Non-commutative polynomial optimization in quantum physics

Antonio Acín
ICREA Professor at ICFO-Institut de Ciencies Fotoniques, Barcelona
AXA Chair in Quantum Information Science

Computational aspects of commutative and noncommutative positive polynomials
8th European Congress of Mathematics, Portoroz, 21 June 2021

Polynomial optimization problems

$$\bar{p} = \min_{x_1,\ldots,x_n} p(x_1,\ldots,x_n)$$

$$\text{s.t.} \quad q_j(x_1,\ldots,x_n) \geq 0$$

where $x = (x_1,\ldots,x_n) \in R^n$

and p and q_j are polynomials of bounded degree $\leq d$.

Polynomial optimization problems

$$\bar{p} = \min_{x_1,\ldots,x_n} p(x_1,\ldots,x_n)$$

$$\text{s.t.} \quad q_j(x_1,\ldots,x_n) \geq 0$$

where $x = (x_1,\ldots,x_n) \in R^n$

and p and q_j are polynomials of bounded degree $\leq d$.

Lasserre and Parrilo introduced a hierarchy of semi-definite programming relaxations whose optima converge to the searched solution.

$$p^{(1)} \leq p^{(2)} \leq \ldots \leq p^{(N)} \rightarrow \bar{p}$$

Polynomial optimization problems

$$\overline{p} = \min_{x_1,\ldots,x_n} p(x_1,\ldots,x_n)$$

$$\text{s.t.} \quad q_j(x_1,\ldots,x_n) \geq 0$$

where $x = (x_1,\ldots,x_n) \in R^n$

and p and q_j are polynomials of bounded degree $\leq d$.

Lasserre and Parrilo introduced a hierarchy of semi-definite programming relaxations whose optima converge to the searched solution.

$$p^{(1)} \leq p^{(2)} \leq \ldots \leq p^{(N)} \rightarrow \overline{p}$$

Convergence can be proven using Putinar's result on Positivstellensatz.

Non-commutative polynomial optimization

$$\bar{p} = \min_{|\psi\rangle, X_1,\ldots,X_n} \langle\psi| P(X_1,\ldots,X_n) |\psi\rangle$$

$$\text{s.t.} \quad Q_j(X_1,\ldots,X_n) \geq 0$$

where $X_1, \ldots, X_n$ are now non-commuting bounded operators, of arbitrary dimension, and P and Q_j are Hermitian polynomial operators of bounded degree $\leq d$.

ICFO

Non-commutative polynomial optimization

$$\bar{p} = \min_{|\psi\rangle, X_1,\ldots,X_n} \langle\psi|P(X_1,\ldots,X_n)|\psi\rangle$$
$$\text{s.t.} \quad Q_j(X_1,\ldots,X_n) \geq 0$$

where $X_1, \ldots, X_n$ are now non-commuting bounded operators, of arbitrary dimension, and P and Q_j are Hermitian polynomial operators of bounded degree $\leq d$.

We (see also Doherty, Liang, Toner and Wehner) introduced a hierarchy of semi-definite programming relaxations whose optima converge to the searched solution.

$$p^{(1)} \leq p^{(2)} \leq \ldots \leq p^{(N)} \rightarrow \bar{p}$$

Non-commutative polynomial optimization

$$\bar{p} = \min_{|\psi\rangle, X_1,\ldots,X_n} \langle\psi|P(X_1,\ldots,X_n)|\psi\rangle$$
$$\text{s.t.} \quad Q_j(X_1,\ldots,X_n) \geq 0$$

where $X_1, \ldots, X_n$ are now non-commuting bounded operators, of arbitrary dimension, and P and Q_j are Hermitian polynomial operators of bounded degree $\leq d$.

We (see also Doherty, Liang, Toner and Wehner) introduced a hierarchy of semi-definite programming relaxations whose optima converge to the searched solution.

$$p^{(1)} \leq p^{(2)} \leq \ldots \leq p^{(N)} \rightarrow \bar{p}$$

M. Navascués. S. Pironio, AA, Phys. Rev. Lett. 98, 010401 (2007); New J. Phys. 10 (7), 073013 (2008).

S. Pironio, M. Navascués, AA, SIAM J. Optim. 20, 2157 (2010).

Hierarchy of SDP relaxations

We consider the set of monomials of a given degree ≤ k on the previous operators, where each monomial is defined by a vector of indices α. The degree of the monomial is $|\alpha|=k$.

Example:

$$Y_{\alpha=(1,\bar{3},6,6)} = X_1 X_3^* X_6^2$$

ICFO

Hierarchy of SDP relaxations

We consider the set of monomials of a given degree ≤ k on the previous operators, where each monomial is defined by a vector of indices α. The degree of the monomial is $|\alpha|=k$.

Example:

$$Y_{\alpha=(1,\bar{3},6,6)} = X_1 X_3^* X_6^2$$

We consider maps from this set to complex numbers: $\Lambda\left(Y_\alpha\right) = y_\alpha \in C$

ICFO

Hierarchy of SDP relaxations

For a given sequence, we define the moment matrix M_k of degree k as

$$\left(M_k\right)_{\alpha,\beta} = \Lambda\left(X_{\bar{\alpha}} X_{\beta}\right)$$

$$|\alpha|,|\beta| \leq k$$

$$M_1 = \begin{pmatrix} 1 & y_1 & y_2 & y_{\bar{1}} & y_{\bar{2}} \\ y_{\bar{1}} & y_{\bar{1}1} & y_{\bar{1}2} & y_{\bar{1}\bar{1}} & y_{\bar{1}\bar{2}} \\ y_{\bar{2}} & y_{\bar{2}1} & y_{\bar{2}2} & y_{\bar{2}\bar{1}} & y_{\bar{2}\bar{2}} \\ y_1 & y_{11} & y_{12} & y_{1\bar{1}} & y_{1\bar{2}} \\ y_2 & y_{21} & y_{22} & y_{2\bar{1}} & y_{2\bar{2}} \end{pmatrix}$$

Hierarchy of SDP relaxations

For a given sequence, we define the moment matrix M_k of degree k as

$$\left(M_k\right)_{\alpha,\beta} = \Lambda\left(X_{\bar{\alpha}} X_\beta\right)$$

$$|\alpha|,|\beta| \le k$$

$$M_1 = \begin{pmatrix} 1 & y_1 & y_2 & y_{\bar{1}} & y_{\bar{2}} \\ y_{\bar{1}} & y_{\bar{1}1} & y_{\bar{1}2} & y_{\bar{1}\bar{1}} & y_{\bar{1}\bar{2}} \\ y_{\bar{2}} & y_{\bar{2}1} & y_{\bar{2}2} & y_{\bar{2}\bar{1}} & y_{\bar{2}\bar{2}} \\ y_1 & y_{11} & y_{12} & y_{1\bar{1}} & y_{1\bar{2}} \\ y_2 & y_{21} & y_{22} & y_{2\bar{1}} & y_{2\bar{2}} \end{pmatrix}$$

For a polynomial $P(X) = \sum p_\delta X_\delta$ the localizing matrix $L_{P,k}$ of degree k is defined as

$$\left(L_{P,k}\right)_{\alpha,\beta} = \sum p_\delta \Lambda\left(X_{\bar{\alpha}} X_\delta X_\beta\right)$$

$$M_k = L_{1,k}$$

$$|\alpha|,|\beta| \le k$$

Hierarchy of SDP relaxations

Every specific choice of operators X_i and state ψ defines a map Λ:

$$\Lambda\left(X_\alpha\right) = \left\langle \psi \middle| X_\alpha \middle| \psi \right\rangle$$

For these maps, all localizing matrices defined for positive polynomials are positive.

Hierarchy of SDP relaxations

Every specific choice of operators X_i and state ψ defines a map Λ:

$$\Lambda\left(X_\alpha\right)=\langle\psi|X_\alpha|\psi\rangle$$

For these maps, all localizing matrices defined for positive polynomials are positive.

Proof:

$$\langle v|L_{P,k}|v\rangle=\sum_{\alpha,\beta}v_\alpha^*\left(L_{P,k}\right)_{\alpha,\beta}v_\beta=\sum_{\alpha,\beta}v_\alpha^*\sum_\delta p_\delta\Lambda\left(X_{\bar{\alpha}}X_\delta X_\beta\right)v_\beta=$$

$$\sum_{\alpha,\beta}v_\alpha^*\sum_\delta p_\delta\langle\psi|X_{\bar{\alpha}}X_\delta X_\beta|\psi\rangle v_\beta=\langle\psi|\left(\sum_\alpha v_\alpha^* X_{\bar{\alpha}}\right)\left(\sum_\delta p_\delta X_\delta\right)\left(\sum_\beta v_\beta X_\beta\right)|\psi\rangle\geq 0$$

Hierarchy of SDP relaxations

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

Hierarchy of SDP relaxations

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

Relaxation of order k:

$$p^{(k)} = \min \sum p_\delta y_\delta$$
$$\text{s.t.} \quad M_k \geq 0, L_{Q_j, k-\deg(Q_j)/2} \geq 0$$

ICFO

Hierarchy of SDP relaxations

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

Relaxation of order k:

$$p^{(k)} = \min \sum p_\delta y_\delta$$
$$\text{s.t.} \quad M_k \geq 0, L_{Q_j, k-\deg(Q_j)/2} \geq 0$$

Clearly:

$$p^{(1)} \leq p^{(2)} \leq \ldots \leq \bar{p}$$

Convergence of the hierarchy

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

Positivity domain: $S_Q = \{ (X_1, \ldots, X_n) \text{ s.t. } Q_j(X_1, \ldots, X_n) \geq 0 \}$

Convergence of the hierarchy

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

Positivity domain: $S_Q = \{(X_1, \ldots, X_n) \text{ s.t. } Q_j(X_1, \ldots, X_n) \geq 0\}$

Quadratic module: $M_Q = \left\{ P \text{ s.t. } P = \sum_i F_i^* F_i + \sum_{i,j} G_{i,j}^* Q_j G_{i,j} \right\}$

ICFO

Convergence of the hierarchy

$$\bar{p} = \min \langle \psi | P(X_1,\ldots,X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1,\ldots,X_n) \geq 0$$

Positivity domain: $S_Q = \{(X_1,\ldots,X_n) \text{ s.t. } Q_j(X_1,\ldots,X_n) \geq 0\}$

Quadratic module: $M_Q = \left\{ P \text{ s.t. } P = \sum_i F_i^* F_i + \sum_{i,j} G_{i,j}^* Q_j G_{i,j} \right\}$

M_Q is Archimedean if $\exists C \text{ s.t. } C - X_1^* X_1 - \ldots - X_n^* X_n \in M_Q$

Convergence of the hierarchy

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

Positivity domain: $S_Q = \{(X_1, \ldots, X_n) \text{ s.t. } Q_j(X_1, \ldots, X_n) \geq 0\}$

Quadratic module: $M_Q = \left\{ P \text{ s.t. } P = \sum_i F_i^* F_i + \sum_{i,j} G_{i,j}^* Q_j G_{i,j} \right\}$

M_Q is Archimedean if $\exists C \text{ s.t. } C - X_1^* X_1 - \ldots - X_n^* X_n \in M_Q$

If S_Q is bounded, we can make M_Q Archimedean by choosing a large enough C and adding to the set of polynomial constraints the condition:

$$C - X_1^* X_1 - \ldots - X_n^* X_n$$

Convergence of the hierarchy

If M_Q is Archimedean: $$\lim_{k\to\infty} p^{(k)} = \overline{p}$$

The proof is constructed from the primal problem of the relaxations.

Convergence of the hierarchy

If M_Q is Archimedean: $\lim_{k\to\infty} p^{(k)} = \bar{p}$

The proof is constructed from the primal problem of the relaxations.

Convergence can be established at a finite step whenever the optimal solution y_k for relaxation of order k is such that:

$$\operatorname{rank}(M_k) = \operatorname{rank}\left(M_{k-\max(d_i)}\right)$$

Convergence of the hierarchy

Consider the problem:

$$\lambda^{(k)} = \max_{\lambda, B_i, C_{ij}} \lambda$$

$$\text{s.t. } P(X_1, \ldots, X_n) - \lambda = \sum_i B_i^* B_i + \sum_{i,j} C_{i,j}^* Q_j C_{i,j}$$

$$\max_i \deg(B_i) \leq k, \max_i \deg(C_{i,j}) \leq k - d_i$$

Convergence of the hierarchy

Consider the problem:

$$\lambda^{(k)} = \max_{\lambda, B_i, C_{ij}} \lambda$$

$$\text{s.t.}\;\; P(X_1,\ldots,X_n) - \lambda = \sum_i B_i^* B_i + \sum_{i,j} C_{i,j}^* Q_j C_{i,j}$$

$$\max_i \deg(B_i) \leq k, \max_i \deg(C_{i,j}) \leq k - d_i$$

This problem can be cast in a sdp form, and proven to be the dual of step *k* before.

$$\lambda^{(k)} \leq p^{(k)} \leq \overline{p}$$

Convergence of the hierarchy

$P(X_1,\ldots,X_n)-(\bar{p}-\varepsilon)$ is positive in S_Q for any ε>0.

Convergence of the hierarchy

$P(X_1,\ldots,X_n)-(\bar{p}-\varepsilon)$ is positive in S_Q for any ε>0.

↓ Helton and McCullough Positivellensatz

$$P(X_1,\ldots,X_n)-(\bar{p}-\varepsilon)=\sum_i B_i^* B_i+\sum_{i,j} C_{i,j}^* Q_j C_{i,j}$$

Convergence of the hierarchy

$P(X_1,\ldots,X_n)-(\overline{p}-\varepsilon)$ is positive in S_Q for any ε>0.

↓ Helton and McCullough Positivellensatz

$$P(X_1,\ldots,X_n)-(\overline{p}-\varepsilon)=\sum_i B_i^* B_i+\sum_{i,j} C_{i,j}^* Q_j C_{i,j}$$

This defines a feasible point for the previous problem, so one has:

$$\overline{p}-\varepsilon \le \lambda^{(k)} \le p^{(k)} \le \overline{p} \quad \forall \varepsilon > 0$$

ICFO

Relation to classical SDP hierarchies

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$

$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

Relation to classical SDP hierarchies

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$

$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$

$$[X_i, X_j] = 0 \ \forall i, j$$

Relation to classical SDP hierarchies

$$\bar{p} = \min \langle\psi|P(X_1,\ldots,X_n)|\psi\rangle$$
$$\text{s.t.} \quad Q_j(X_1,\ldots,X_n) \geq 0$$
$$[X_i, X_j] = 0 \ \forall i,j$$

$\Longleftrightarrow$

$$\bar{p} = \min p(x_1,\ldots,x_n)$$
$$\text{s.t.} \quad q_j(x_1,\ldots,x_n) \geq 0$$

Relation to classical SDP hierarchies

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad Q_j(X_1, \ldots, X_n) \geq 0$$
$$[X_i, X_j] = 0 \ \forall i, j$$

$\Longleftrightarrow$

$$\bar{p} = \min p(x_1, \ldots, x_n)$$
$$\text{s.t.} \quad q_j(x_1, \ldots, x_n) \geq 0$$

$$\bar{p} = \min \langle \psi | P(X_1, \ldots, X_n) | \psi \rangle$$
$$\text{s.t.} \quad X_i^2 - X_i = 0$$

$$\bar{p} = \min p(x_1, \ldots, x_n)$$
$$\text{s.t.} \quad x_i^2 - x_i = 0$$

ICFO

Relation to classical SDP hierarchies

$$\bar{p} = \min \langle\psi|P(X_1,\ldots,X_n)|\psi\rangle$$
$$\text{s.t.} \quad Q_j(X_1,\ldots,X_n) \geq 0$$
$$[X_i, X_j] = 0 \ \forall i,j$$

⟷

$$\bar{p} = \min p(x_1,\ldots,x_n)$$
$$\text{s.t.} \quad q_j(x_1,\ldots,x_n) \geq 0$$

$$\bar{p} = \min \langle\psi|P(X_1,\ldots,X_n)|\psi\rangle$$
$$\text{s.t.} \quad X_i^2 - X_i = 0$$

↓

$$p^{(1)} = \bar{p}$$ Easy!

$$\bar{p} = \min p(x_1,\ldots,x_n)$$
$$\text{s.t.} \quad x_i^2 - x_i = 0$$

↓

NP-hard

Why do we care about this?

Quantum physics

The postulates of quantum theory:

Quantum physics

The postulates of quantum theory:

1. A complex Hilbert space of dimension d is associated to any physical system. The state of the system is specified by a normalised ray in this space, $|\psi\rangle \in \mathbb{C}^d$ such that $\langle\psi|\psi\rangle = 1$.

Quantum physics

The postulates of quantum theory:

1. A complex Hilbert space of dimension d is associated to any physical system. The state of the system is specified by a normalised ray in this space, $|\psi\rangle \in \mathbb{C}^d$ such that $\langle\psi|\psi\rangle = 1$.

2. A measurement is defined by a set of orthogonal projectors M acting on the same space, $M = \{M\}_{r=1\ldots R}$, such that $\sum_{r=1\ldots R} M_r = 1$.

Quantum physics

The postulates of quantum theory:

1. A complex Hilbert space of dimension d is associated to any physical system. The state of the system is specified by a normalised ray in this space, $|\psi\rangle \in \mathbb{C}^d$ such that $\langle\psi|\psi\rangle = 1$.

2. A measurement is defined by a set of orthogonal projectors M acting on the same space, $M = \{M\}_{r=1\ldots R}$, such that $\sum_{r=1\ldots R} M_r = 1$.

3. When implementing the measurement defined by M on a system in state $|\psi\rangle$, result r is obtained with probability $\Pr(r) = \langle\psi|M_r|\psi\rangle$.

Quantum physics

The postulates of quantum theory:

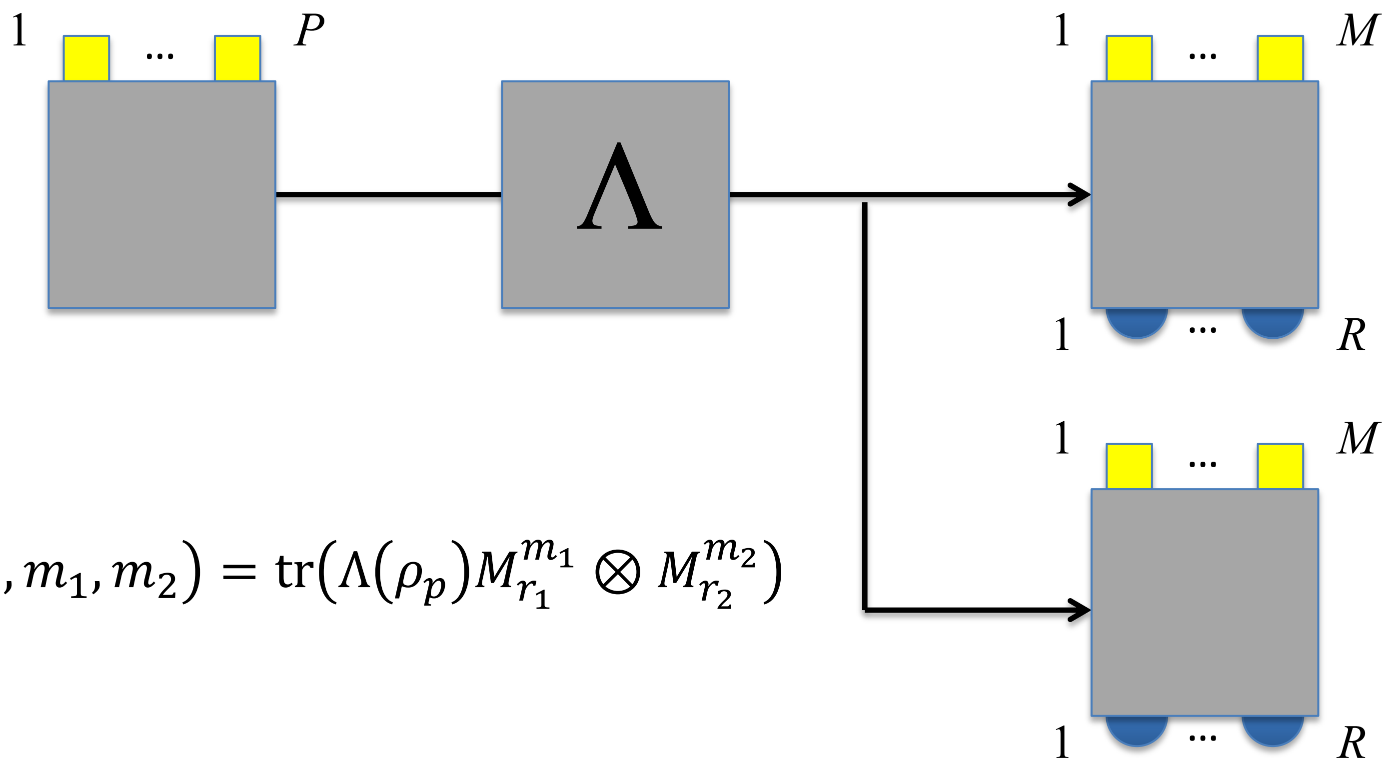
1. A complex Hilbert space of dimension d is associated to any physical system. The state of the system is specified by a normalised ray in this space, $|\psi\rangle \in \mathbb{C}^d$ such that $\langle\psi|\psi\rangle = 1$.

2. A measurement is defined by a set of orthogonal projectors M acting on the same space, $M = \{M\}_{r=1\ldots R}$, such that $\sum_{r=1\ldots R} M_r = 1$.

3. When implementing the measurement defined by M on a system in state $|\psi\rangle$, result r is obtained with probability $\Pr(r) = \langle\psi|M_r|\psi\rangle$.

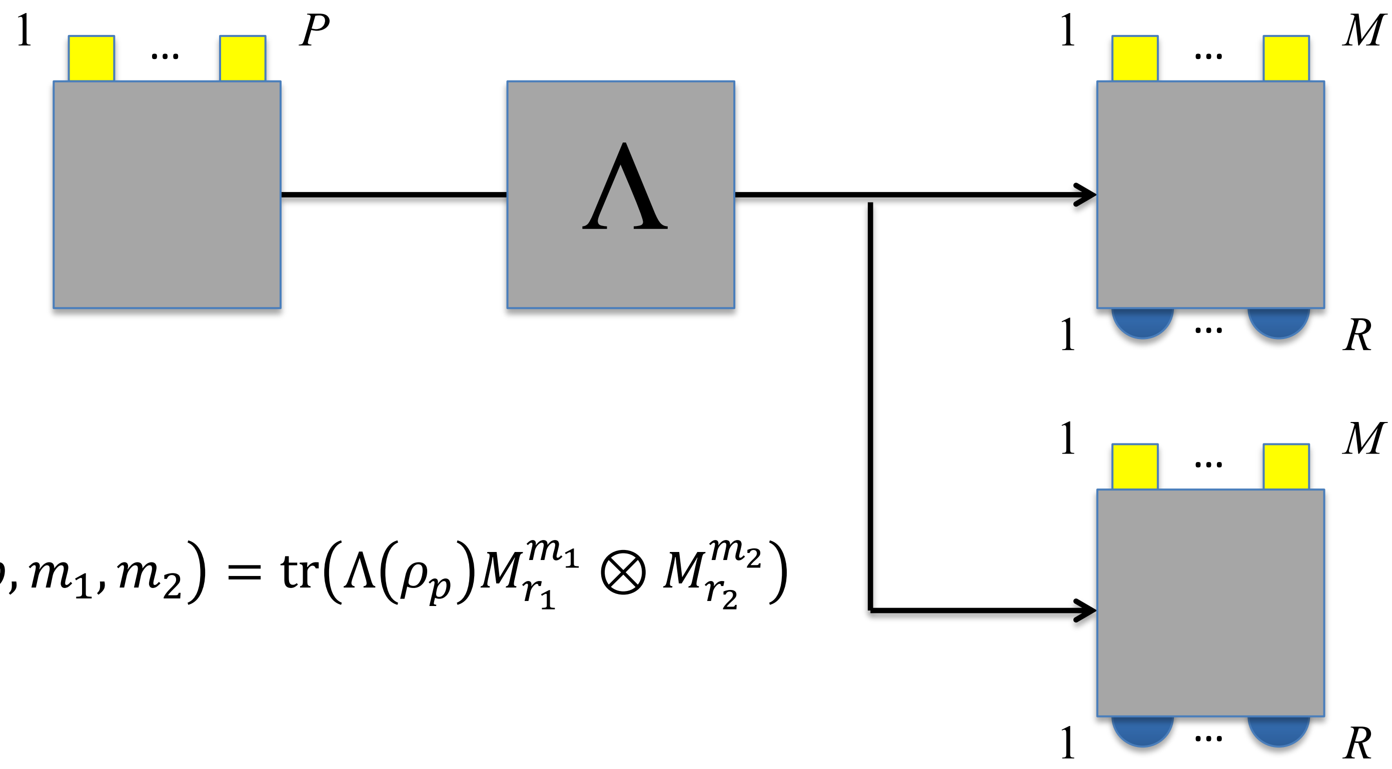
4. When combining two systems, A and B, with corresponding Hilbert spaces $\mathbb{C}^{d_A}$ and $\mathbb{C}^{d_B}$, the Hilbert space of the joint system is the tensor product of the two spaces.

Statistics in quantum experiments



$$P(r_1, r_2 | p, m_1, m_2) = \mathrm{tr}\left(\Lambda(\rho_p) M_{r_1}^{m_1} \otimes M_{r_2}^{m_2}\right)$$

Statistics in quantum experiments



$$P(r_1, r_2 | p, m_1, m_2) = \mathrm{tr}\left(\Lambda(\rho_p) M_{r_1}^{m_1} \otimes M_{r_2}^{m_2}\right)$$

Quantum physics is a natural source of problems involving polynomials of operators.

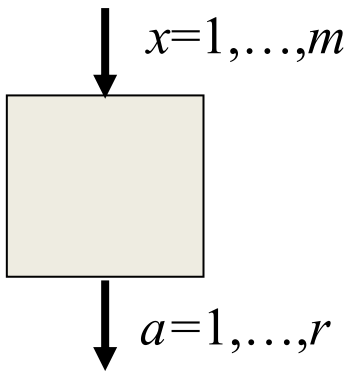
Characterization of Quantum Correlations

Navascués, Pironio, Acin, PRL 2007, NJP 2009

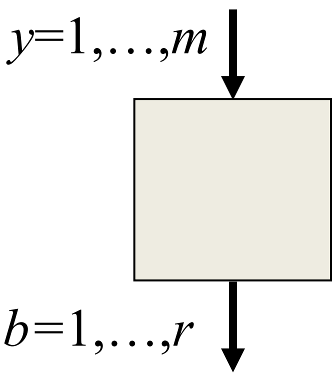
Physical correlations

The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.

Alice



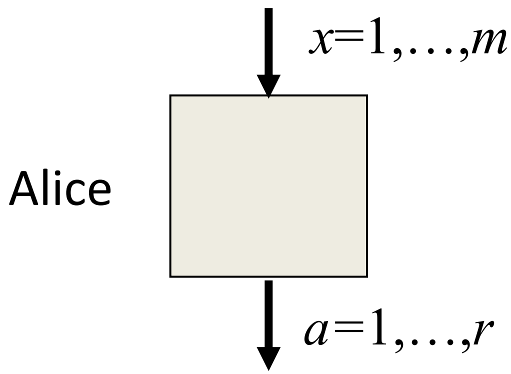
$$p(a,b|x,y)$$



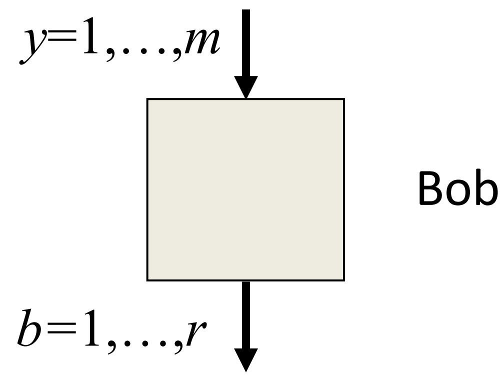
Bob

Physical correlations

The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.



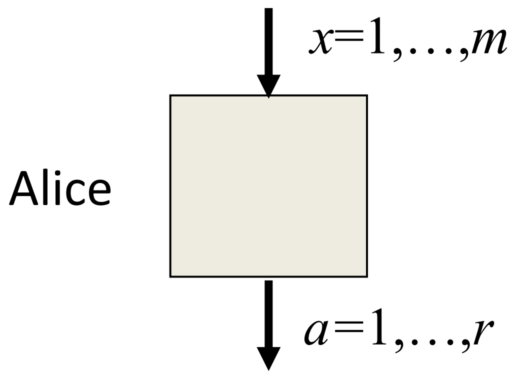
$$p(a,b|x,y)$$



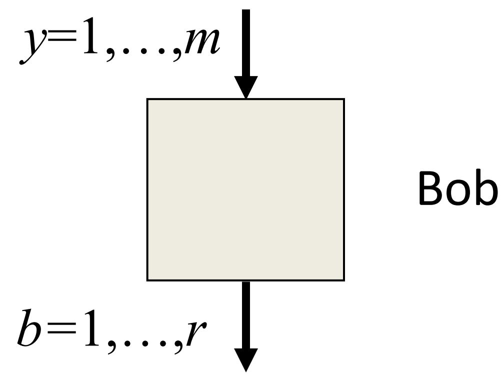
$$p(a,b|x,y) = \begin{pmatrix} p(1,1|1,1) & p(1,2|1,1) & \cdots & p(r,r|1,1) \\ & & & \\ & & & \end{pmatrix} \qquad \sum_{a,b} p(a,b|1,1) = 1$$

Physical correlations

The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.



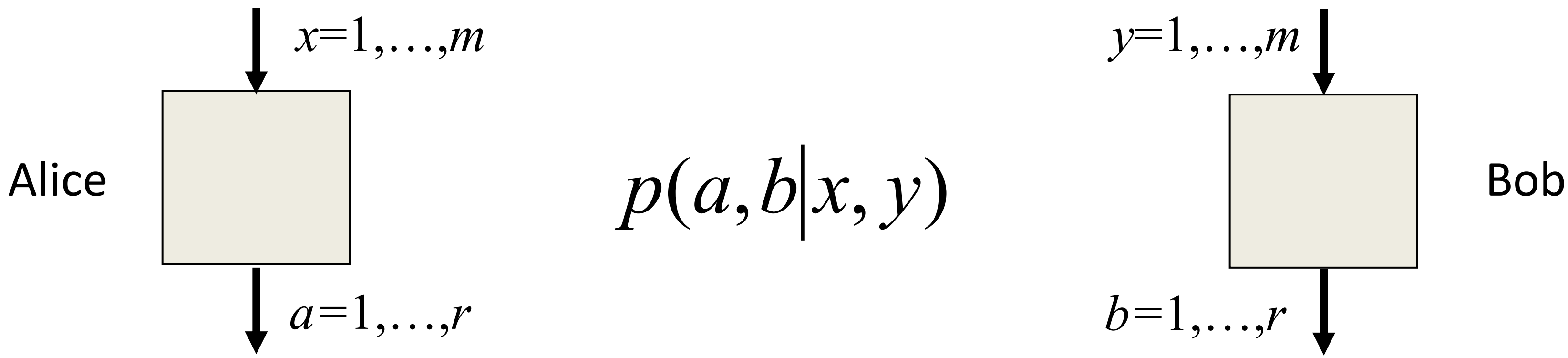
$$p(a,b|x,y)$$



$$p(a,b|x,y) = \begin{pmatrix} p(1,1|1,1) & p(1,2|1,1) & \cdots & p(r,r|1,1) \\ p(1,1|1,2) & p(1,2|1,2) & \cdots & p(r,r|1,2) \\ & & & \\ & & & \end{pmatrix}$$

Physical correlations

The object we deal with is a conditional probability distribution of the outputs given the inputs, which encapsulates the correlations among devices.



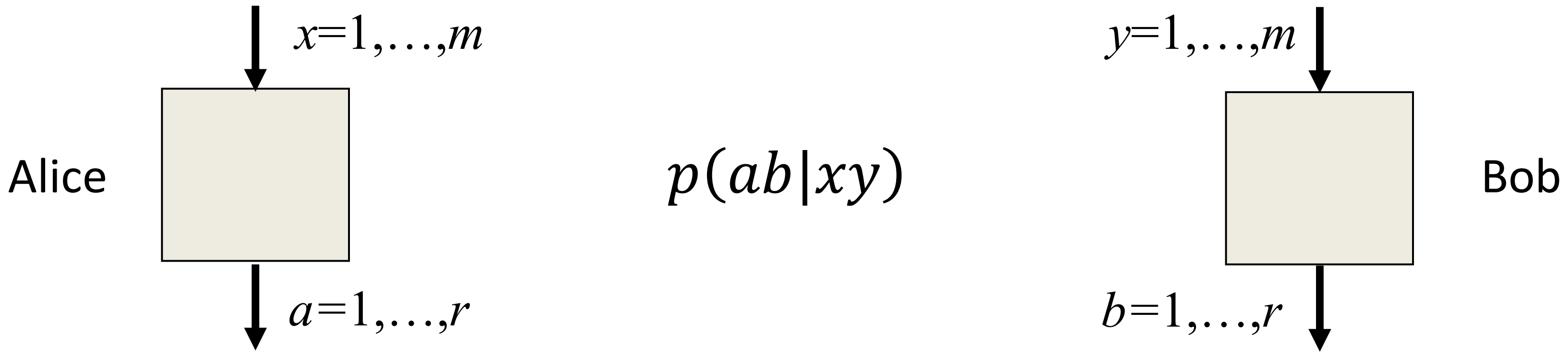
$$p(a,b|x,y)=\begin{pmatrix} p(1,1|1,1) & p(1,2|1,1) & \cdots & p(r,r|1,1) \\ p(1,1|1,2) & p(1,2|1,2) & \cdots & p(r,r|1,2) \\ \vdots & \vdots & \ddots & \vdots \\ p(1,1|m,m) & p(1,2|m,m) & \cdots & p(r,r|m,m) \end{pmatrix}$$

$$p(a,b|x,y)\in\Re^{m^2r^2}$$

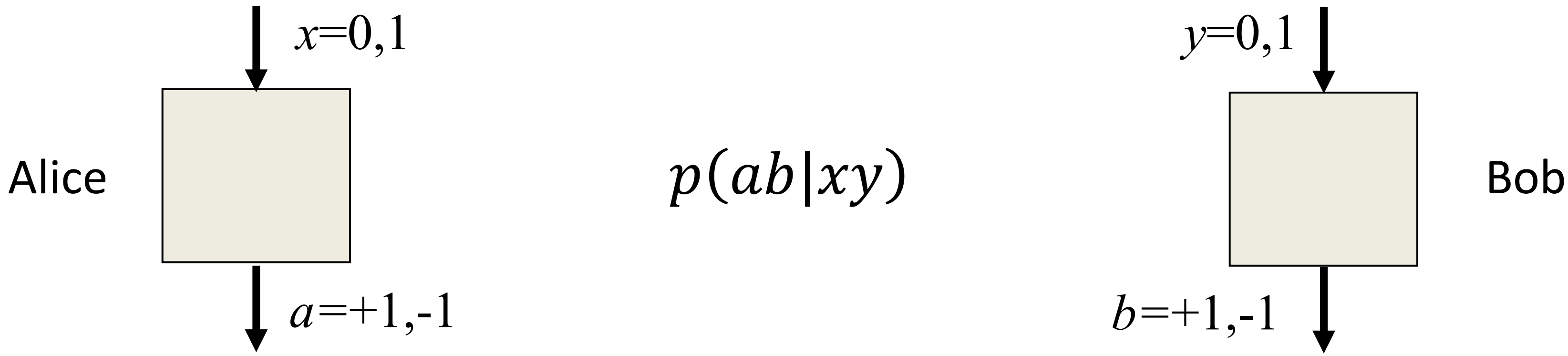
$$p(a,b|x,y)\geq 0$$

$$\sum_{a,b}p(a,b|x,y)=1$$

Example

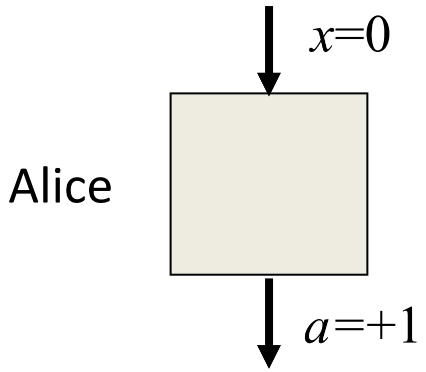


Example

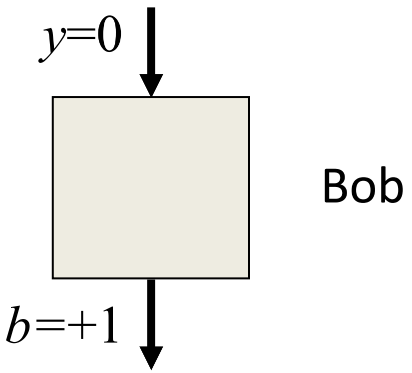


$$p(ab|xy) = \begin{pmatrix} p(+1,+1|0,0) & p(+1,-1|0,0) & p(-1,+1|0,0) & p(-1,-1|0,0) \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example



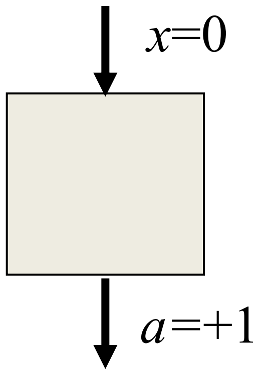
$$p(+1,+1|0,0) = \frac{1}{2}$$



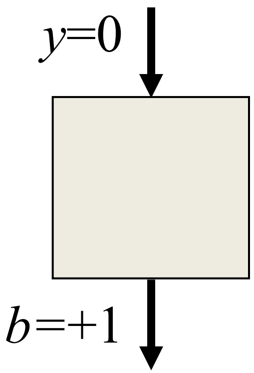
$$p(ab|xy) = \begin{pmatrix} p(+1,+1|0,0) & p(+1,-1|0,0) & p(-1,+1|0,0) & p(-1,-1|0,0) \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

Alice



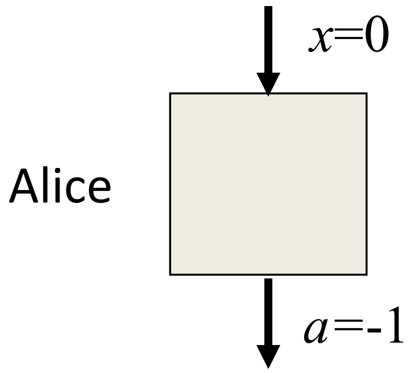
$$p(+1,+1|0,0) = \frac{1}{2}$$



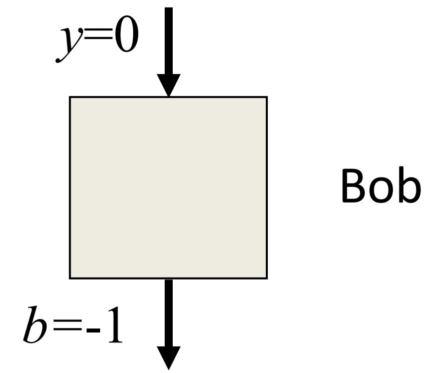
Bob

$$p(ab|xy) = \begin{pmatrix} 1/2 & p(+1,-1|0,0) & p(-1,+1|0,0) & p(-1,-1|0,0) \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example



$$p(-1,-1|0,0) = \frac{1}{2}$$

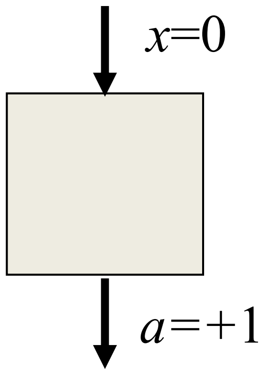


$$p(ab|xy) = \begin{pmatrix} 1/2 & p(+1,-1|0,0) & p(-1,+1|0,0) & 1/2 \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

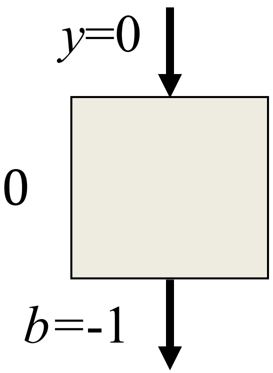
ICFO

Example

Alice



$$p(+1,-1|0,0) = p(-1,+1|0,0) = 0$$



Bob

$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ p(+1,+1|0,1) & p(+1,-1|0,1) & p(-1,+1|0,1) & p(-1,-1|0,1) \\ p(+1,+1|1,0) & p(+1,-1|1,0) & p(-1,+1|1,0) & p(-1,-1|1,0) \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ p(+1,+1|1{,}0) & p(+1,-1|1{,}0) & p(-1,+1|1{,}0) & p(-1,-1|1{,}0) \\ p(+1,+1|1{,}1) & p(+1,-1|1{,}1) & p(-1,+1|1{,}1) & p(-1,-1|1{,}1) \end{pmatrix}$$

Example

$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ p(+1,+1|1,1) & p(+1,-1|1,1) & p(-1,+1|1,1) & p(-1,-1|1,1) \end{pmatrix}$$

Example

$$p(ab|xy) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$

Physical correlations

Physical principles translate into limits on correlations.

Physical correlations

Physical principles translate into limits on correlations.

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

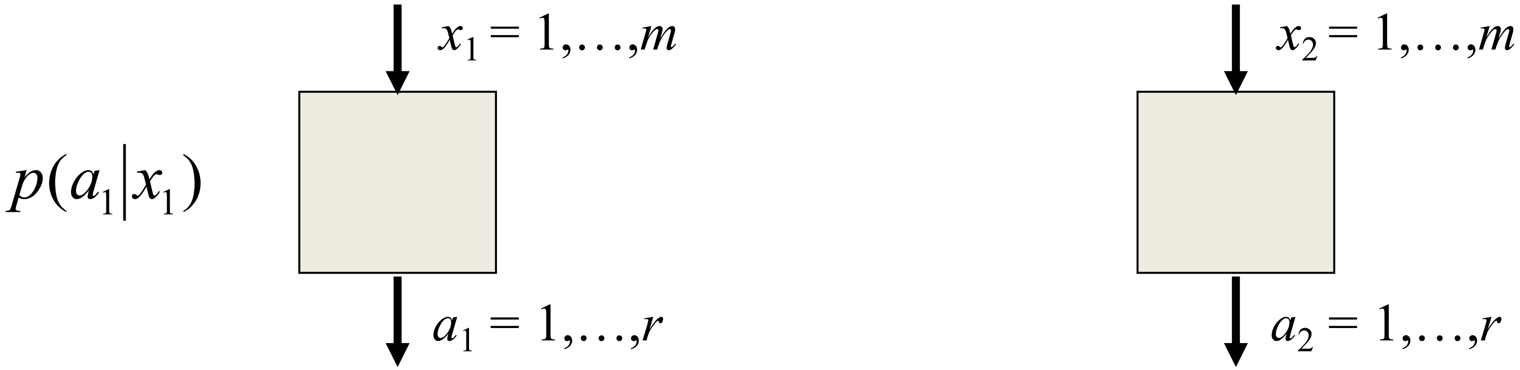
$$\sum_{a_{k+1},\ldots,a_N} p(a_1,\ldots,a_N | x_1,\ldots,x_N) = p(a_1,\ldots,a_k | x_1,\ldots,x_k)$$

Physical correlations

Physical principles translate into limits on correlations.

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

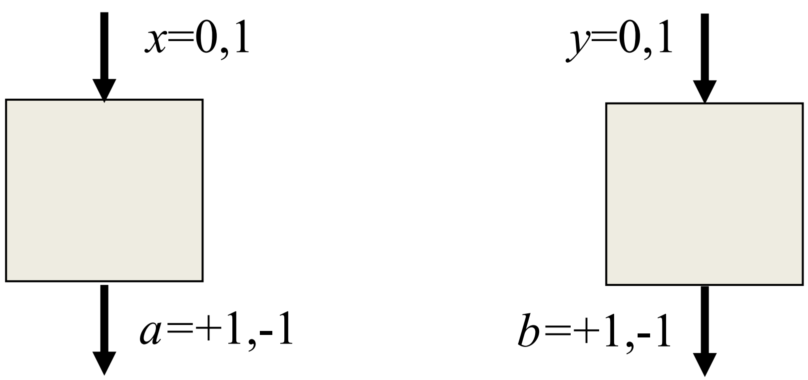
$$\sum_{a_{k+1},\ldots,a_N} p(a_1,\ldots,a_N|x_1,\ldots,x_N) = p(a_1,\ldots,a_k|x_1,\ldots,x_k)$$



Physical correlations

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

$$\sum_{a_{k+1},\ldots,a_N} p(a_1,\ldots,a_N | x_1,\ldots,x_N) = p(a_1,\ldots,a_k | x_1,\ldots,x_k)$$

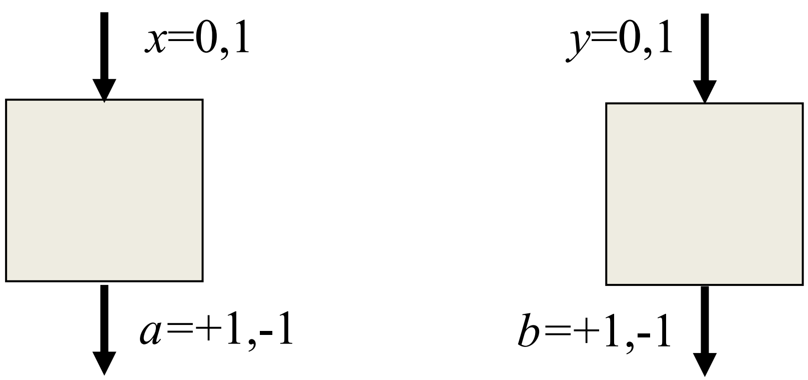


	++	+−	−+	−−
00	1/2	0	0	1/2
01	1/2	0	0	1/2
10	1/2	0	0	1/2
11	0	1/2	1/2	0

Physical correlations

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

$$\sum_{a_{k+1},\ldots,a_N} p(a_1,\ldots,a_N|x_1,\ldots,x_N) = p(a_1,\ldots,a_k|x_1,\ldots,x_k)$$



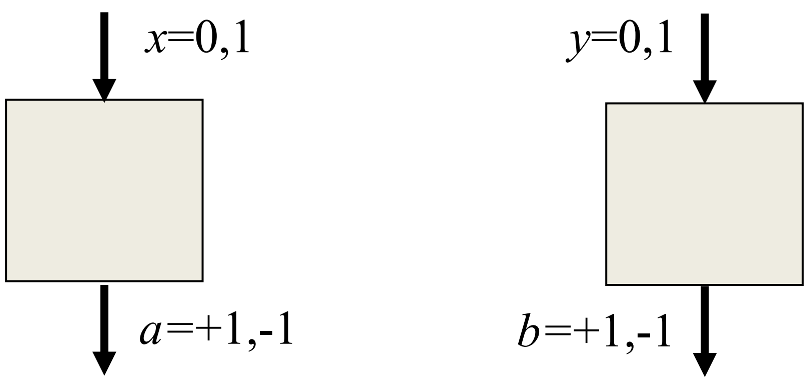
	+ +	+ −	− +	− −
00	1/2	0	0	1/2
01	1/2	0	0	1/2
10	1/2	0	0	1/2
11	0	1/2	1/2	0

$$p_A(+1|0) = p(+1,+1|00) + p(+1,-1|00) = \frac{1}{2}$$

Physical correlations

No-signalling correlations: correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

$$\sum_{a_{k+1},\ldots,a_N} p(a_1,\ldots,a_N | x_1,\ldots,x_N) = p(a_1,\ldots,a_k | x_1,\ldots,x_k)$$



	$++$	$+-$	$-+$	$--$
00	1/2	0	0	1/2
01	1/2	0	0	1/2
10	1/2	0	0	1/2
11	0	1/2	1/2	0

$$p_A(+1|0) = p(+1,+1|00) + p(+1,-1|00) = \frac{1}{2} = p(+1,+1|01) + p(+1,-1|01)$$

Physical correlations

Classical correlations: correlations established by classical means.

$$p\left(a_1,\ldots,a_N \middle| x_1,\ldots,x_N\right) = \sum_\lambda p(\lambda) D\left(a_1 \middle| x_1, \lambda\right)\ldots D\left(a_N \middle| x_N, \lambda\right)$$

These are the standard "EPR" correlations. Independently of fundamental issues, these are the correlations achievable by classical resources. Bell inequalities define the limits on these correlations.

Physical correlations

Quantum correlations: correlations established by quantum means.

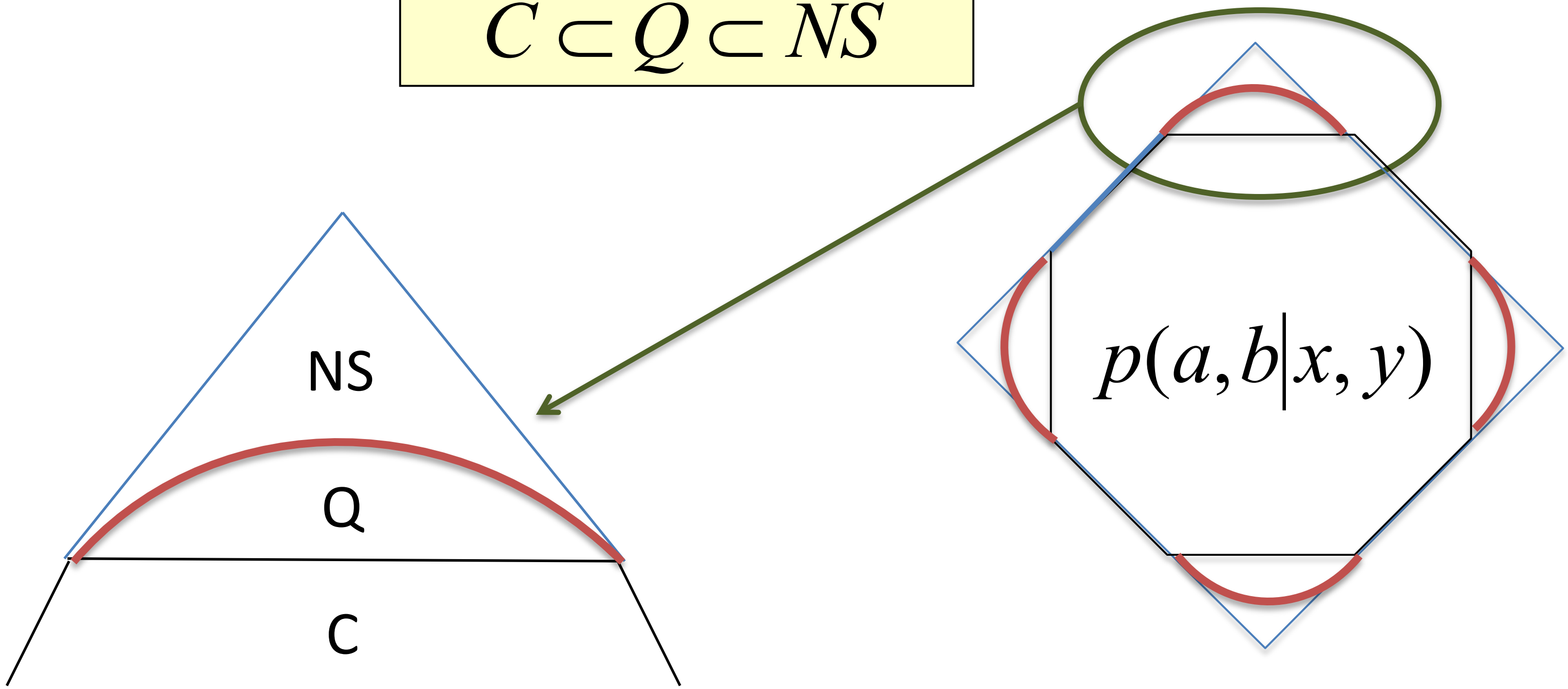
$$p(a_1,\ldots,a_N|x_1,\ldots,x_N) = \langle\Psi|M_{a_1}^{x_1}\otimes\cdots\otimes M_{a_N}^{x_N}|\Psi\rangle$$

$$\sum_{a_i} M_{a_i}^{x_i} = 1 \qquad M_{a'_i}^{x_i} M_{a_i}^{x_i} = \delta_{a_i a'_i} M_{a_i}^{x_i}$$

Everything is expressed in terms of operators (the quantum state and the measurement projectors) acting on a Hilbert space.

Physical correlations

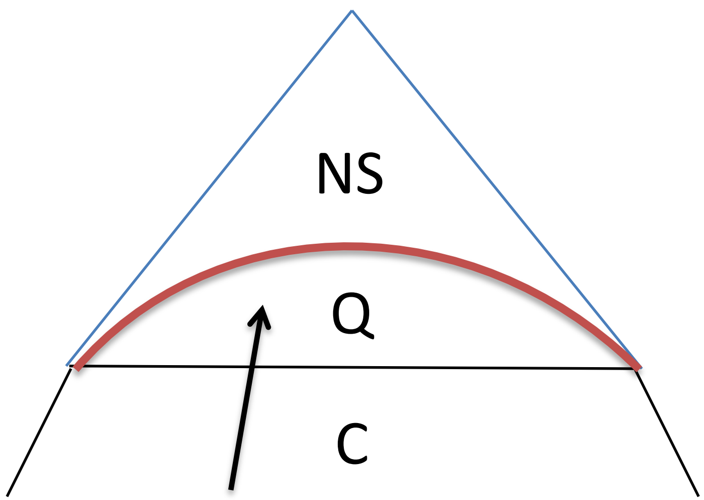
$$C \subset Q \subset NS$$



Physical correlations

Bell

$$C \subset Q \subset NS$$

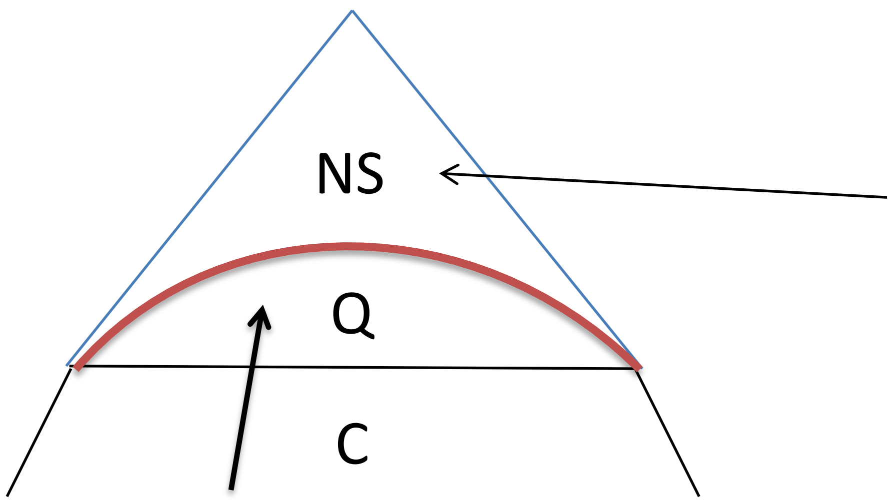


There exist correlations that cannot be explained by a classical model in which (deterministic) classical instructions specify the outcomes of the devices. These quantum correlations are known as **non-local** and they are detected by the violation of a Bell inequality.

Physical correlations

Bell $C \subset Q \subset NS$ Tsirelson

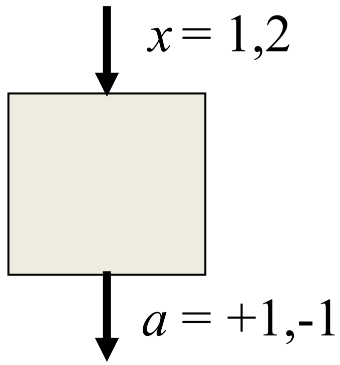
Popescu-Rohrlich



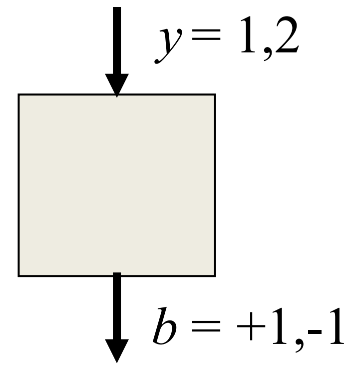
There exist correlations that are compatible with the no-signalling principle but cannot be obtained by performing local measurements on a quantum (entangled) state.

There exist correlations that cannot be explained by a classical model in which (deterministic) classical instructions specify the outcomes of the devices. These quantum correlations are known as **non-local** and they are detected by the violation of a Bell inequality.

Example: CHSH scenario

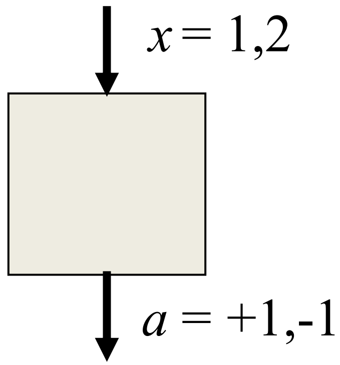


$$CHSH = A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$

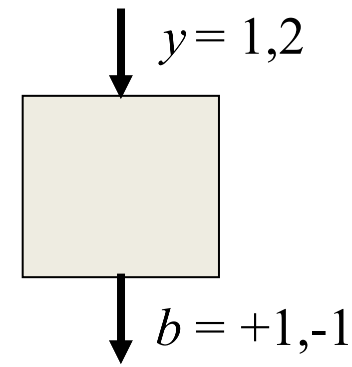


ICFO

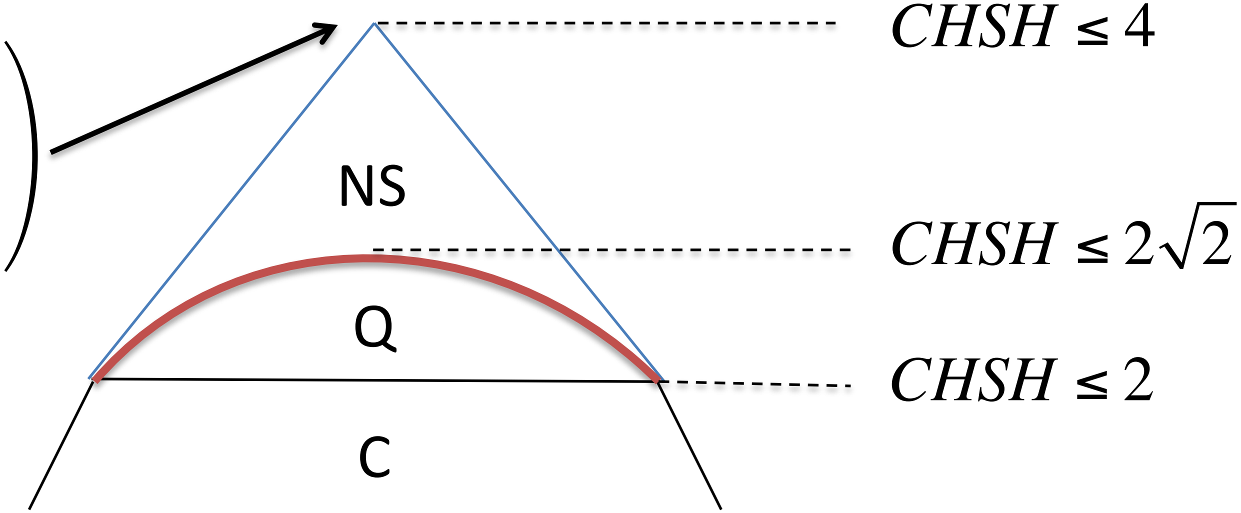
Example: CHSH scenario



$$CHSH = A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$



$$\begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 1/2 & 0 & 0 & 1/2 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$



Characterizing quantum correlations

Given $p(a,b|x,y)$, does it have a quantum realization?

$$p(a,b|x,y) = \langle \Psi | M_a^x \otimes M_b^y | \Psi \rangle$$

$$\sum_a M_a^x = 1$$

$$M_a^x M_{a'}^x = \delta_{a'a} M_a^x$$

Characterizing quantum correlations

Given $p(a,b|x,y)$, does it have a quantum realization?

$$p\left(a,b\middle|x,y\right)=\left\langle\Psi\middle|M_a^x\otimes M_b^y\middle|\Psi\right\rangle$$

$$\sum_a M_a^x = 1$$

$$M_a^x M_{a'}^x = \delta_{a'a} M_a^x$$

Example:

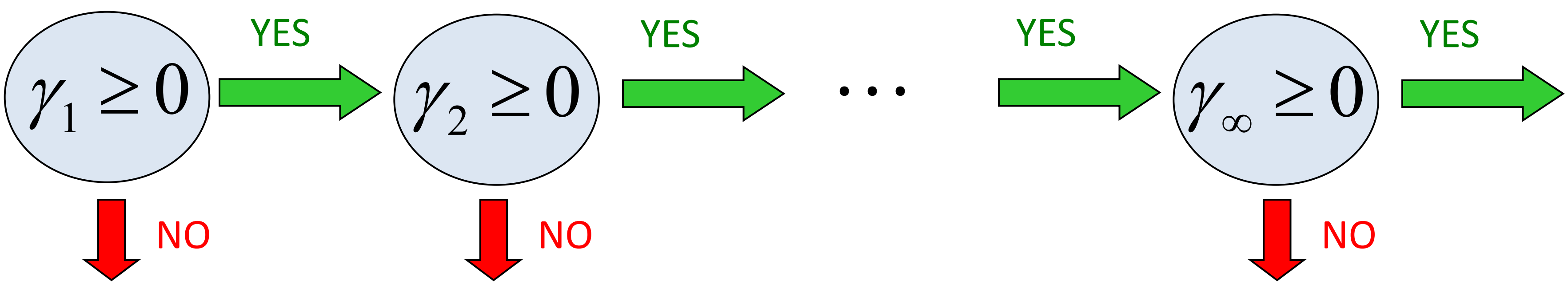
$$p\left(a,b\middle|0,0\right)=p\left(a,b\middle|0,1\right)=p\left(a,b\middle|1,0\right)=\frac{1}{8}\left(2+\sqrt{3},2-\sqrt{3},2-\sqrt{3},2+\sqrt{3}\right)$$

$$p\left(a,b\middle|1,1\right)=\left(0.245,0.255,0.255,0.245\right)$$

Previous work by Tsirelson

NPA hierarchy

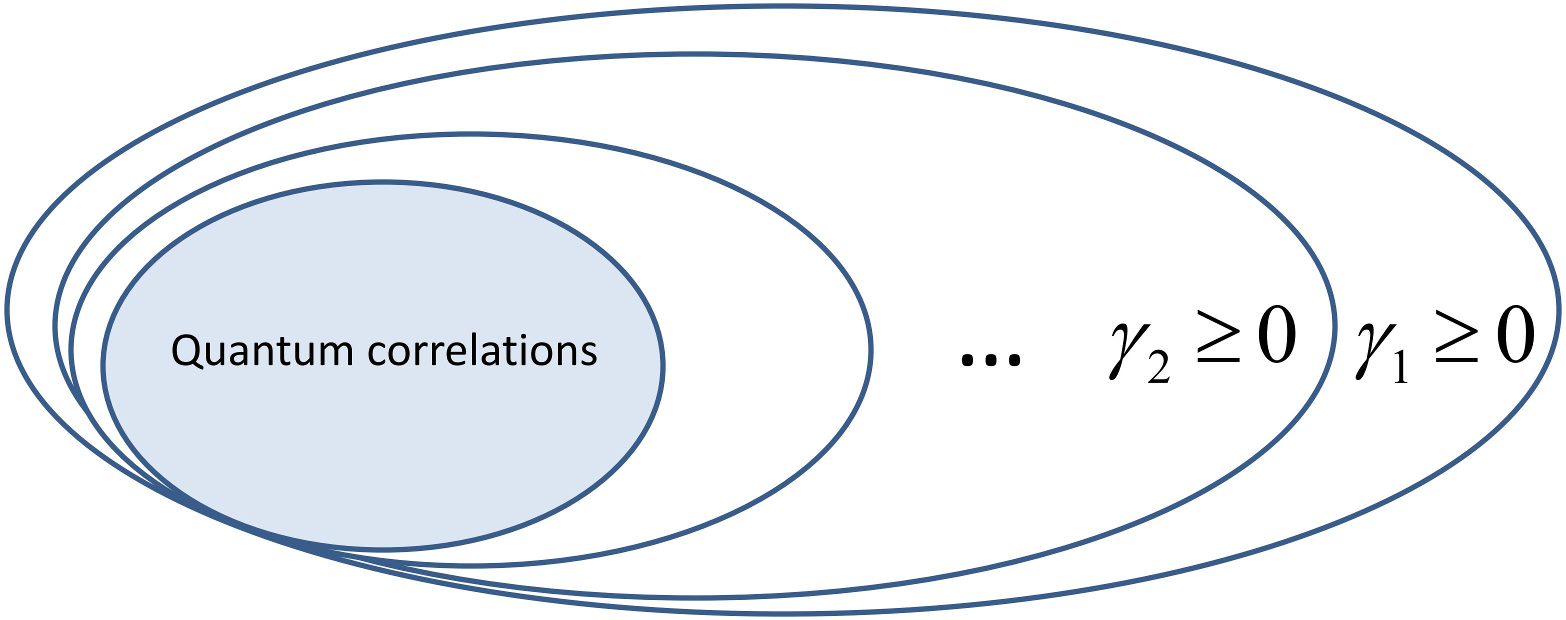
Given a probability distribution $p(a,b|x,y)$, we have defined a hierarchy consisting of a series of tests based on semi-definite programming techniques allowing the detection of supra-quantum correlations.



The hierarchy is asymptotically convergent.

ICFO

NPA hierarchy



Every step in the hierarchy defines a convex set that is included in the previous step. Convergence is provably attained asymptotically.

Characterizing quantum correlations

Example:

$$p(a,b|0,0) = p(a,b|0,1) = p(a,b|1,0) = \frac{1}{8}\left(2+\sqrt{3},2-\sqrt{3},2-\sqrt{3},2+\sqrt{3}\right)$$

$$p(a,b|1,1) = (0.245,0.255,0.255,0.245)$$

Solution: it is not quantum, that is, there exists no quantum state of two particles and local measurements acting on them that produce these correlations.

The experimental observation of these correlations would imply the failure of quantum physics, as Bell violations did for classical physics.

Going beyond NPA

Ground-state energies

A standard problem in physics is to find the ground state energy of a systems of N particles whose interactions are described by a Hamiltonian operator H.

$$\min_{|\psi\rangle} \langle\psi|H|\psi\rangle \qquad \text{subject to some constraints}$$

Ground-state energies

A standard problem in physics is to find the ground state energy of a systems of N particles whose interactions are described by a Hamiltonian operator H.

$$\min_{|\psi\rangle} \langle\psi|H|\psi\rangle$$ subject to some constraints

Variational approach: often, one can guess good candidates to solve this problem. The minimization is performed over a subset of states ➔upper bound.

Ground-state energies

A standard problem in physics is to find the ground state energy of a systems of N particles whose interactions are described by a Hamiltonian operator H.

$$\min_{|\psi\rangle} \langle \psi | H | \psi \rangle$$

subject to some constraints

Variational approach: often, one can guess good candidates to solve this problem. The minimization is performed over a subset of states ➔upper bound.

If the problem can be cast as a non-commutative polynomial optimization, the previous hierarchy provides lower bounds. It complements the standard approach!

Classical spin systems

Classical spin problems: $$\min_{\vec{\sigma}} H(\vec{\sigma}) = \sum_{i,j} J_{i,j}\sigma_i\sigma_j + \sum_i h_i\sigma_i$$

$$\min_{\vec{\sigma}} H(\vec{\sigma}) = \sum_{i,j} J_{i,j}\sigma_i\sigma_j + \sum_i h_i\sigma_i$$

such that:

$\sigma_i^2 - 1 = 0$ for all i

Commutative polynomial optimization:

$$E_1 \leq E_2 \leq \cdots \leq E_\infty \to E_g \leq E_a$$

Quantum spin systems

Quantum spin problems: $$\min_{\vec{\sigma}} H(\vec{\sigma}) = \sum_{i,j} J_{i,j}\sigma_i^x\sigma_j^x + \sum_i h_i\sigma_i^z$$

$$\min_{\vec{\sigma}} H(\vec{\sigma}) = \sum_{i,j} J_{i,j}\sigma_i^x\sigma_j^x + \sum_i h_i\sigma_i^z$$

such that:

$$\sigma_i^\alpha - 1 = 0$$
$$\left[\sigma_j^\alpha, \sigma_k^\beta\right] = 2i\delta_{jk}\epsilon_{\alpha\beta\gamma}\sigma_k^\gamma$$

Non-commutative polynomial optimization:

$$E_1 \leq E_2 \leq \cdots \leq E_\infty \to E_g \leq E_a$$

ICFO

Quantum spin systems

Quantum spin problems: $$\min_{\vec{\sigma}} H(\vec{\sigma}) = \sum_{i,j} J_{i,j}\sigma_i^x\sigma_j^x + \sum_i h_i\sigma_i^z$$

$$\min_{\vec{\sigma}} H(\vec{\sigma}) = \sum_{i,j} J_{i,j}\sigma_i^x\sigma_j^x + \sum_i h_i\sigma_i^z$$

such that:

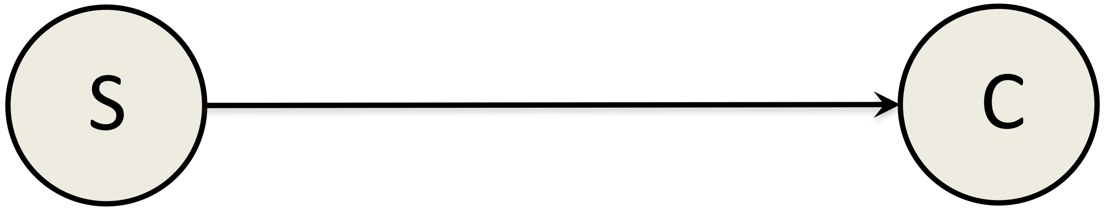
$$\sigma_i^\alpha - 1 = 0$$
$$\left[\sigma_j^\alpha, \sigma_k^\beta\right] = 2i\delta_{jk}\epsilon_{\alpha\beta\gamma}\sigma_k^\gamma$$

Non-commutative polynomial optimization:

$$E_1 \leq E_2 \leq \cdots \leq E_\infty \rightarrow E_g \leq E_a$$

See Jie Wang's talk.

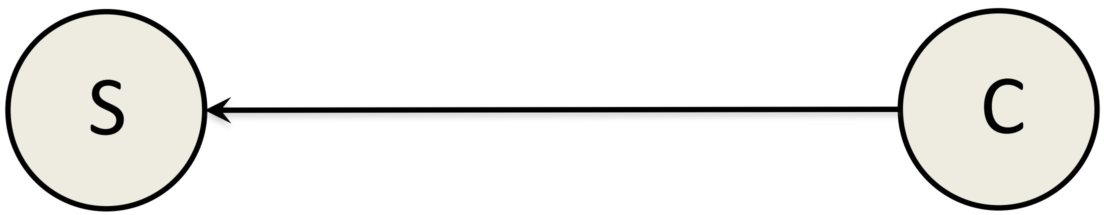
Causal networks



Main question: understand the causes that could be behind the observed correlations among a set of random variables.

ICFO

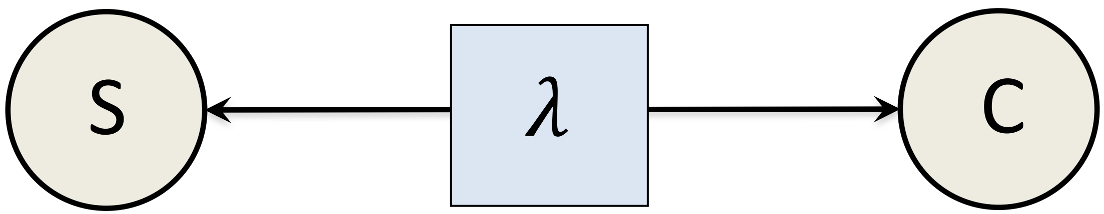
Causal networks



Main question: understand the causes that could be behind the observed correlations among a set of random variables.

Given two correlated variables, either direct causation is possible.

Causal networks



Main question: understand the causes that could be behind the observed correlations among a set of random variables.

Given two correlated variables, either direct causation is possible.

But even more intricate causation patterns could explain the correlations.

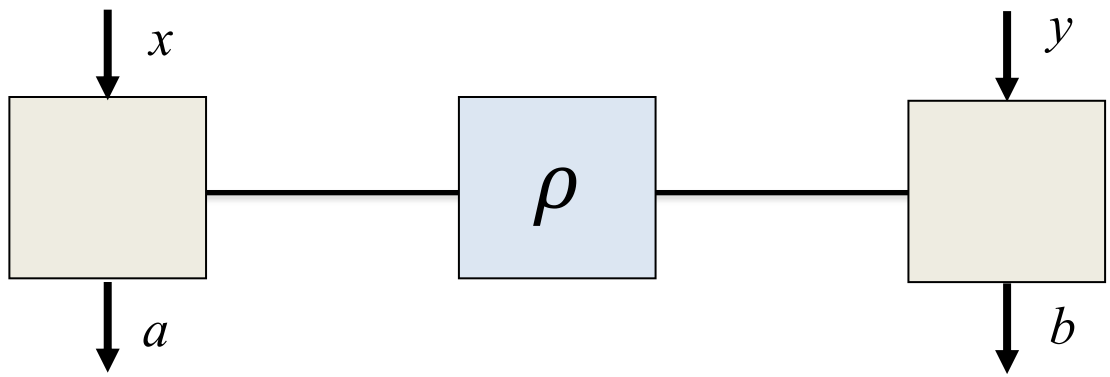
Causal networks

Representation of causality patterns through directed acyiclic graphs. Observed variables are represented by circles, hidden variables by squares and causes by directed edges.

Causal networks

Representation of causality patterns through directed acyiclic graphs. Observed variables are represented by circles, hidden variables by squares and causes by directed edges.

Bell setups can be understood in this language. Fritz, NJP'12; Wood & Spekkens, NJP '15

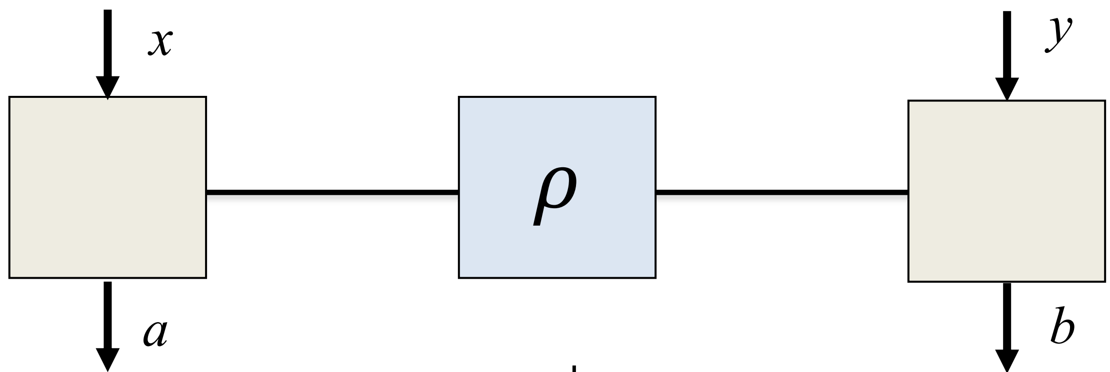


ICFO

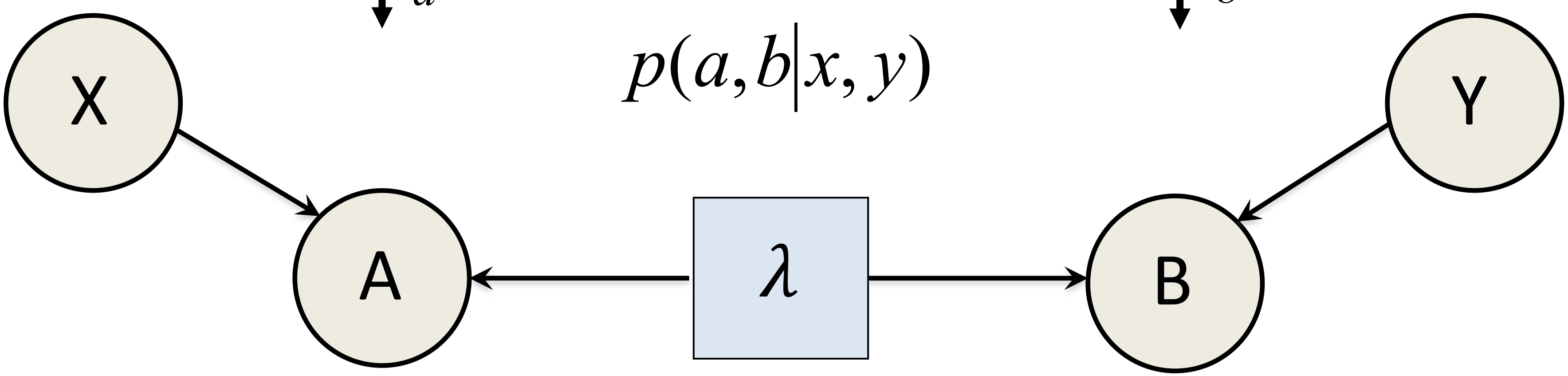
Causal networks

Representation of causality patterns through directed acyiclic graphs. Observed variables are represented by circles, hidden variables by squares and causes by directed edges.

Bell setups can be understood in this language. Fritz, NJP'12; Wood & Spekkens, NJP '15



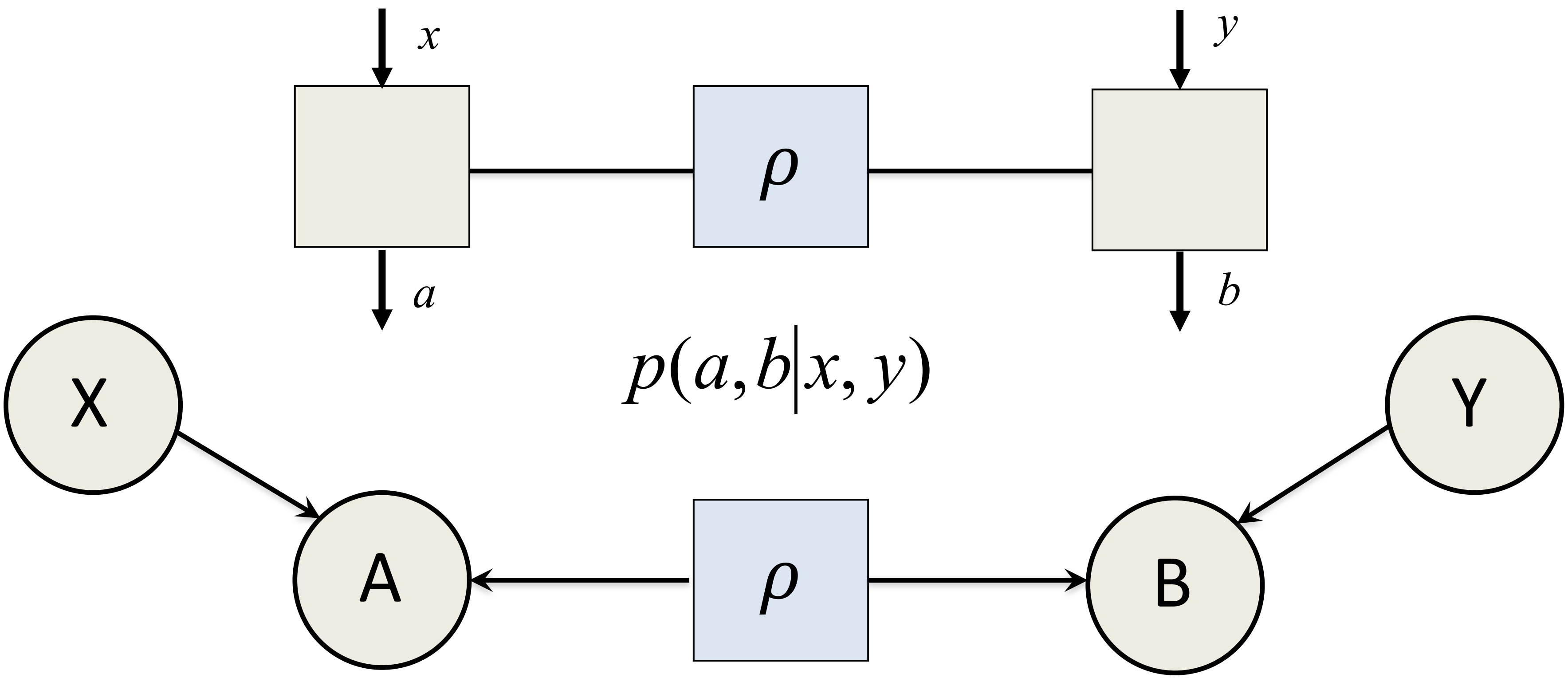
$$p(a,b|x,y)$$



Causal networks

Representation of causality patterns through directed acyiclic graphs. Observed variables are represented by circles, hidden variables by squares and causes by directed edges.

Bell setups can be understood in this language. Fritz, NJP'12; Wood & Spekkens, NJP '15

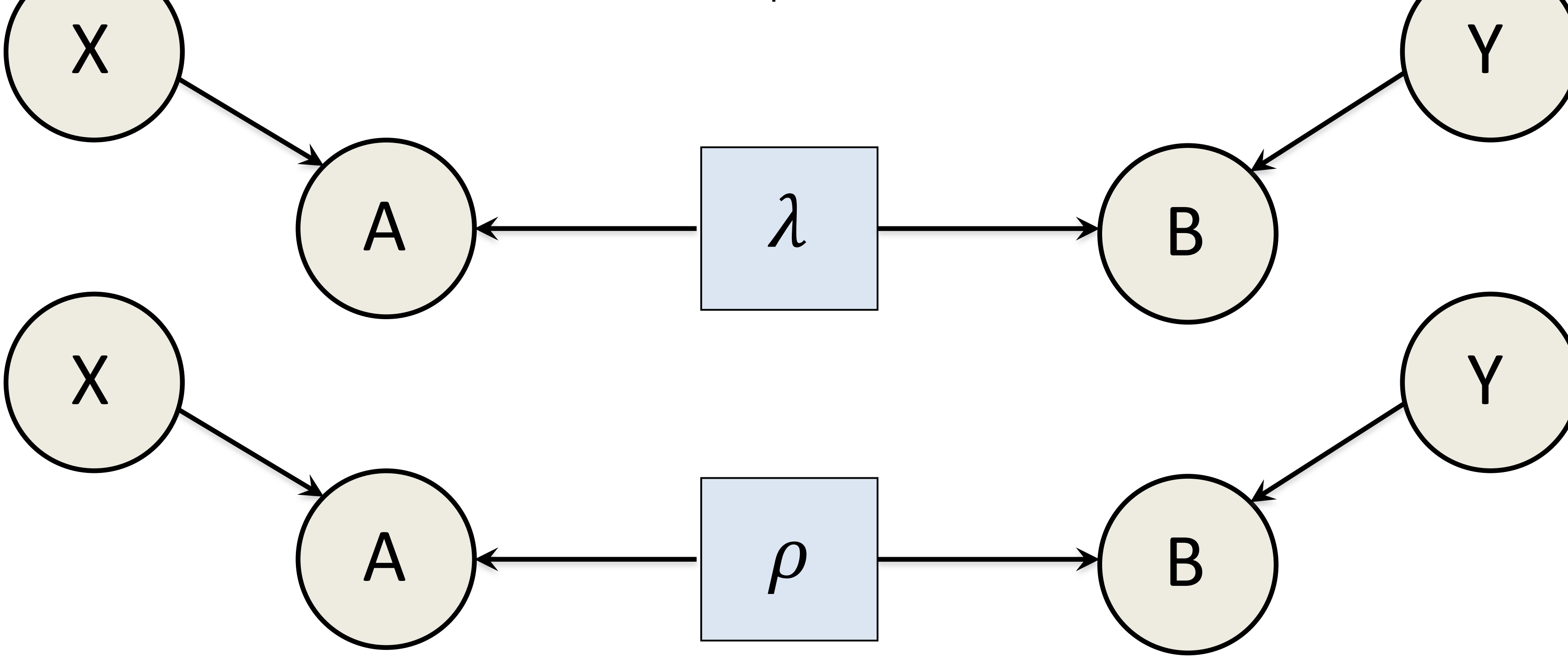


ICFO

Quantum causality

Bell's theorem: nonlocal correlations can be explained by a quantum causal model, but not by the classical counterpart.

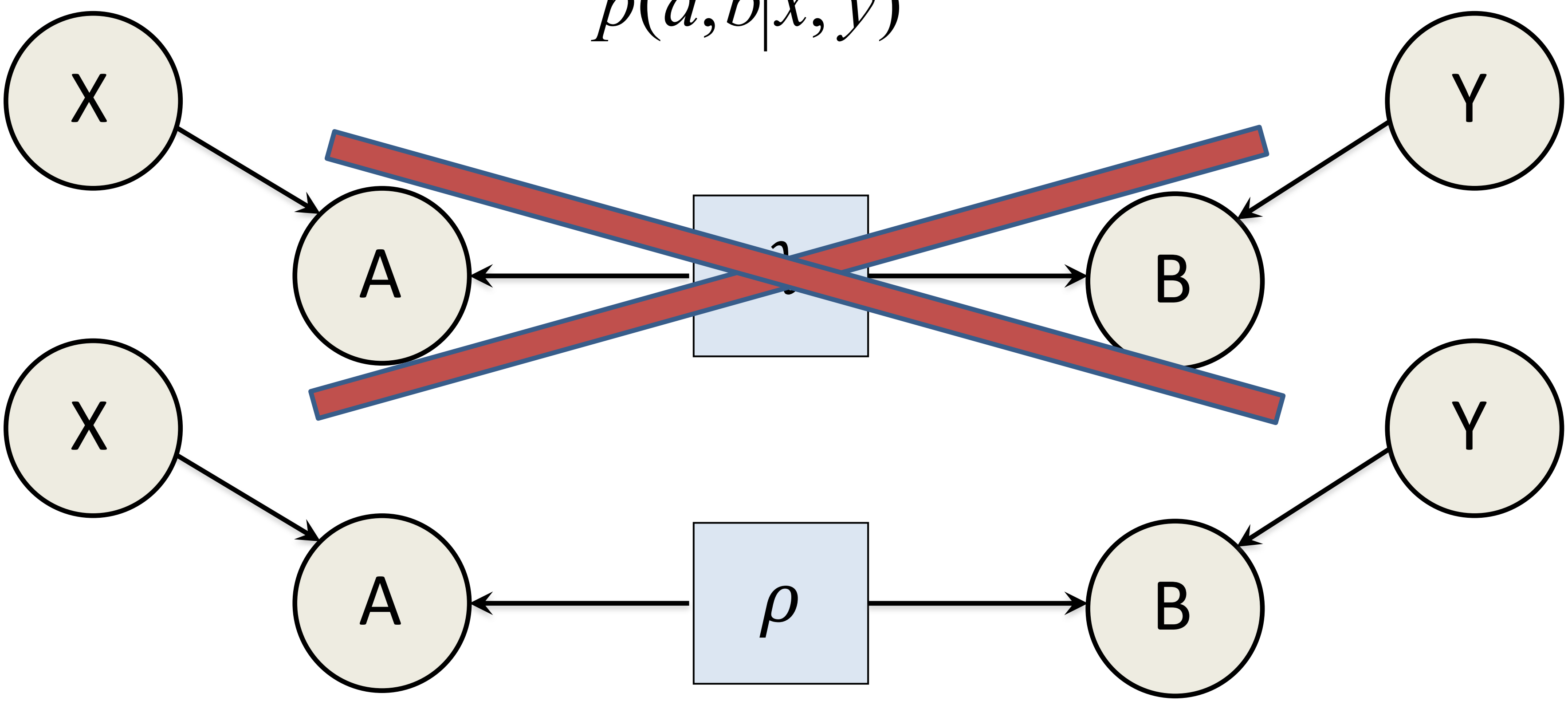
$$p(a,b|x,y)$$



Quantum causality

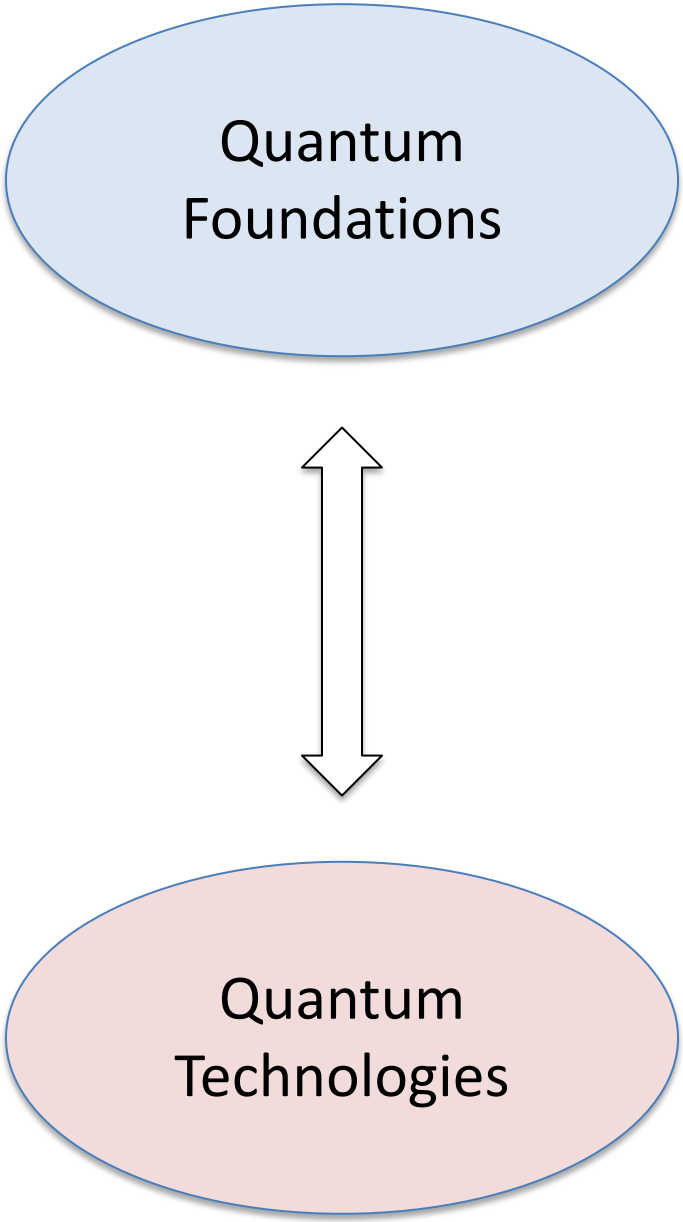
Bell's theorem: nonlocal correlations can be explained by a quantum causal model, but not by the classical counterpart.

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



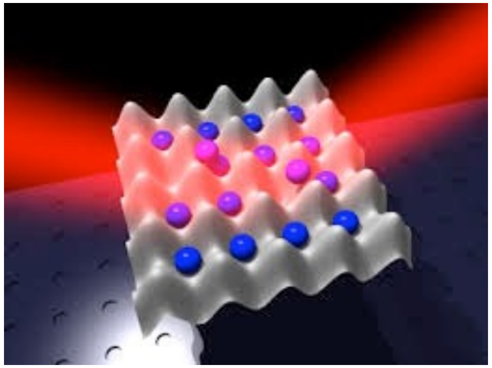
How is causality affected by quantum information?

See Alejandro Pozas-Kerstjens' talk.


Quantum Foundations
Quantum Technologies

Quantum information technologies

Quantum Computer



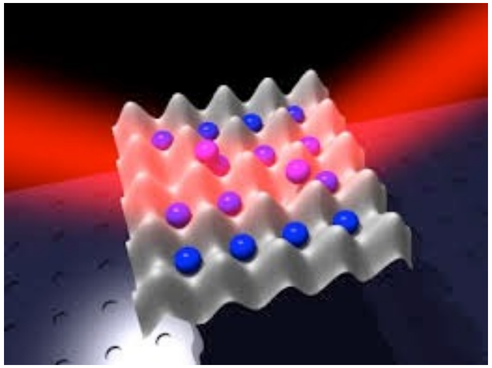
Quantum Simulator

Quantum Cryptography

QRNG

Quantum certification

Is this a Quantum Computer?



Does this properly simulate a quantum system?

Is this cryptographically secure?

Is this quantum random?