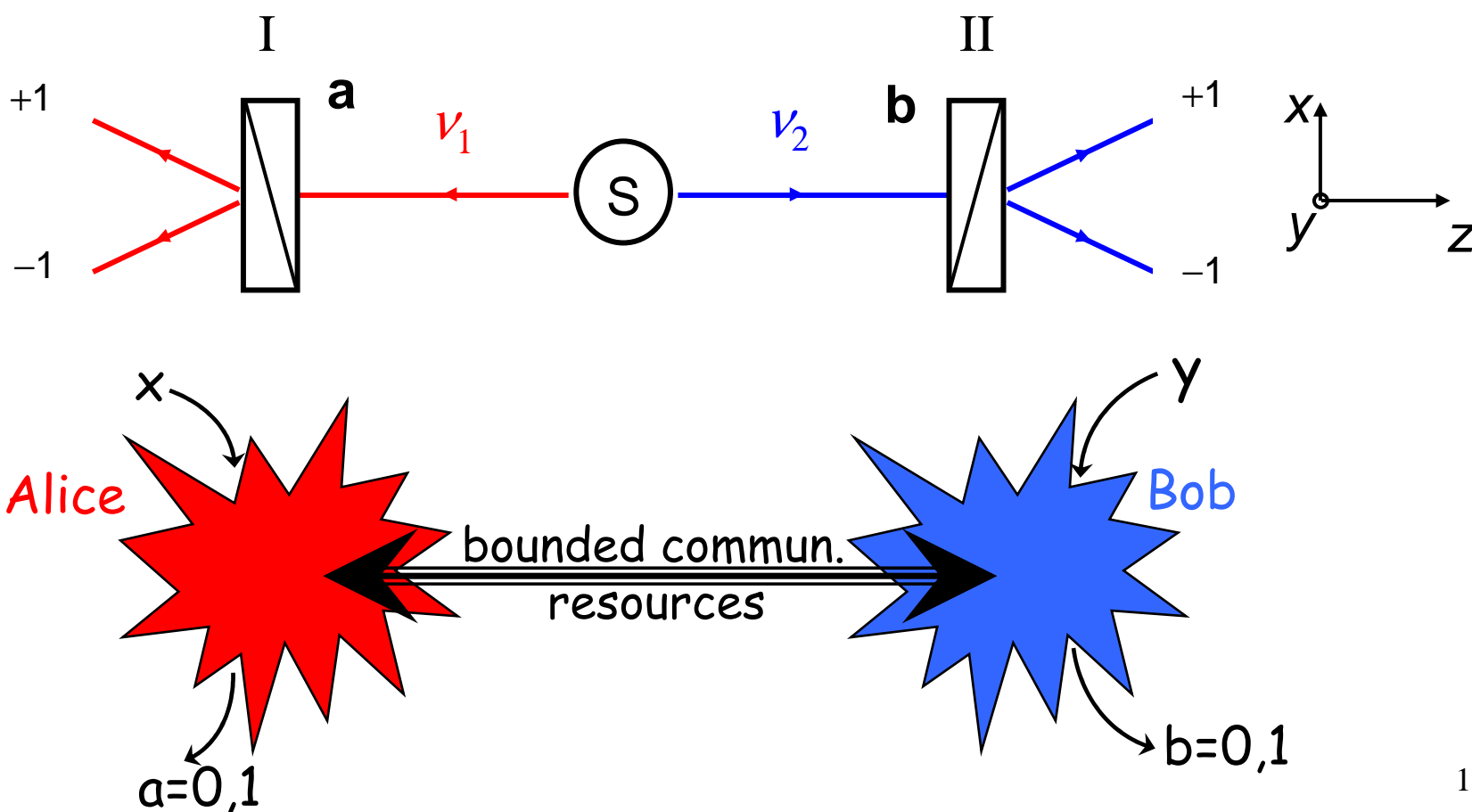




# How communication complexity changed the culture of the foundations of Quantum Mechanics

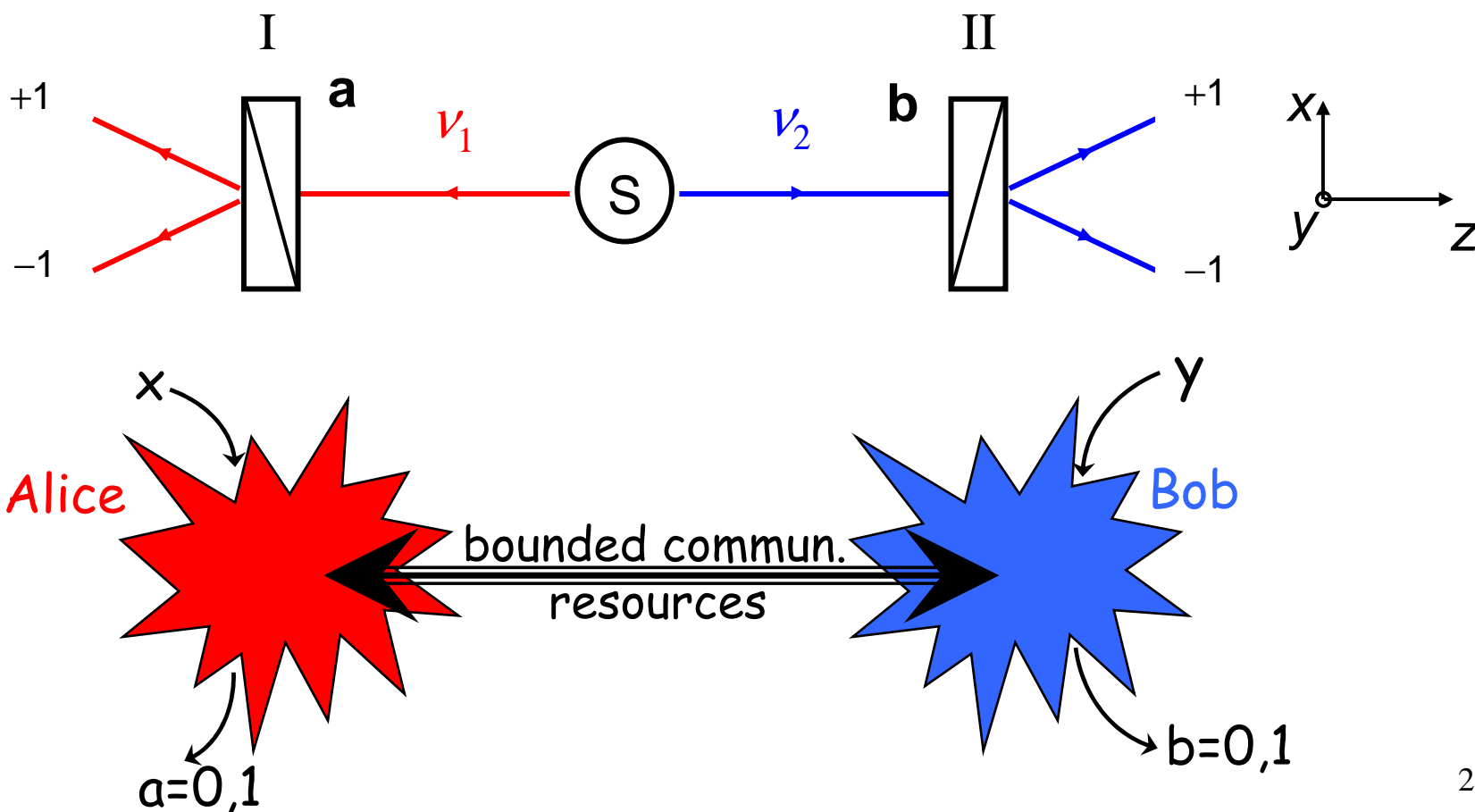
Nicolas Gisin, Group of Applied Physics, University of Geneva





# How communication complexity changed the culture of the foundations of Quantum **Physics**

Nicolas Gisin, Group of Applied Physics, University of Geneva





# Old views of Bell Inequalities

Correlation functions:

$$E(a, b) = \sum_{\alpha, \beta = \pm 1} \alpha \cdot \beta P_{\vec{a}, \vec{b}}(\alpha, \beta)$$

Depends on the arbitrary values of the measurement outcomes  $\alpha$  &  $\beta$  !!!

CHSH-inequality:

$$E(a, b) + E(a, b') + E(a', b) - E(a', b') \leq 2$$

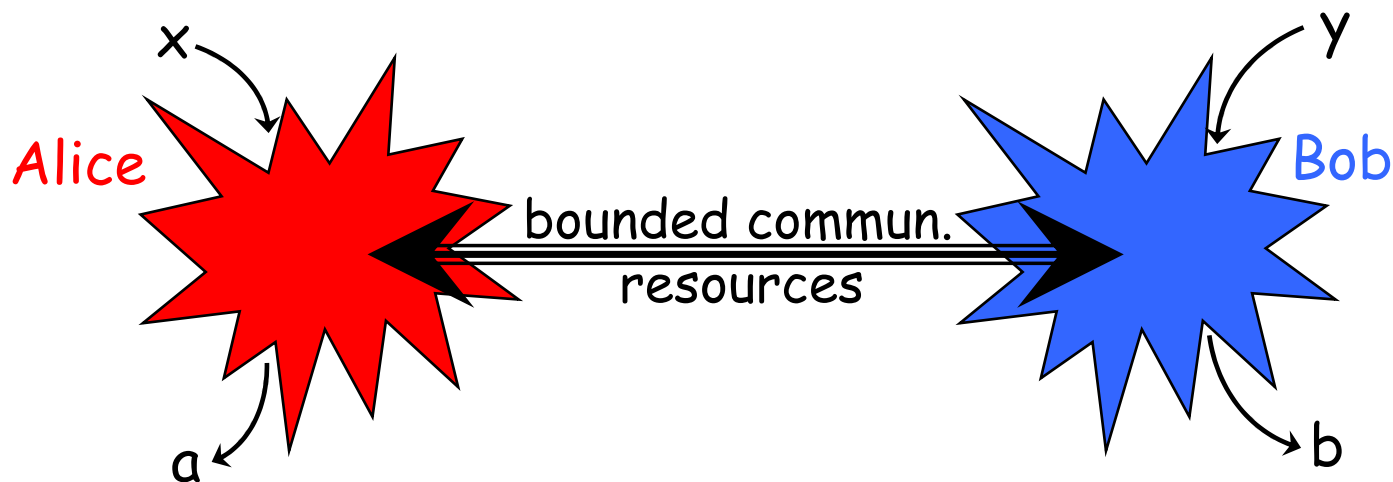
Old terminology:

elements of reality  
space-like separation  
spin  $\frac{1}{2}$ ,  $\{-1, +1\}$   
local hidden variable  
Bell  $\leq$  violation  
singlet state



# Contribution of Computer Science

Players, Alice & Bob, play games with limited resources !

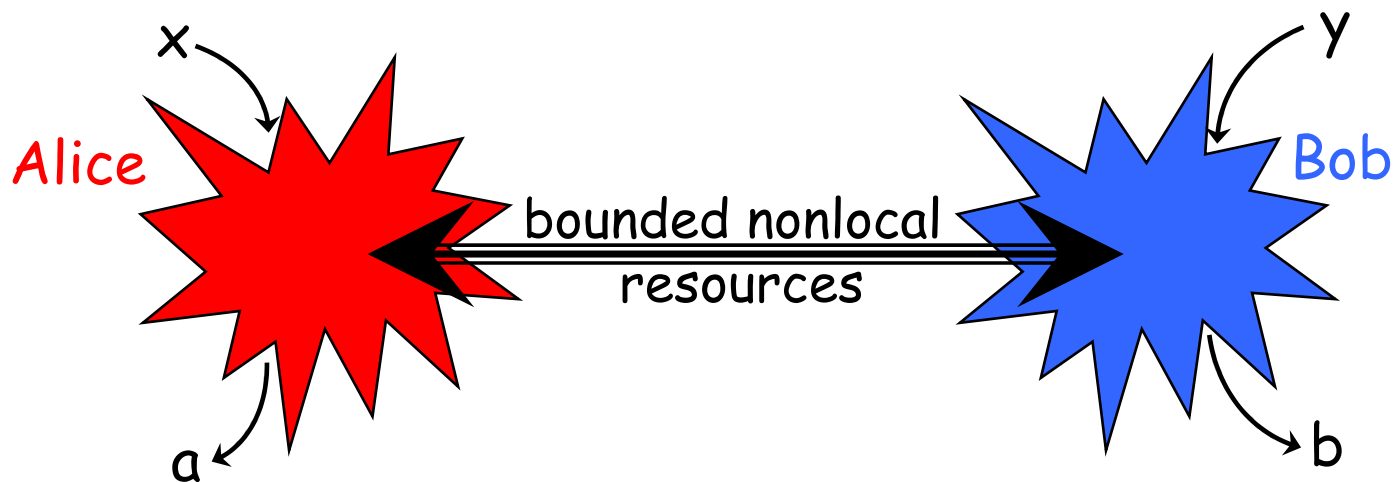


- |                                  |   |                       |
|----------------------------------|---|-----------------------|
| elements of reality              | → | Players               |
| space-like separation            | → | bounded communication |
| spin $\frac{1}{2}$ , $\{-1,+1\}$ | → | bits, $\{0,1\}$       |
| local hidden variable            | → | shared randomness     |
| Bell $\leq$ violation            | → | non-locality          |

against local realism  
↓  
reminiscence of the old religion war and old determinism



## Modern view



$$P(a,b|x,y)$$

conditional probability distributions.

Note: the outputs  $a$  &  $b$  don't need to be numbers!  
their values are irrelevant.

$$E(x,y) = P(a=b|x,y) - P(a \neq b|x,y)$$



# No-communication (no-signaling)

Marginals are independent of the other's settings:

$$\sum_a P(a,b|x,y) = P(b|y)$$

$$\sum_b P(a,b|x,y) = P(a|x)$$

Binary case:  $P(0,1|x,y) = P(0|x) - P(0,0|x,y)$

$$P(1,0|x,y) = P(0|y) - P(0,0|x,y)$$

$$P(1,1|x,y) = 1 - P(0|x) - P(0|y) + P(0,0|x,y)$$

$$\Rightarrow E(x,y) = 4 \cdot P(0,0|x,y) - 2 \cdot P(0|x) - 2 \cdot P(0|y) + 1$$

CHSH: 
$$\left( \begin{array}{c|cc} & -1 & 0 \\ \hline -1 & +1 & +1 \\ 0 & +1 & -1 \end{array} \right) \leq 0$$

$$\begin{aligned} \vec{S} \cdot \vec{P} &= +P(0,0|0,0) + P(0,0|0,1) \\ &\quad + P(0,0|1,0) - P(0,0|1,1) \\ &\quad - P(0|x=0) - P(0|y=0) \\ &\leq 0 \end{aligned}$$

$\vec{S}$



# Examples of generalized tight (i.e. facet) Bell inequalities

Inn22 :

$$\left( \begin{array}{c|cccccc} & -1 & 0 & \dots & 0 & 0 \\ \hline 1-n & +1 & +1 & \dots & +1 & +1 \\ 2-n & +1 & +1 & \dots & +1 & -1 \\ 3-n & +1 & +1 & \dots & -1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & +1 & -1 & 0 & \dots & 0 \end{array} \right) \leq 0$$

CHSH :

$$\left( \begin{array}{c|cc} & -1 & 0 \\ \hline -1 & +1 & +1 \\ 0 & +1 & -1 \end{array} \right) \leq 0$$

I2244 :

$$\left( \begin{array}{c|ccc|ccc} & -1 & -1 & -1 & 0 & 0 & 0 \\ \hline -1 & 1 & 1 & 1 & 0 & 0 & 1 \\ -1 & 1 & 1 & 0 & 0 & 1 & 1 \\ -1 & 1 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 & -1 & -1 \\ 0 & 1 & 1 & 1 & -1 & -1 & -1 \end{array} \right) \leq 0$$

Collins-Gisin  
 JPA, 37, 1775, 2004  
 CGLMP  
 PRL, 88, 040404, 2002



# Inequalities for limited resources

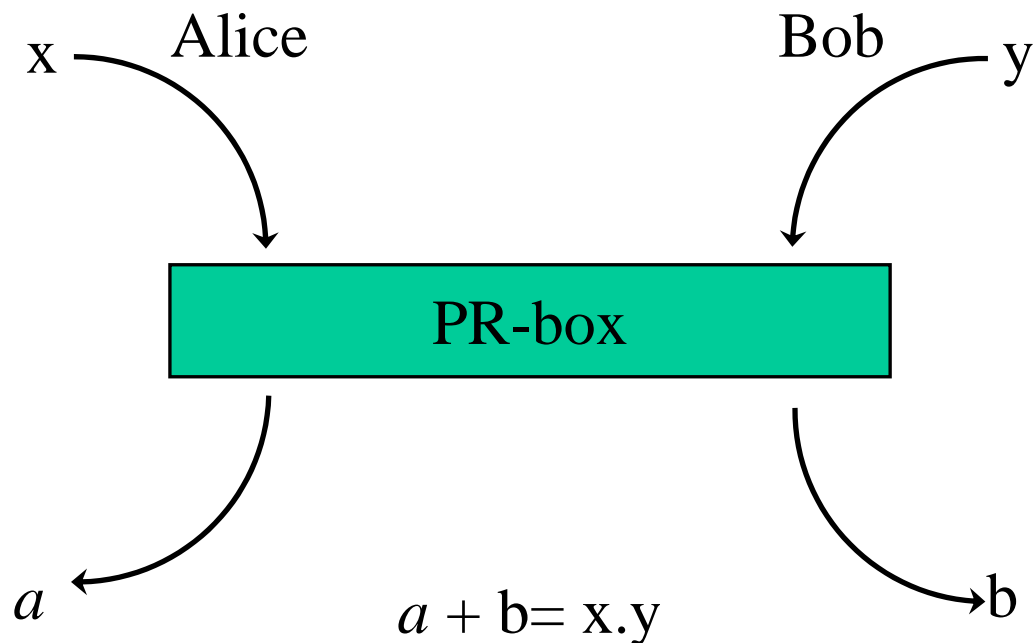
- 1 bit of communication: [D.Bacon & B.Toner, PRL 90,157904,2003](#)  
no violation by any pair of quantum systems  
⇒ motivated to look for a 1-bit simulation model  
⇒ success !! the Bacon-Toner model [PRL 91,187904, 2003](#)

Open question: Can partially entangled qubits be simulated with 1 bit of communication ?

Can binary measurements on larger dimension maximally entangled quDits be simulated with 1 bit of communication ?



# The NonLocal Machine

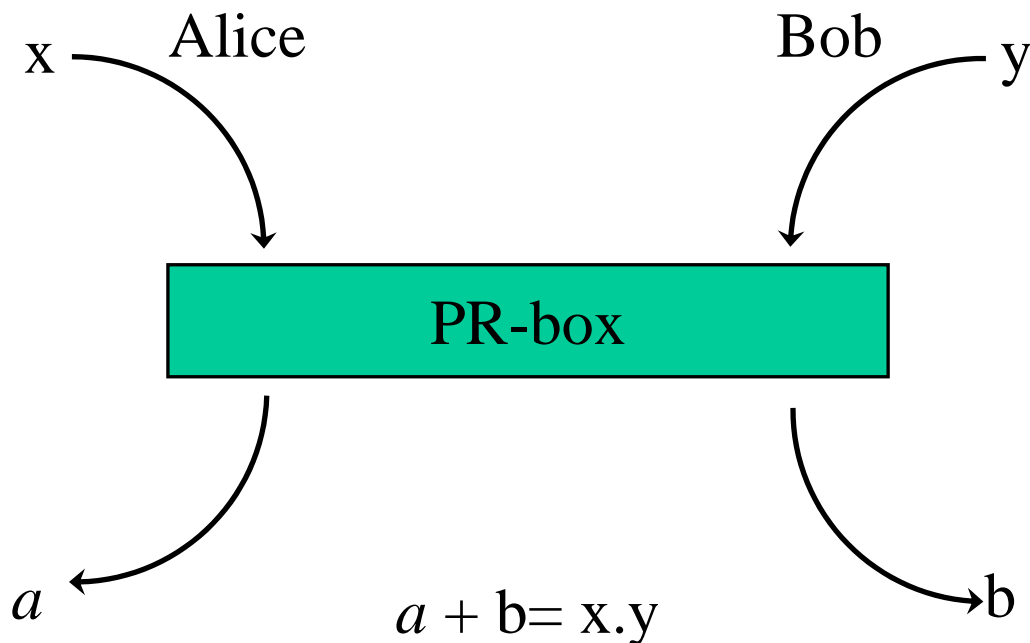


$\text{Prob}(a=1|x,y) = \frac{1}{2}$ , independent of  $y \Rightarrow$  no signaling

$$E(0,0) + E(0,1) + E(1,0) - E(1,1) = 4$$



# The NonLocal Machine

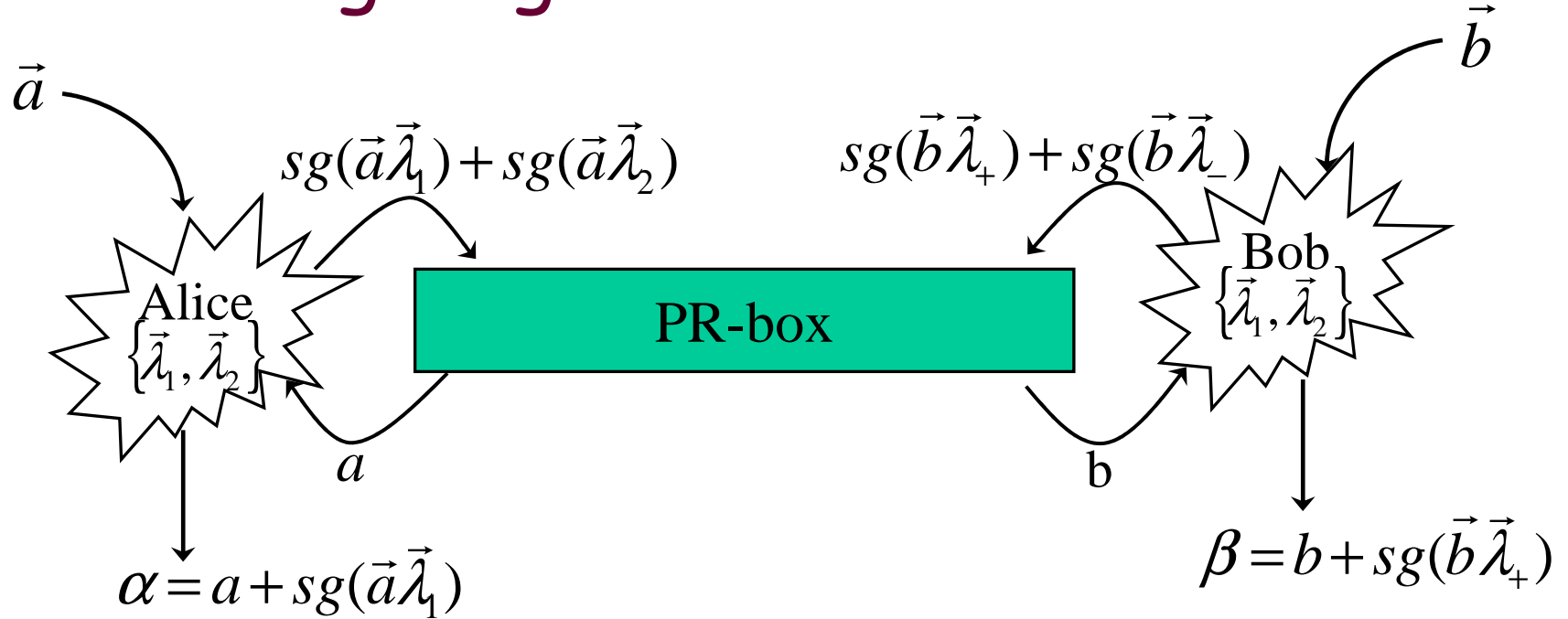


A single bit of communication suffices to simulate the PR-box (assuming shared randomness). But the PR-box does not allow any communication.

Hence, the PR-box is a strictly weaker resource than communication.



# Simulating singlets with the NL Machine



where  $\vec{\lambda}_1$  and  $\vec{\lambda}_2$  are distributed uniformly on  $S^{(2)}$ ,

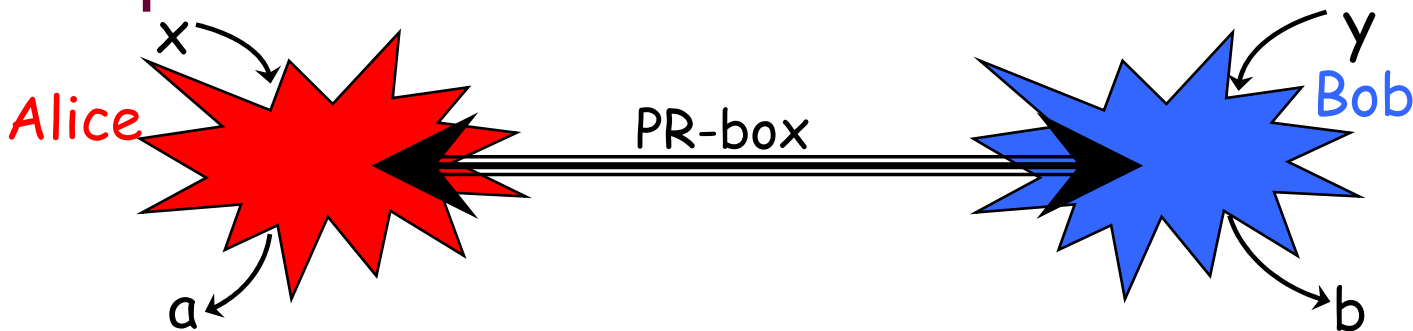
$$sg(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases} \quad \text{and } \vec{\lambda}_{\pm} = \vec{\lambda}_1 \pm \vec{\lambda}_2$$

Given  $\vec{a}$  &  $\vec{b}$ , the statistics of  $\alpha$  &  $\beta$  is that of the singlet state:

$$E(\alpha, \beta | \vec{a}, \vec{b}) = \frac{1 - \vec{a} \cdot \vec{b}}{2}$$

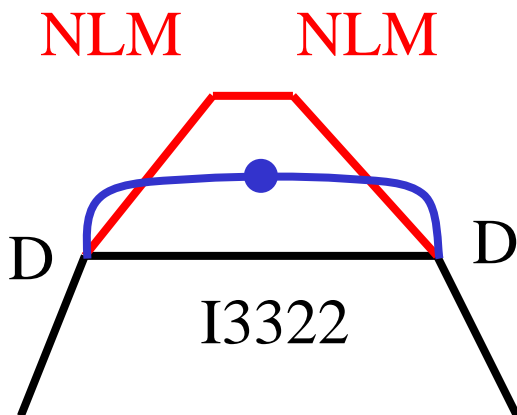


# Inequalities for limited resources: 1 PRbox

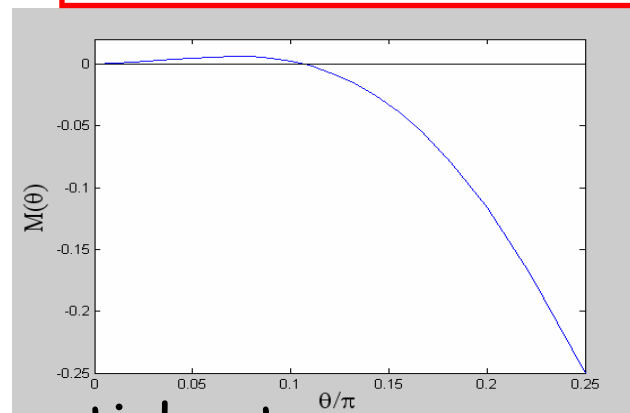


$$M_{3322} : \left( \begin{array}{c|ccc} & -2 & 0 & 0 \\ \hline -2 & +1 & +1 & +1 \\ -1 & +1 & +1 & -1 \\ 0 & +1 & -1 & 0 \end{array} \right) \leq 0$$

Geometrical intuition:



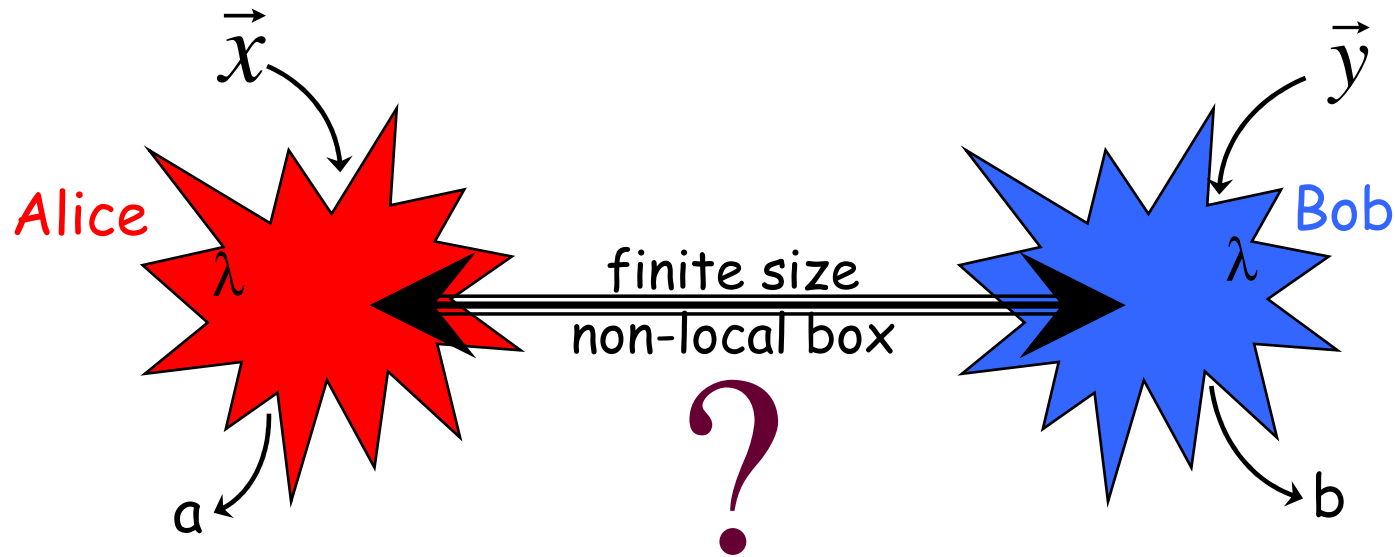
- Very partially entangled states can't be simulated with 1 PR-box
- max entangled qubits can be simulated with 1 PR-box
- Partially entangled states are more nonlocal than the singlet !
- [A.Méthot & V.Scarani](#)  
[quant-ph/0601210](#)



partial ent. max ent.



# Resource to simulated partially entangled qubit pairs



such that  $P(a,b|x,y)$  equals the quantum prediction for  $\psi = \cos(\theta)|0,0\rangle + \sin(\theta)|1,1\rangle$



# Entanglement detection

state tomography

$$P(\mathbf{a}, \mathbf{b} | \mathbf{A}, \mathbf{B})$$

$$\Rightarrow \rho$$

entanglement witness  $W$

$\langle W \rangle \geq 0$  for all separable  $\rho$

$$P(\mathbf{a}_i, \mathbf{b}_j | \mathbf{A}_i, \mathbf{B}_j)$$

where

$$W = \sum c_{ij} A_i \circ B_j$$

$$\sum c_{ij} a_i b_j P(\mathbf{a}_i, \mathbf{b}_j | \mathbf{A}_i, \mathbf{B}_j) < 0 \\ \Rightarrow \text{entanglement}$$

Like in all experimental sciences,  
the analysis is based on conditional probabilities:  
the probability of observing  $\mathbf{a}$  and  $\mathbf{b}$   
when performing the measurements  $\mathbf{x}$  and  $\mathbf{y}$ ,  
i.e. on  $P(\mathbf{a}, \mathbf{b} | \mathbf{x}, \mathbf{y})$



# 注意!

state tomography and entanglement witness assume one knows the dimension of the relevant Hilbert space !!!

**Example:**

**State tomography on the singlet**

$$P(a,b|S_A,S_B) = \begin{cases} \frac{1}{2} \delta(a \neq b) & \text{if } S_A = S_B \\ \frac{1}{4} & \text{if } S_A \neq S_B \end{cases}$$

**If  $\dim H = 2 \times 2$ , then singlet**

**But if  $\dim H = 8 \times 8$ , then the same correlation can be obtained from a separable state: consider 3 qubit pairs labelled x,y,z in state**

$$\begin{aligned} \rho = & \frac{1}{2} \left( |0,1\rangle_z \langle 0,1| + |1,0\rangle_z \langle 1,0| \right) \\ & + \frac{1}{2} \left( |0,1\rangle_x \langle 0,1| + |1,0\rangle_x \langle 1,0| \right) \\ & + \frac{1}{2} \left( |0,1\rangle_y \langle 0,1| + |1,0\rangle_y \langle 1,0| \right) \end{aligned}$$

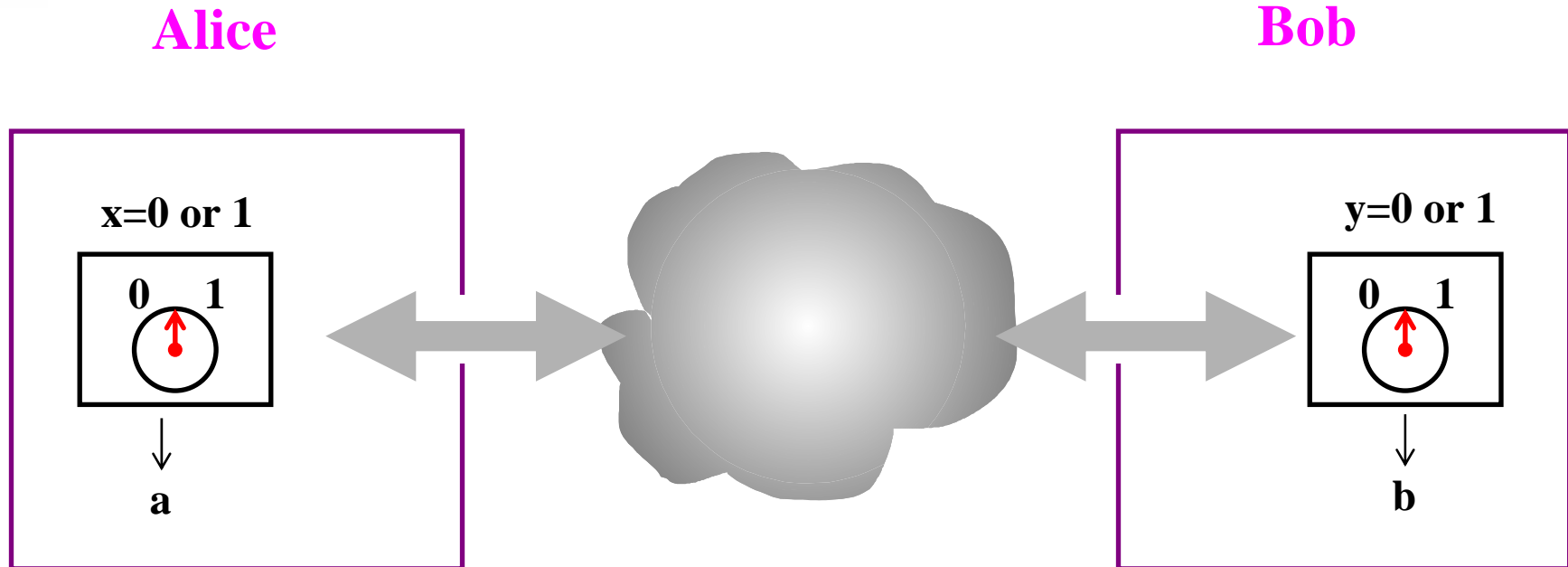


# Nonlocality as a resource

- The only entanglement witnesses that “witness entanglement without auxiliary assumptions about the Hilbert space dimension” are Bell inequalities !



# Basics of QKD



After publicly announcing a fair sample of their data,  
Alice and Bob's information is entirely contained  
in the conditional probability

$$\underline{\underline{p(a,b|x,y)}}$$



# Hidden assumptions in "unconditional" security proofs of QKD

$$P(\underbrace{a, b}_{\text{measurements outcomes}} \mid \underbrace{x, y}_{\text{bases choices}})$$

measurements outcomes      bases choices

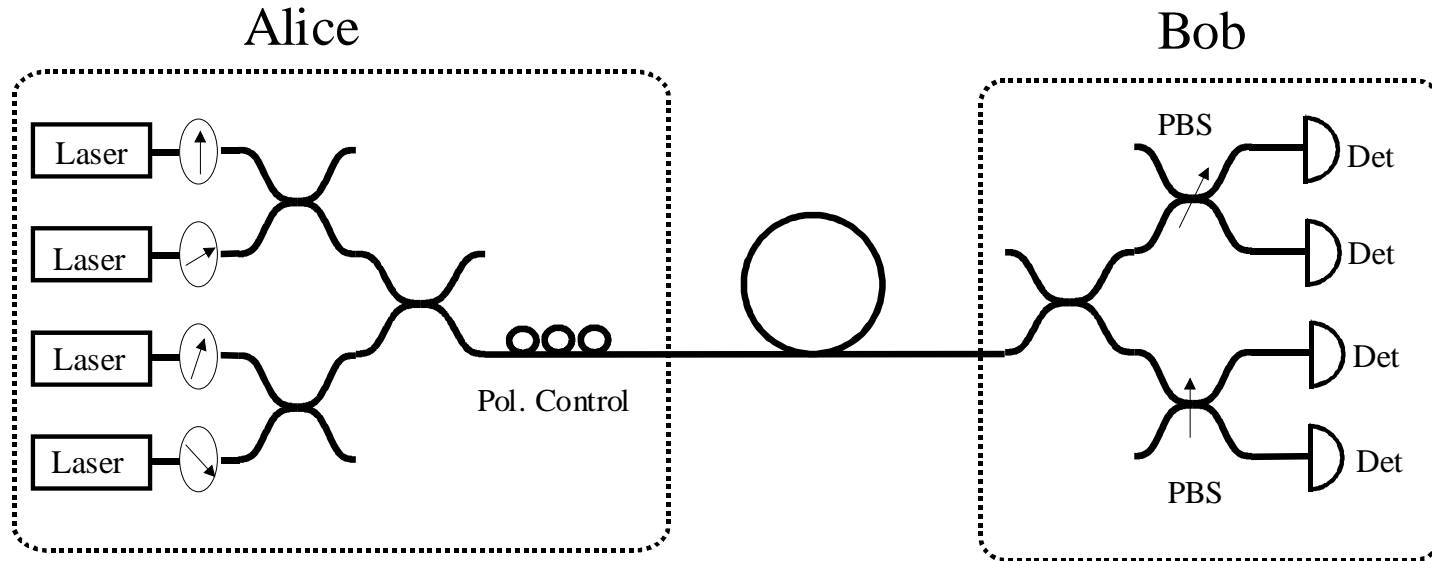
**Example of BB84:**  $P(a=b|x=y) \approx 1$  &  $P(a,b|x \neq y) \approx 1/4$

Eve's power limited only by quantum laws       ~~$\Rightarrow$  secure secret key~~  
and Alice and Bob's Q systems are       $\Rightarrow$  secure secret key  
2-dimensional

$$\frac{1}{4} \left( |0,0\rangle_{ab} \langle 0,0| + |1,1\rangle_{ab} \langle 1,1| \right)_z \otimes \left( |0,0\rangle_{ab} \langle 0,0| + |1,1\rangle_{ab} \langle 1,1| \right)_x$$

This is a real threat to actual implementations of QKD, known as « side channels ».

# Polarization Encoding (1)



**The same threat affects all protocols such that  $p(a,b|x,y)$  admits a local hidden variable model. Indeed, the quantum state could contain this lhv and Eve hold a copy of it:**

$$p(a,b|x,y) = \sum_{\lambda} p_{\lambda} p(a|x,\lambda) p(b|y,\lambda) \Rightarrow \Psi_{ABE} = \sum |\lambda_A\rangle_A \otimes |\lambda_B\rangle_B \otimes |\lambda_A, \lambda_B\rangle_E$$

**where  $\lambda_A = (x \mapsto a)$   $\lambda_B = (y \mapsto b)$**  19



# Nonlocality as a resource

- The only entanglement witnesses that “witness entanglement without auxiliary assumptions about the Hilbert space dimension” are Bell inequalities !
- The only correlations out of which one can distil secret bits (as in QKD) are those violating a Bell inequality ! [PRL97, 120405, 2006](#)



# Conclusion

- Quantum Mechanics  $\Rightarrow$  Quantum Physics
- There is still a lot to learn from Bell-like inequalities, i.e. from conditions on the possible/impossible origin of correlations.
- Examples:
  1. Find resources allowing one to simulate partial entanglement.
  2. Find a condition whose violation implies a lower bound on the dimension of the Hilbert space.