidade de prever o resultado duma acção* }
- { *Capacidade de prever o resultado duma acção* } ⇐ { Regras + consequências }
- A natureza dinâmica (temporal) do conhecimento humano !
- {Aquisição de conhecimento} = {1. Perguntas
  2. Registo das respostas
  3. Compressão da informação}
- As perguntas podem ser reduzidas a perguntas binárias ("SIM", "NÃO")

2. Formalização do processo de observação. A algebra da medida (J. Schwinger)

- Instrumentos ⇔ Observáveis (a)
- Medição ⇔ Filtragem dum conjunto
- Símbolo de medida : a ⇔ M(a)



A matemática como metáfora

- Considerando a Matemática como uma Metáfora, a própria interpretação do conhecimento matemático é um acto altamente criativo.
  Num certo sentido a Matemática é uma novela acerca da Natureza e da Humanidade. E não se pode dizer precisamente o que é que a Matemática nos ensina, do mesmo modo que não se pode dizer exactamente o que a leitura de “Guerra e Paz” nos ensina.
  O conhecimento é incorporado ele próprio no acto de repensar esse ensinamento.
  (Y. I. Manin)

A matemática como metáfora

- Considerando a Matemática como uma Metáfora, a própria interpretação do conhecimento matemático é um acto altamente criativo.
  Num certo sentido a Matemática é uma novela acerca da Natureza e da Humanidade. E não se pode dizer precisamente o que é que a Matemática nos ensina, do mesmo modo que não se pode dizer exactamente o que a leitura de “Guerra e Paz” nos ensina.
  O conhecimento é incorporado ele próprio no acto de repensar esse ensinamento.
  (Y. I. Manin)

- Usemos pois a matemática, construindo uma algebra para os símbolos de medida

Algebra dos simbolos de medida
(uma observável)

$M(a) + M(a') = M(a') + M(a)$	filtros em paralelo comutam
$\sum_i M(a^i) = 1$	$1 =$ passa tudo
0	filtro que rejeita tudo
$M(a).M(a') = \delta\,(\mathrm{a,a'})\, M(a)$	dois filtros sucessivos
$1.1 = 1$	
$0.0 = 0$	
$1.0 = 0.1 = 0$	
$1.M(a) = M(a).1 = M(a)$	
$0.M(a) = M(a).0 = 0$	
$M(a) + 0 = M(a)$	

- Observáveis compatíveis $A=\{a_1,a_2,a_3, ...\}$

  $M(a_i)\, M(a_k)\, M(a_i) = M(a_k)\, M(a_i)$

  (filtragem em relação a qualquer observável não altera a pureza do conjunto selecionado por qualquer outra)

  $M(a_i)M(a_k)=M(a_k)M(a_i)$ comutatividade

- Conjunto completo de observáveis compatíveis A

  A medição duma qualquer observável que não seja função das observáveis em A produz um conjunto no qual as observáveis de A já não têm valores definidos.

  (a)= conjunto de valores dum conjunto completo

Duas modalidades :

- 1) Modalidade clássica

  Todas as observáveis são compatíveis
  Todos os simbolos de medida comutam

  $M(a)\ M(a') = \delta(a , a')\ M(a)$

- 2) Modalidade quântica

  Algumas observáveis não são compatíveis

  O que fazer com $M(a)\ M(b) = ?$
  Inventa-se um novo simbolo ------ $M(a,b)$.

  Significa uma selecção em relação a (a) e depois uma transformação das propriedades do conjunto selecionado para as propriedades de (b)

  É uma extensão da algebra pré-existente, uma vez que

  $M(a,a) = M(a)$

  Quais as propriedades de $M(a,b)$?

As propriedades de M{a,b} ?

- No caso de variáveis compatíveis

  $M(a,b)\ M(c,d) = \delta(b,c)\ M(a,d)$

  $\delta(b,c)$ é um número : 0 ou 1

  Sugere :

- Para observáveis incompatíveis

  $M(a,b)\ M(c,d) = \langle b|c\rangle\ M(a,d)$

  $\langle b|c\rangle$ também um elemento dum corpo de números
  Existirá incompatibilidade sempre que $\langle b|c\rangle \neq 0, 1$

Propriedades de <b|c> (função de transformação)

- Função de transformação

$$\begin{aligned} M(a,b) &= 1.M(a,b).1 \\ &= \sum_{c,d} M(c)M(a,b)M(d) \\ &= \sum_{c,d} < c|a >< b|d > M(c,d) \end{aligned}$$

- Completude

$$M(a).M(c) = < a|c > M(a,c) = \sum_b M(a).M(b).M(c)$$

$$= \sum_b < a|b >< b|c > M(a,c)$$

$$\begin{aligned} < a|c > &= \sum_b < a|b >< b|c > \\ \delta(a,a') &= \sum_b < a|b >< b|a' > \end{aligned}$$

Probabilidades

- Porque $M(a)\,M(b) = \langle a|b\rangle\, M(a,b)$, $\langle a|b\rangle$ deverá estar relacionado com a probabilidade de que estados preparados com propriedades (b) possam ser encontrados com propriedades (a)
- Contudo não pode ser uma probabilidade porque a algebra dos simbolos é invariante para

  $M(a,b) \rightarrow \lambda(a)\, M(a,b)\, \lambda^{-1}(b)$

  $\langle a|b\rangle \rightarrow \lambda^{-1}(a)\, \langle a|b\rangle\, \lambda(b)$
- A escolha invariante mais simples é :

  $p(a,b) = \langle a|b\rangle\langle b|a\rangle$
- Para p(a,b) ser real

  $\langle a|b\rangle = \langle b|a\rangle^{*}$

  Corpo complexo

Probabilidades

- Porque $M(a)\,M(b) = \langle a|b\rangle\, M(a,b)$, $\langle a|b\rangle$ deverá estar relacionado com a probabilidade de que estados preparados com propriedades (b) possam ser encontrados com propriedades (a)
- Contudo não pode ser uma probabilidade porque a algebra dos simbolos é invariante para

  $M(a,b) \rightarrow \lambda(a)\, M(a,b)\, \lambda^{-1}(b)$

  $\langle a|b\rangle \rightarrow \lambda^{-1}(a)\, \langle a|b\rangle\, \lambda(b)$
- A escolha invariante mais simples é :

  $p(a,b) = \langle a|b\rangle\langle b|a\rangle$
- Para p(a,b) ser real

  $\langle a|b\rangle = \langle b|a\rangle^{*}$

  Corpo complexo
- Esta escolha é a teoria quântica ou a "modalidade quântica do conhecimento". É a escolha mais simples compatível com a hipótese de que nem todas as observáveis são compatíveis.
- É esta incompatibilidade que está na base do modelo quântico, não o indeterminismo ou qualquer outra propriedade obscura. Todos os chamados paradoxos da teoria quântica são o resultado de fazer perguntas sobre aspectos incompatíveis. Como dizem Feshbach e Weisskopf : "Sempre que se faz uma pergunta tôla obtém-se uma resposta tôla".

3. Codificações

- **No caso clássico :**
  A algebra dos simbolos de medida pode ser codificada por uma algebra Booleana de conjuntos com as operações de união e intersecção.
- **No caso quântico :**
  # Codificação por espaço de Hilbert (o mais popular)
  # Espaço de fase clássico com uma algebra deformada (parêntesis de Moyal)
  # Codificação tomográfica

Codificação por espaço de Hilbert

A cada estado (definido por um conjunto completo de observáveis) corresponde um vector $|a>$ num espaço vectorial V

$$V = \{\{|a>\}, +, (F, +, .)\}$$

Propriedades

$$|a> \in V \quad , \quad |b> \in V \quad \Longrightarrow \quad |a> + |b> \in V$$
$$|a> \in V \quad , \quad \lambda \in F \quad \Longrightarrow \quad \lambda|a> \in V$$
$$\lambda(|a> + |b>) = \lambda|a> + \lambda|b>$$

Espaço dual V^* = Espaço das aplicações lineares $V \rightarrow F$

$$V = \{\{<a|\}, +, (F, +, .)\}$$
$$V \rightarrow F :< a|b> \in F, <a| \in V^*, |b> \in V$$

(No espaço de Hilbert há uma identificação canónica de V e V^* através de

$$<a|b> = (a, b)$$

sendo (a, b) o producto escalar

Em geral pode-se estabelecer uma correspondência antilinear $\lambda|a> \rightarrow \lambda^* <a|$, mas não necessariamente o inverso, porque pode haver elementos em V^* sem correspondente em V.

Codificação por espaço de Hilbert

Algebra da medida nesta codificação

$$M(a,b) = |a><b|$$

Os $M(a,b)$ são operadores em V. Em particular

$$A = \sum_a a|a><a|$$

é um operador que ao actuar em $|a>$

$$A|a> = a|a>$$

Deste modo as **observáveis podem ser identificadas com operadores deste tipo e os valores da observável são os valores próprios do operador.**

Todas as relações da algebra da medida são agora verificadas trivialmente

$$|a><b||c><d| = <b|c> |a><d|$$

Probabilidade

$$p(a,b) = <b|a><a|b> = |<a|b>|^2$$

etc.

Codificação por espaço de Hilbert

Evolução temporal

Transformações que preservam as probabilidades têm de ser representadas por operadores unitários ou antiunitários

$$< U\,b|U\,a >=< b|a >$$

ou

$$< Ab|Aa >=< b|a >^{*}$$

Para sistemas com invariância para translação no tempo, a evolução temporal tem de ser representada por um operador unitário

$$|\psi\,(t)\rangle = e^{-iHt}\,|\psi\,(0)\rangle$$

Ao gerador das translações no tempo chama-se Hamiltoniana. Assim

$$i\frac{\partial}{\partial t}\,|\psi\,(t)\rangle = H\,|\psi\,(t)\rangle$$

temos a equação de Schrödinger.

Codificação por espaço de Hilbert

- **Resumindo** :

  Nesta codificação

  # *Os estados são* (representados por) *Vectores* num espaço vectorial

  # *Observações* (representadas por) *Projeções*

  # *Observáveis* (representadas por) *Operadores com espectro real*

  # *Transformações* que preservam a probabilidade (representadas por) *Operadores unitários*

  # *Evolução temporal* (representada pela) acção dum operador unitário particular

4. Algumas consequências da modalidade quântica.

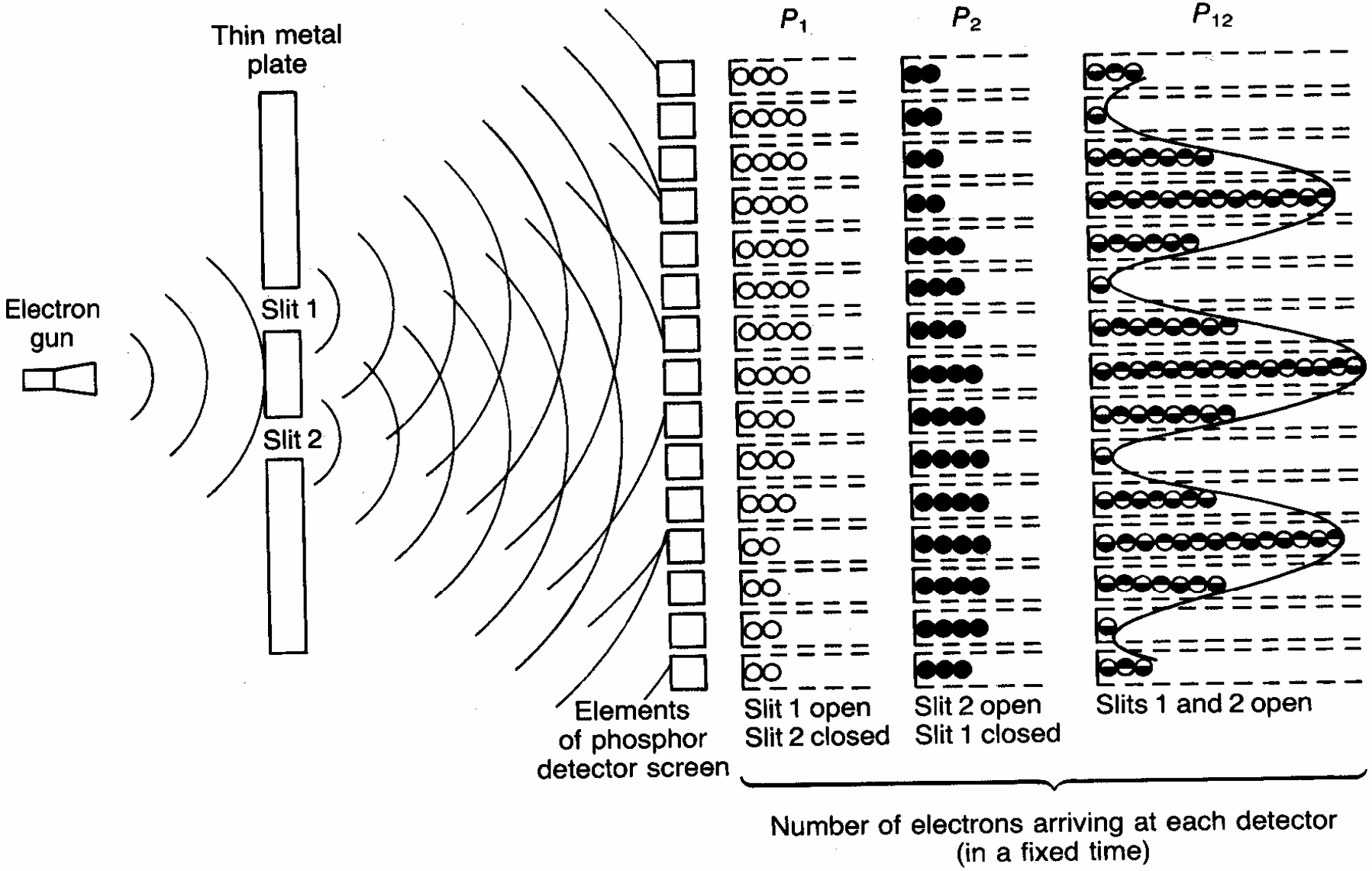
(consequências não-óbvias duma hipótese simples – a existência de observáveis incompatíveis)

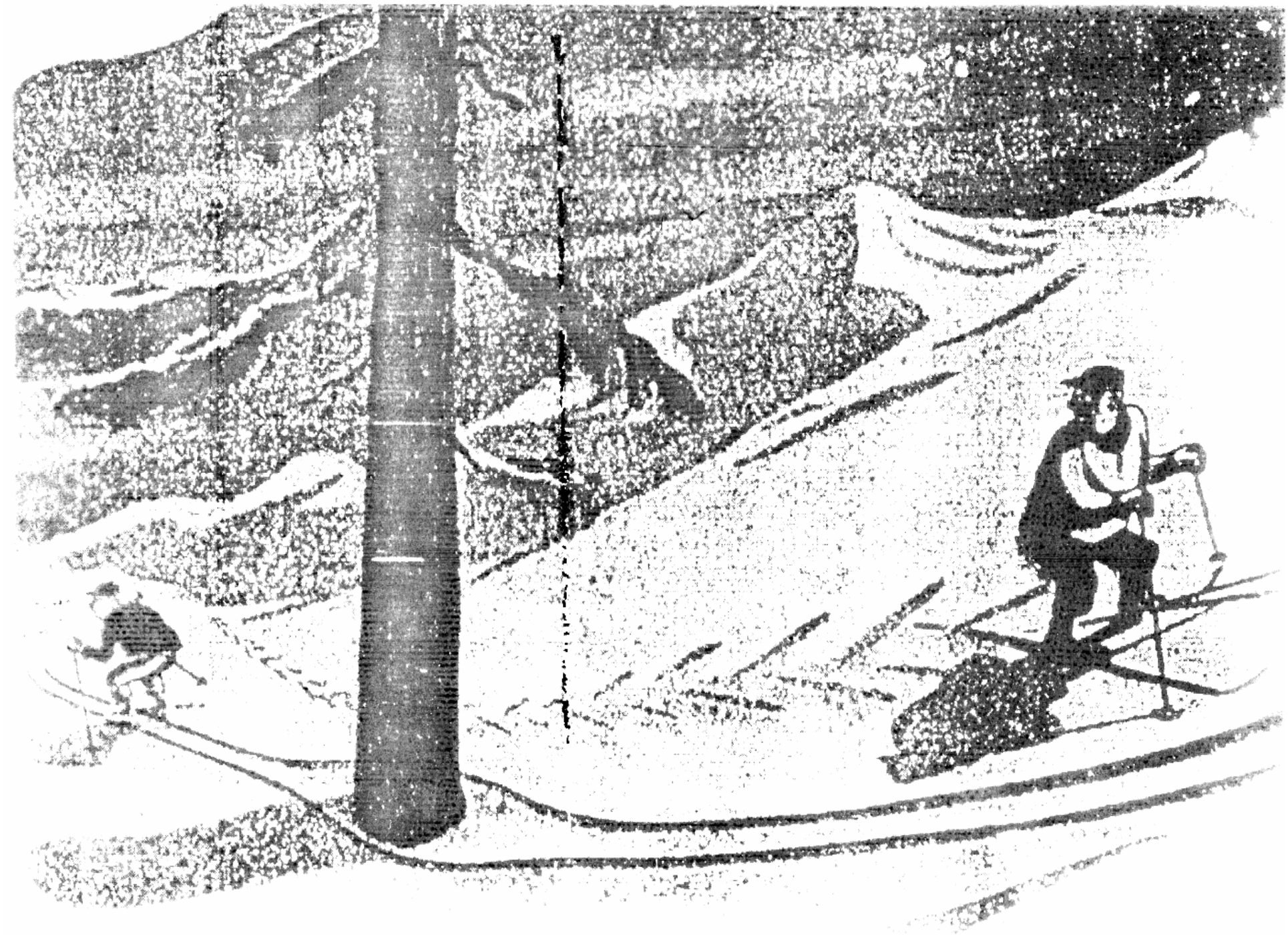
- Sobreposição
- Entrelaçamento

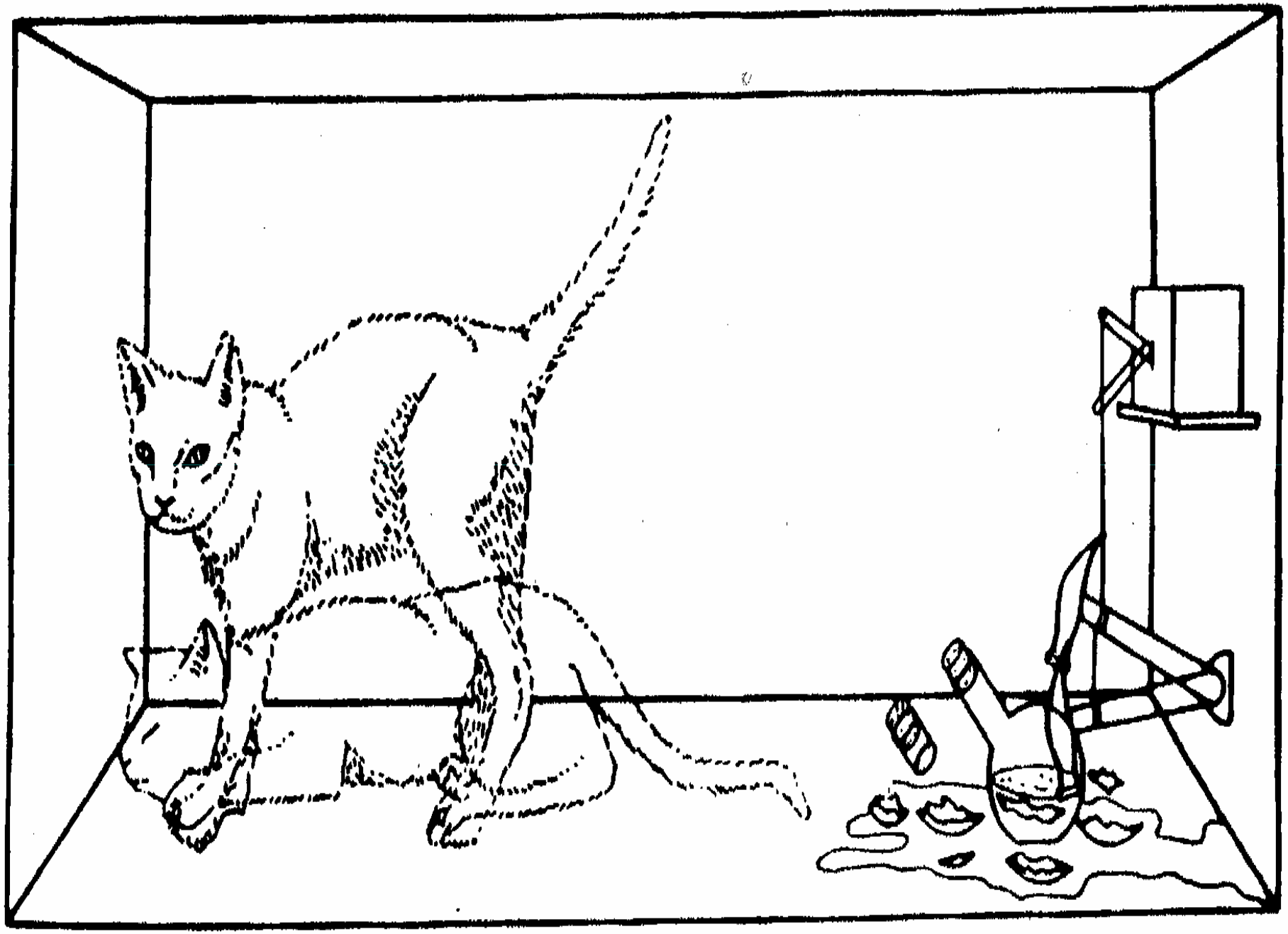
Sobreposição

- Se $\Phi \in H$ e $\Psi \in H$ representam estados então $\Phi+\Psi \in H$ também é um estado porque o espaço de Hilbert é linear
- Esta é uma propriedade familiar para as ondas clássicas. Significa que propriedades do tipo ondulatório são gerais para sistemas quânticos
- Ao fazer uma medida sobre o estado $\Phi+\Psi$, (se Φ e Ψ representarem propriedades exclusivas) obtém-se ou Φ ou Ψ com probabilidade 1/2
- Se o resultado for Φ o estado depois da medida é Φ (a medida é uma projeção num subespaço)

Propriedades ondulatórias da matéria







Entrelaçamento

- Espaços compostos = Produtos tensoriais de espaços de Hilbert , $H \otimes H$
- Estados factorizados

  $a \otimes b = |a\, b\rangle \in H \otimes H$

- Estados entrelaçados

  $|a_1\, b_1\rangle + |a_2\, b_2\rangle$

  Significa que se se fizer uma medida sobre o primeiro sistema e o resultado for a_1 então o segundo sistema fica automáticamente no estado b_1
  Não-localidade da teoria quântica

5 .Observáveis não-compatíveis na Natureza

Na Física

- **Posição** (x) e **Momento** (p_x)
- **Posição** (x) e **Momento Angular** (L_z)
- **Tempo** (t) e **Energia** (E)

Noutros domínios (?)

Preço (no sentido de valor monetário) and **Posse**

O preço só é realmente bem definido no momento da transação, isto é quando a posse muda. No resto do tempo é apenas uma grandeza virtual.

Tempo e **Producto Nacional**

Um certo intervalo de tempo é necessário para se ter uma ideia aproximada do Producto Nacional. É a mesma situação que se verifica com o **Tempo** e a **Energia** na Física.

(Notar que a incompatibilidade é um conceito operacional, significando observação simultânea. Pode-se sempre **falar** de energia num certo instante de tempo, mas observá-los (**medi-los**) simultâneamente é uma questão completamente diferente)

- Resumindo:
- Na modalidade clássica :
  Estados (situações) codificados como conjuntos com algebra booleana
- Na modalidade quântica :
  Estados (situações) codificados como vectores num espaço de Hilbert
- E sempre que houver variáveis incompatíveis é a modalidade quântica que deve ser aplicada, seja qual for o domínio

6. Jogos

- **Teoria dos jogos:**
  Estudo de problemas de escolha dentro dum quadro de valores (função de utilidade)

- Matemática, Economia, Biologia, Ciências Sociais, Comunicação

Jogos

- Jogos Estáticos e Jogos Dinâmicos
- Estratégias puras e Estratégias mixtas
- Informação Completa ou Incompleta
- Estratégia s_K dominada por s_P se $P(s_1,s_2,...,s_p,...,s_n)>P(s_1,s_2,...,s_k,...,s_n)$ para todos os $s_1,s_2,...,s_n$
- Eliminação iterativa das estratégias dominadas

Jogos – Equilíbrio de Nash

- $(s_1,s_2,...,s_k,...,s_n)$ é um equilíbrio de Nash se

  $P(s_1,s_2,...,s_k,...,s_n)>P(s_1,s_2,...,s_k',...,s_n)$

  para todos os s_k'
- Nenhum jogador pode melhorar a sua recompensa alterando a sua estratégia, supondo fixas as estratégias dos outros jogadores
- Todo o jogo de N jogadores, com estratégias finitas, tem pelo menos um equilíbrio de Nash, em estratégias puras ou mixtas
- Na Economia, Equilíbrio de Nash ⇔ Decisão racional (Homo Oeconomicus)

Equilíbrio de Nash. Alguns exemplos

- Cidade ou aldeia ?
  Amigo ou inimigo ?

	C	A
C	1,1	(2,5)
A	(5,2)	-1,-1

Equilíbrio de Nash. Alguns exemplos

- O dilema do prisioneiro

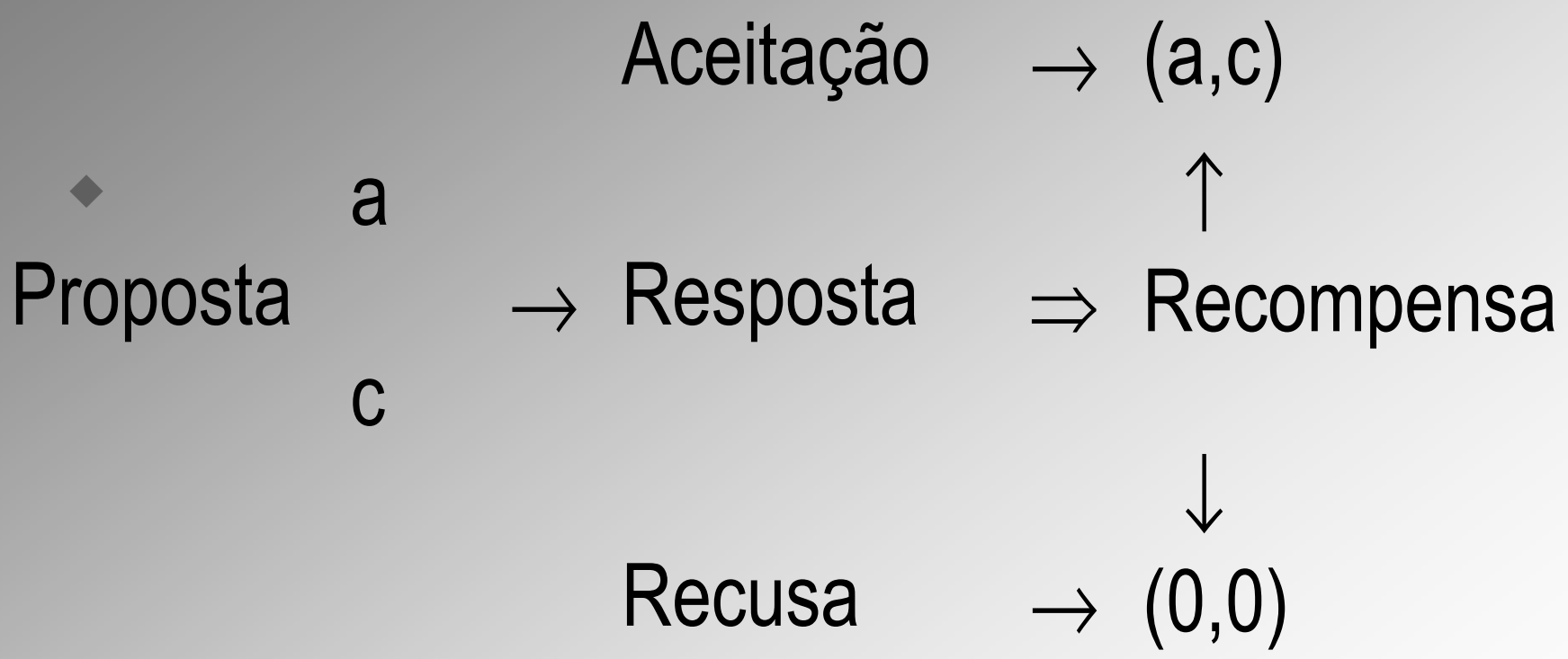
	C	T
C	1,1	-3,3
T	3,-3	(-1,-1)

Equilíbrio de Nash. Alguns exemplos

- A batalha dos sexos

(Maria,João)	Ópera	Televisão
Ópera	(5,2)	1,1
Televisão	1,1	(2,5)

O jogo do ultimato



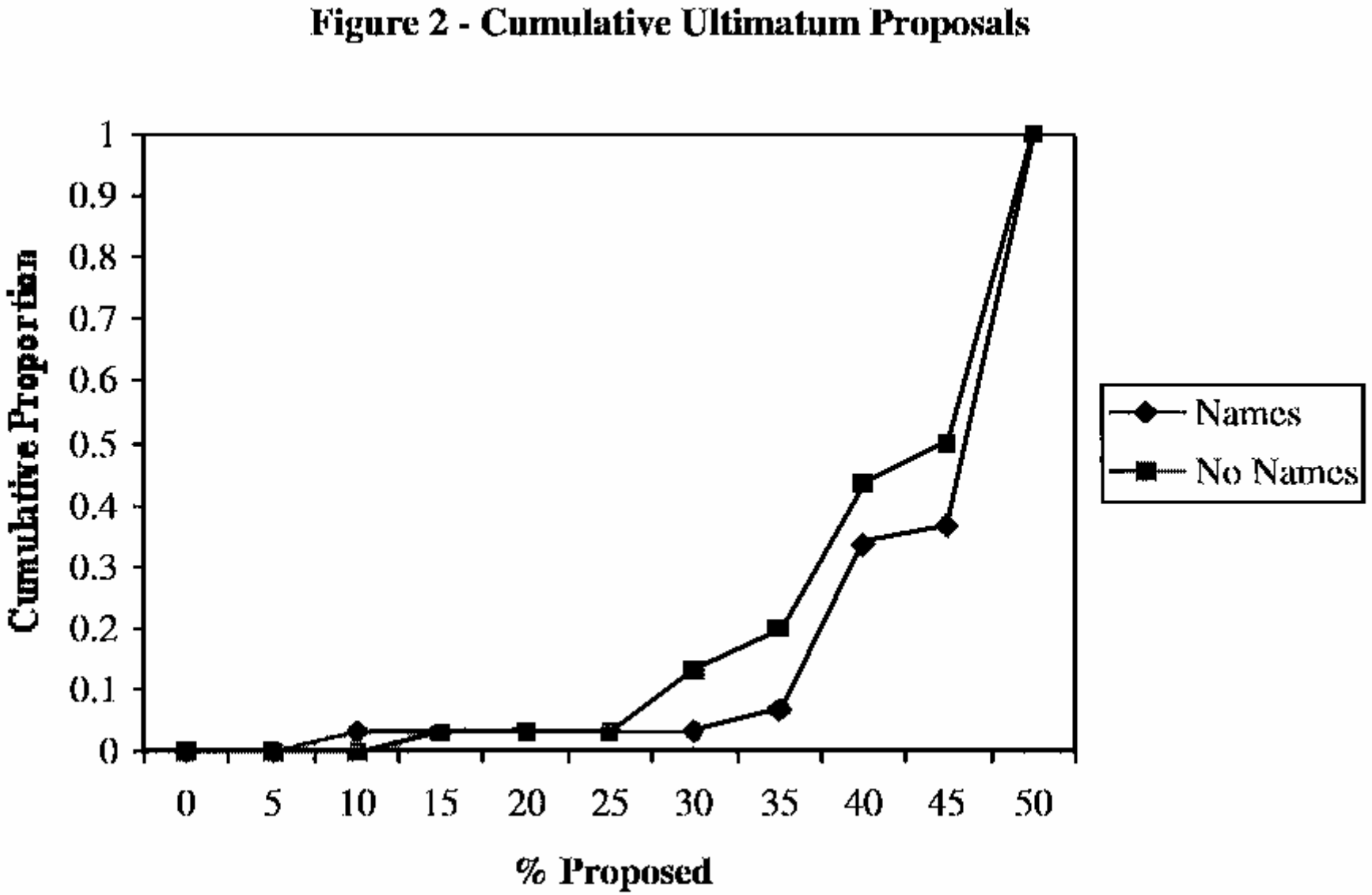
O jogo do ultimato

- a+c=2b , a>>c, (Exemplo: a=99, c=1, b=50)

	R0	R1
P0	(a,c)	0,0
P1	b,b	0,0

Equilíbrio de Nash e jogos experimentais

- Estudantes universitários



Equilíbrio de Nash e jogos experimentais

- Pequenas sociedades

Table 1. Ethnographic Summary of Societies

Group	Language Family	Environment	Economic Base	Residence	Complexity	Researcher	PC	MI
Machiguenga	Arawakan	Tropical Forest	Horticulture	Bilocal semi nomadic	Family	Henrich, Smith	1	4
Quichua	Quichua	Tropical Forest	Horticulture	Sedentary/ Semi-nomadic	Family	Patton	1	2
Achuar	Jivaroan	Tropical Forest	Horticulture	Sedentary/ Semi-nomadic	Family plus extended ties	Patton	5	2
Hadza	Khoisan/Isolate	Savanna-Woodlands	Foraging	Nomadic	Band	Marlowe	4	1
Ach	Tupi-Guarani	Semi-tropical Woodlands	Horticulture/ Foraging	Sedentary-Nomadic	Band	Hill, Gurven	6	4
Tsimane	Macro-Panoan Isolate	Tropical Forest	Horticulture	Semi-nomadic	Family	Gurven	1	3
Au	Torricelli/ Wapei	Mountainous Tropical Forest	Foraging/ Horticulture	Sedentary	Village	Tracer	3	5
Gnau	Torricelli/ Wapei	Mountainous Tropical Forest	Foraging/ Horticulture	Sedentary	Village	Tracer	3	5
Mapuche	Isolate	Temperate Plains	Small scale farming	Sedentary	Family plus extended ties	Henrich	2	6
Torguuds	Mongolian	High latitude desert Seasonally-flooded grassland	Pastoralism	Transhumance	Clan	Gil-White	2	8
Kazakhs	Turkic	High-latitude Desert Seasonally-flooded grassland	Pastoralism	Transhumance	Clan	Gil-White	2	8
Sangu	Bantu	Savanna-Woodlands Seasonally-flooded grassland	Agro-Pastoralists	Sedentary or Nomadic	Clan-Chiefdom	McElreath	5	8
Orma	Cushitic	Savanna-Woodlands	Pastoralism	Sedentary or Nomadic	Multi-Clan Chiefdom	Ensminger	2	9
Lamalera	Malayo-Polynesian	Island Tropical coast	Foraging-Trade	Sedentary	Village	Alvard	7	7
Shona	Niger-Congo	Savanna-Woodlands	farming	Sedentary	Village	Barr	5	8

Table 2 : Ultimatum Game Experiments

Group	Sample Size	Stake	Mean	Mode (% sample)[1]	Rejections	Low rejections [2]
Lamalera[3]	19	10	0.57	0.50 (63%)	4/20 (sham)[4]	3/8 (sham)
Ach	51	1	0.48	0.40 (22%)	0/51	0/2
Shona (Resettled)	86	1	0.45	0.50 (69%)	6/86	4/7
Shona (all)	117	1	0.44	0.50 (65%)	9/118	6/13
Orma	56	1	0.44	0.50 (54%)	2/56	0/0
Au	30	1.4	0.43	0.3 (33%)	8/30	1/1
Achuar	14	1	0.43	0.50 (36%)	2/15[5]	1/3
Sangu (herders)	20	1	0.42	0.50 (40%)	1/20	1/1
Sangu (farmers)	20	1	0.41	0.50 (35%)	5/20	1/1
Sangu	40	1	.41	0.50 (38%)	6/40	2/2
Shona (Unresettled)	31	1	0.41	0.50 (55%)	3/31	2/6
Hadza (big camp)	26	3	0.40	0.50 (35%)	5/26	4/5
Gnau	25	1.4	0.38	0.4 (32%)	10/25	3/6
Tsimane	70	1.2	0.37	0.5/0.3 (44%)	0/70	0/5
Kazakh	10	8	0.36	0.38 (50%)	0/10	0/1
Torguud	10	8	0.35	0.25 (30%)	1/10	0/0
Mapuche	31	1	0.34	0.50/0.33 (42%)	2/31	2/12
Hadza (all camps)	55	3	0.33	0.20/0.50 (47%)	13/55	9/21
Hadza (small camp)	29	3	0.27	0.20 (38%)	8/29	5/16
Quichua	15	1	0.25	0.25 (47%)	0/14[6]	0/3
Machiguenga	21	2.3	0.26	0.15/0.25 (72%)	1	1/10

Equilíbrio de Nash e jogos experimentais

- A hipótese “Homo Oeconomicus” é rejeitada em todos os casos
- O comportamento do jogador está fortemente relacionado com as normas sociais existentes nas suas sociedades e com a estrutura de mercado
- A decisões humanas envolvem uma mistura de interesse egoísta e um fundo de normas sociais (interiorizadas)
- Sai o “Homo Oeconomicus”
- Entra o “Homo Reciprocans” (Samuel Bowles, Herbert Gintis)
- Reciprocidade forte

Jogos quânticos

- Num jogo clássico o espaço das estratégias é um espaço discreto ou um simplex (estratégias mixtas)
- Num jogo quântico o espaço das estratégias é um espaço linear (espaço de Hilbert)
- Dado um estado inicial, as decisões dos jogadores são operações (unitárias) nesse espaço

Jogos quânticos. Um exemplo

A batalha dos sexos (Clássico)

		João	
		O(0)	T(1)
Maria	O(0)	(α, β)	(γ, γ)
	T(1)	(γ, γ)	(β, α)

$\alpha > \beta > \gamma$

Estratégias mixtas :

Maria $\mathrm{O} \rightarrow p$, $\mathrm{T} \rightarrow (1-p)$

João $\mathrm{O} \rightarrow q$, $\mathrm{T} \rightarrow (1-q)$

3 equilíbrios de Nash (clássicos) :

$p = 1, q = 1 \qquad (\alpha, \beta)$

$p = 0, q = 0 \qquad (\beta, \alpha)$

$p = \frac{\alpha-\gamma}{\alpha+\beta-2\gamma}, q = \frac{\beta-\gamma}{\alpha+\beta-2\gamma} \qquad (P', P')$

$$\alpha > \beta > P' = \frac{\alpha\beta - \gamma^2}{\alpha + \beta - 2\gamma} > \gamma$$

Jogos quânticos. Um exemplo

		João O(0)	João T(1)
Maria	O(0)	(α, β)	(γ, γ)
	T(1)	(γ, γ)	(β, α)

$$\alpha > \beta > \gamma$$

A batalha dos sexos (Quântico)

 # Estado inicial :

Qualquer combinação linear de

{|00> , |01> , |10> , |11>}

 # Estratégias

$$A, B \in \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ ou } \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

 # Estado inicial factorizado = Jogo clássico

 # Estado inicial entrelaçado :

$$(|00\rangle + |11\rangle)$$

$$p_I = 1, q_I = 1 \qquad \left(\frac{\alpha+\beta}{2}, \frac{\alpha+\beta}{2}\right)$$

$$p_I = 0, q_I = 0 \qquad \left(\frac{\alpha+\beta}{2}, \frac{\alpha+\beta}{2}\right)$$

$$p_I = \frac{1}{2}, q_I = \frac{1}{2} \qquad \left(\frac{\alpha+\beta+2\gamma}{4}, \frac{\alpha+\beta+2\gamma}{4}\right)$$

 # Melhor solução quando os dois jogadores usam a mesma estratégia

 # Porque $\frac{\alpha+\beta}{2} > \beta$ **, é melhor que o melhor caso clássico**

 # Entrelaçamento como um contrato

7. *Computação determinista, não-determinista e quântica.*

(Enquadramento computacional para problems de decisão)

Máquina de Turing M com k fitas de trabalho com alfabeto Γ e uma fita de entrada com alfabeto Σ.

Em cada momento a configuração c da máquina é o conteúdo das k fitas de trabalho, os $k+1$ ponteiros e o estado corrente. Seja $\mathcal{C}(x)$ de cardinalidade N o conjunto de todas as possíveis configurações para a entrada x.

CASO CLÁSSICO

Função de transição : (matriz $N \times N$)

$\delta : Q \times \Sigma \times \Gamma^k \times Q \times \Gamma^k \times \{L, R\}^{k+1} \rightarrow \{0, 1\}$

Q = conjunto de estados

Se for possível ir de c_i para c_j num só passo

$T(c_i, c_j) = 1$. Senão $T(c_i, c_j) = 0$.

Computação determinista:

Só um elemento em cada linha é diferente de zero.

($T^k(c_i, c_j)$ é o número de trajectos de comprimento k que levam de c_i a c_j)

CASOS NÃO-CLÁSSICOS

Computação probabilista:

δ pode tomar valores não-binários e mais de um elemento em cada linha pode ser diferente de zero

$$\delta : Q \times \Sigma \times \Gamma^k \times Q \times \Gamma^k \times \{L, R\}^{k+1} \rightarrow [0, 1]$$

com a condição

$$\sum_{q_2, b_1 \cdots b_k, p_0, p_1 \cdots p_k} \delta\left(q_1, s, a_1 \cdots a_k, q_2, b_1 \cdots b_k, p_0, p_1 \cdots p_k\right) = 1$$

para todos os valores $q_1, s, a_1 \cdots a_k$ do estado inicial e dos simbolos lidos nas fitas de entrada e de trabalho.

Neste caso os valores da matriz de transição estão entre 0 e 1 sendo a soma ao longo das linhas igual a um. Chamam-se matrizes estocásticas. Preservam a norma $\mathcal{L}^1$ ($\mathcal{L}^1(v) = \mathcal{L}^1(Tv)$ para qualquer $N-$vector v).

Computação quântica:

δ pode tomar valores arbitrários (positivos ou negativos) ou mesmo valores complexos

As probabilidades de aceitação (depois de k passos computacionais) serão $\left|T^k\left(c_i, c_j\right)\right|^2$ com a condição

$$\sum_{q_2, b_1 \cdots b_k, p_0, p_1 \cdots p_k} \left|\delta\left(q_1, s, a_1 \cdots a_k, q_2, b_1 \cdots b_k, p_0, p_1 \cdots p_k\right)\right|^2 = 1$$

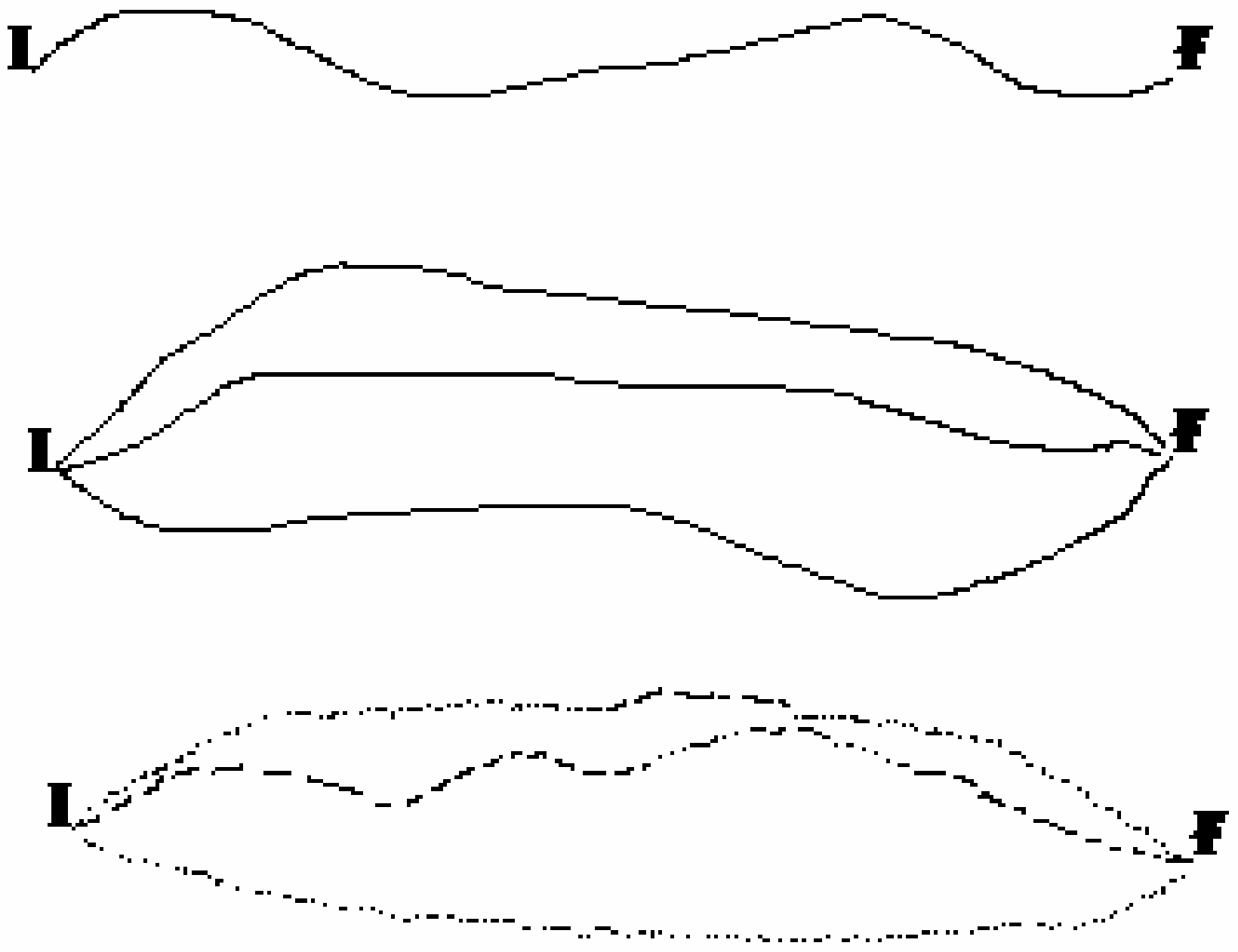
Ou seja,

$$\mathcal{L}^2(v) = \mathcal{L}^2(Tv) = \sum_{i=1}^{N} |v_i|^2$$

isto é, a matriz de transição é unitária.

Em todos os casos as probabilidades de transição entre estados iniciais e finais são positivas e normalizadas.

A diferença entre os diversos modelos computacionais é o metodo pelo qual o resultado é obtido


I
F
I
F
I
F

Computação quântica

- Resolução de problemas em tempo polinomial

  - Procura em bases de dados em tempo $\sqrt{N}$

  - Factorização em tempo polinomial (violação de RSA)

Criptografia quântica

Construção de chaves baseadas nas leis e limitações da modalidade quântica, em vez da complexidade computacional de certas operações

Estabelecimento duma chave (One time pad)

Polarizador A

$$|\updownarrow\rangle = 1$$
$$|\leftrightarrow\rangle = 0$$

Polarizador B

$$|\nearrow\rangle = 1$$
$$|\nwarrow\rangle = 0$$
$$|\updownarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle)$$
$$|\leftrightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle)$$
$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle)$$
$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle)$$

Analisando $|\updownarrow\rangle$ com o polarizador B ($|\nearrow\rangle\langle\nearrow| + |\nwarrow\rangle\langle\nwarrow|$) obtem-se 0 ou 1 com probabilidade $\frac{1}{2}$

A resposta coincide (com probabilidade um) com o código do emissor só se os dois polarizadores forem concordantes.

Criptografia quântica

A **Maria** envia de cada vez um fotão num dos quatro estados ao acaso.

O **João** usa os polarizadores A ou B também ao acaso. Depois de grande número de ensaios o João revela publicamente a sua sequência de polarizadores $AABABABBAA\ldots$

A **Maria** revela os casos em que houve coincidência nos polarizadores. Os casos não-coincidentes são deitados fora. Os resultados dos casos coincidentes são uma chave aleatória comum.

Interferência externa é detectada pela falta de coincidência numa parte da chave que é revelada publicamente. No caso das mensagens estarem a ser interceptadas o erro médio é 1/4.

Referências

- Julian Schwinger; *"Quantum mechanics: Symbolism of Atomic Measurements",* Springer 2000
- J. M. Jauch; "*Foundations of Quantum Mechanics"* Addison-Wesley 1968.
- RVM; "*Deformations, stable theories and fundamental constants*" Journal of Physics A 27(1994) 1
- RVM*; "Network dependence of strong reciprocity*" Advances in Complex Systems 7 (2004) 1-12
- D. A. Meyer; *"Quantum Strategies",* Phys. Rev. Lett. 82 (1999) 1052.
- J. Eisert, M. Wilkens and M. Lewenstein; "*Quantum Games and Quantum Strategies",* Phys. Rev. Lett. 83 (1999) 3077.
- RVM; "*Quantum ultimatum game*", Quantum Inf. Process. (2005)
- G. Alber et al.; "*Quantum information"*, Springer, Berlin 2001.
- E. Bernstein and U. Vazirani; "*Quantum complexity theory"*, Siam Journal of Computing 26 (1997) 1411-1473.


Fim