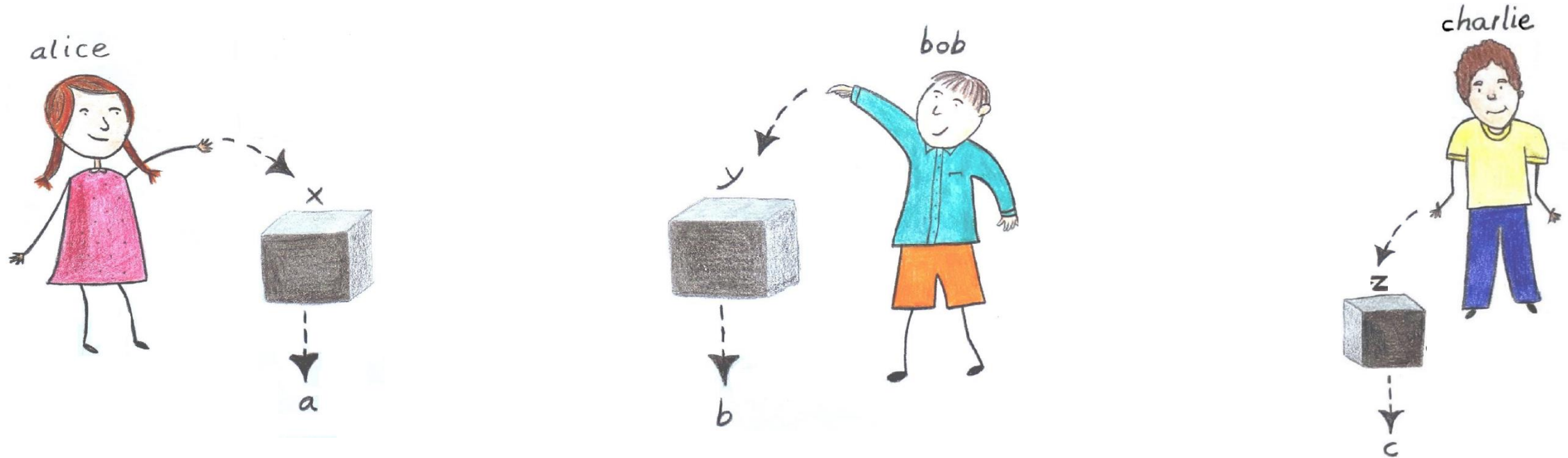


Bell Theorem and its generalizations



IP PARIS

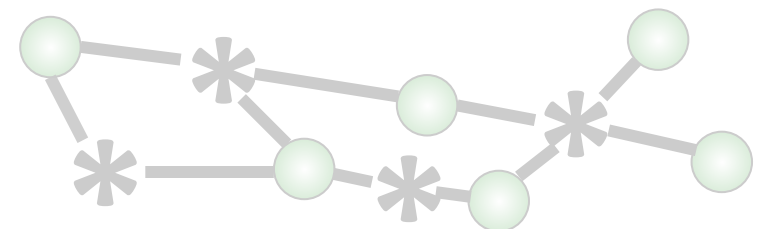
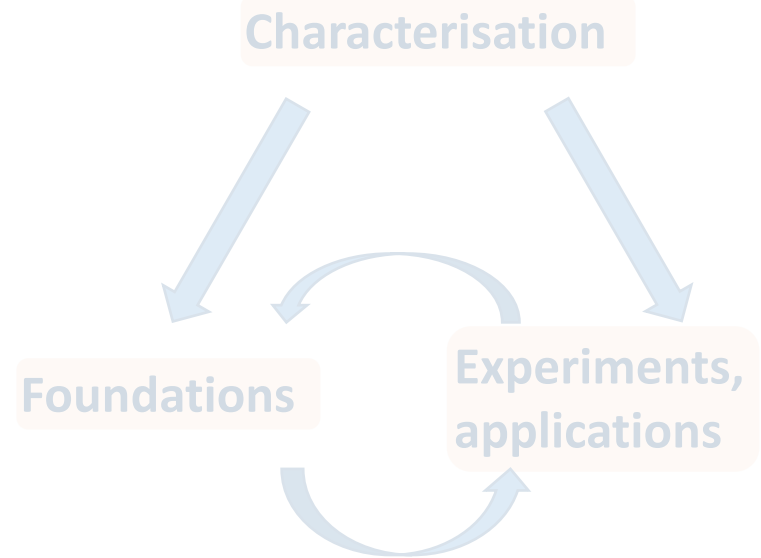
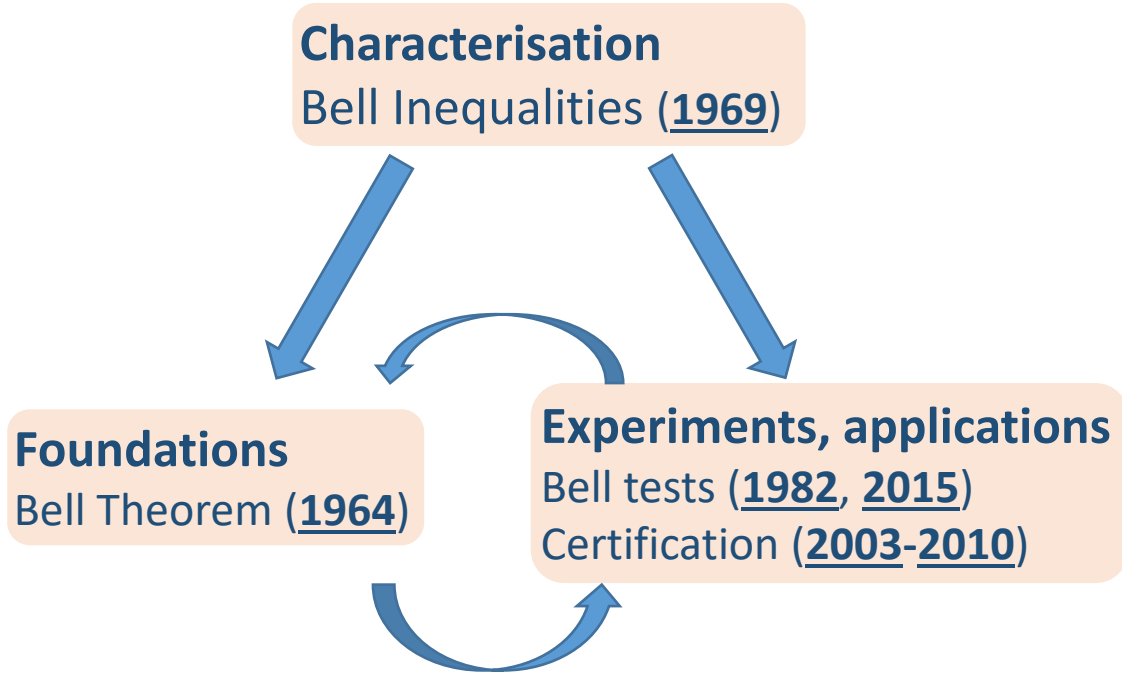
Inria

Grace Seminar

Marc-Olivier Renou
Junior Professor Chair INRIA Paris Saclay
Computer Science Laboratory / Center for Theoretical Physics
Ecole Polytechnique

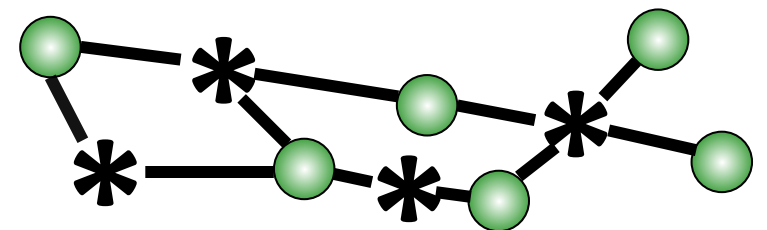
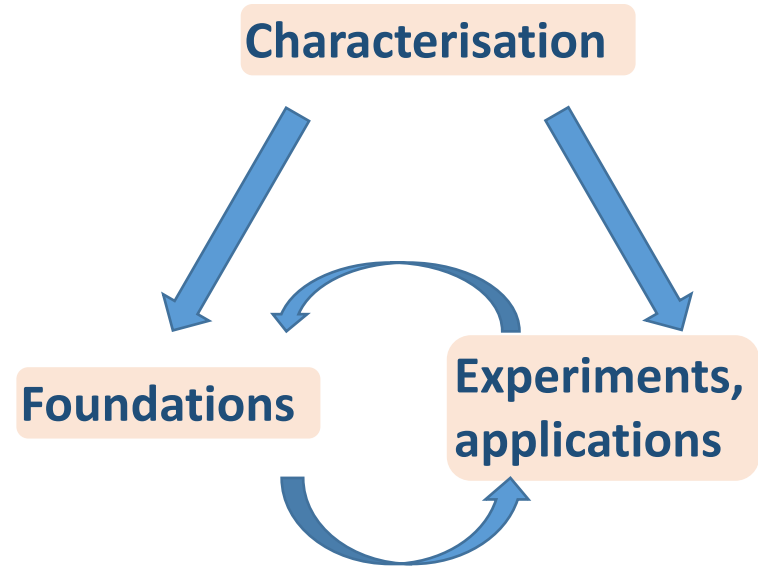
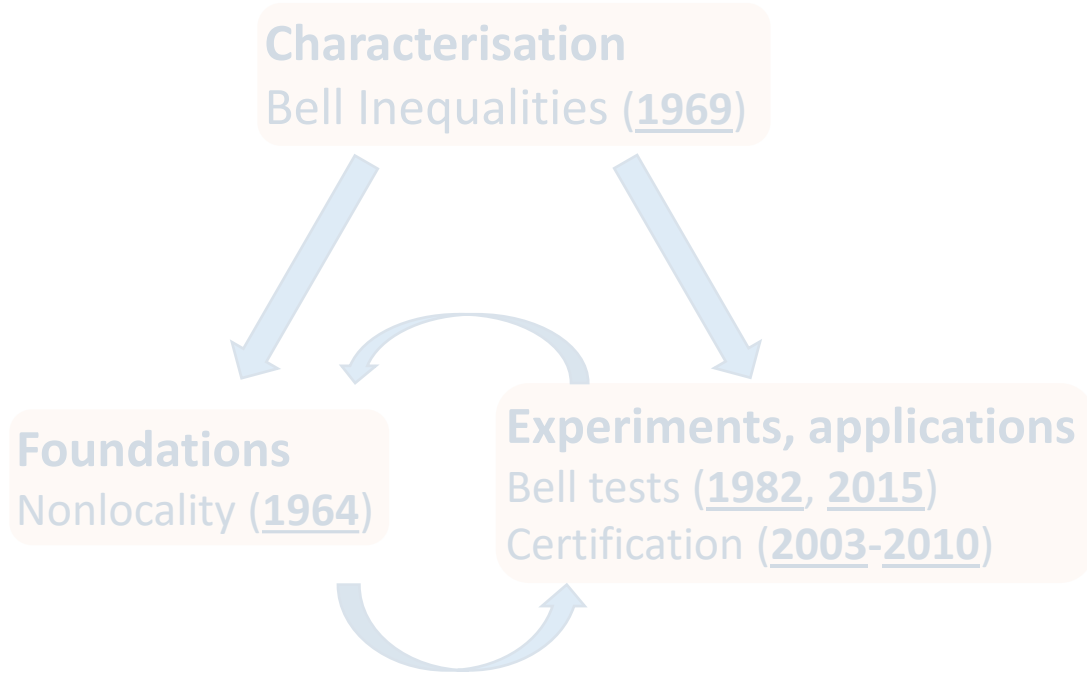
Overview

Single state quantum correlations



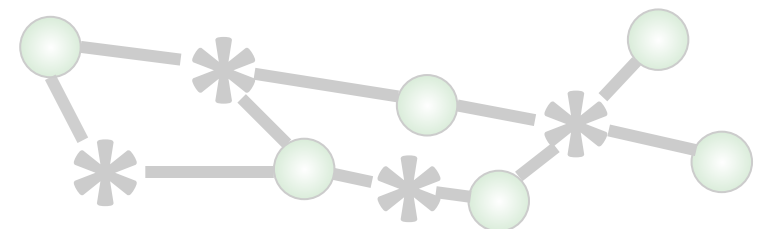
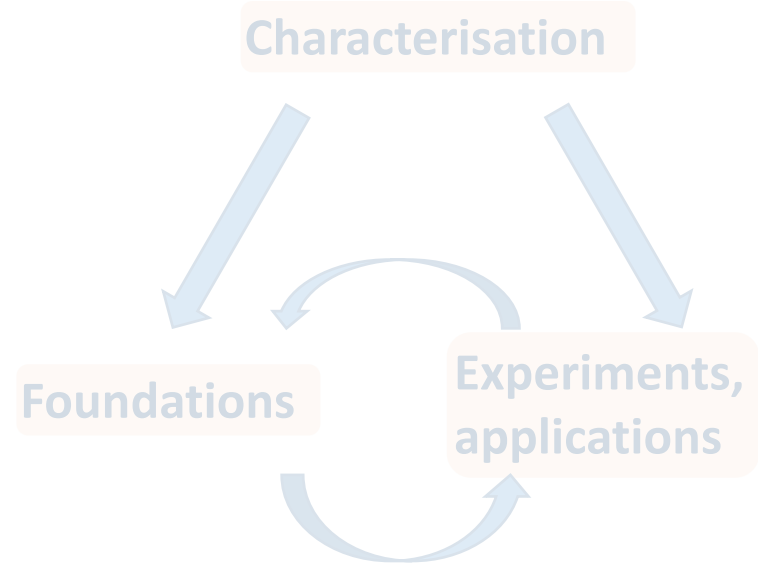
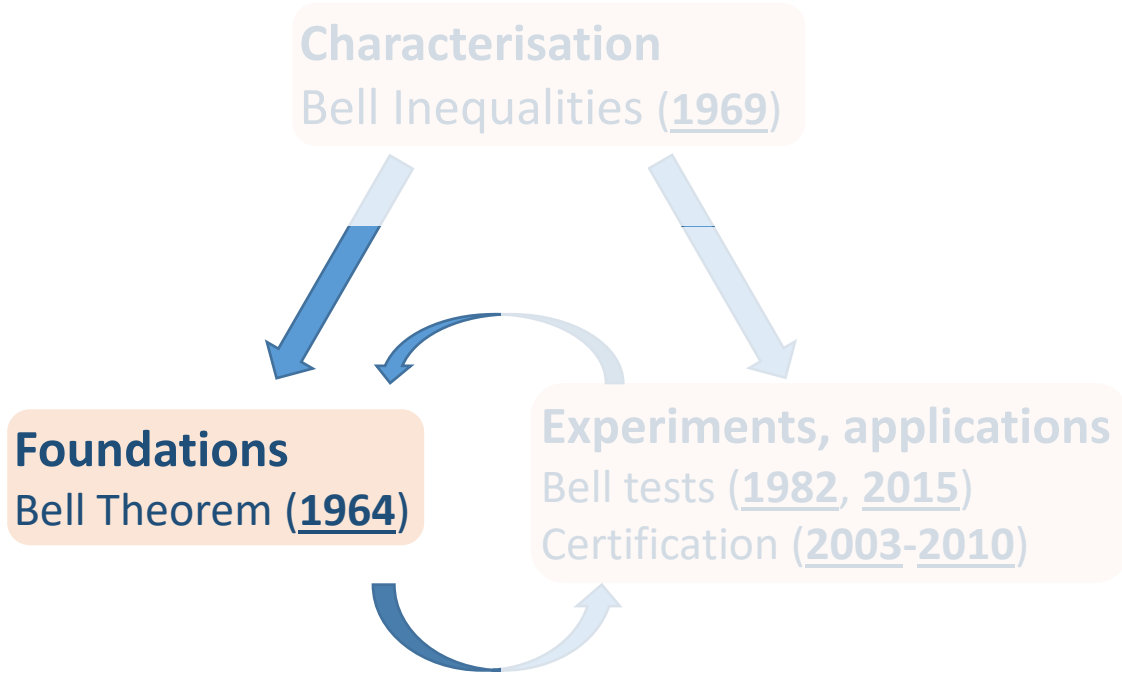
Overview

Causal network quantum correlations



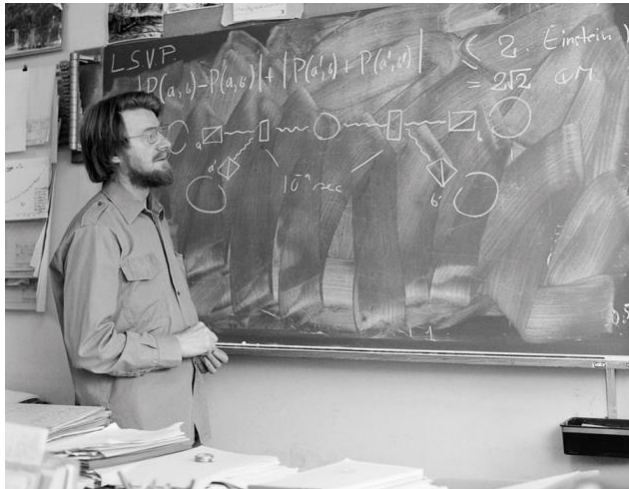
Overview

Single state quantum correlations



Bell theorem

the Bell theorem is not about quantum theory



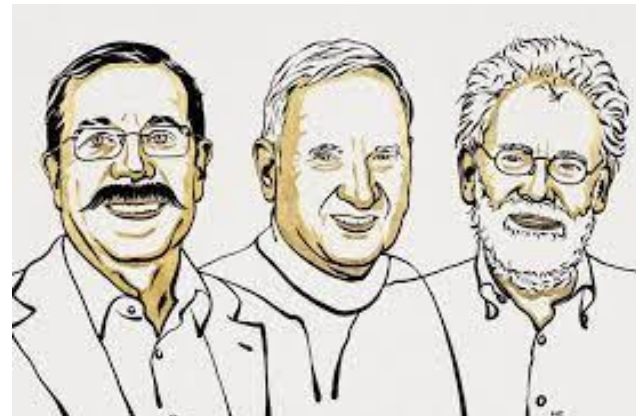
Bell's theorem 1964

Bell theorem:

Quantum theory predictions incompatible with 'a natural notion of locality'

Main ingredient:

'classical physics correlations \neq quantum correlations



Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



Detective (e.g., Einstein)



Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)

- Master Quantum theory



Detective (e.g., Einstein)

- Believes in some 'classical principles':



Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



- Master Quantum theory

Detective (e.g., Einstein)



- Believes in some 'classical principles':
 - One can apply the logical "or" on unknown information
 - If a box contains unknown information, this information « takes the value λ_1 or λ_2 or ... »

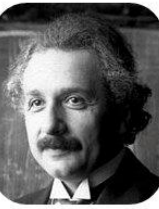
Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



- Master Quantum theory

Detective (e.g., Einstein)



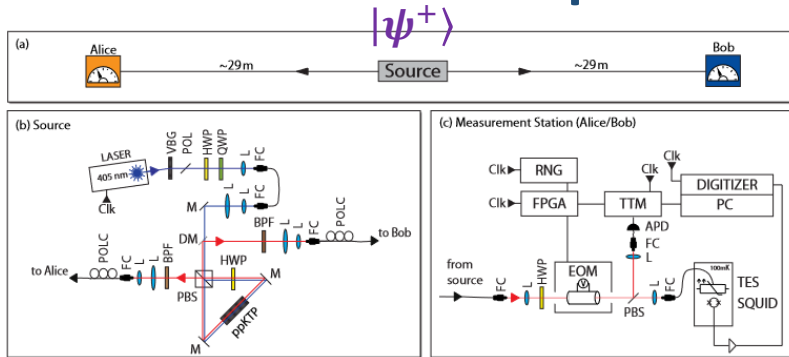
- Believes in some 'classical principles':
 - One can apply the logical "or" on unknown information
 - If a box contains unknown information, this information « takes the value λ_1 or λ_2 or ... »
 - Information carriers do not travel faster than light

Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



- Master Quantum theory
- Construct a **concrete experiment**



Detective (e.g., Einstein)



- Believes in some 'classical principles':
 - One can apply the logical "or" on unknown information
 - If a box contains unknown information, this information « takes the value λ_1 or λ_2 or ... »
 - Information carriers do not travel faster than light

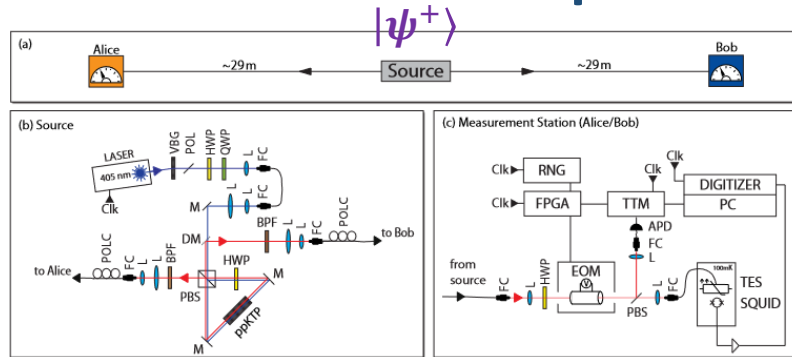
$$|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$$

Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



- Master Quantum theory
- Construct a **concrete experiment**



- Obtains **concrete experimental results**

➤ $P(a, b|x, y)$ such that $\text{CHSH} = 2\sqrt{2}$
i.e. $p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$

Detective (e.g., Einstein)



- Believes in some 'classical principles':
 - One can apply the logical "or" on unknown information
 - If a box contains unknown information, this information « takes the value λ_1 or λ_2 or ... »
 - Information carriers do not travel faster than light

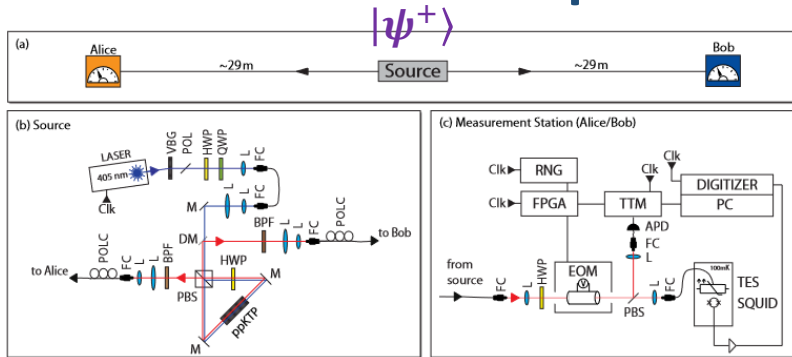
$$|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$$

Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



- Master Quantum theory
- Construct a **concrete experiment**



- Obtains **concrete experimental results**

➤ $P(a, b|x, y)$ such that $\text{CHSH} = 2\sqrt{2}$
 i.e. $p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$

Detective (e.g., Einstein)



- Believes in some 'classical principles':
 - One can apply the logical "or" on unknown information
 - If a box contains unknown information, this information « takes the value λ_1 or λ_2 or ... »
 - Information carriers do not travel faster than light
- Tries to explain these **observed** experimental results. '**Any far-fetched explanation**' is allowed.

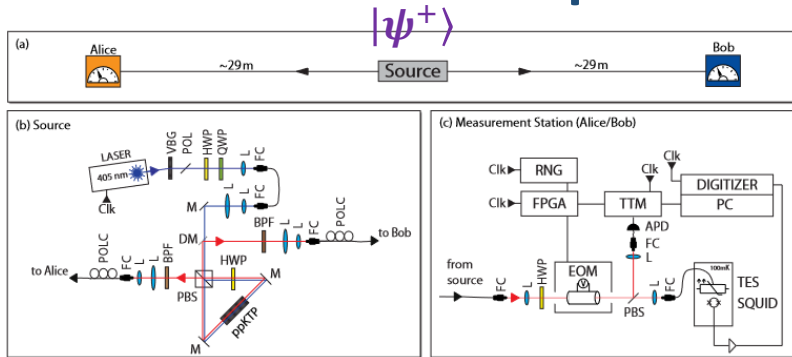
$$|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$$

Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



- Master Quantum theory
- Construct a **concrete experiment**



- Obtains **concrete experimental results**

➤ $P(a, b|x, y)$ such that $\text{CHSH} = 2\sqrt{2}$
 i.e. $p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$

Detective (e.g., Einstein)



- Believes in some 'classical principles':
 - One can apply the logical "or" on unknown information
 - If a box contains unknown information, this information « takes the value λ_1 or λ_2 or ... »
 - Information carriers do not travel faster than light
- Tries to explain these **observed** experimental results. 'Any far-fetched explanation' is allowed.
- Fails: is restricted to $\text{CHSH} \leq 2$
 i.e. $p(a \oplus b = x \cdot y) \leq 0.75$

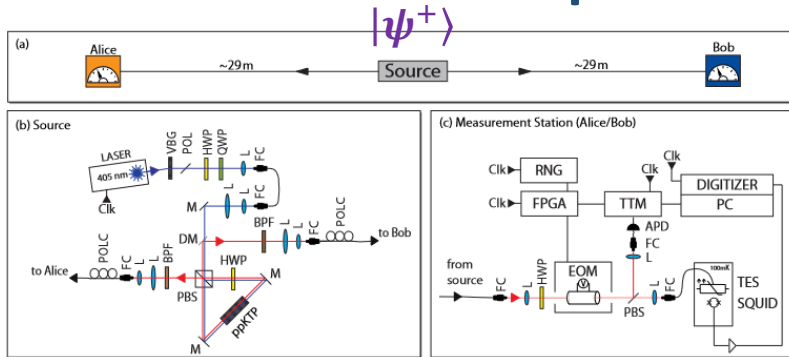
$$|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$$

Bell theorem: 'with the eyes of a detective'

Experimentalist (e.g., Aspect)



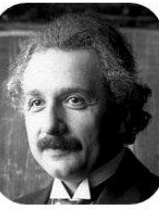
- Master Quantum theory
- Construct a **concrete experiment**



- Obtains **concrete experimental results**

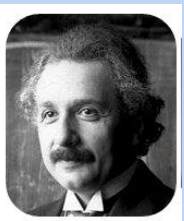
➤ $P(a, b|x, y)$ such that $\text{CHSH} = 2\sqrt{2}$
i.e. $p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$

Detective (e.g., Einstein)



- Believes in some 'classical principles':
 - One can apply the logical "or" on unknown information
 - If a box contains unknown information, this information « takes the value λ_1 or λ_2 or ... »
 - Information carriers do not travel faster than light
- Tries to explain these **observed** experimental results. 'Any far-fetched explanation' is allowed.
- Fails: is restricted to $\text{CHSH} \leq 2$
i.e. $p(a \oplus b = x \cdot y) \leq 0.75$

Bell Theorem [1964, 1969]: Proof of the failure of the detective



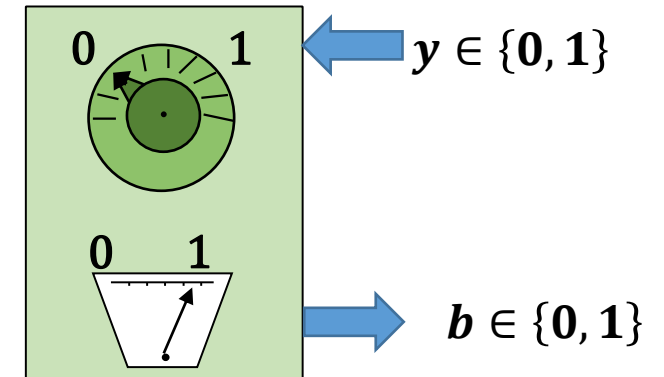
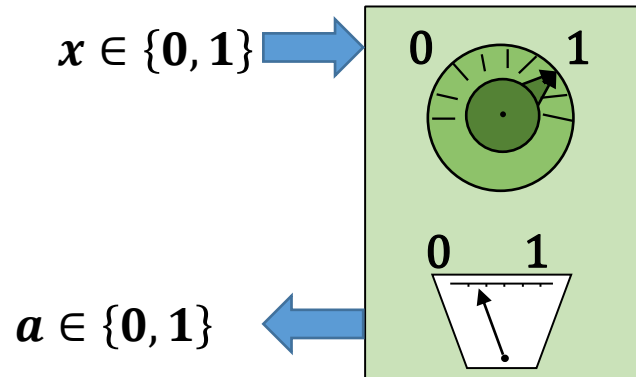
The CHSH experiment

as observed by the detective

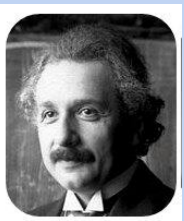
Alice, in Bordeaux

and

Bob, in Saclay



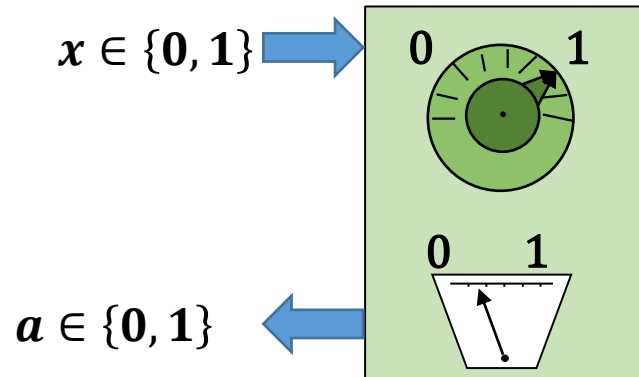
can select a measurement 0 or 1 **at random**
and obtain a result 0 or 1



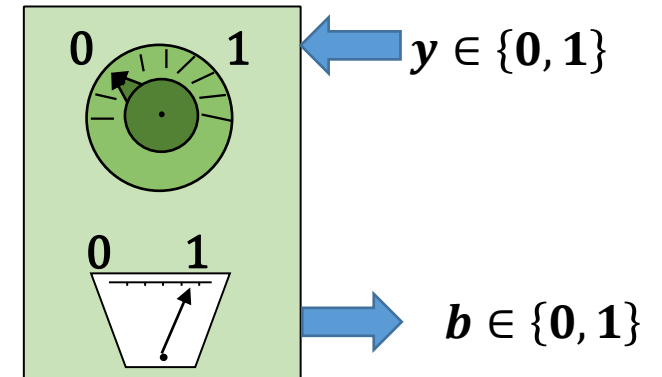
The CHSH experiment

as observed by the detective

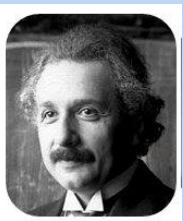
Alice, in Bordeaux



Bob, in Saclay



They do it many time, to
accumulate statistics



CHSH inequality

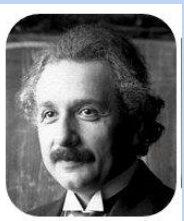
CHSH game



Game

- Many test $N \gg 1$ of the device, in different rounds $i = 1, \dots, N$, with uniformly **random** inputs $x^{(i)}, y^{(i)}$, outputs $a^{(i)}, b^{(i)}$
- Accumulation of statistics

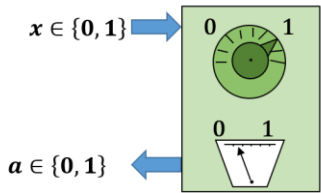
i	$x^{(i)}$	$a^{(i)}$	$y^{(i)}$	$b^{(i)}$	
1	1	0	0	0	
2	0	1	0	1	
3	0	0	0	0	
4	1	0	1	1	
5	0	1	1	0	
6	1	1	0	1	
7	1	1	1	1	
8	1	0	0	0	



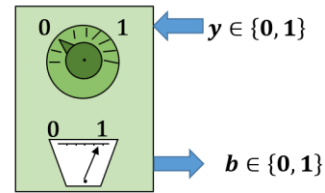
CHSH inequality

CHSH game

Alice, in Bordeaux



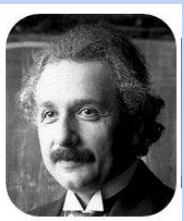
Bob, in Saclay



i	$x^{(i)}$	$a^{(i)}$	$y^{(i)}$	$b^{(i)}$	$S^{(i)}$
1	1	0	0	0	1
2	0	1	0	1	1
3	0	0	0	0	1
4	1	0	1	1	1
5	0	1	1	0	0
6	1	1	0	1	1
7	1	1	1	1	0
8	1	0	0	0	1

Game

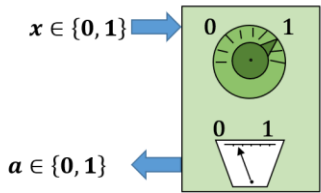
- Many test $N \gg 1$ of the device, in different rounds $i = 1, \dots, N$, with uniformly **random** inputs $x^{(i)}, y^{(i)}$, outputs $a^{(i)}, b^{(i)}$
- Accumulation of statistics
- Score at round i :
 - If $a \oplus b = x \cdot y : S^{(i)} = 1$
 - If $a \oplus b \neq x \cdot y : S^{(i)} = 0$



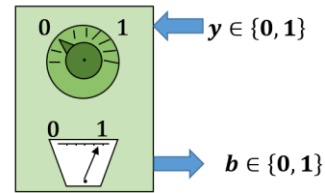
CHSH inequality

CHSH game

Alice, in Bordeaux



Bob, in Saclay

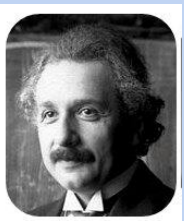


i	$x^{(i)}$	$a^{(i)}$	$y^{(i)}$	$b^{(i)}$	$S^{(i)}$
1	1	0	0	0	1
2	0	1	0	1	1
3	0	0	0	0	1
4	1	0	1	1	1
5	0	1	1	0	0
6	1	1	0	1	1
7	1	1	1	1	0
8	1	0	0	0	1

Game

- Many test $N \gg 1$ of the device, in different rounds $i = 1, \dots, N$, with uniformly **random** inputs $x^{(i)}, y^{(i)}$, outputs $a^{(i)}, b^{(i)}$
- Accumulation of statistics
- Score at round i :
 - If $a \oplus b = x \cdot y : S^{(i)} = 1$
 - If $a \oplus b \neq x \cdot y : S^{(i)} = 0$
- Mean score:

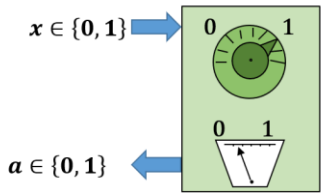
$$\langle S \rangle = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_i S^{(i)} = p(a \oplus b = x \cdot y)$$



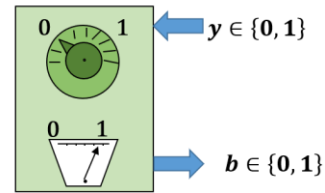
CHSH inequality

CHSH game

Alice, in Bordeaux



Bob, in Saclay



i	$x^{(i)}$	$a^{(i)}$	$y^{(i)}$	$b^{(i)}$	$S^{(i)}$
1	1	0	0	0	1
2	0	1	0	1	1
3	0	0	0	0	1
4	1	0	1	1	1
5	0	1	1	0	0
6	1	1	0	1	1
7	1	1	1	1	0
8	1	0	0	0	1

Game

- Many test $N \gg 1$ of the device, in different rounds $i = 1, \dots, N$, with uniformly **random** inputs $x^{(i)}, y^{(i)}$, outputs $a^{(i)}, b^{(i)}$

- Accumulation of statistics

- Score at round i :

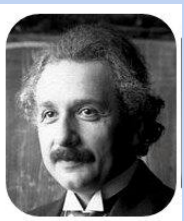
- If $a \oplus b = x \cdot y : S^{(i)} = 1$
- If $a \oplus b \neq x \cdot y : S^{(i)} = 0$

- Mean score:

$$\langle S \rangle = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_i S^{(i)} = p(a \oplus b = x \cdot y)$$

- The detective sees

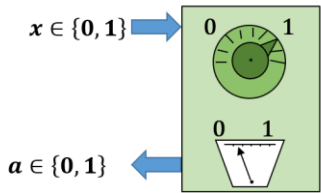
$$p(a \oplus b = x \cdot y) \approx 0.85$$



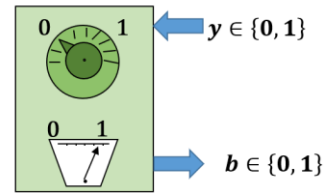
CHSH inequality

CHSH game

Alice, in Bordeaux



Bob, in Saclay



i	$x^{(i)}$	$a^{(i)}$	$y^{(i)}$	$b^{(i)}$	$S^{(i)}$
1	1	0	0	0	1
2	0	1	0	1	1
3	0	0	0	0	1
4	1	0	1	1	1
5	0	1	1	0	0
6	1	1	0	1	1
7	1	1	1	1	0
8	1	0	0	0	1

Game

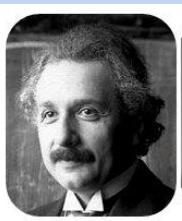
- Many test $N \gg 1$ of the device, in different rounds $i = 1, \dots, N$, with uniformly **random** inputs $x^{(i)}, y^{(i)}$, outputs $a^{(i)}, b^{(i)}$
- Accumulation of statistics
- Score at round i :
 - If $a \oplus b = x \cdot y : S^{(i)} = 1$
 - If $a \oplus b \neq x \cdot y : S^{(i)} = 0$
- Mean score:

$$\langle S \rangle = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_i S^{(i)} = p(a \oplus b = x \cdot y)$$

➤ The detective sees

$$p(a \oplus b = x \cdot y) \approx 0.85$$

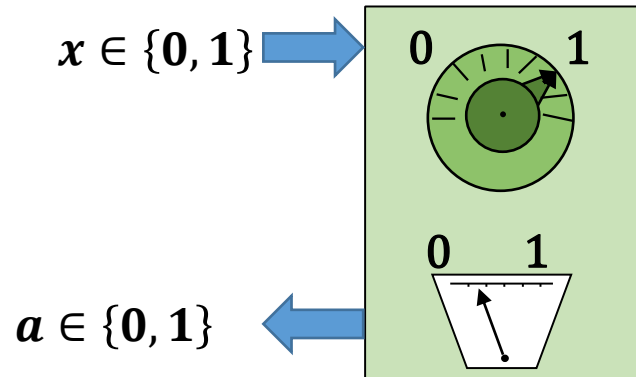
$$\Leftrightarrow \text{CHSH} \equiv \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle = 2\sqrt{2}$$



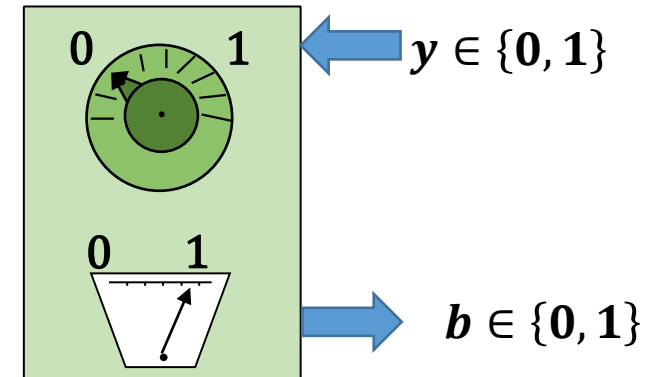
The CHSH experiment

as observed by the detective

Alice, in Bordeaux



Bob, in Saclay



Correlated behavior:

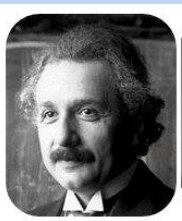
○ If $x = y = 1$:

$$p(a = b) < p(a \neq b)$$

○ If not:

$$p(a = b) > p(a \neq b)$$

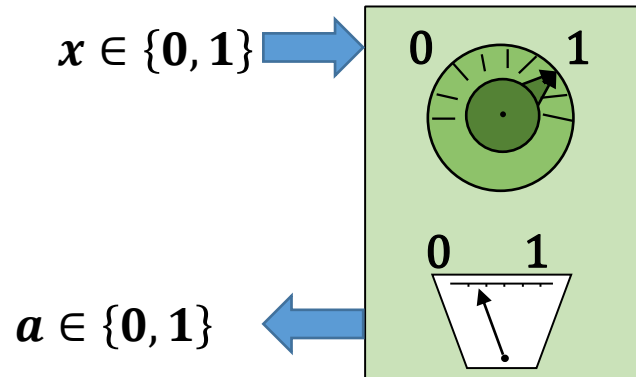
$$p(a \oplus b = x \cdot y) \approx 0.85$$



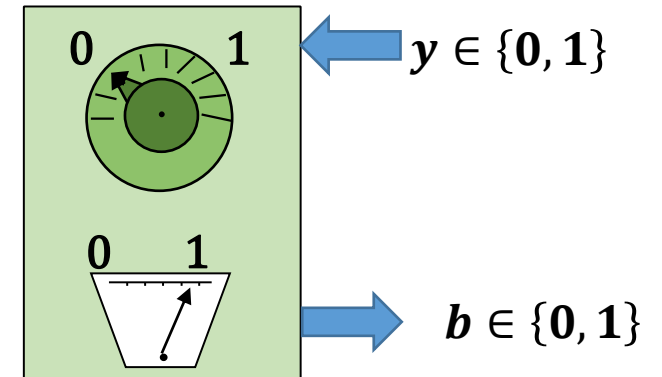
The CHSH experiment

as observed by the detective

Alice, in Bordeaux



Bob, in Saclay



Correlated behavior:

○ If $x = y = 1$:

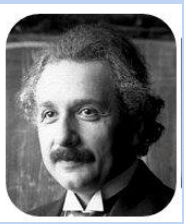
$$p(a = b) < p(a \neq b)$$

○ If not:

$$p(a = b) > p(a \neq b)$$

$$p(a \oplus b = x \cdot y) \approx 0.85$$

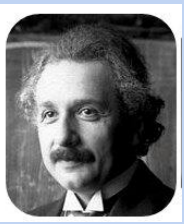
➤ **Detective's question:** Where does it come from?



Correlations = Influence or Common Cause

Only two possibilities:

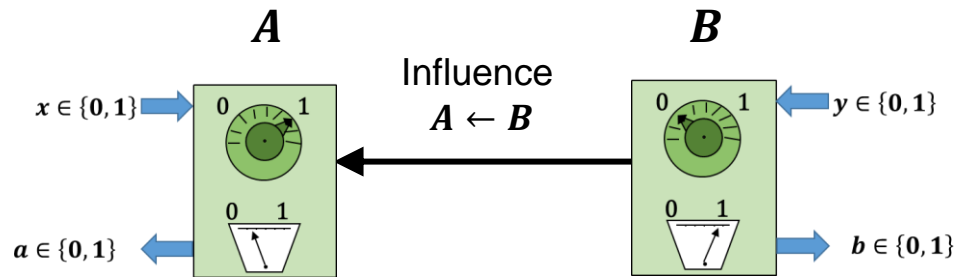
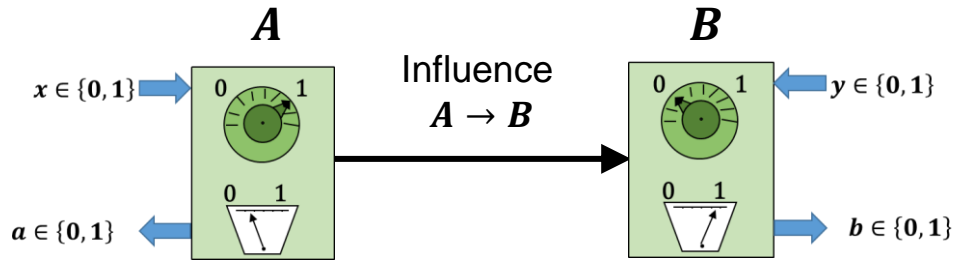


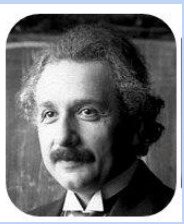


Correlations = Influence or Common Cause

Only two possibilities:

Influence

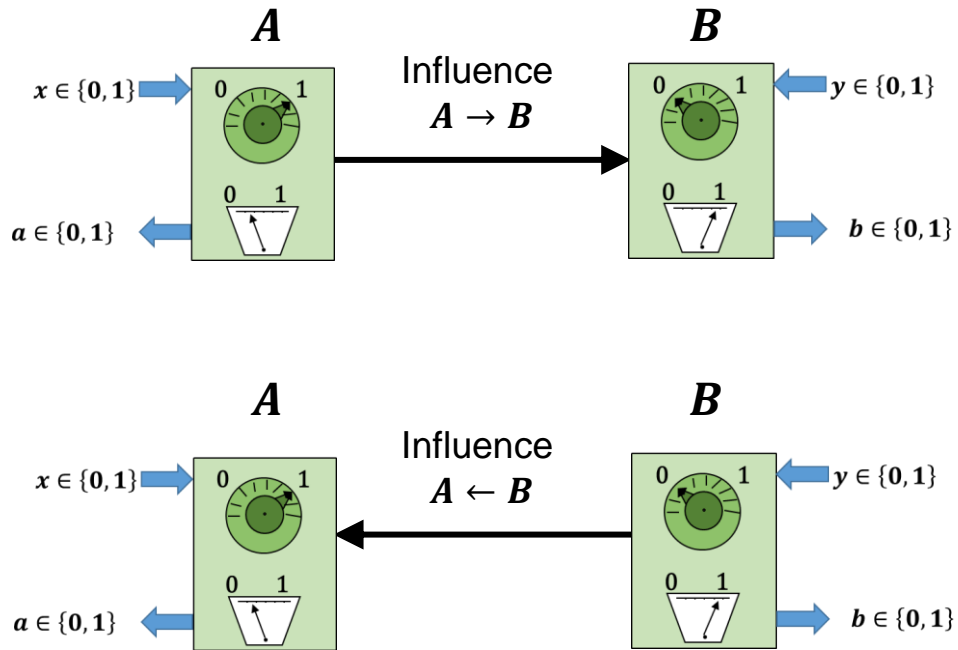




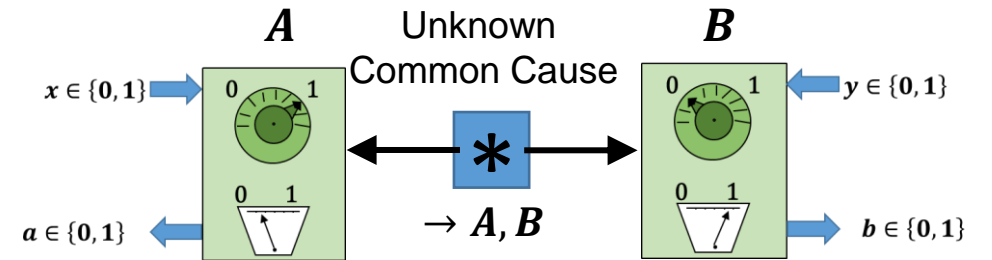
Correlations = Influence or Common Cause

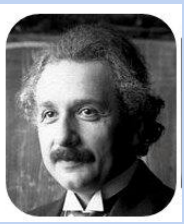
Only two possibilities:

Influence



Common cause

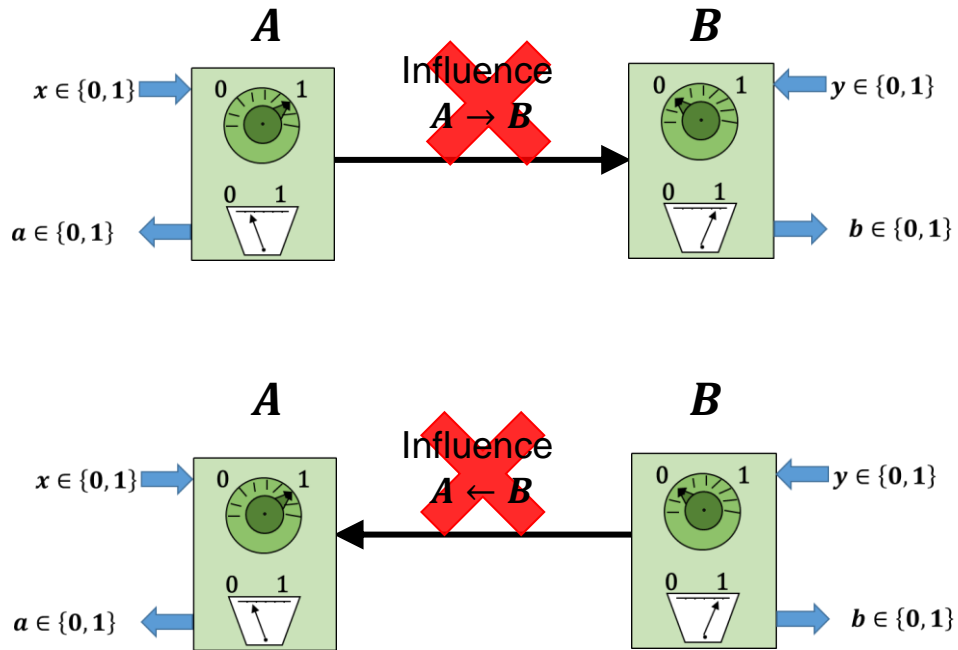




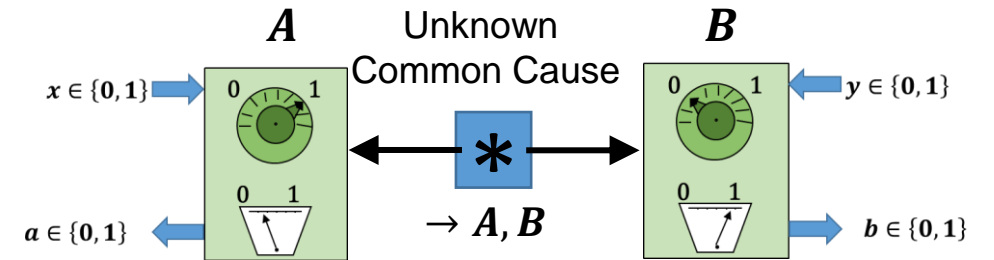
Correlations = Influence or Common Cause

Only two possibilities:

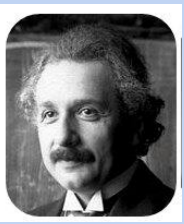
Influence



Common cause



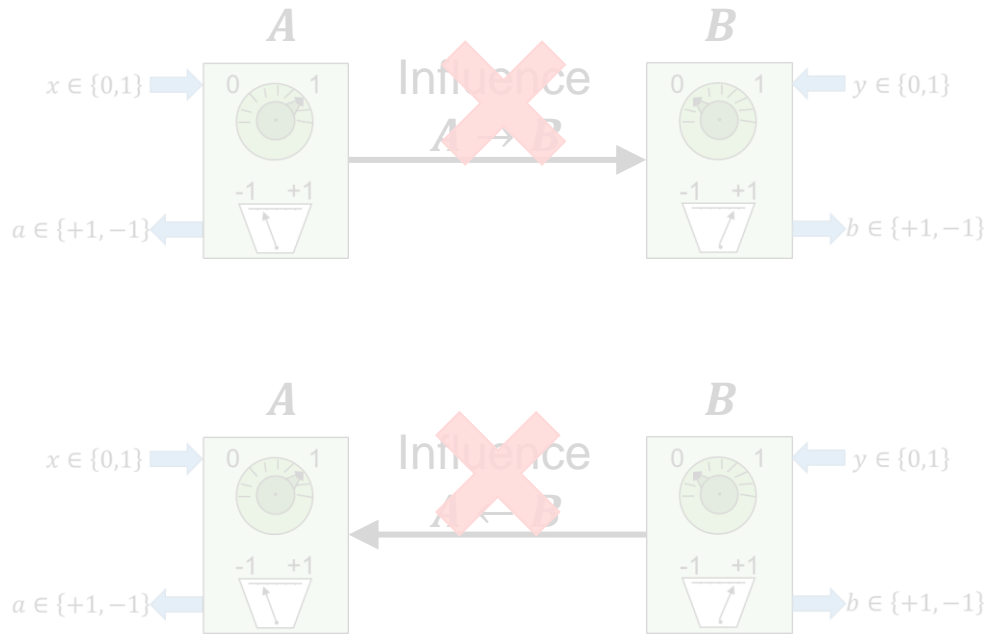
Space-like separation = Distance + Synchronization + no faster than light communications
= **No-Signalling Hypothesis**



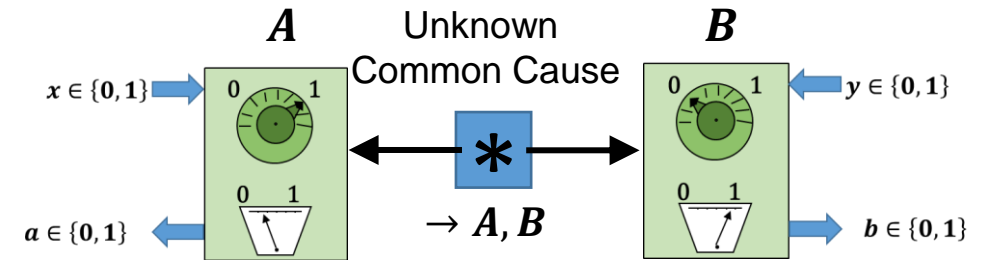
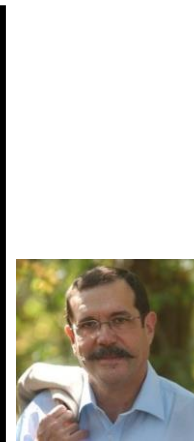
Correlations = Influence or Common Cause

Only two possibilities:

Influence

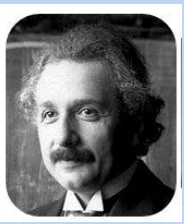


Common cause



- The experimentalist agrees with deduction: for him, it is $|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$

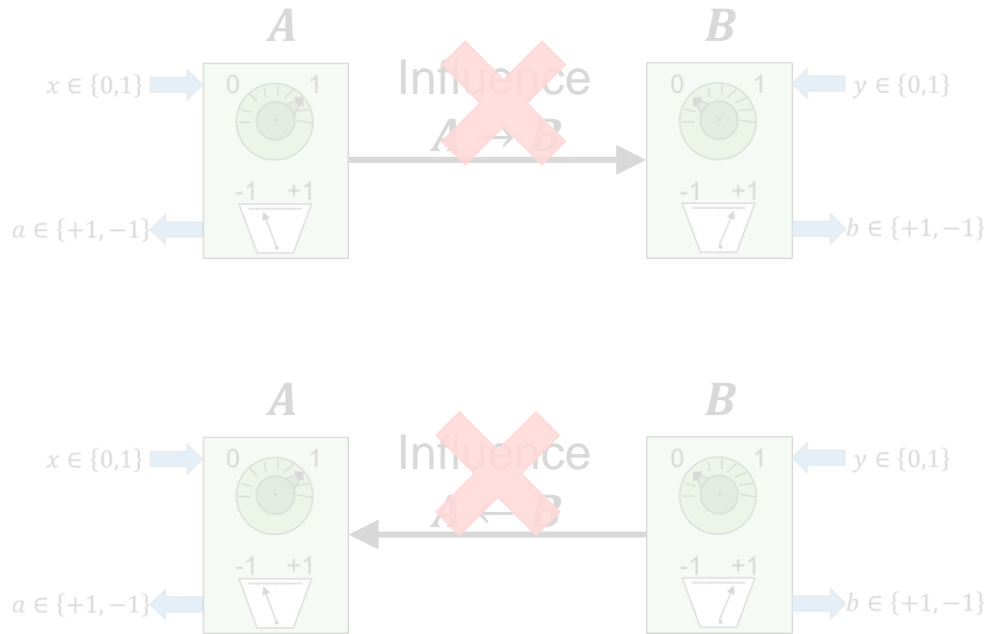
Space-like separation = Distance + Synchronisation
 = **No-Signalling Hypothesis**



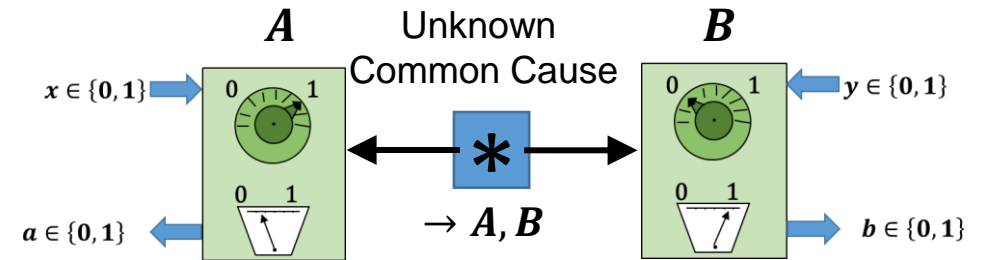
Correlations = Influence or Common Cause

Only two possibilities:

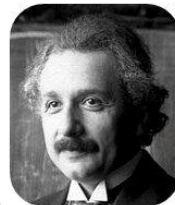
Influence



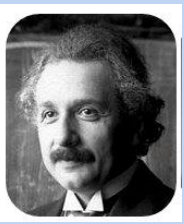
Common cause



- The experimentalist agrees with deduction: for him, it is $|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$
- For the detective, the detectors might not use the photons.



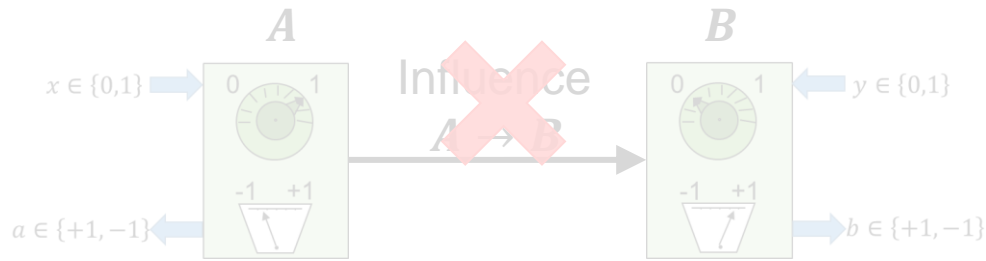
Space-like separation = Distance + Synchronisation
 = No-Signalling Hypothesis



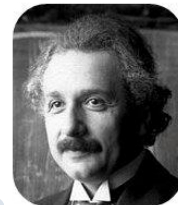
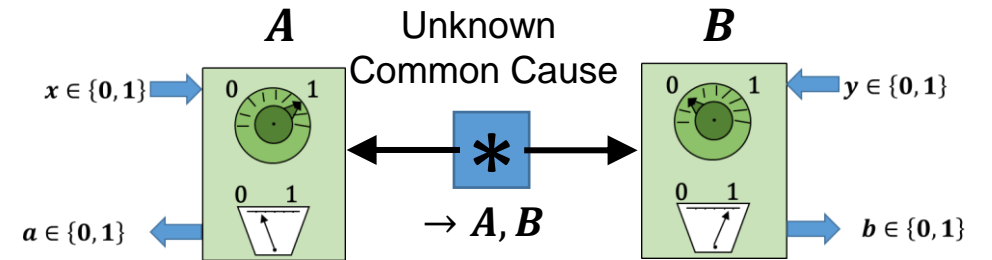
Correlations = Influence or Common Cause

Only two possibilities:

Influence

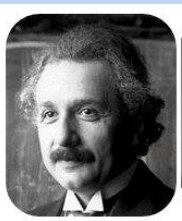


Common cause



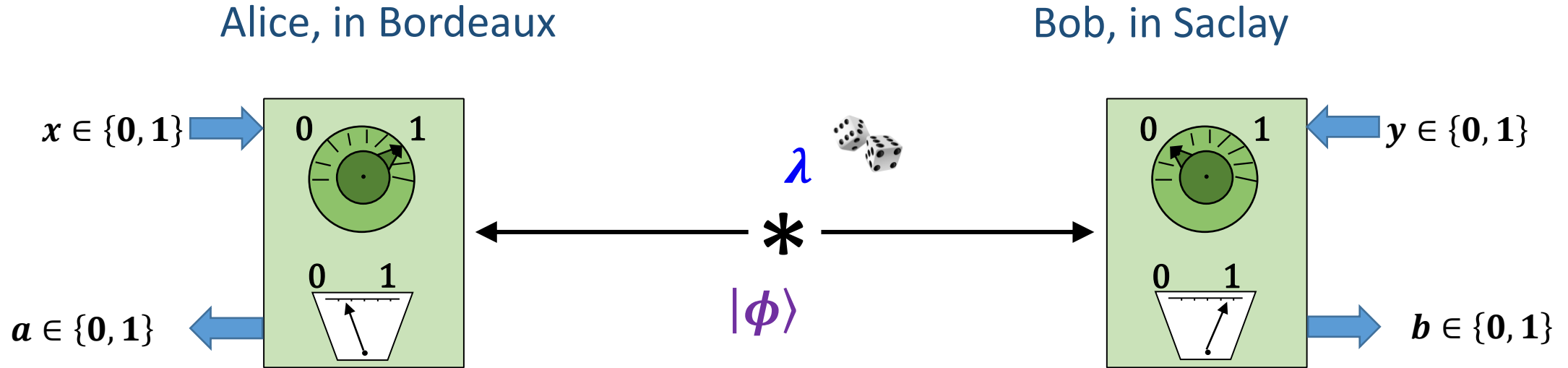
- The experimentalist **agrees** with deduction: for him, it is $|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$
- For the detective, **the detectors might not use the photons.**
- Could be seismic vibrations, cosmic rays, ...
Whatever it is, this is the « Common Cause ».

Space-like separation = Distance + Synchronisation
= **No-Signalling Hypothesis**



The CHSH experiment

as observed by the detective



We must have a pre-established source of correlations

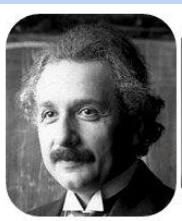
Classical source

local source of randomness λ

\neq

Quantum source $|\phi\rangle$



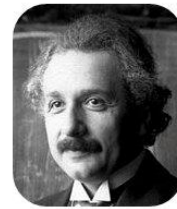


CHSH inequality

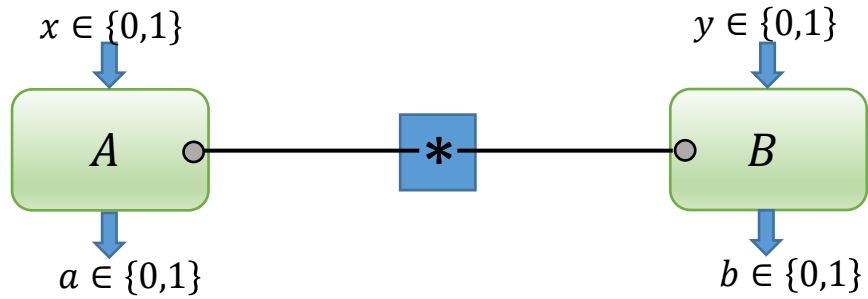
The detective model: LHV model

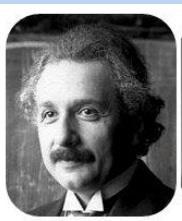
Local Hidden Variable model

= 'classical physics' = 'shared randomness'



Local strategies





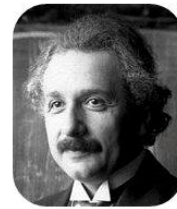
CHSH inequality

The detective model: LHV model

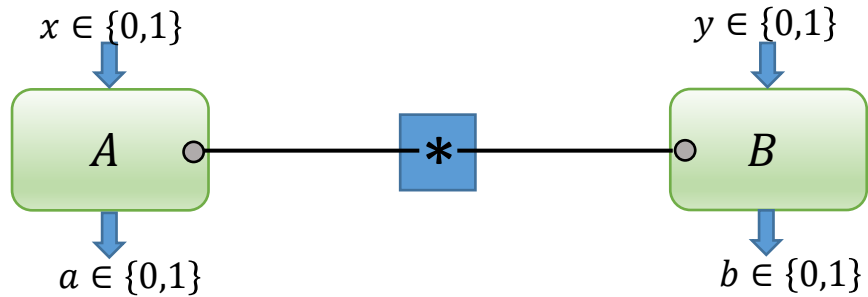
Local Hidden Variable model

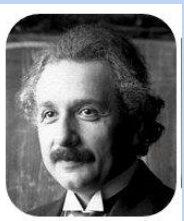
= 'classical physics' = 'shared randomness'

- Two carriers of information **travel contiguously** from source to parties



Local strategies



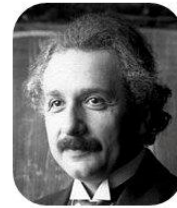


CHSH inequality

The detective model: LHV model

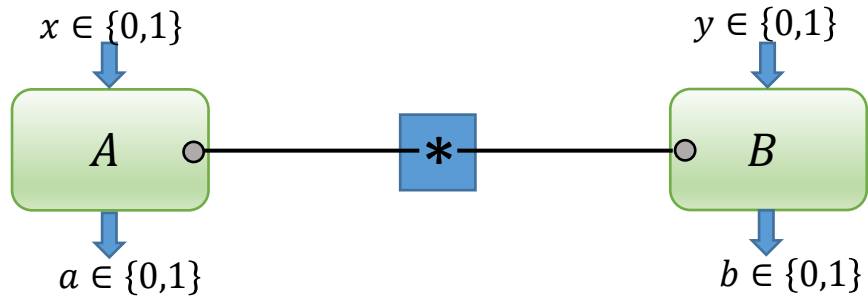
Local Hidden Variable model

= 'classical physics' = 'shared randomness'



- Two carriers of information **travel contiguously** from source to parties
- Each party measures one of the two

Local strategies



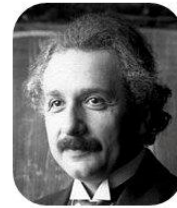


CHSH inequality

The detective model: LHV model

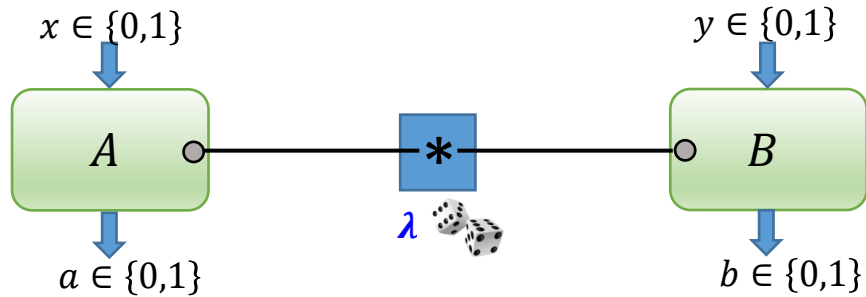
Local Hidden Variable model

= 'classical physics' = 'shared randomness'



- Two carriers of information **travel contiguously** from source to parties
- Each party measures one of the two
 - λ : carried information. It takes value λ_1 **or** λ_2 **or** ... : shared randomness distributed as $d\lambda$

Local strategies



The experimentalist **does not agree** with this second detective deduction

In $|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$, even far, the two photons are "one system"

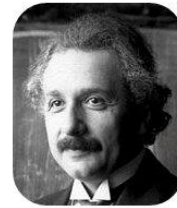


CHSH inequality

The detective model: LHV model

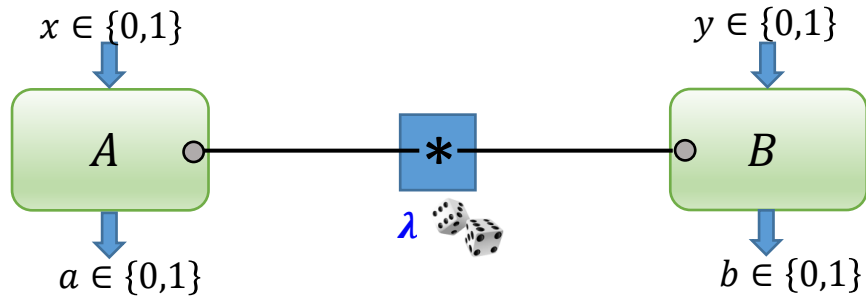
Local Hidden Variable model

= 'classical physics' = 'shared randomness'



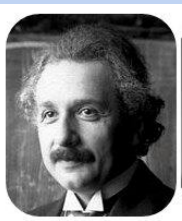
- Two carriers of information **travel contiguously** from source to parties
- Each party measures one of the two
 - λ : carried information. It takes value λ_1 **or** λ_2 **or** ... : shared randomness distributed as $d\lambda$
 - a is a function of x, λ
 - b is a function of y, λ

Local strategies



The experimentalist **does not agree** with this second detective deduction

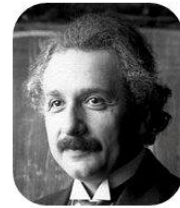
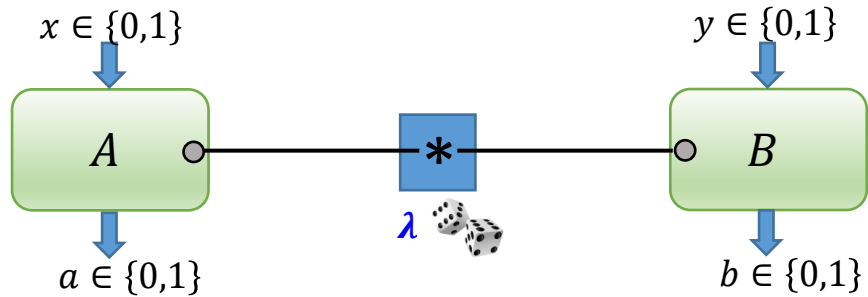
In $|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$, even far, the two photons are "one system"



CHSH inequality

The detective model: LHV model

Local strategies



Local Hidden Variable model

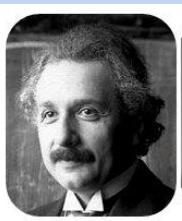
= 'classical physics' = 'shared randomness'

- Two carriers of information **travel contiguously** from source to parties
- Each party measures one of the two
 - λ : carried information. It takes value λ_1 **or** λ_2 **or** ... : shared randomness distributed as $d\lambda$
 - a is a function of x, λ
 - b is a function of y, λ
 - $p(ab|xy) = \int d\lambda p(a|x\lambda)p(b|y\lambda)$



The experimentalist **does not agree** with this second detective deduction

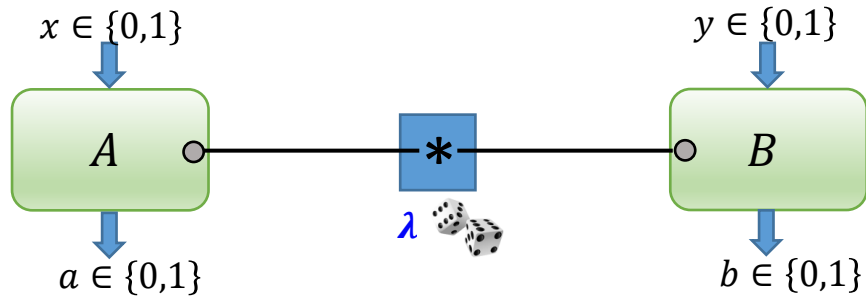
In $|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$, even far, the two photons are "one system"



CHSH inequality

The detective model: LHV model

Local strategies

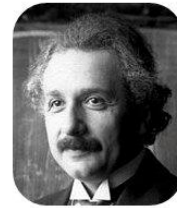


The experimentalist **does not agree** with this second detective deduction

In $|\psi^+\rangle = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$, even far, the two photons are “one system”

Local Hidden Variable model

= ‘classical physics’ = ‘shared randomness’

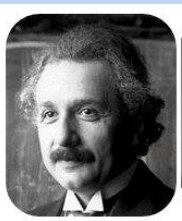


- Two carriers of information **travel contiguously** from source to parties
- Each party measures one of the two
 - λ : carried information. It takes value λ_1 **or** λ_2 **or** ... : shared randomness distributed as $d\lambda$
 - a is a function of x, λ
 - b is a function of y, λ
 - $p(ab|xy) = \int d\lambda p(a|x\lambda)p(b|y\lambda)$

Bell Theorem [CHSH]:

1. **For any** LHV model λ :

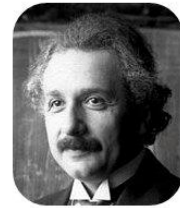
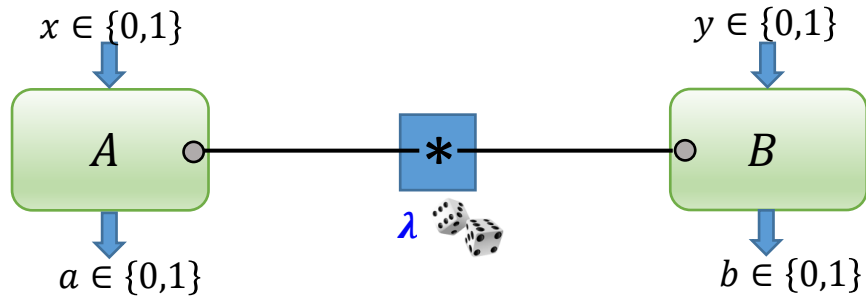
$$S = p(a \oplus b = x \cdot y) \leq \frac{3}{4} = 0.75$$



CHSH inequality

The detective model: LHV model

Local strategies



Local Hidden Variable model

= 'classical physics' = 'shared randomness'

- Two carriers of information **travel contiguously** from source to parties
- Each party measures one of the two
 - λ : carried information. It takes value λ_1 **or** λ_2 **or** ... : shared randomness distributed as $d\lambda$
 - a is a function of x, λ
 - b is a function of y, λ
 - $p(ab|xy) = \int d\lambda p(a|x\lambda)p(b|y\lambda)$

Bell Theorem [CHSH]:

1. **For any** LHV model λ :

$$S = p(a \oplus b = x \cdot y) \leq \frac{3}{4} = 0.75$$

PROOF (1.):

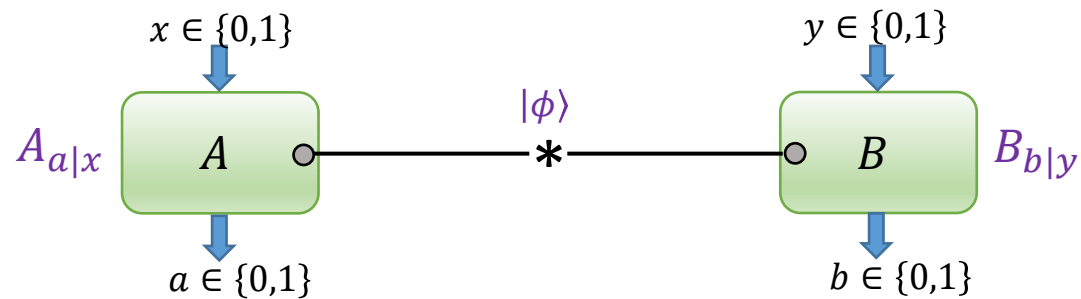
- $p(ab|xy)$ is a linear superposition of deterministic strategies
- Deterministic strategies have $S \leq \frac{3}{4}$
- $S = p(a \oplus b = x \cdot y)$ is a linear score

CHSH inequality

Quantum model



Quantum strategy



Quantum strategy

- The parties share a quantum state $|\phi\rangle$
- They have measurement operators $A_{a|x}, B_{b|y}$

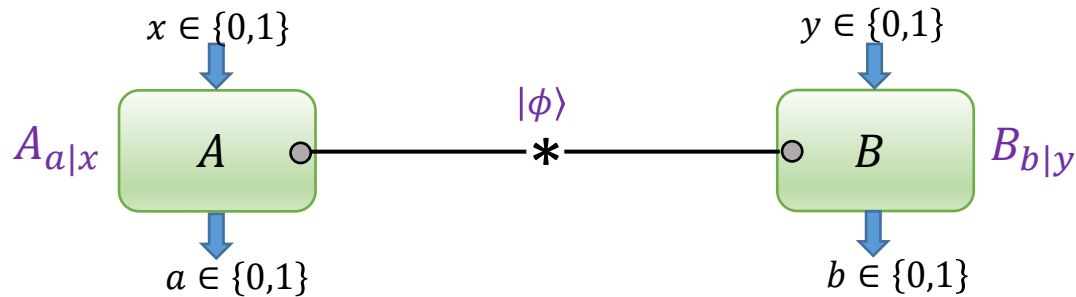
- The observation probabilities are:
$$p(ab|xy) = \langle \phi | A_{a|x} \otimes B_{b|y} | \phi \rangle$$

CHSH inequality

Quantum model



Quantum strategy



Quantum strategy

- The parties share a quantum state $|\phi\rangle$
- They have measurement operators $A_{a|x}, B_{b|y}$
- The observation probabilities are:
$$p(ab|xy) = \langle \phi | A_{a|x} \otimes B_{b|y} | \phi \rangle$$

Bell Theorem [CHSH, 1964, 1969]:

1. For any LHV model λ :

$$S = p(a \oplus b = x \cdot y) \leq \frac{3}{4} = 0.75$$

2. For some quantum strategy:

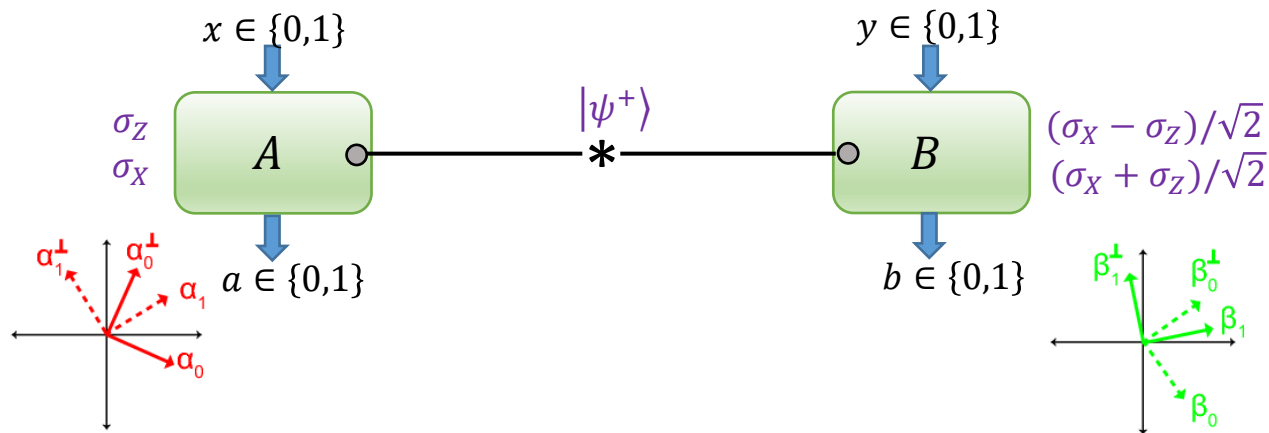
$$S = p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$$

CHSH inequality

Quantum model



Quantum strategy



Quantum strategy

- The parties share a quantum state $|\phi\rangle$
- They have measurement operators $A_{a|x}, B_{b|y}$
- The observation probabilities are:

$$p(ab|xy) = \langle \phi | A_{a|x} \otimes B_{b|y} | \phi \rangle$$

Bell Theorem [CHSH, 1964, 1969]:

1. For any LHV model λ :

$$S = p(a \oplus b = x \cdot y) \leq \frac{3}{4} = 0.75$$

2. For some quantum strategy:

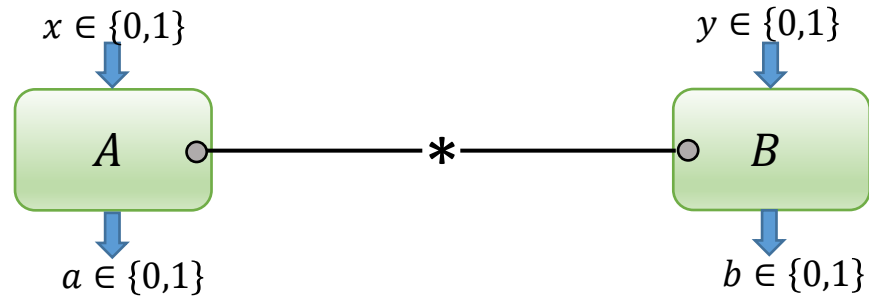
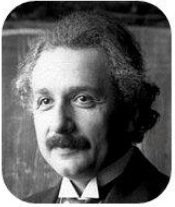
$$S = p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$$

PROOF (2.):

- $|\phi\rangle = |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- Alice measures σ_Z, σ_X
- Bob measures $\frac{\sigma_X \pm \sigma_Z}{\sqrt{2}}$

CHSH inequality

Quantum model



Quantum strategy

- The parties share a quantum state $|\phi\rangle$
- They have measurement operators $A_{a|x}, B_{b|y}$
- The observation probabilities are:
 $p(ab|xy) = \langle \phi | A_{a|x} \otimes B_{b|y} | \phi \rangle$

Bell Theorem [CHSH, 1964, 1969]:

1. For any LHV model λ :

$$S = p(a \oplus b = x \cdot y) \leq \frac{3}{4} = 0.75$$

2. For some quantum strategy:

$$S = p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$$

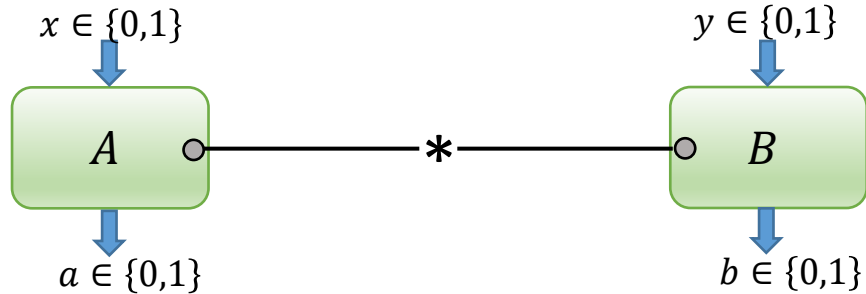
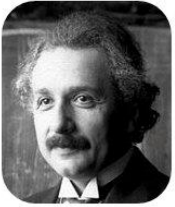
PROOF (2.) [for the detective] :

Look at the experiment, **no need to understand quantum theory!**

➤ Bell theorem is 'not about' quantum theory

CHSH inequality

Quantum model



Quantum strategy

- The parties share a quantum state $|\phi\rangle$
- They have measurement operators $A_{a|x}, B_{b|y}$
- The observation probabilities are:
$$p(ab|xy) = \langle \phi | A_{a|x} \otimes B_{b|y} | \phi \rangle$$

Bell Theorem [CHSH, 1964, 1969]:

1. For any LHV model λ :

$$S = p(a \oplus b = x \cdot y) \leq \frac{3}{4} = 0.75$$

2. For some quantum strategy:

$$S = p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$$

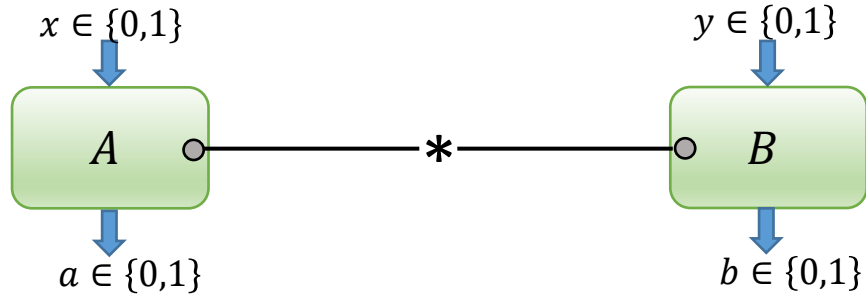
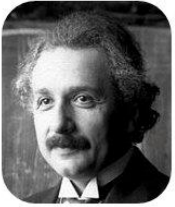
PROOF (2.) [for the detective] :

Look at the experiment, **no need to understand quantum theory!**

- Bell theorem is **'not about'** quantum theory
- Bell theorem is **about** any theory of physics explaining **operational observations**

CHSH inequality

Quantum model



Quantum strategy

- The parties share a quantum state $|\phi\rangle$
- They have measurement operators $A_{a|x}, B_{b|y}$
- The observation probabilities are:
$$p(ab|xy) = \langle \phi | A_{a|x} \otimes B_{b|y} | \phi \rangle$$

Bell Theorem [CHSH, 1964, 1969]:

1. For any LHV model λ :

$$S = p(a \oplus b = x \cdot y) \leq \frac{3}{4} = 0.75$$

2. For some quantum strategy:

$$S = p(a \oplus b = x \cdot y) = \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$$

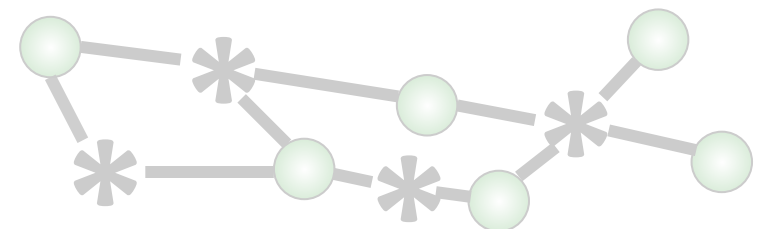
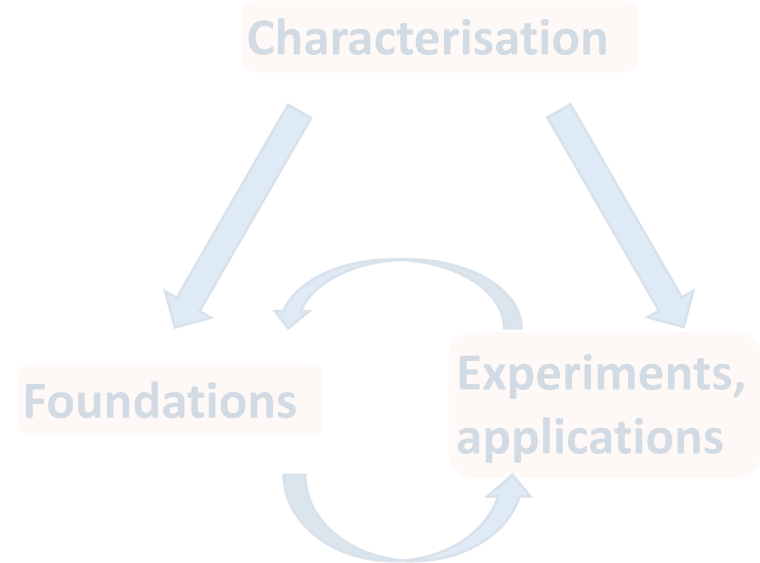
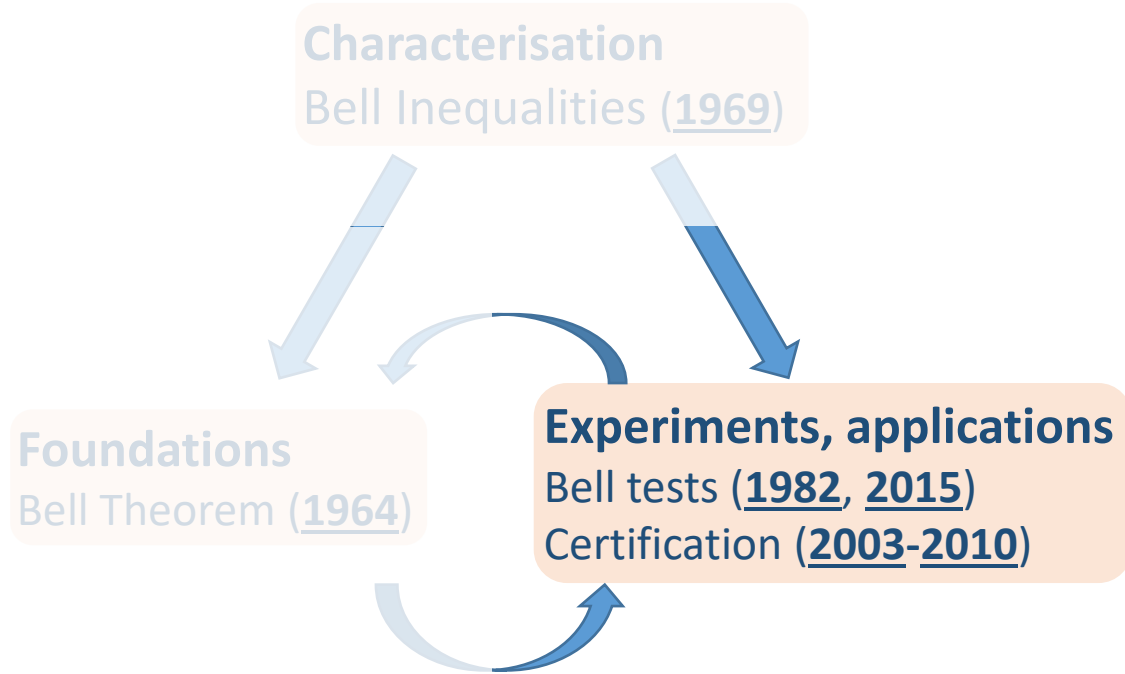
PROOF (2.) [for the detective] :

Look at the experiment, **no need to understand quantum theory!**

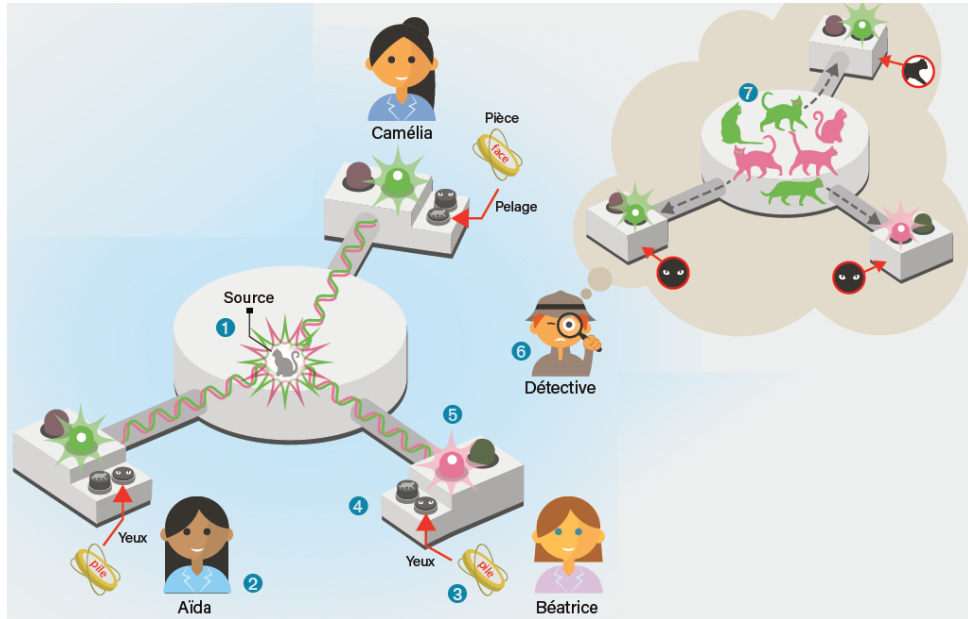
- Bell theorem is **'not about'** quantum theory
- Bell theorem is **about** any theory of physics explaining **operational observations**
- Such theory must be **more crazy than any crazy explanation compatible with the classical principles**

Overview

Single state quantum correlations



Consequences for Physics foundations, applications



M-O. Renou, N. Brunner, N. Gisin, La non-localité quantique à l'ère des réseaux
Pour la Science Octobre 2021

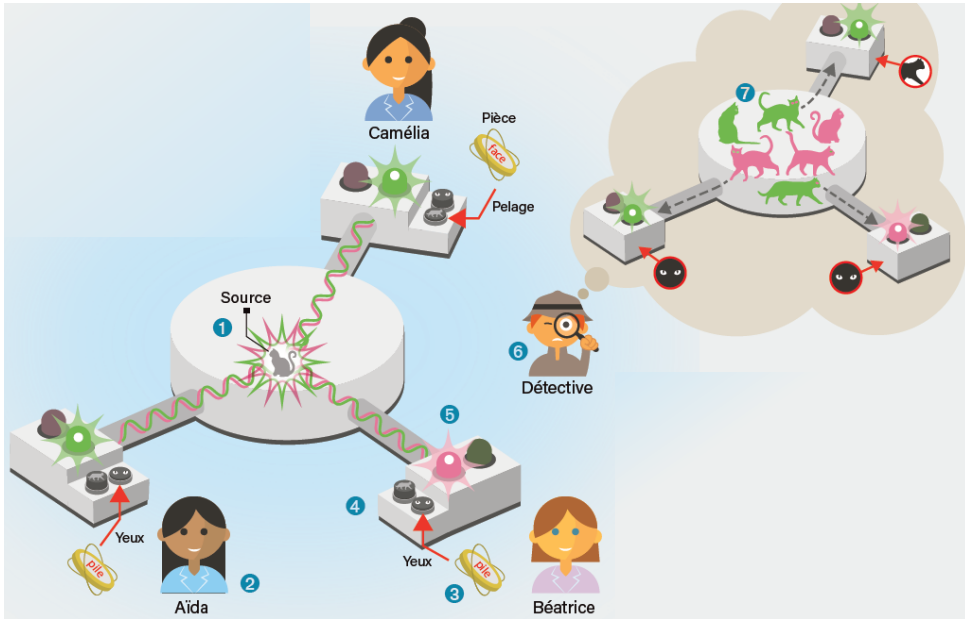
Any theory of physics explaining operational observations:

- Is Nonlocal
- Is Contextual
- Does not allow cloning of information
- Is non determinist



Aspect experiment 1981

Consequences for Physics foundations, applications



M-O. Renou, N. Brunner, N. Gisin, La non-localité quantique à l'ère des réseaux
Pour la Science Octobre 2021



Aspect experiment 1981



Commercial Quantum Random Number Generator

Any theory of physics explaining operational observations:

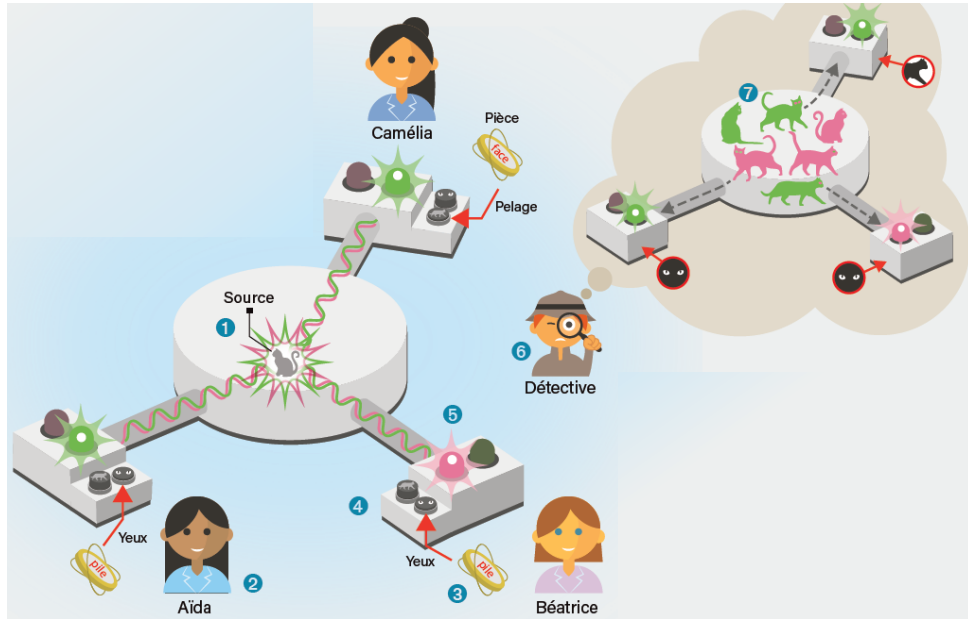
- Is Nonlocal
- Is Contextual
- Does not allow cloning of information
- Is non determinist

Applications :

Can be certified *Device Independently*, from the observed correlations only, even if an adversary controls the devices

- Nonlocality
 - DI certification of quantum devices (2003)
- No cloning
 - DI quantum key distribution (2007)
- Non determinist
 - DI quantum random number generation (2010)

Consequences for Physics foundations, applications



M-O. Renou, N. Brunner, N. Gisin, La non-localité quantique à l'ère des réseaux
Pour la Science Octobre 2021



Aspect experiment 1981



Commercial Quantum Random Number Generator

Any theory of physics explaining operational observations:

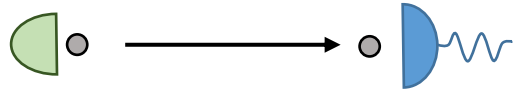
- Is Nonlocal
- Is Contextual
- **Does not allow cloning of information**
- Is non determinist

Applications :

Can be certified *Device Independently*, from the observed correlations only, even if an adversary controls the devices

- Nonlocality
 - DI certification of quantum devices (2003)
- **No cloning**
 - **DI quantum key distribution (2007)**
- Non determinist
 - DI quantum random number generation (2010)

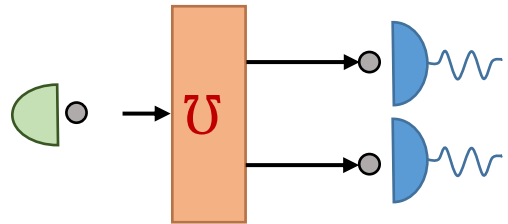
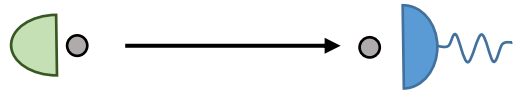
No-cloning from Bell theorem



What is a cloner?

- Causal process with an information carrier traveling

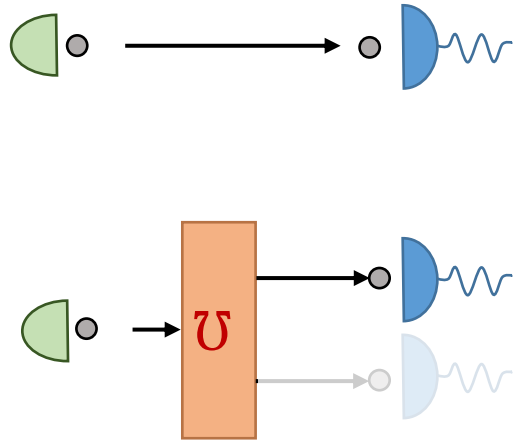
No-cloning from Bell theorem



What is a cloner?

- Causal process with an information carrier traveling
- Insert a cloner:
 - Process duplicated after the cloner

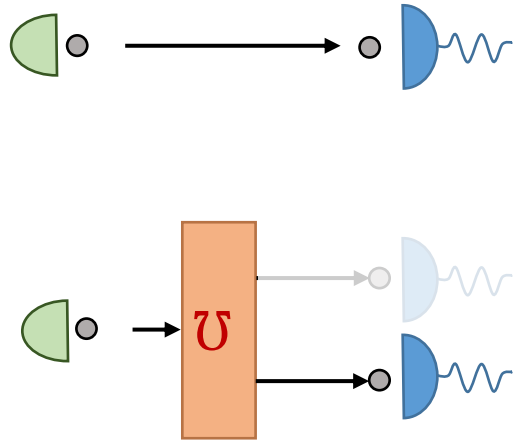
No-cloning from Bell theorem



What is a cloner?

- Causal process with an information carrier traveling
- Insert a cloner:
 - Process duplicated after the cloner
 - if one is ignored, we are back to the initial situation

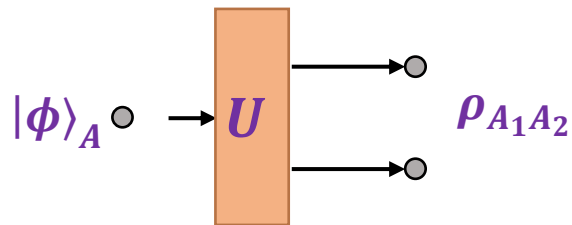
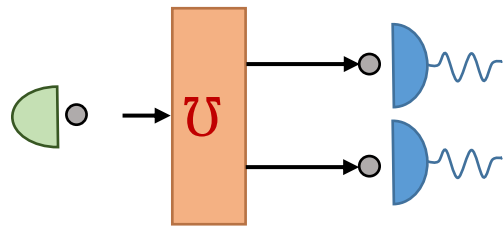
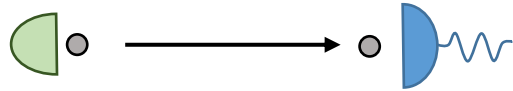
No-cloning from Bell theorem



What is a cloner?

- Causal process with an information carrier traveling
- Insert a cloner:
 - Process duplicated after the cloner
 - if one is ignored, we are back to the initial situation

No-cloning from Bell theorem



$$\text{s.t. } \rho_{A_1} := \text{Tr}_{A_2}(\rho_{A_1 A_2}) = |\phi\rangle_{A_1}$$
$$\rho_{A_2} := \text{Tr}_{A_1}(\rho_{A_1 A_2}) = |\phi\rangle_{A_2}$$

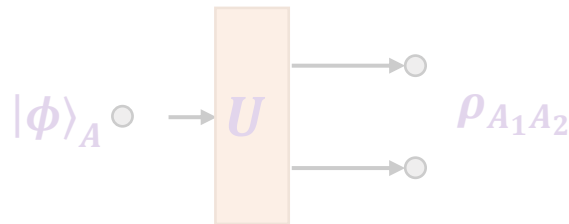
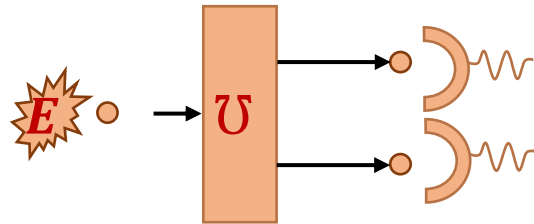
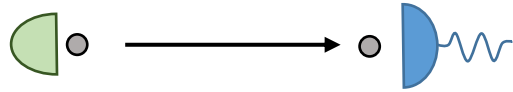
What is a cloner?

- Causal process with an information carrier traveling
- Insert a cloner:
 - Process duplicated after the cloner
 - if one is ignored, we are back to the initial situation

According to Quantum Theory

➤ Does not exist

No-cloning from Bell theorem



What is a cloner?

- Causal process with an information carrier traveling
- Insert a cloner:
 - Process duplicated after the cloner
 - if one is ignored, we are back to the initial situation

According to Quantum Theory

- Does not exist

According to an other 'reasonable theory'

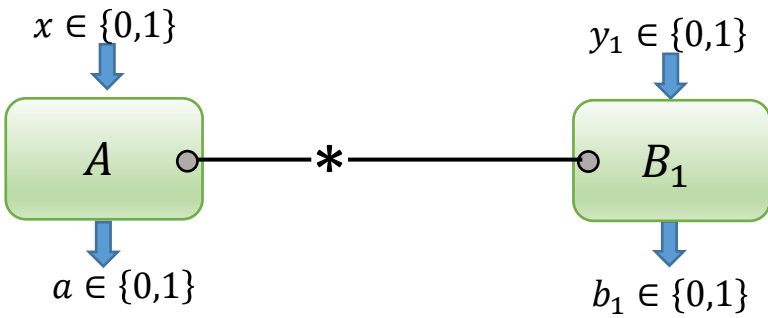
- Cannot exist!
- Consequence of Bell theorem

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) \approx 0.85$$

Proof by contradiction

- Start from the CHSH game

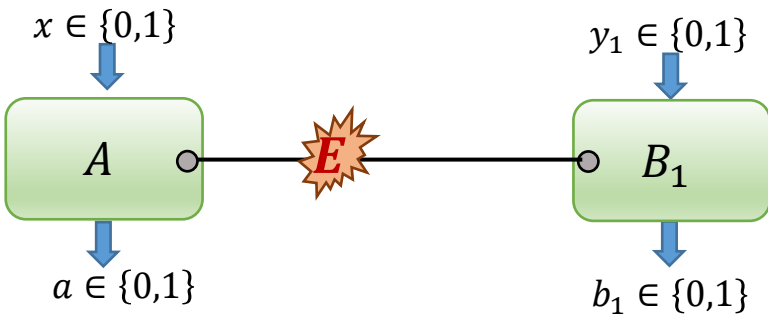


No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) \approx 0.85$$

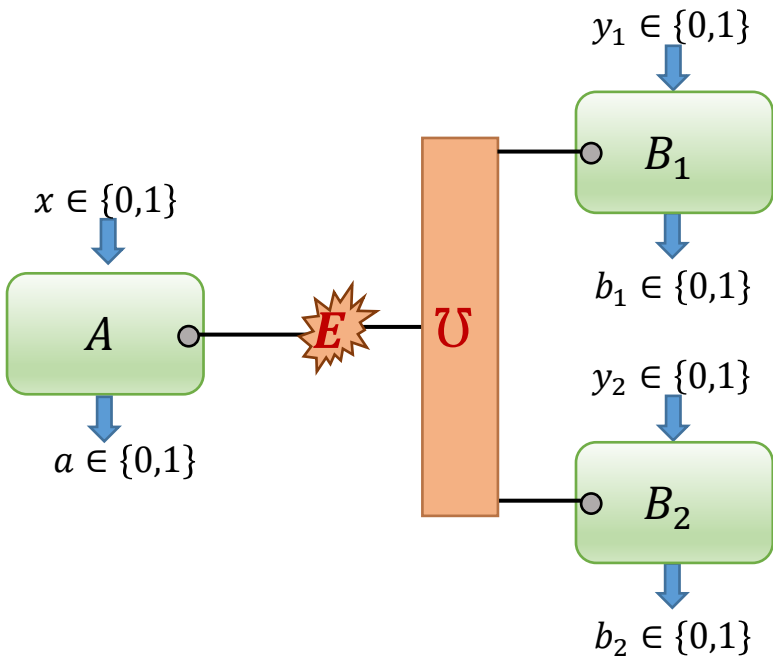
Proof by contradiction

- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning



No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) \approx 0.85$$

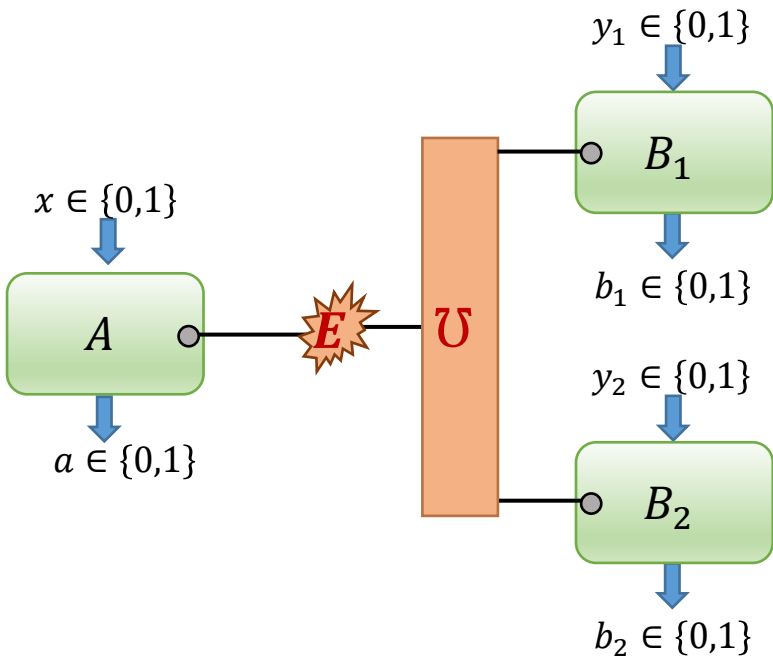


Proof by contradiction

- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) \approx 0.85$, $P(a \oplus b_2 = x \cdot y_2) \approx 0.85$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



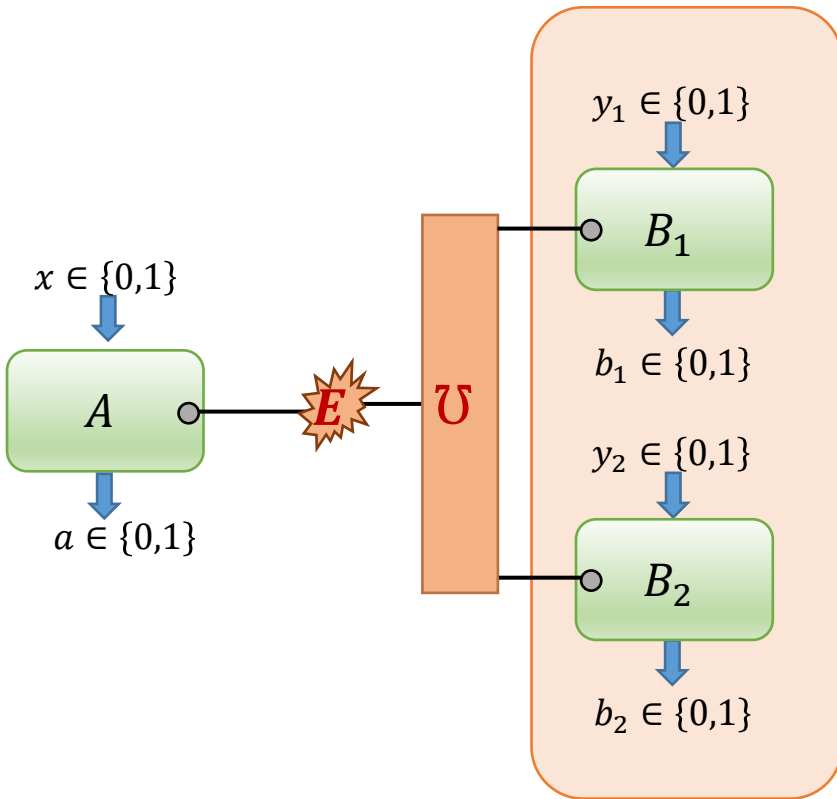
Proof by contradiction

- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof **0.85** \rightarrow **1**

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



Proof by contradiction

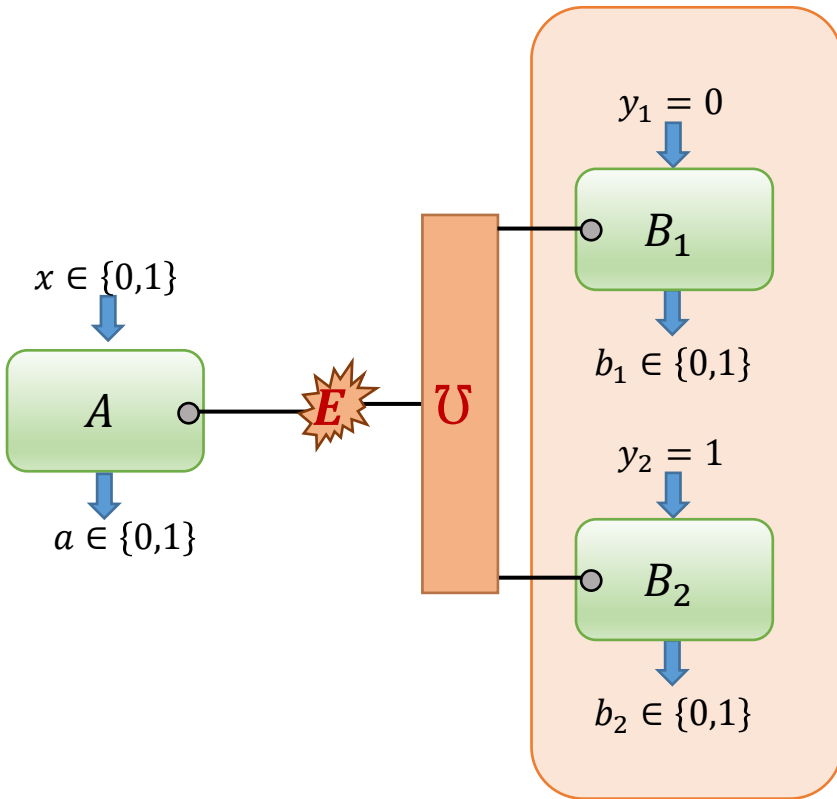
- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof **0.85** \rightarrow **1**

- Place B_1, B_2 in a same location:

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



Proof by contradiction

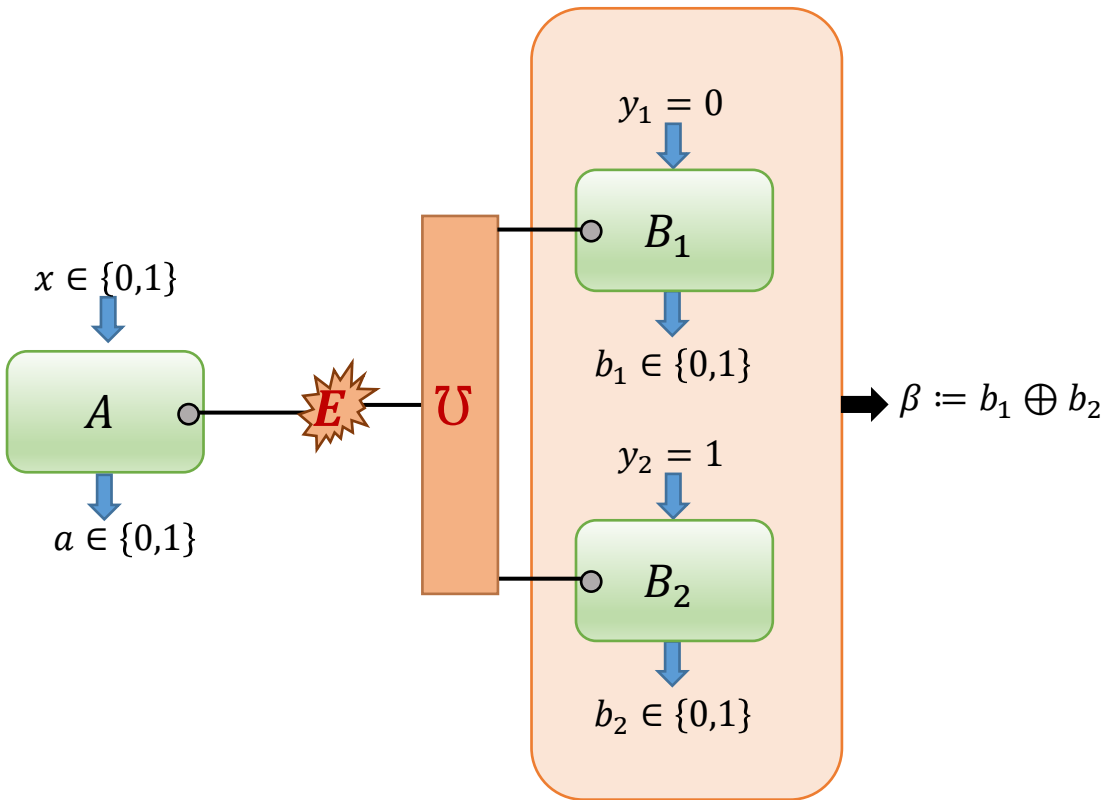
- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof **0.85** \rightarrow **1**

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



Proof by contradiction

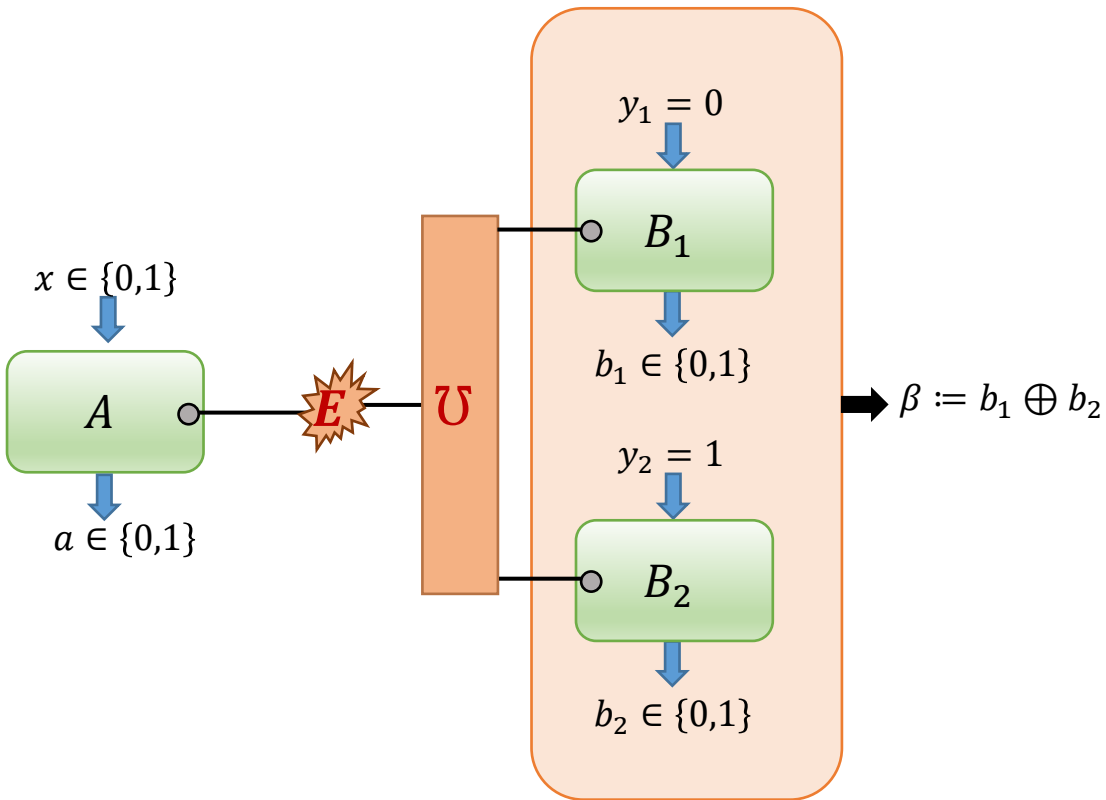
- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof 0.85 \rightarrow 1

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



We have:

$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0$$

Proof by contradiction

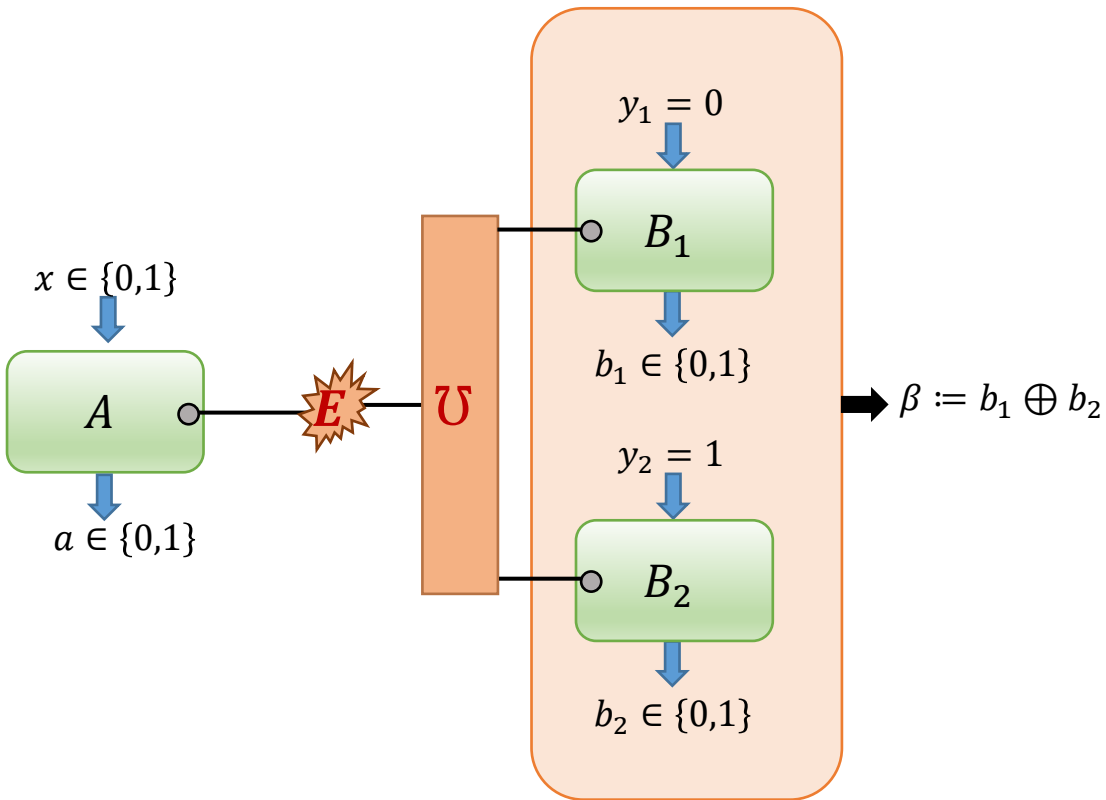
- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof **0.85** \rightarrow **1**

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



We have:

$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$

Proof by contradiction

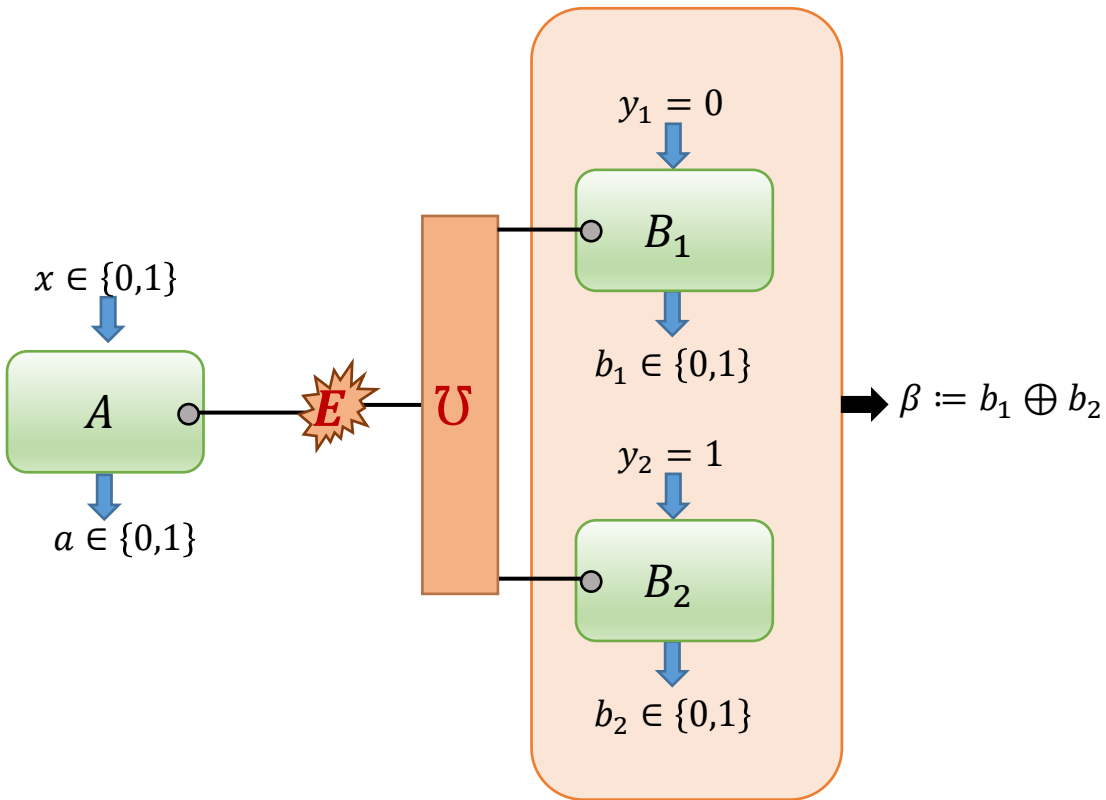
- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof **0.85** \rightarrow **1**

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



Proof by contradiction

- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof 0.85 \rightarrow 1

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$

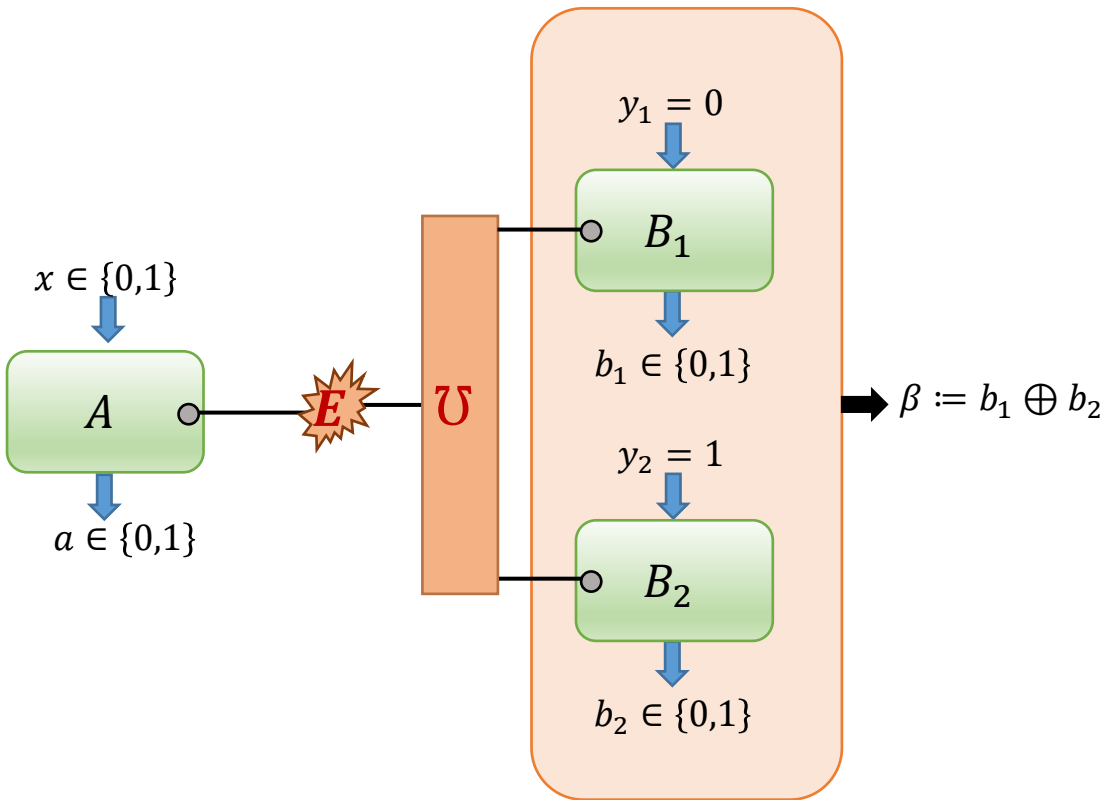
We have:

$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$

$$a \oplus b_2 = x \cdot y_2 = x \cdot 1 = x: b_1 = a \oplus x$$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



Proof by contradiction

- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof 0.85 \rightarrow 1

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$

We have:

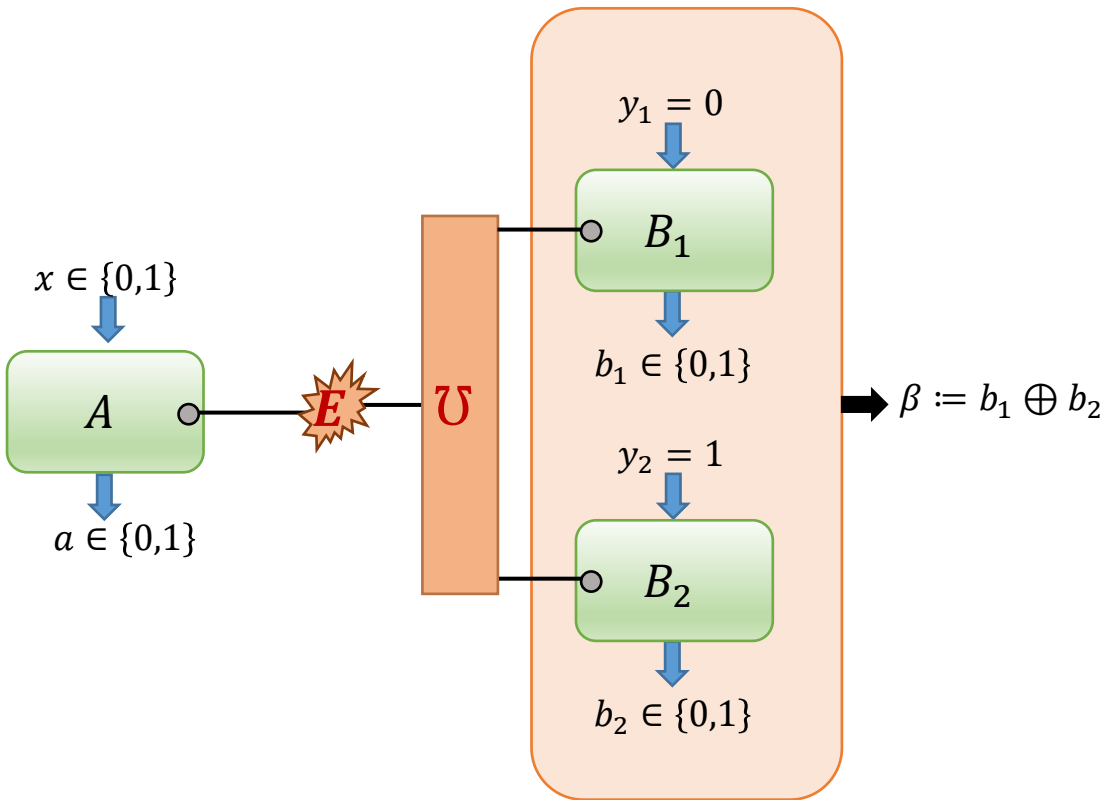
$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$

$$a \oplus b_2 = x \cdot y_2 = x \cdot 1 = x: b_1 = a \oplus x$$

$$\text{Hence } \beta = b_1 \oplus b_2 = a \oplus a \oplus x = x$$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



Proof by contradiction

- Start from the CHSH game
- Assume some 'reasonable' theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof **0.85** \rightarrow **1**

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$
 - Then $\beta = x$!

We have:

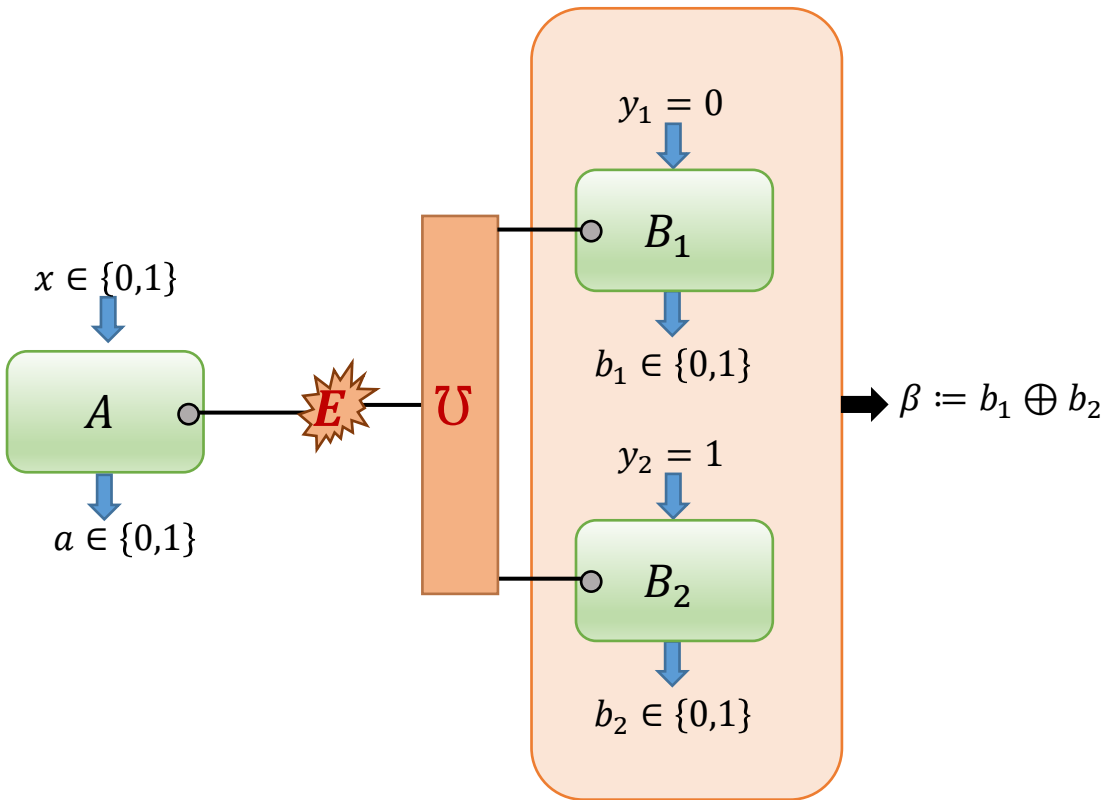
$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$

$$a \oplus b_2 = x \cdot y_2 = x \cdot 1 = x: b_1 = a \oplus x$$

$$\text{Hence } \beta = b_1 \oplus b_2 = a \oplus a \oplus x = x$$

No-cloning from Bell theorem


$$P(a \oplus b = x \cdot y) = 1$$



Proof by contradiction

- Start from the CHSH game
- Assume some ‘reasonable’ theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof 0.85 → 1

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$
 - Then $\beta = x!$
 - “Signalling”!  Not ‘reasonable’ !

We have:

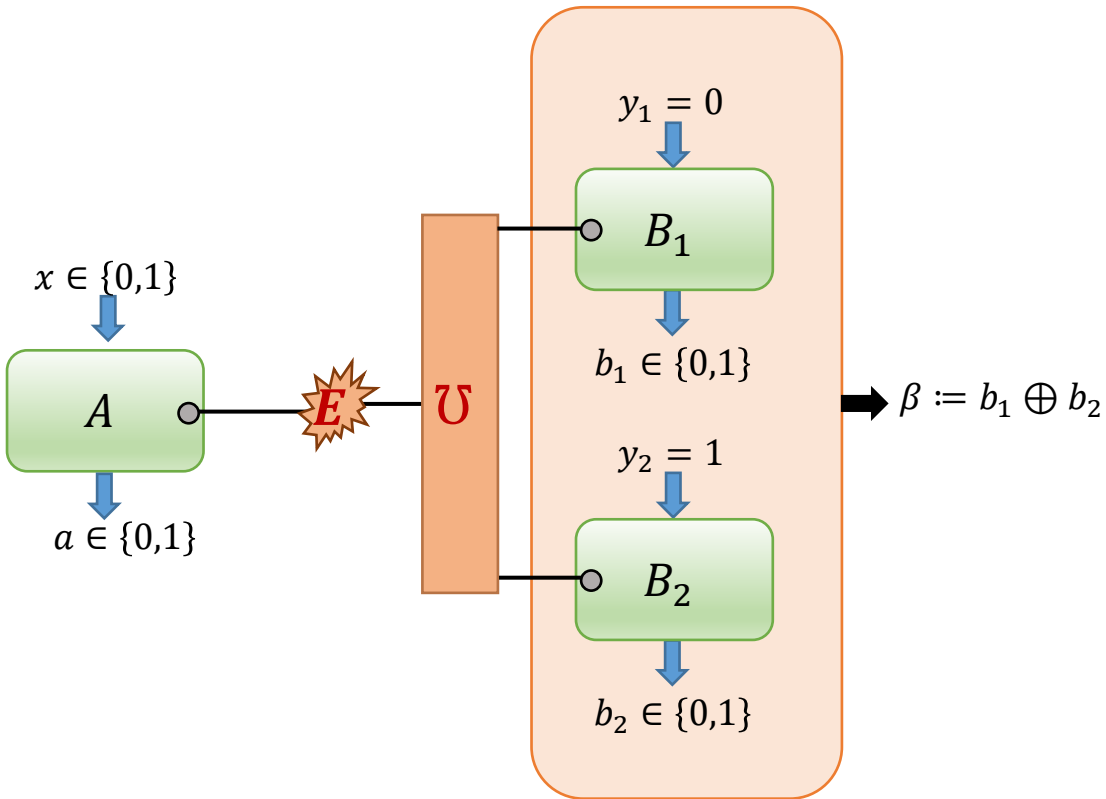
$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$

$$a \oplus b_2 = x \cdot y_2 = x \cdot 1 = x: b_1 = a \oplus x$$

$$\text{Hence } \beta = b_1 \oplus b_2 = a \oplus a \oplus x = x$$

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



We have:

$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$


$$a \oplus b_2 = x \cdot y_2 = x \cdot 1 = x: b_1 = a \oplus x$$

$$\text{Hence } \beta = b_1 \oplus b_2 = a \oplus a \oplus x = x$$

Proof by contradiction

- Start from the CHSH game
- Assume some ‘reasonable’ theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof 0.85 \rightarrow 1

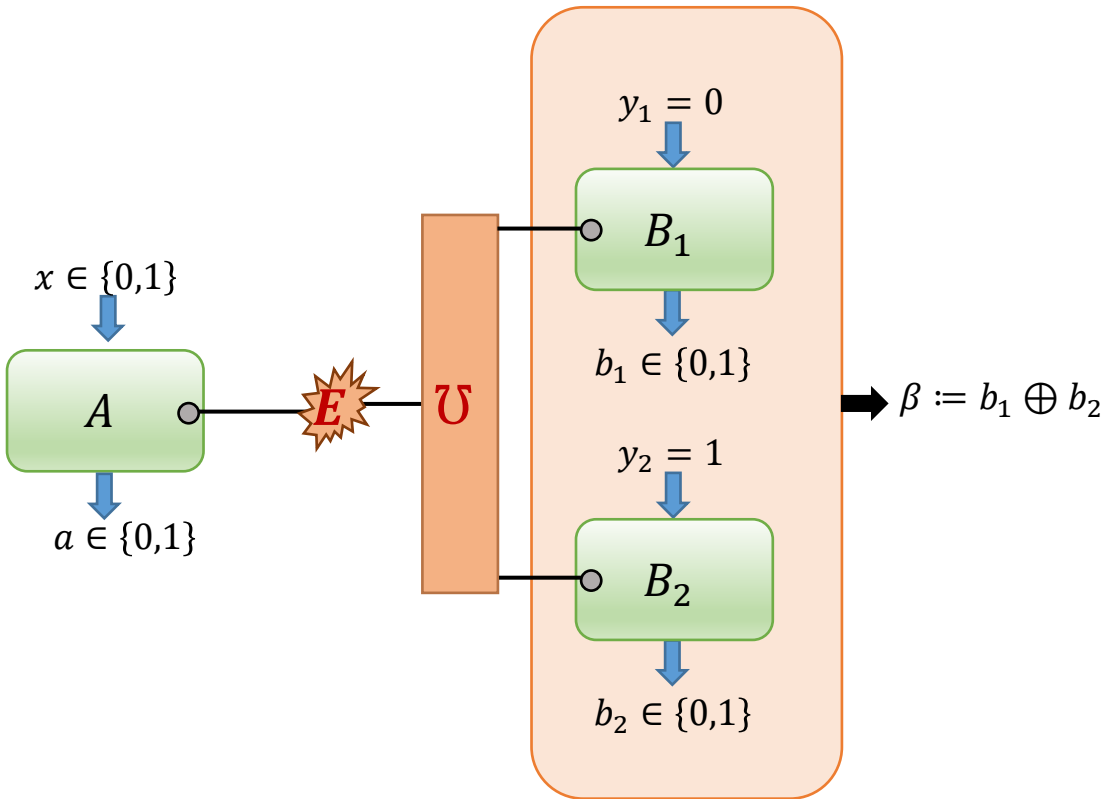
- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$
 - Then $\beta = x$!
 - “Signalling”!  Not ‘reasonable’ !

Without simplification? 0.85

- With **1** : ‘maximally signalling’

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



We have:

$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$


$$a \oplus b_2 = x \cdot y_2 = x \cdot 1 = x: b_1 = a \oplus x$$

$$\text{Hence } \beta = b_1 \oplus b_2 = a \oplus a \oplus x = x$$

Proof by contradiction

- Start from the CHSH game
- Assume some ‘reasonable’ theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof 0.85 → 1

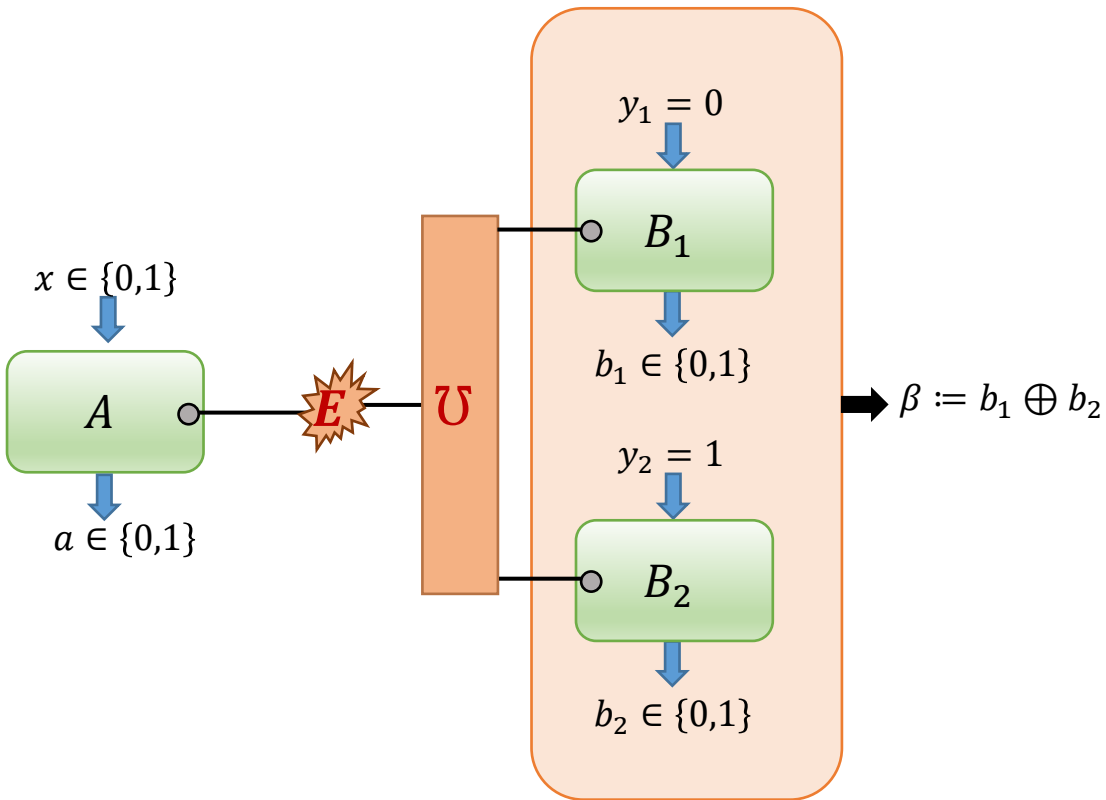
- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$
 - Then $\beta = x$!
 - “Signalling”!  Not ‘reasonable’ !

Without simplification? 0.85

- With 1 : ‘maximally signalling’
- ‘ ϵ signalling’ is already not reasonable as can be amplified

No-cloning from Bell theorem

$$P(a \oplus b = x \cdot y) = 1$$



We have:

$$a \oplus b_1 = x \cdot y_1 = x \cdot 0 = 0: b_1 = a$$


$$a \oplus b_2 = x \cdot y_2 = x \cdot 1 = x: b_1 = a \oplus x$$

$$\text{Hence } \beta = b_1 \oplus b_2 = a \oplus a \oplus x = x$$

Proof by contradiction

- Start from the CHSH game
- Assume some ‘reasonable’ theory of physics explains it and allows for cloning
- Insert the cloner:
 - obtain $P(a, b_1, b_2 | x, y_1, y_2)$
 - such that $P(a \oplus b_1 = x \cdot y_1) = 1$, $P(a \oplus b_2 = x \cdot y_2) = 1$

Simplification of the proof 0.85 \rightarrow 1

- Place B_1, B_2 in a same location:
 - take $y_1 = 0, y_2 = 1$, output $\beta := b_1 \oplus b_2$
 - Then $\beta = x$!
 - “Signalling”!  Not ‘reasonable’ !

Without simplification? 0.85

- With **1** : ‘maximally signalling’
- ‘ ϵ signalling’ is already not reasonable as can be amplified
- As soon as **CHSH** $>$ **2**, the proof holds: no ‘reasonable’ theory of physics with cloning can explain any CHSH violation

Device independence

General idea

Proofs that “*any reasonable future theory of physics*” satisfies:

Non locality / Randomness / No cloning / ...

Device independence

General idea

Proofs that “*any reasonable future theory of physics*” satisfies:

Non locality / Randomness / No cloning / ...

Proofs of the correct working of practical devices:

Quantum Randomness / Quantum Cryptography / ...

Device independence

General idea

Proofs that “*any reasonable future theory of physics*” satisfies:

Non locality / Randomness / No cloning / ...

Proofs of the correct working of practical devices:

Quantum Randomness / Quantum Cryptography / ...

Proofs valid under very weak hypothesis:

X Trusted sources / measurements

X Trusted Quantum Theory

Device independence

General idea

Proofs that “*any reasonable future theory of physics*” satisfies:

Non locality / Randomness / No cloning / ...

Proofs of the correct working of practical devices:

Quantum Randomness / Quantum Cryptography / ...

Proofs valid under very weak hypothesis:

~~X Trusted sources / measurements~~

~~X Trusted Quantum Theory (except some applications)~~

Device independence

General idea

Proofs that “*any reasonable future theory of physics*” satisfies:

Non locality / Randomness / No cloning / ...

Proofs of the correct working of practical devices:

Quantum Randomness / Quantum Cryptography / ...

Proofs valid under very weak hypothesis:

~~X Trusted sources / measurements~~

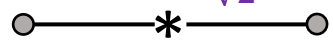
~~X Trusted Quantum Theory (except some applications)~~

✓ **No Signalling**

✓ **No super-determinism**

Device independence

Foundational physics

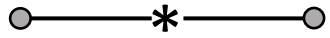
$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$


- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties
 - Entanglement

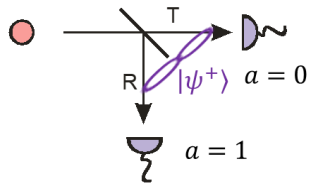
Device independence

Foundational physics

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$



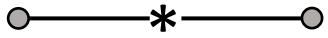
- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties
 - Entanglement
 - Intrinsic randomness



Device independence

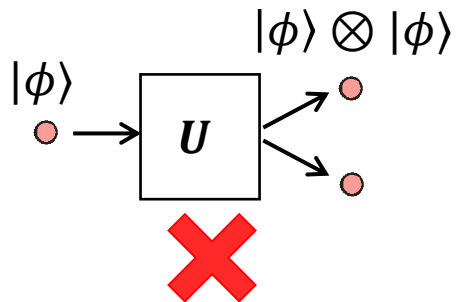
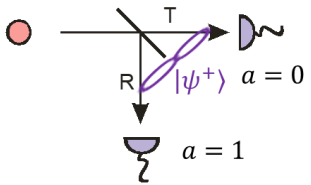
Foundational physics

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$



- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties

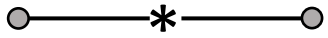
- Entanglement
- Intrinsic randomness
- No cloning of information



Device independence

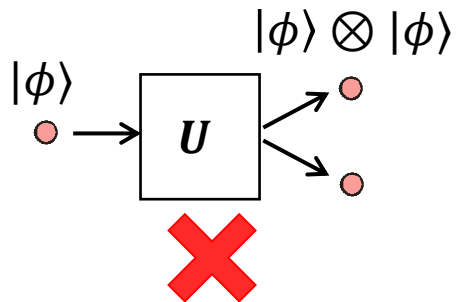
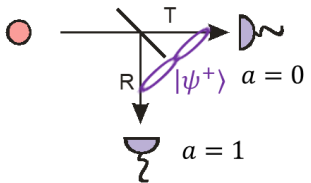
Foundational physics

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$



- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties

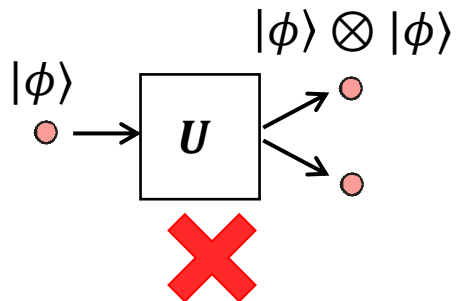
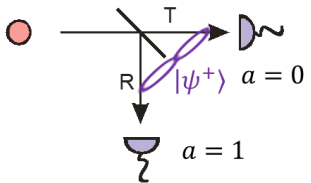
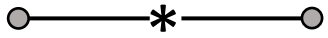
- Entanglement
- Intrinsic randomness
- No cloning of information
- ...



Device independence

Foundational physics

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

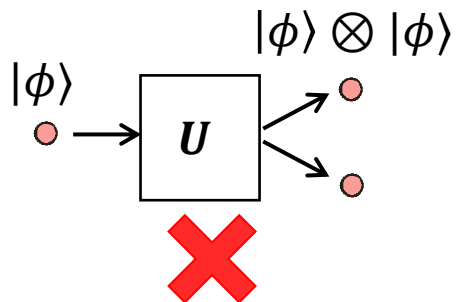
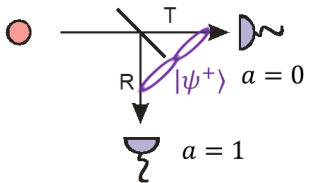
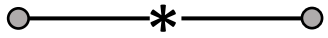


- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties
 - Entanglement
 - Intrinsic randomness
 - No cloning of information
 - ...
- Can we imagine a **future theory** which:
 - Does not have these ‘unpleasant’ properties
 - Is consistent with the CHSH game

Device independence

Foundational physics

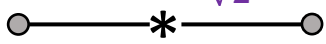
$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

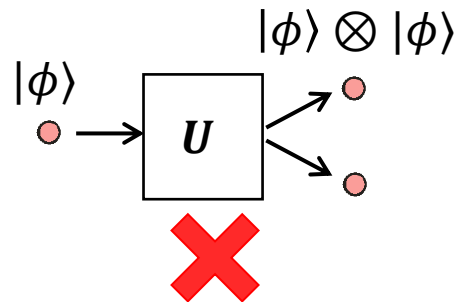
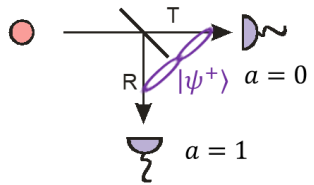
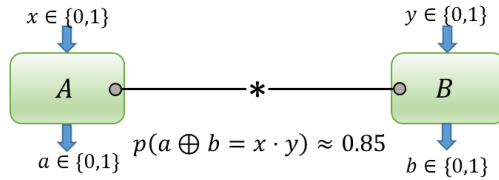


- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties
 - Entanglement
 - Intrinsic randomness
 - No cloning of information
 - ...
 - Can we imagine a **future theory** which:
 - Does not have these ‘unpleasant’ properties
 - Is consistent with the CHSH game
- Corollaries of Bell theorem : No!

Device independence

Foundational physics

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$


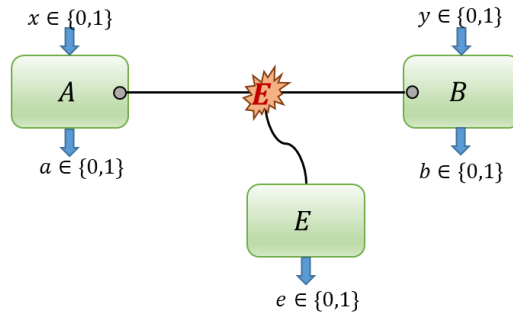
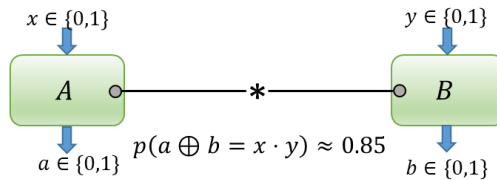
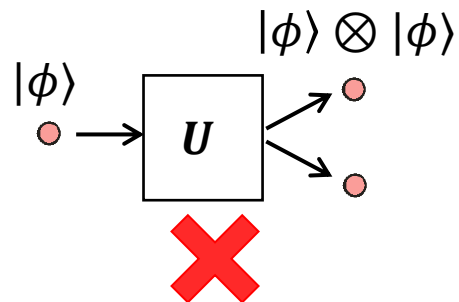
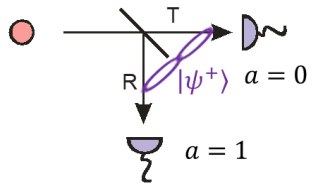
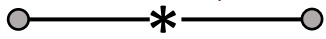


- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties
 - Entanglement
 - Intrinsic randomness
 - No cloning of information
 - ...
 - Can we imagine a **future theory** which:
 - Does not have these ‘unpleasant’ properties
 - Is consistent with the CHSH game
- Corollaries of Bell theorem : No!

Device independence

Foundational physics

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$



- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties

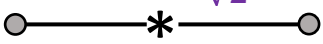
- Entanglement
- Intrinsic randomness
- No cloning of information
- ...

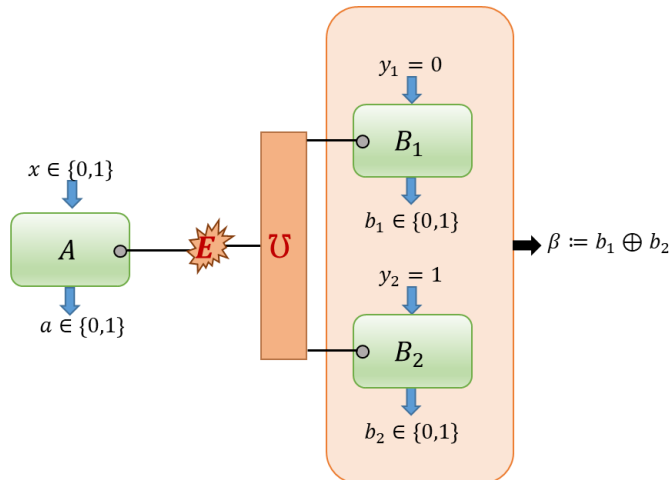
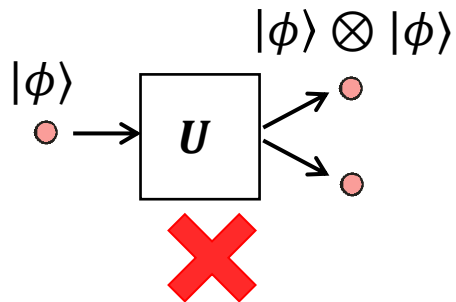
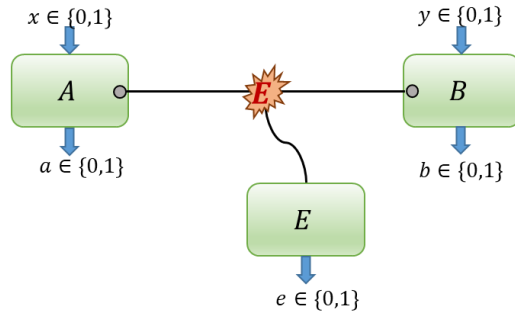
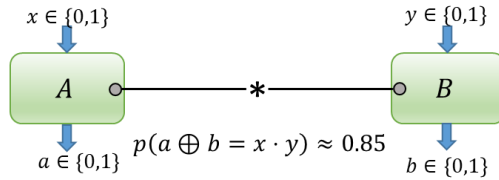
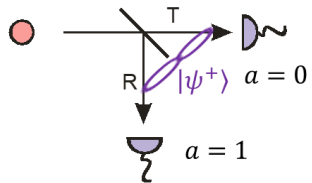
- Can we imagine a **future theory** which:
 - Does not have these ‘unpleasant’ properties
 - Is consistent with the CHSH game

➤ Corollaries of Bell theorem : No!

Device independence

Foundational physics

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$




- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties

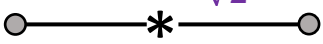
- Entanglement
- Intrinsic randomness
- No cloning of information
- ...

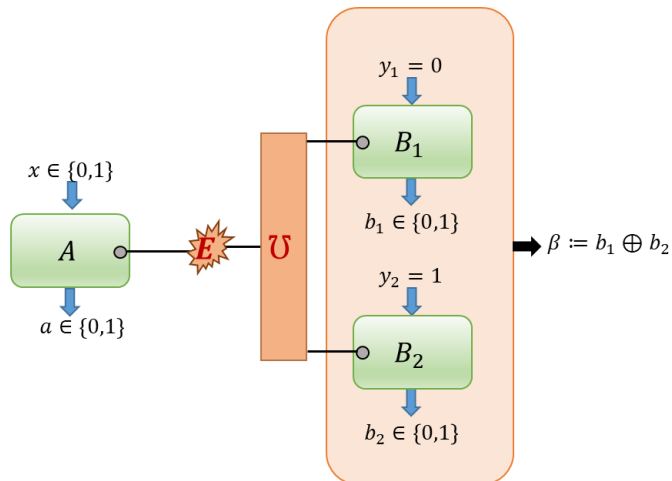
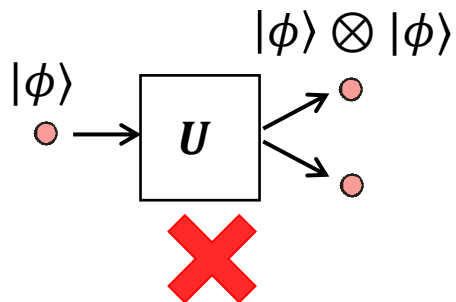
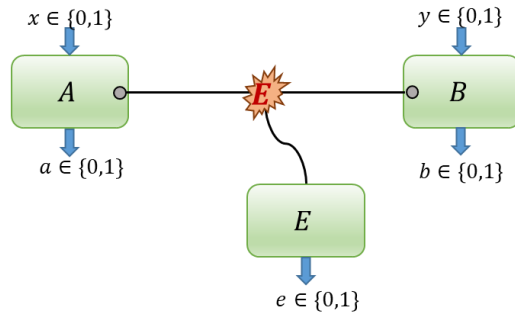
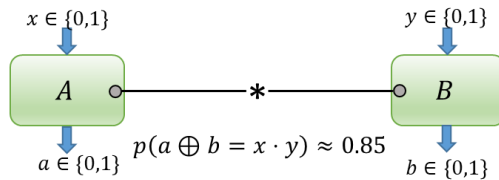
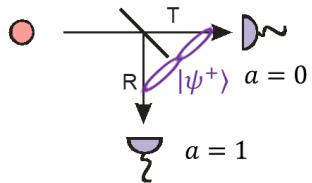
- Can we imagine a **future theory** which:
 - Does not have these ‘unpleasant’ properties
 - Is consistent with the CHSH game

➤ Corollaries of Bell theorem : No!

Device independence

Foundational physics

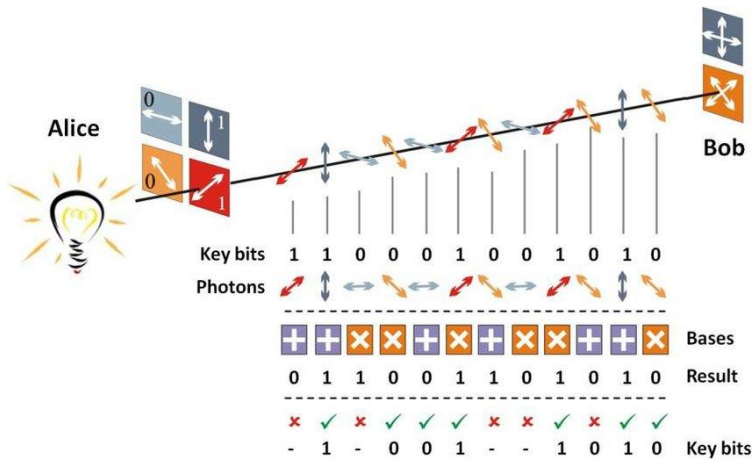
$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$




- Quantum theory has many ‘not intuitive’, ‘nonclassical’ properties
 - Entanglement
 - Intrinsic randomness
 - No cloning of information
 - ...
 - Can we imagine a **future theory** which:
 - Does not have these ‘unpleasant’ properties
 - Is consistent with the CHSH game
- Corollaries of Bell theorem : No!
- ‘**Device/theory Independent**’ certification of these properties

Device independence

Applications of quantum physics: QKD

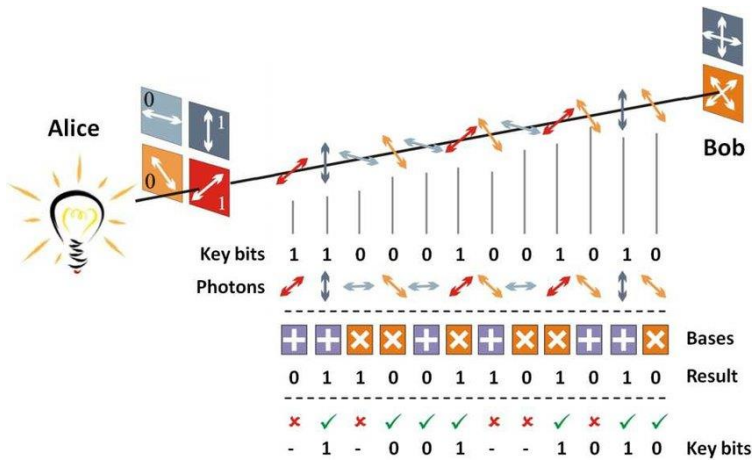


BB84 protocol

- Quantum Key Distribution (QKD)
 - BB84 protocol

Device independence

Applications of quantum physics: QKD

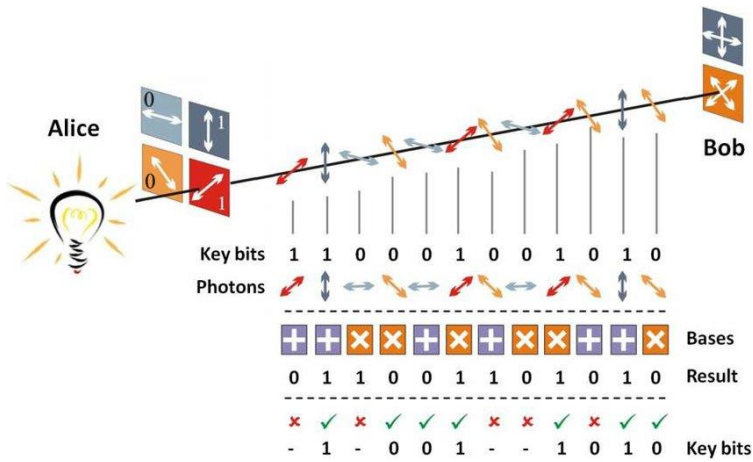


BB84 protocol

- Quantum Key Distribution (QKD)
 - BB84 protocol
 - **A, B** agree on a key, proven to be **private**

Device independence

Applications of quantum physics: QKD

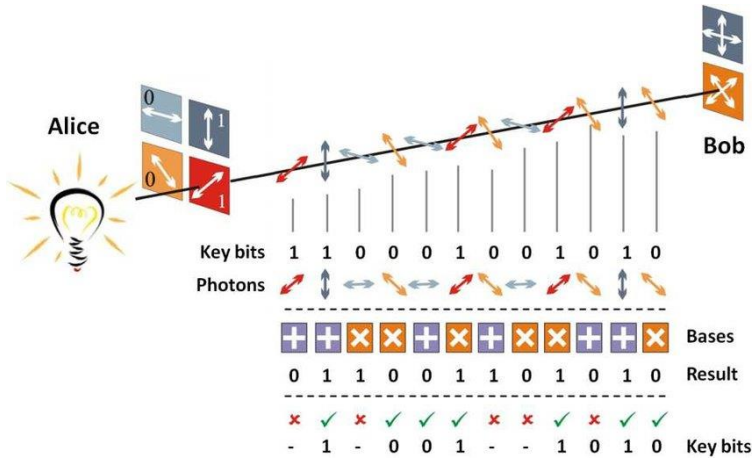


BB84 protocol

- Quantum Key Distribution (QKD)
 - BB84 protocol
 - **A, B** agree on a key, proven to be **private**
 - Assumptions:
 - perfect single photon sources
 - Perfect polarization measurements

Device independence

Applications of quantum physics: QKD



BB84 protocol

- Quantum Key Distribution (QKD)

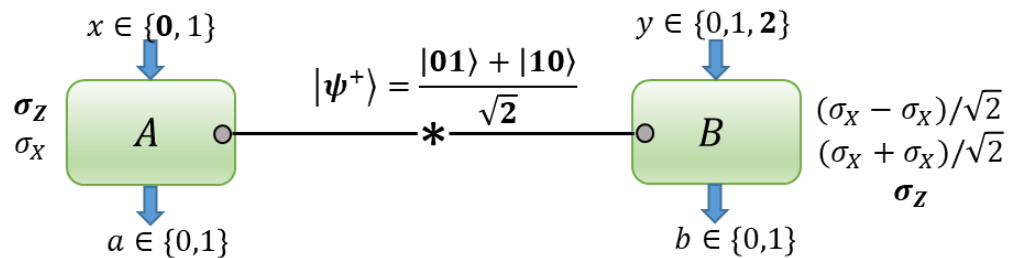
- BB84 protocol

- **A, B** agree on a key, proven to be **private**

- Assumptions:

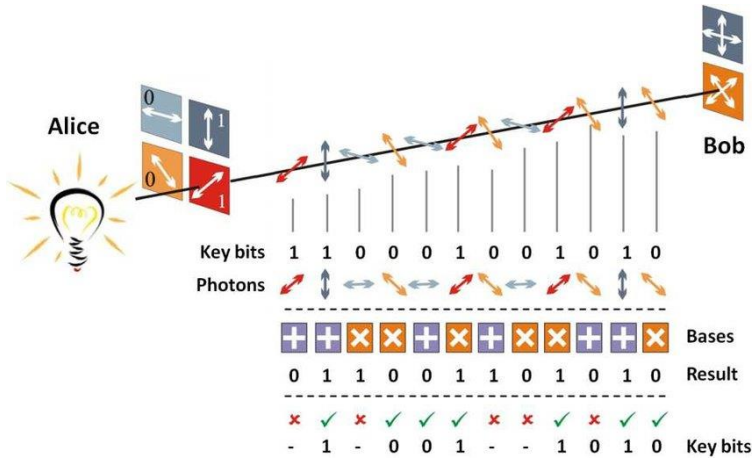
- perfect single photon sources
- Perfect polarization measurements

- Bell theorem : DI QKD



Device independence

Applications of quantum physics: QKD



BB84 protocol

- Quantum Key Distribution (QKD)

- BB84 protocol

- **A, B** agree on a key, proven to be **private**

- Assumptions:

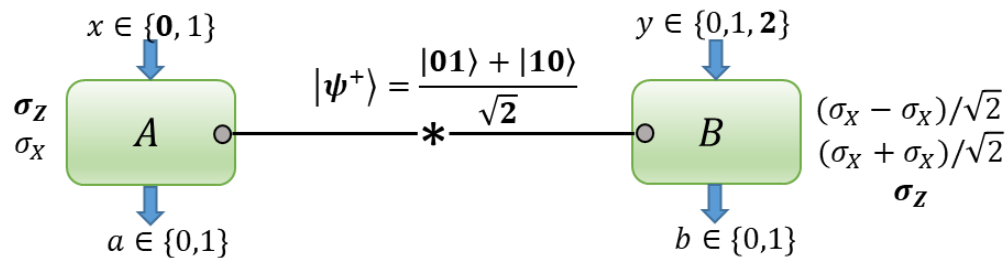
- perfect single photon sources

- Perfect polarization measurements

- Bell theorem : DI QKD

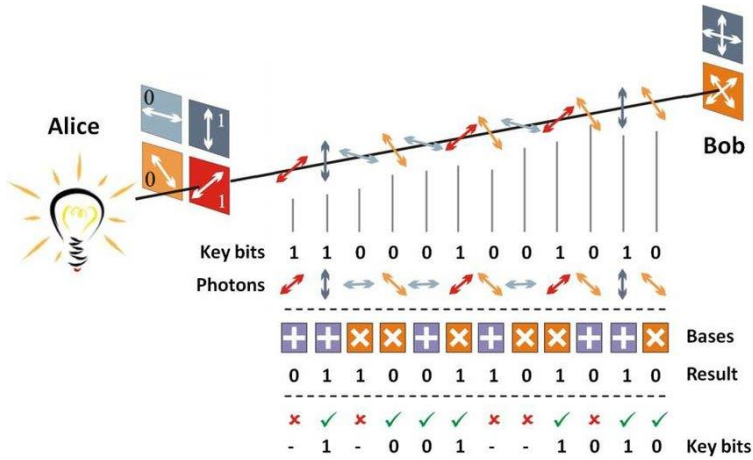
- Assuming quantum theory

Theorem: If for $x, y \in \{0, 1\}$, $P(a \oplus b = x \cdot y) \approx 0.85$, then for $x = 0, y = 2$: $a = 1 - b$ shared, secret.



Device independence

Applications of quantum physics: QKD



BB84 protocol

- Quantum Key Distribution (QKD)

- BB84 protocol

- **A, B** agree on a key, proven to be **private**

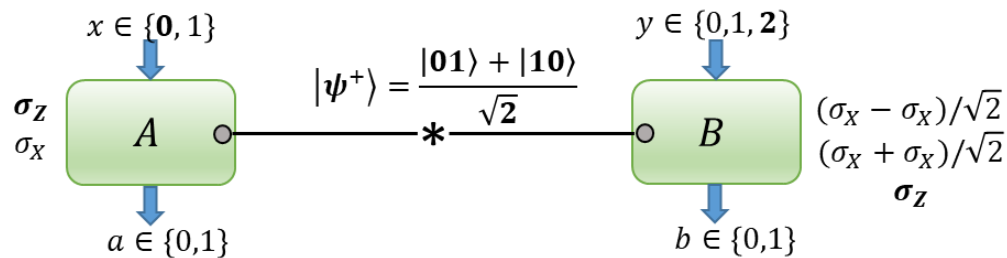
- Assumptions:

- perfect single photon sources
 - Perfect polarization measurements

- Bell theorem : DI QKD

- Assuming quantum theory

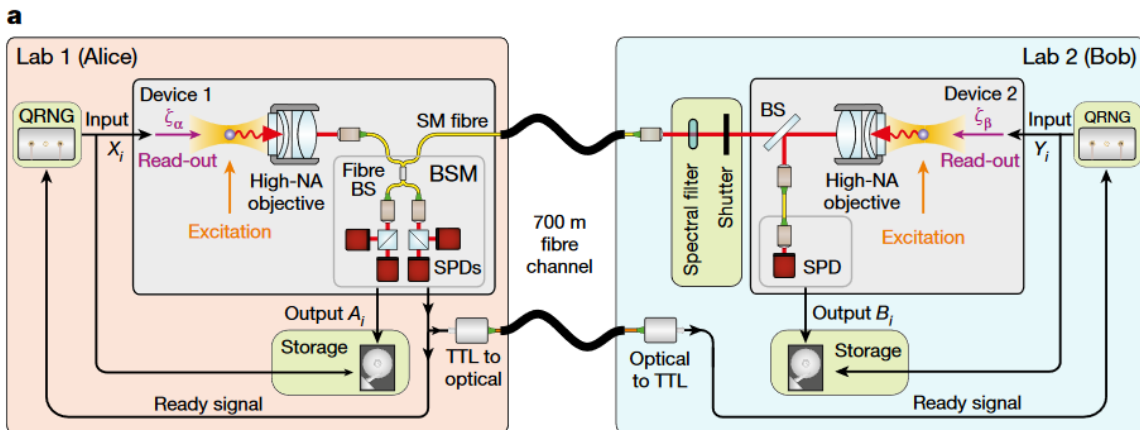
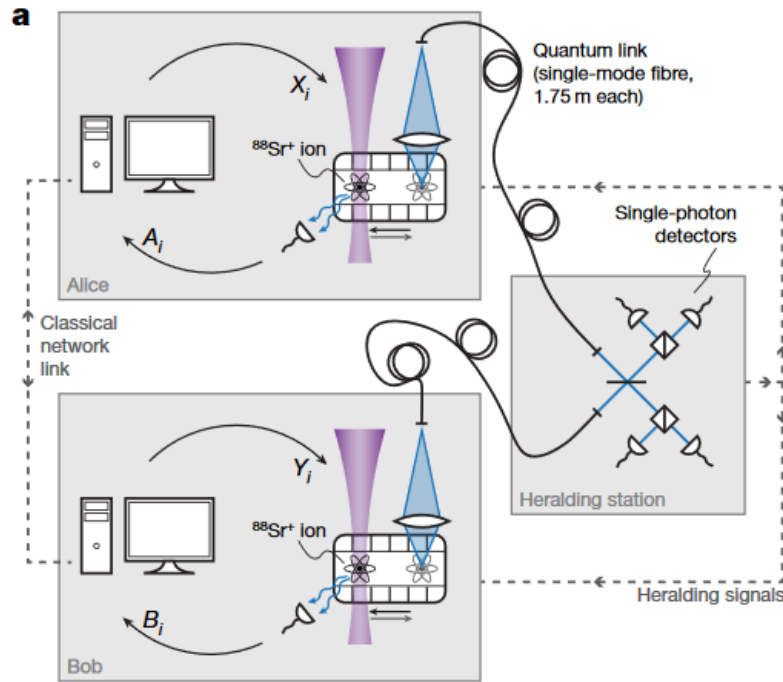
Theorem: If for $x, y \in \{0, 1\}$, $P(a \oplus b = x \cdot y) \approx 0.85$, then for $x = 0, y = 2$: $a = 1 - b$ shared, secret.



- ‘Device Independent’ certification of quantum key distribution

Device independence

Applications of quantum physics: QKD



- Quantum Key Distribution (QKD)

- BB84 protocol

- A, B agree on a key, proven to be **private**

- Assumptions:

- perfect single photon sources

- Perfect polarization measurements

- Bell theorem : DI QKD

- Assuming quantum theory

Theorem: If for $x, y \in \{0, 1\}$, $P(a \oplus b = x \cdot y) \approx 0.85$, then for $x = 0, y = 2$: $a = 1 - b$ shared, secret.

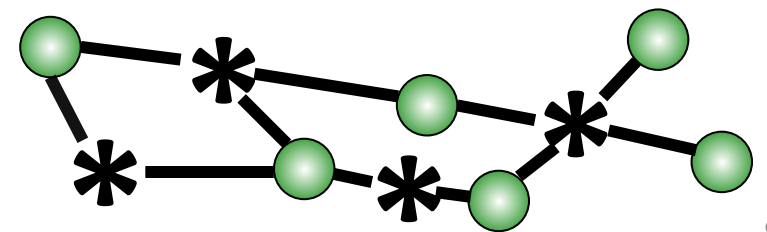
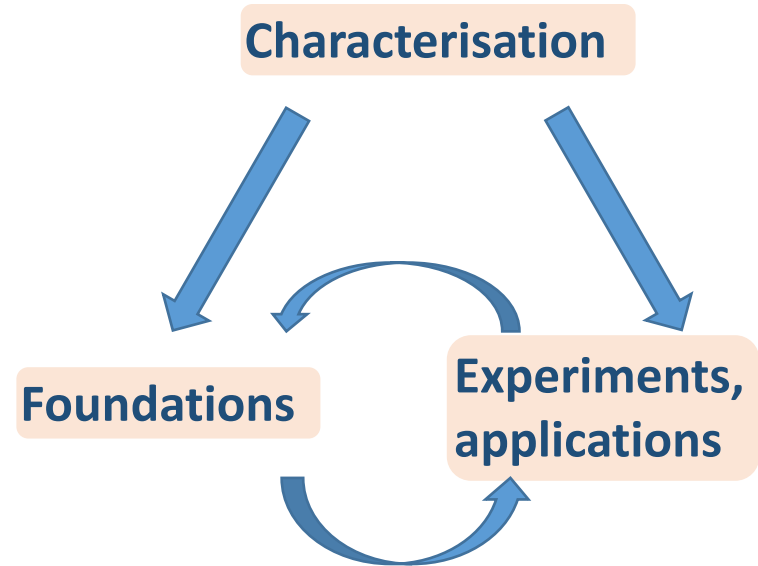
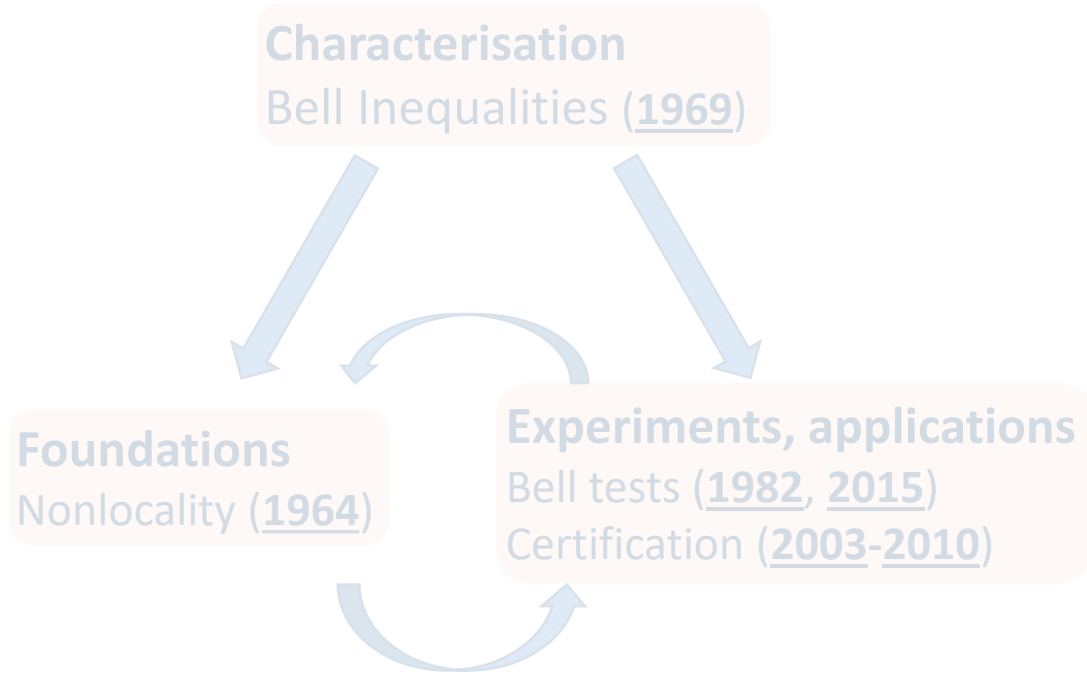
- 2022: First two experimental realisation

- 1st expt: 95628 key bits in 8 hours, 2m distance

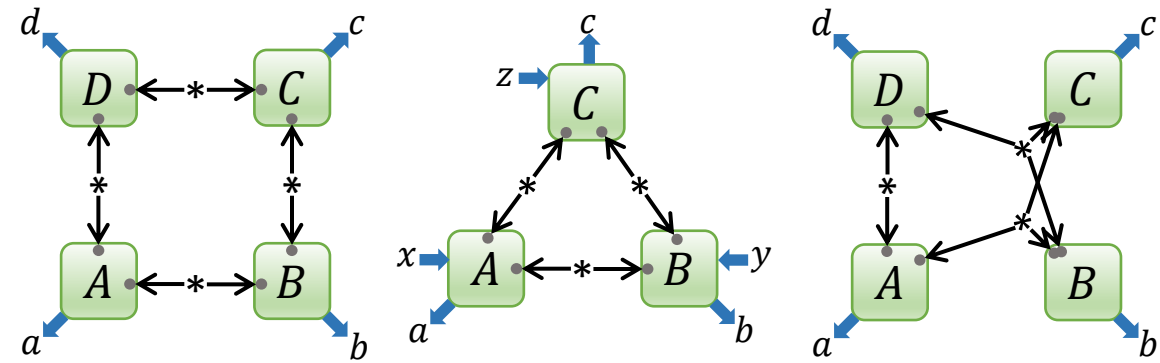
- 2nd expt: Only valid in 'infinite running time', 700m

Overview

Causal network quantum correlations



Causal network quantum correlations



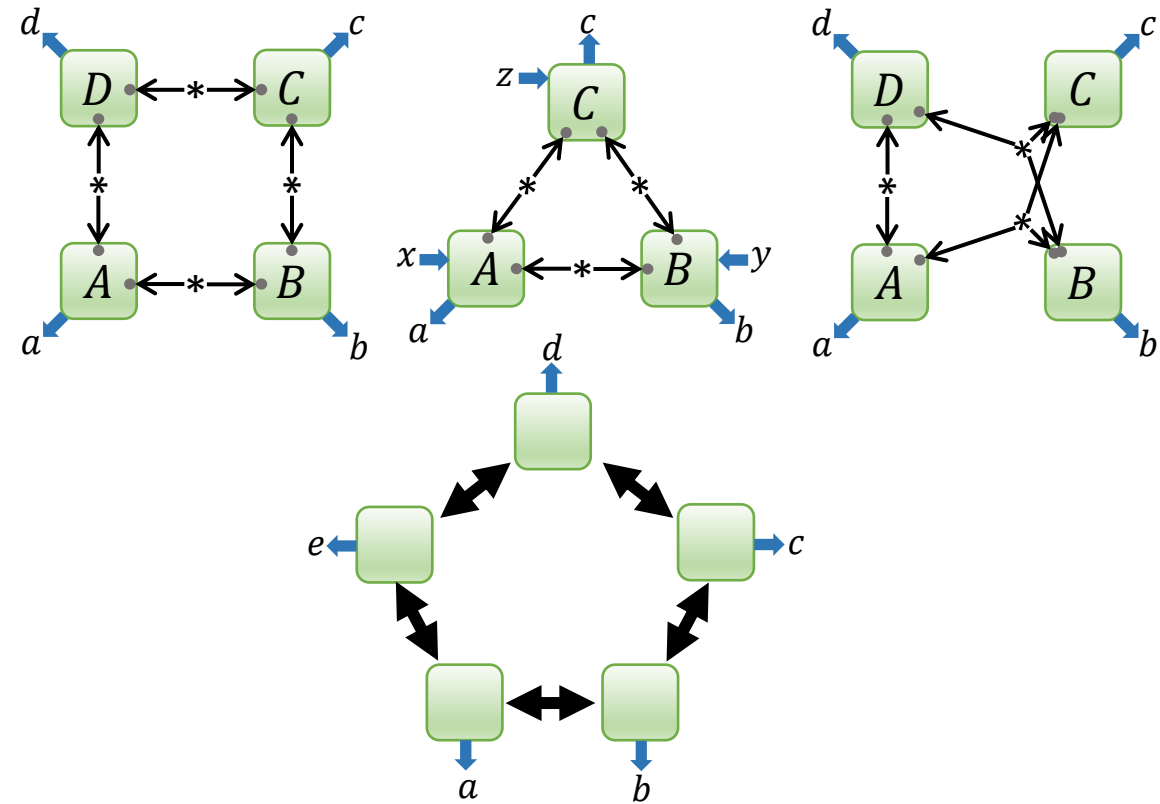
(Quantum) causal network:

Several hidden sources distributed and measured in a quantum network

Can they win a concrete game, e.g.

$p(\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} = \mathbf{x} \cdot \mathbf{y} \cdot \mathbf{z}) > 0.7$, with classical/quantum theory?

Causal network quantum correlations



(Quantum) causal network:

Several hidden sources distributed and measured in a quantum network

Can they win a concrete game, e.g.

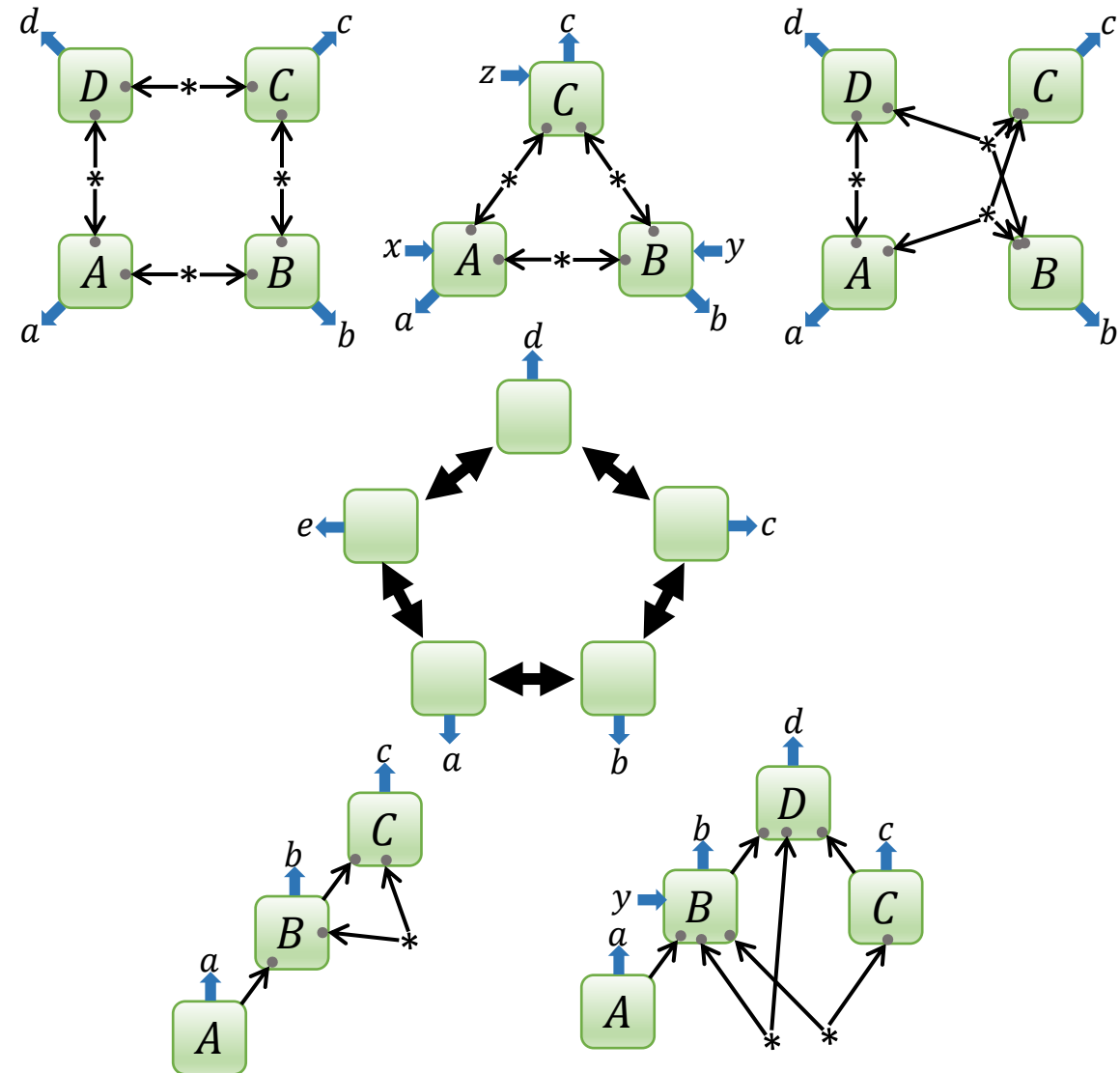
$p(\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{c} = \mathbf{x} \cdot \mathbf{y} \cdot \mathbf{z}) > 0.7$, with classical/quantum theory?

(Quantum) distributed computing structure:

Several processors exchange information (e.g., synchronisation, limited number of communications steps).

Can they find a proper coloring, that is $a \neq b, \dots, e \neq a$, with 1 synchronised communication step and classical/quantum theory?

Causal network quantum correlations



(Quantum) causal network:

Several hidden sources distributed and measured in a quantum network

Can they win a concrete game, e.g.

$p(a \oplus b \oplus c = x \cdot y \cdot z) > 0.7$, with classical/quantum theory?

(Quantum) distributed computing structure:

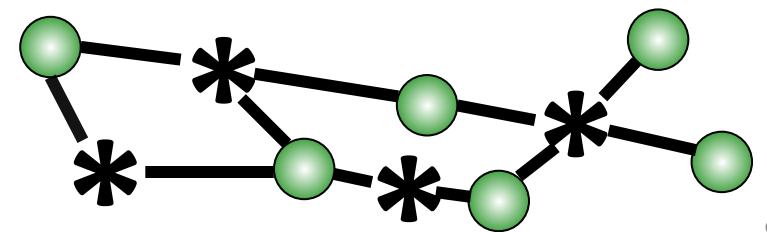
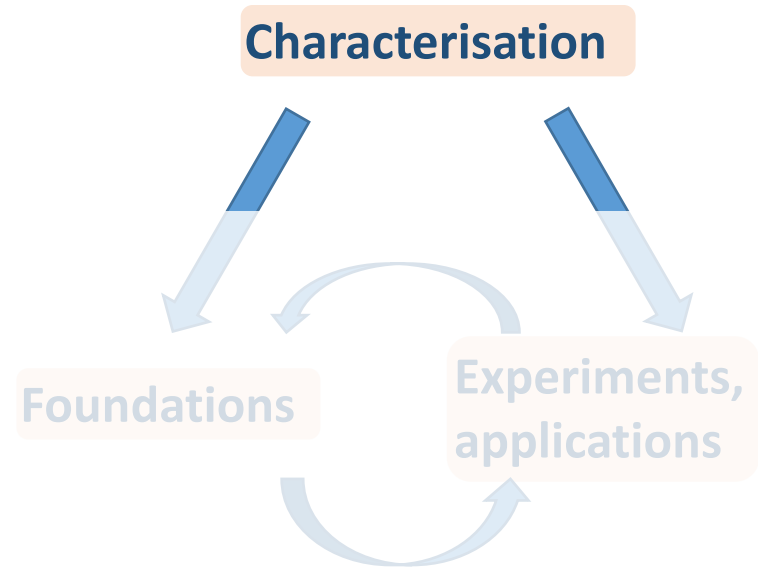
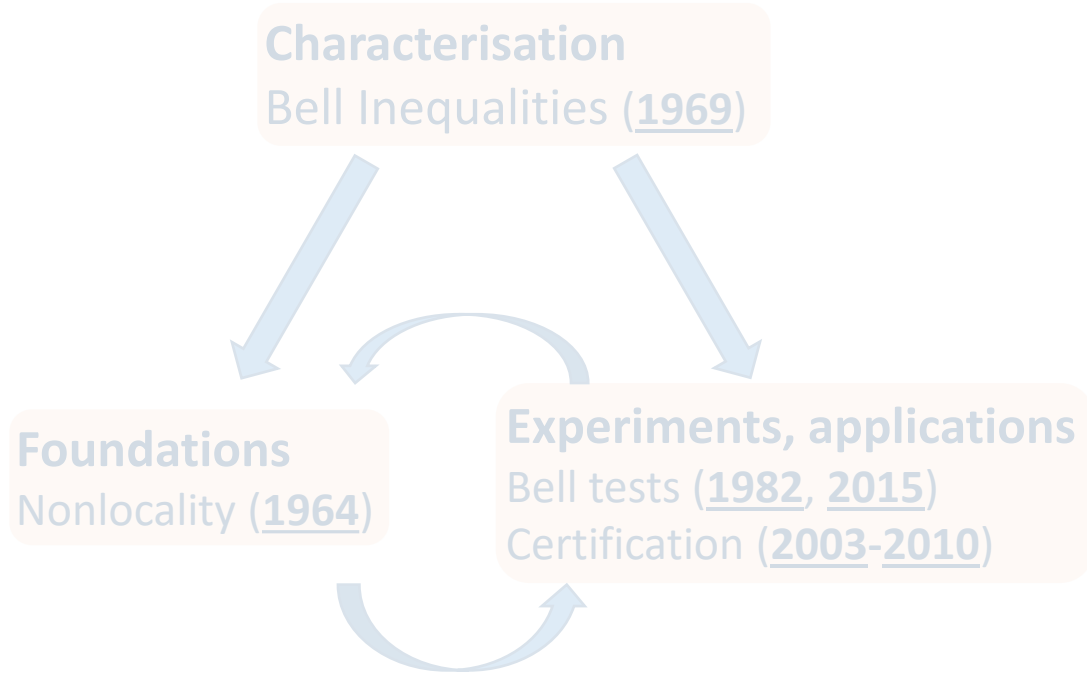
Several processors exchange information (e.g., synchronisation, limited number of communications steps).

Can they find a proper coloring, that is $a \neq b, \dots, e \neq a$, with 1 synchronised communication step and classical/quantum theory?

(Quantum) causal structure:

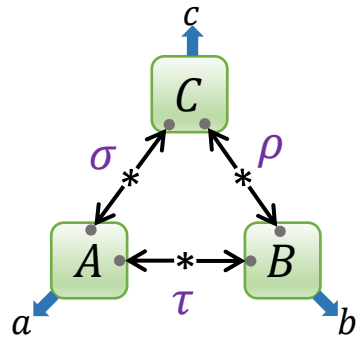
Causal structure involving hidden sources and non-hidden causes

Characterisation



Characterisation

Genuine triangle nonlocality



Concrete ρ, σ, τ and
measurements

➤ Give \mathcal{P}

Genuine nonlocality in the triangle network (2019)

M-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, S. Beigi, Phys. Rev. Lett. 123, 140401 (2019)

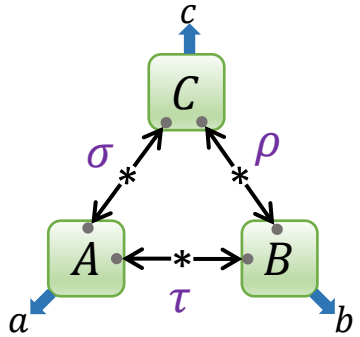
M-O. Renou, S. Beigi, Phys. Rev. Lett. 128, 060401 (2022)

M-O. Renou, S. Beigi, Phys. Rev. A 105, 022408 (2022)

A. Pozas-Kerstjens, N. Gisin, **M-O. Renou**, Phys. Rev. Lett. 130, 090201 (2023)

Characterisation

Genuine triangle nonlocality



Concrete ρ, σ, τ and
measurements

➤ Give \mathcal{P}

Genuine nonlocality in the triangle network (2019)

- Goal:
 - Find quantum experiment with statistics \mathcal{P}

M-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, S. Beigi, Phys. Rev. Lett. 123, 140401 (2019)

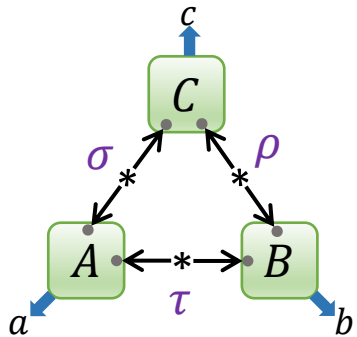
M-O. Renou, S. Beigi, Phys. Rev. Lett. 128, 060401 (2022)

M-O. Renou, S. Beigi, Phys. Rev. A 105, 022408 (2022)

A. Pozas-Kerstjens, N. Gisin, M-O. Renou, Phys. Rev. Lett. 130, 090201 (2023)

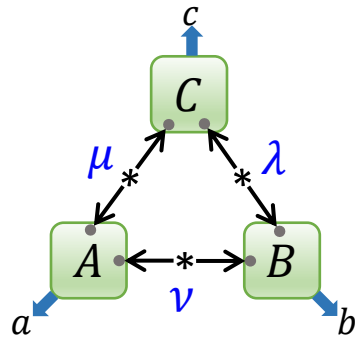
Characterisation

Genuine triangle nonlocality



Concrete ρ, σ, τ and measurements

- Give P



$\forall \lambda, \mu, \nu$ and processing

- Cannot give P

Genuine nonlocality in the triangle network (2019)

- Goal:
 - Find quantum experiment with statistics P
 - Such that a classical detective cannot explain it

M-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, S. Beigi, Phys. Rev. Lett. 123, 140401 (2019)

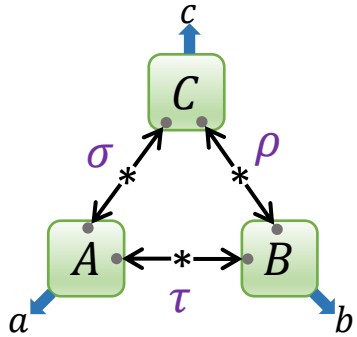
M-O. Renou, S. Beigi, Phys. Rev. Lett. 128, 060401 (2022)

M-O. Renou, S. Beigi, Phys. Rev. A 105, 022408 (2022)

A. Pozas-Kerstjens, N. Gisin, M-O. Renou, Phys. Rev. Lett. 130, 090201 (2023)

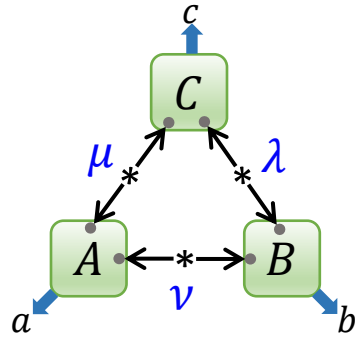
Characterisation

Genuine triangle nonlocality



Concrete ρ, σ, τ and measurements

- Give P



$\forall \lambda, \mu, \nu$ and processing

- Cannot give P

Genuine nonlocality in the triangle network (2019)

- Goal:
 - Find quantum experiment with statistics P
 - Such that a classical detective cannot explain it
- Generalisation to other networks
 - Method fundamentally different from standard Bell arguments

M-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, S. Beigi, Phys. Rev. Lett. 123, 140401 (2019)

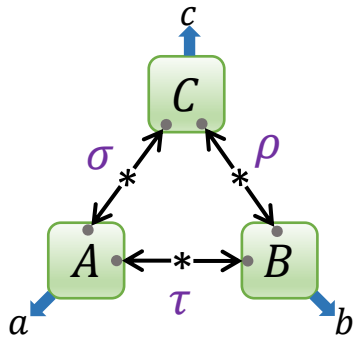
M-O. Renou, S. Beigi, Phys. Rev. Lett. 128, 060401 (2022)

M-O. Renou, S. Beigi, Phys. Rev. A 105, 022408 (2022)

A. Pozas-Kerstjens, N. Gisin, M-O. Renou, Phys. Rev. Lett. 130, 090201 (2023)

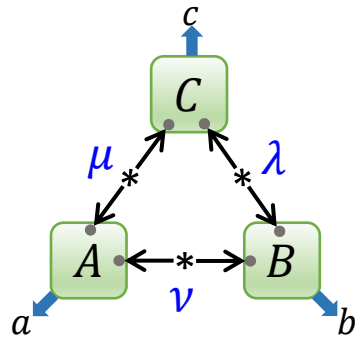
Characterisation

Genuine triangle nonlocality



Concrete ρ, σ, τ and measurements

- Give \mathcal{P}



$\forall \lambda, \mu, \nu$ and processing

- Cannot give \mathcal{P}

Genuine nonlocality in the triangle network (2019)

- Goal:

- Find quantum experiment with statistics \mathcal{P}
- Such that a classical detective cannot explain it

- Generalisation to other networks

- Method fundamentally different from standard Bell arguments
- This allows new applications: « certify randomness without inputs »

M-O. Renou, E. Bäumer, S. Boreiri, N. Brunner, N. Gisin, S. Beigi, Phys. Rev. Lett. 123, 140401 (2019)

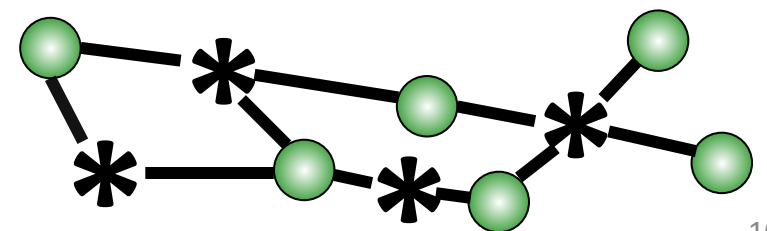
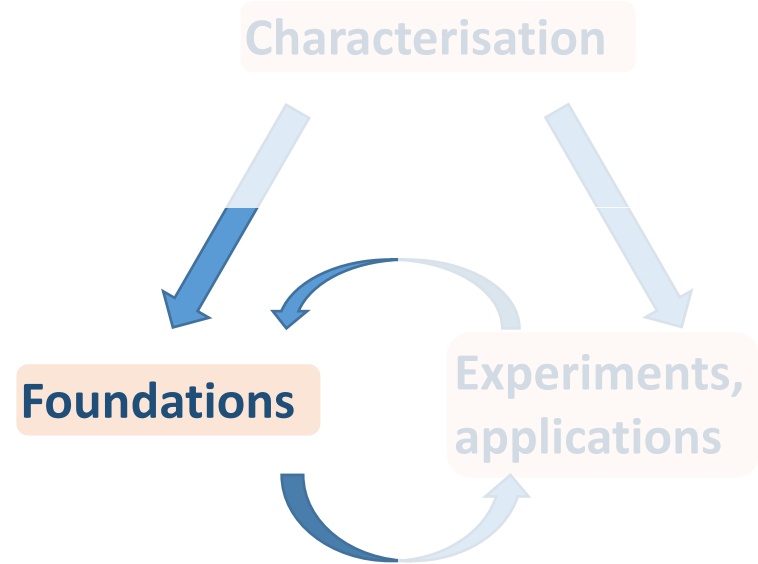
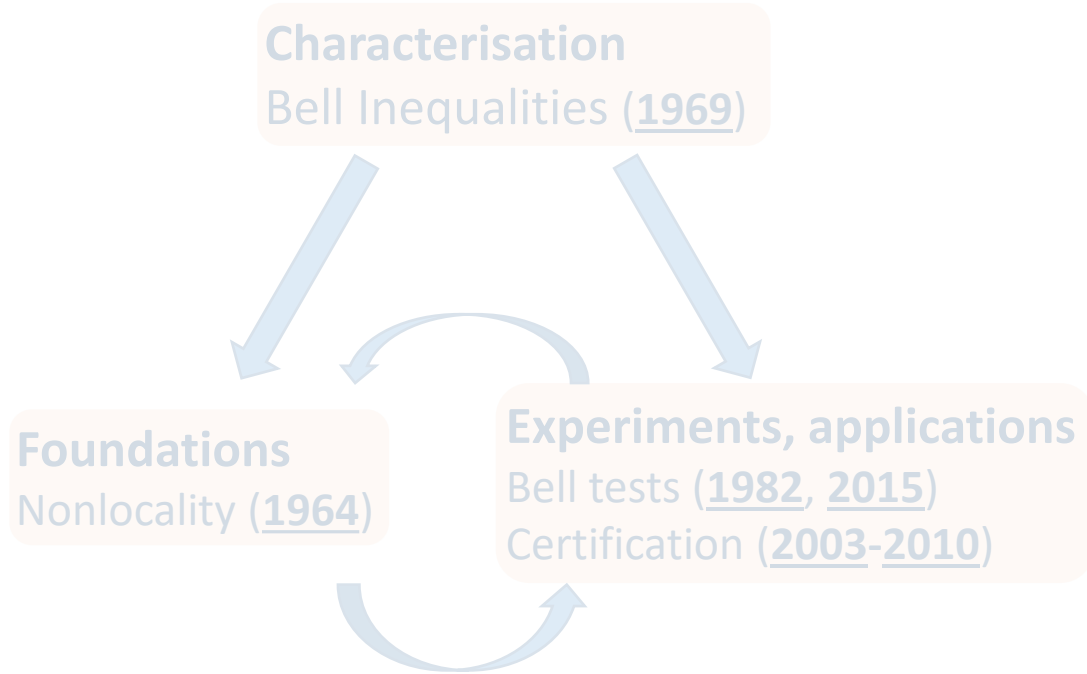
M-O. Renou, S. Beigi, Phys. Rev. Lett. 128, 060401 (2022)

M-O. Renou, S. Beigi, Phys. Rev. A 105, 022408 (2022)

A. Pozas-Kerstjens, N. Gisin, M-O. Renou, Phys. Rev. Lett. 130, 090201 (2023)

P. Sekatski, S. Boreiri, N. Brunner, arXiv:2209.09921 (2022)

Foundations



Foundations

\mathbb{R} -QT can be experimentally ruled out

Experimentalist

- Master standard Quantum Theory

Detective

- Believes in \mathbb{R} -QT

Foundations

\mathbb{R} -QT can be experimentally ruled out

Experimentalist

- Master standard Quantum Theory

1 Particle S

(i) $_{\mathbb{C}}$ State: operator $\rho_S \succcurlyeq \mathbf{0}$ of \mathbb{C} -Hilbert Space \mathcal{H}_S with $\text{Tr}(\rho_S) = 1$

(ii) Measurement: operators $\mathbf{M} = \{M_r\} \in \mathcal{H}_S$, $M_r \succcurlyeq \mathbf{0}$, $M_r^2 = M_r$, $\sum_r M_r = \text{Id}$

(iii) Born rule: result r has probability $P(r) = \text{Tr}(\rho_S \cdot M_r)$

2 Particles $\{S, T\}$

(iv) Hilbert space: $\mathcal{H}_{ST} = \mathcal{H}_S \otimes \mathcal{H}_T$.

Independent preparations of ρ_S, σ_T : State $\rho_{ST} = \rho_S \otimes \sigma_T$

Detective

- Believes in \mathbb{R} -QT

1 Particle S

(i) $_{\mathbb{R}}$ State: operator $\rho_S \succcurlyeq \mathbf{0}$ of \mathbb{R} -Hilbert Space \mathcal{H}_S with $\text{Tr}(\rho_S) = 1$

(ii) Measurement: operators $\mathbf{M} = \{M_r\} \in \mathcal{H}_S$, $M_r \succcurlyeq \mathbf{0}$, $M_r^2 = M_r$, $\sum_r M_r = \text{Id}$

(iii) Born rule: result r has probability $P(r) = \text{Tr}(\rho_S \cdot M_r)$

2 Particles $\{S, T\}$

(iv) Hilbert space: $\mathcal{H}_{ST} = \mathcal{H}_S \otimes \mathcal{H}_T$.

Independent preparations of ρ_S, σ_T : State $\rho_{ST} = \rho_S \otimes \sigma_T$

Foundations

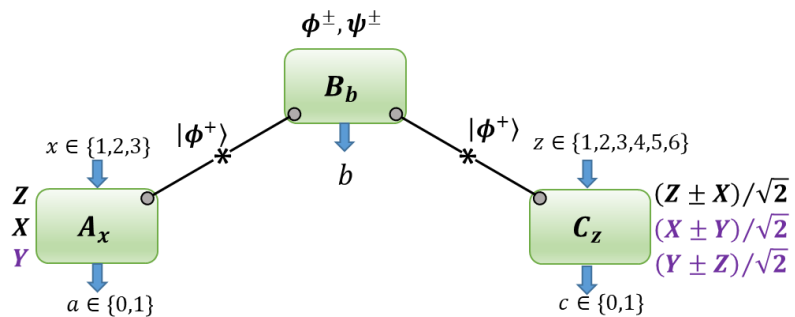
\mathbb{R} -QT can be experimentally ruled out

Experimentalist

Detective

- Master standard Quantum Theory
- Construct a **concrete experiment**

- Believes in \mathbb{R} -QT



- Obtains **experimental results** (statistics)

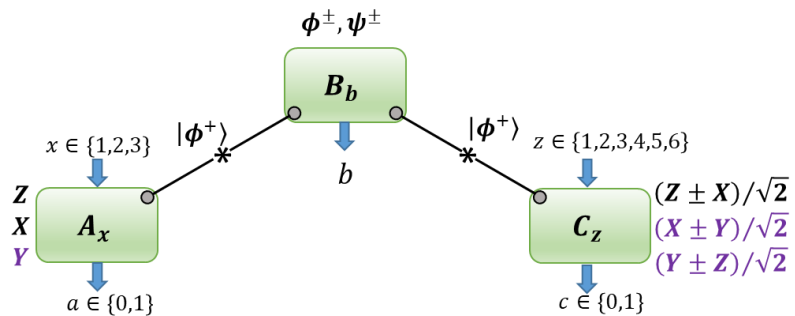
$$P(abc|xz): \begin{cases} \text{CHSH}^b(1, 2; 1, 2) = 2\sqrt{2} \\ \text{CHSH}^b(2, 3; 3, 4) = 2\sqrt{2} \\ \text{CHSH}^b(3, 1; 5, 6) = 2\sqrt{2} \end{cases}$$

Foundations

\mathbb{R} -QT can be experimentally ruled out

Experimentalist

- Master standard Quantum Theory
- Construct a **concrete experiment**

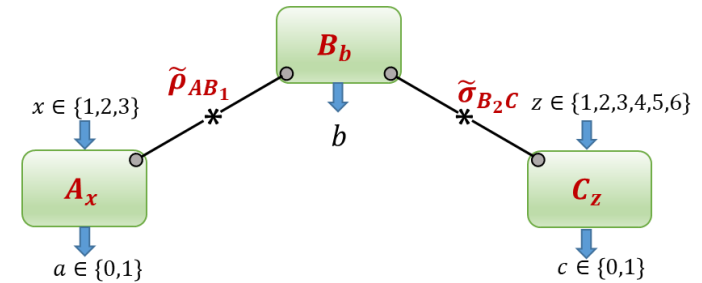


- Obtains **experimental results** (statistics)

$$P(abc|xz): \begin{cases} \text{CHSH}^b(1, 2; 1, 2) = 2\sqrt{2} \\ \text{CHSH}^b(2, 3; 3, 4) = 2\sqrt{2} \\ \text{CHSH}^b(3, 1; 5, 6) = 2\sqrt{2} \end{cases}$$

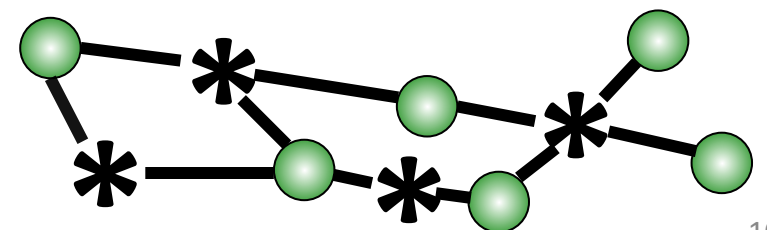
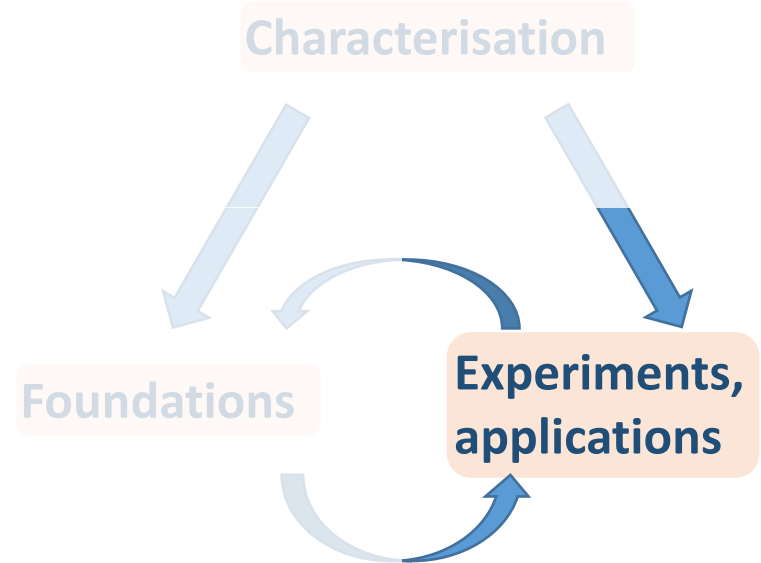
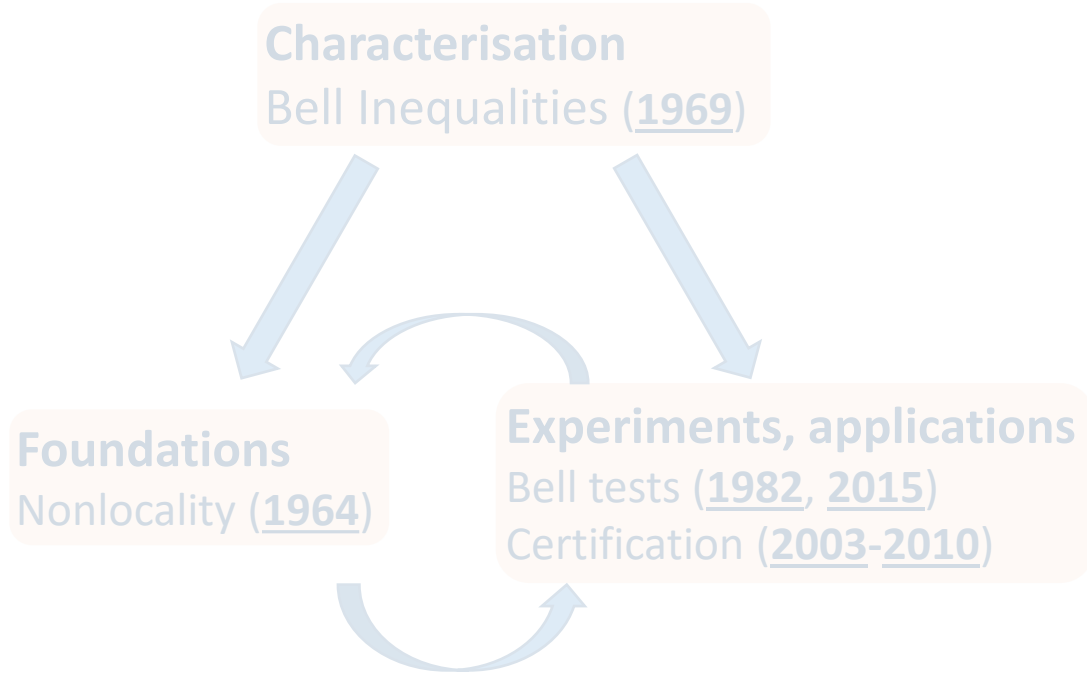
Detective

- Believes in \mathbb{R} -QT
- Tries to explain these **experimental results**. Any 'crazy' explanation compatible with \mathbb{R} -QT is possible.



➤ **Fails**

Applications



Foundations

Bipartite exotic sources are not enough

Experimentalist

Detective

- Master standard Quantum Theory

➤ Involves bipartite entangled sources

$$\leftarrow * \rightarrow$$
$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Foundations

Bipartite exotic sources are not enough

Experimentalist

- Master standard Quantum Theory

➤ Involves bipartite entangled sources



$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Detective

- Accepteded that only “more crazy theory than any crazy explanation compatible with classical physics”

Foundations

Bipartite exotic sources are not enough

Experimentalist

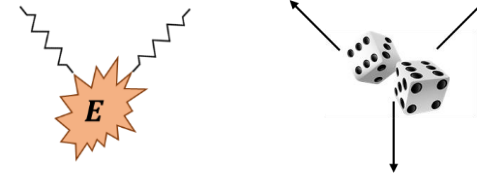
- Master standard Quantum Theory

➤ Involves bipartite entangled sources

$$\leftarrow * \rightarrow$$
$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Detective

- Accepted **ed** that only “**more crazy theory** than any crazy explanation compatible with classical physics”
 - Accepts bipartite « crazy » sources and shared randomness




Foundations

Bipartite exotic sources are not enough

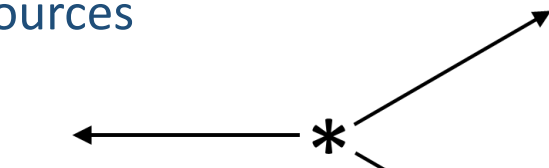
Experimentalist

- Master standard Quantum Theory

- Involves bipartite entangled sources

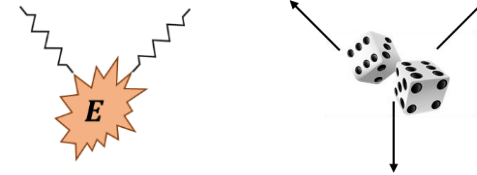

$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Involves tripartite (and n-partite) entangled sources


$$|\phi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Detective

- Accepted **ed** that only “**more crazy theory** than any crazy explanation compatible with classical physics”
 - Accepts bipartite « crazy » sources and shared randomness




Foundations

Bipartite exotic sources are not enough

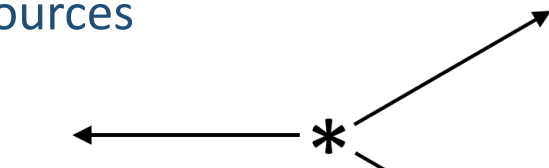
Experimentalist

- Master standard Quantum Theory

- Involves bipartite entangled sources

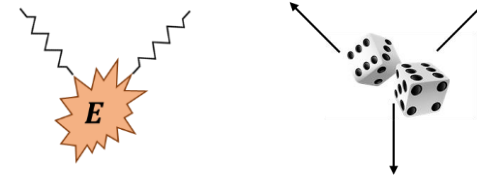

$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Involves tripartite (and n-partite) entangled sources

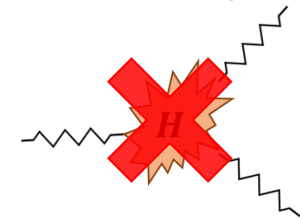

$$|\phi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Detective

- Accepted **ed** that only “**more crazy theory** than any crazy explanation compatible with classical physics”
 - Accepts bipartite « crazy » sources and shared randomness



- However, would like to keep this craziness of low degree:
 - Rejects tripartite (or more) « crazy » sources




Foundations

Bipartite exotic sources are not enough

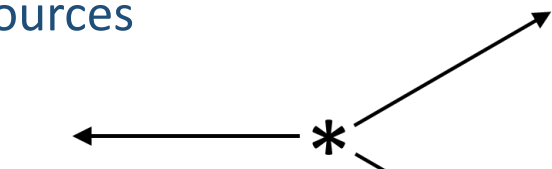
Experimentalist

- Master standard Quantum Theory

- Involves bipartite entangled sources


$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Involves tripartite (and n-partite) entangled sources

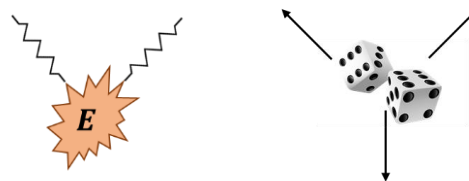

$$|\phi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

- **The foundations of QT:** is tripartite entanglement really needed?

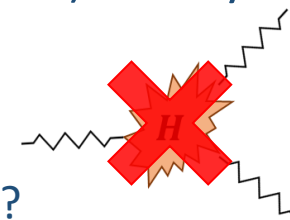
Important question for:

Detective

- Accepted **ed** that only “**more crazy theory** than any crazy explanation compatible with classical physics”
 - Accepts bipartite « crazy » sources and shared randomness



- However, would like to keep this craziness of low degree:
 - Rejects tripartite (or more) « crazy » sources




Foundations

Bipartite exotic sources are not enough


Experimentalist

- Master standard Quantum Theory

- Involves bipartite entangled sources


$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Involves tripartite (and n-partite) entangled sources

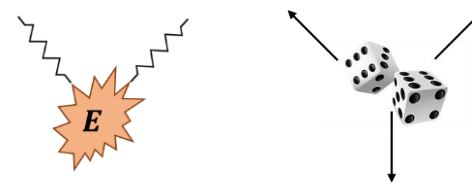

$$|\phi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

- **The foundations of QT:** is tripartite entanglement really needed?

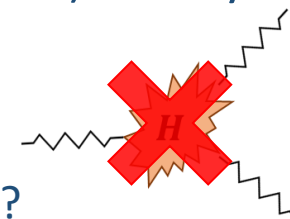
Important question for: ➤ **Applications of QT:** Can I do **more** with tripartite entanglement, what?

Detective

- Accepted **ed** that only “**more crazy theory** than any crazy explanation compatible with classical physics”
 - Accepts bipartite « crazy » sources and shared randomness



- However, would like to keep this craziness of low degree:
 - Rejects tripartite (or more) « crazy » sources




Foundations

Bipartite exotic sources are not enough


Experimentalist

- Master standard Quantum Theory

- Involves bipartite entangled sources


$$|\phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- Involves tripartite (and n-partite) entangled sources


$$|\phi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Important question for:

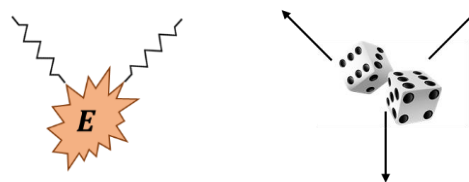
- **The foundations of QT:** is tripartite entanglement really needed?

- **Applications of QT:** Can I do **more** with tripartite entanglement, what?

- **Benchmark Q systems:** How to prove « I can produce tripartite entanglement »?

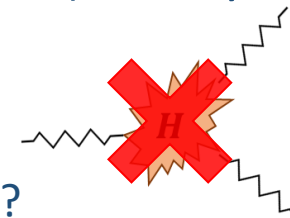
Detective

- Accepted **ed** that only “**more crazy theory** than any crazy explanation compatible with classical physics”
 - Accepts bipartite « crazy » sources and shared randomness



- However, would like to keep this craziness of low degree:

- Rejects tripartite (or more) « crazy » sources



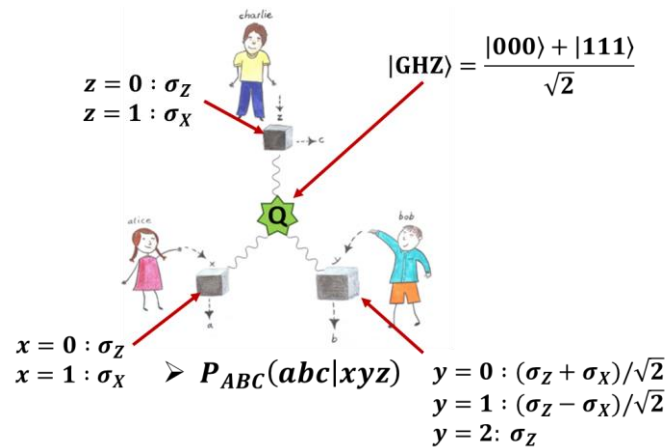
Foundations

Bipartite exotic sources are not enough

Experimentalist

Detective

- Master standard Quantum Theory
- Construct a **concrete experiment**



- Obtains **experimental results** (statistics)

$$\langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle = 2,$$

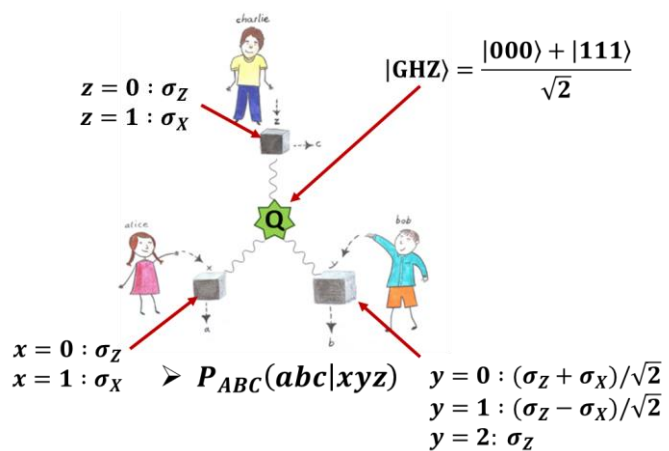
$$\langle A_0 B_0 \rangle^{C_1=1} + \langle A_0 B_1 \rangle^{C_1=1} + \langle A_1 B_0 \rangle^{C_1=1} - \langle A_1 B_1 \rangle^{C_1=1} = 2\sqrt{2}$$

Foundations

Bipartite exotic sources are not enough

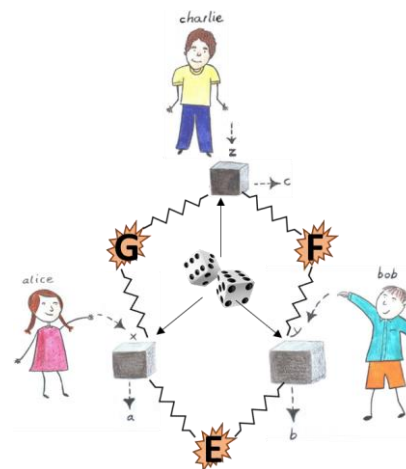
Experimentalist

- Master standard Quantum Theory
- Construct a **concrete experiment**



Detective

- Believes in bipartite « crazy » sources and shared randomness



- Obtains **experimental results** (statistics)

$$\langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle = 2,$$

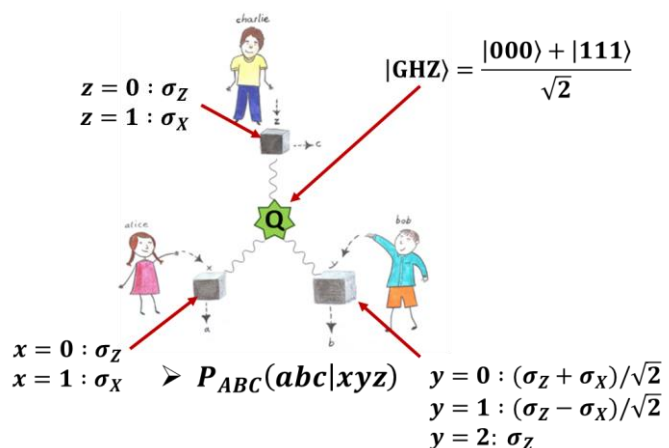
$$\langle A_0 B_0 \rangle^{C_1=1} + \langle A_0 B_1 \rangle^{C_1=1} + \langle A_1 B_0 \rangle^{C_1=1} - \langle A_1 B_1 \rangle^{C_1=1} = 2\sqrt{2}$$

Foundations

Bipartite exotic sources are not enough

Experimentalist

- Master standard Quantum Theory
- Construct a **concrete experiment**



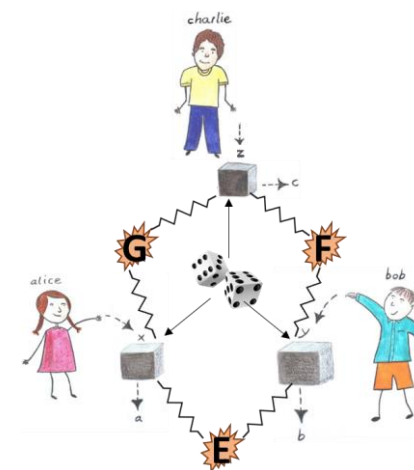
- Obtains **experimental results** (statistics)

$$\langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle = 2,$$

$$\langle A_0 B_0 \rangle^{C_1=1} + \langle A_0 B_1 \rangle^{C_1=1} + \langle A_1 B_0 \rangle^{C_1=1} - \langle A_1 B_1 \rangle^{C_1=1} = 2\sqrt{2}$$

Detective

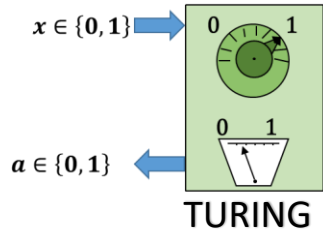
- Believes in bipartite « crazy » sources and shared randomness



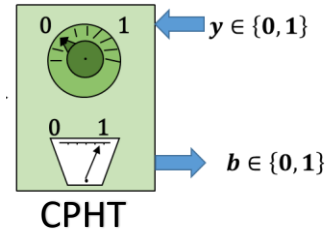
- If the crazy sources satisfy causality and can be duplicated in independent copies:
 - **Detective explanation must fail**

Applications

Certification of all pure states



$$\text{CHSH} = 2\sqrt{2}$$

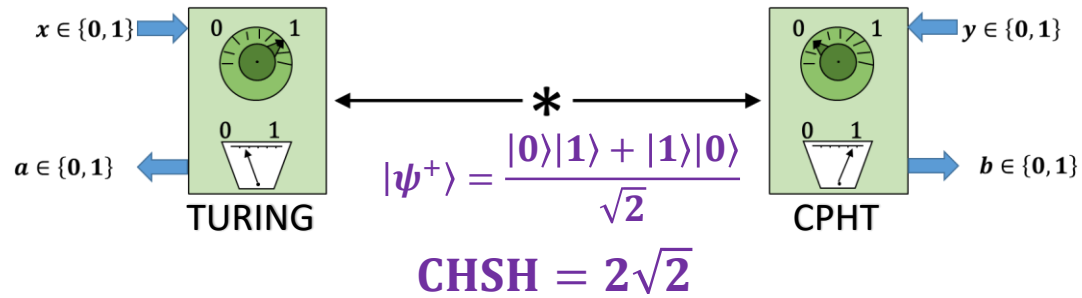


State certification: “self-testing”

- **Observation: $\text{CHSH} = 2\sqrt{2}$**

Applications

Certification of all pure states



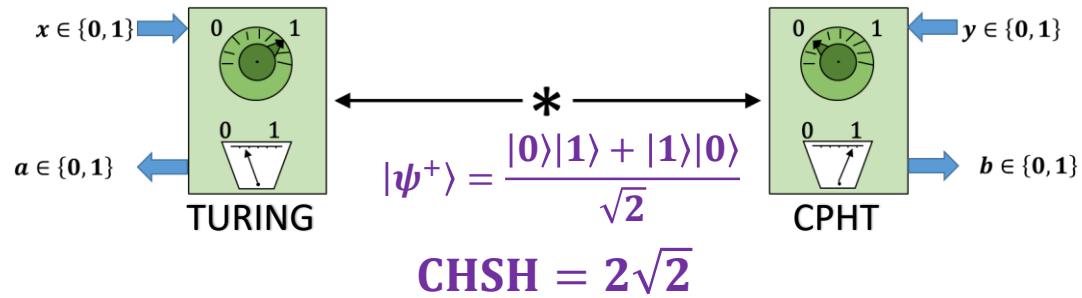
State certification: “self-testing”

- **Observation: $\text{CHSH} = 2\sqrt{2}$**

➤ This **certifies** that the quantum state $|\psi^+\rangle = \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}}$ was produced

Applications

Certification of all pure states



State certification: “self-testing”

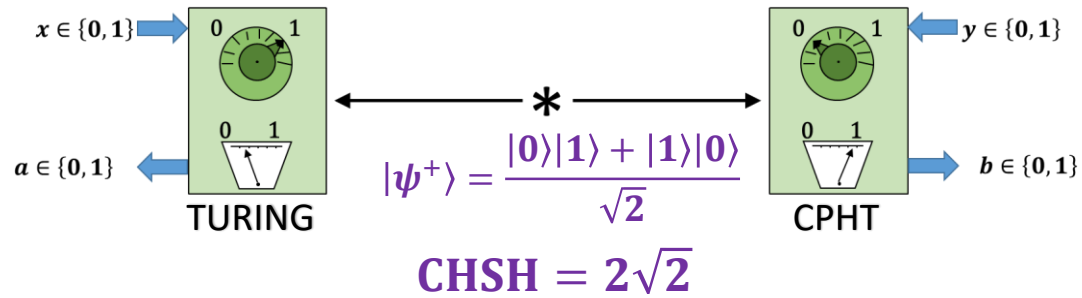
- **Observation: $\text{CHSH} = 2\sqrt{2}$**

➤ This **certifies** that the quantum state $|\psi^+\rangle = \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}}$ was produced

Open question: is there an operational way to test all pure states?

Applications

Certification of all pure states



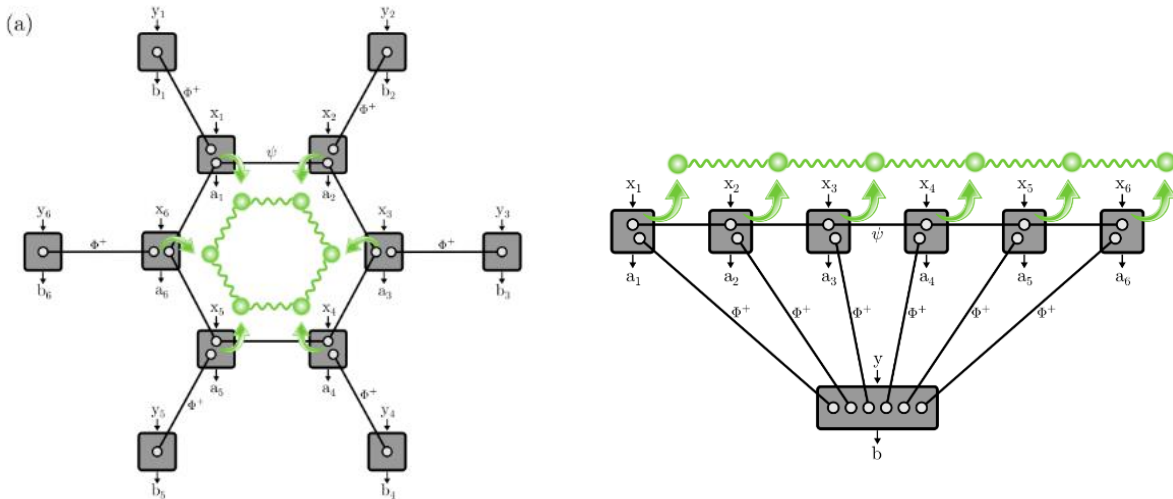
State certification: “self-testing”

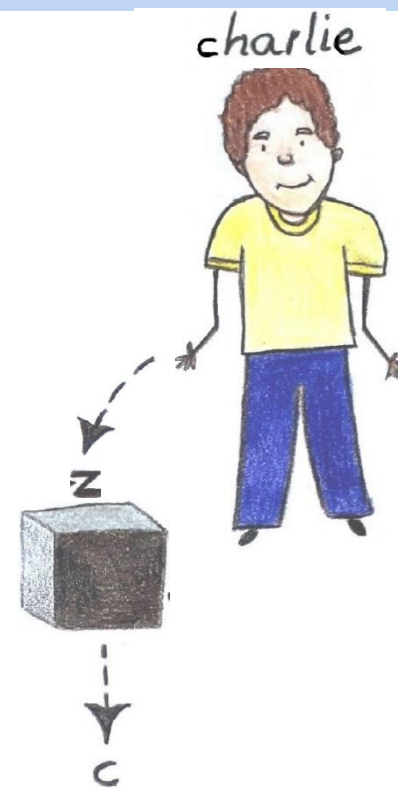
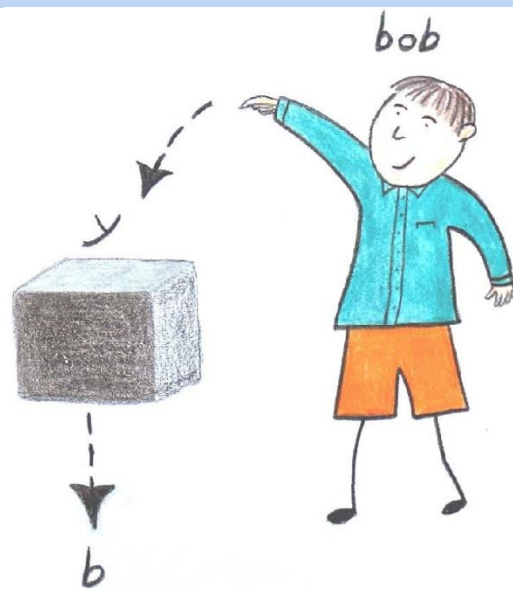
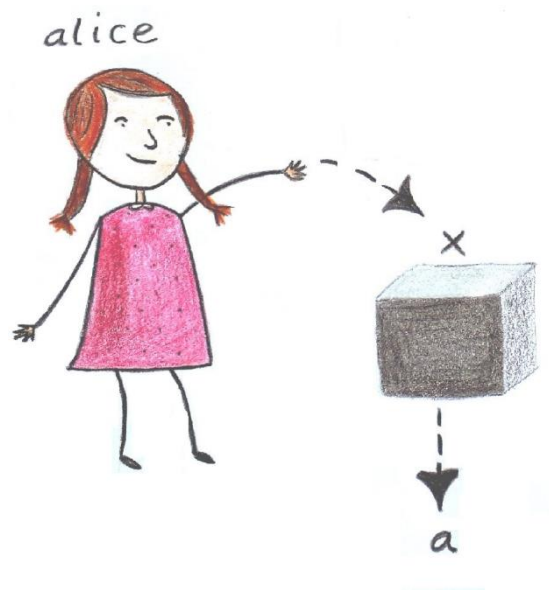
- **Observation: CHSH = $2\sqrt{2}$**

➤ This **certifies** that the quantum state $|\psi^+\rangle = \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}}$ was produced

Open question: is there an operational way to test all pure states?

➤ Answer: yes, considering network correlations



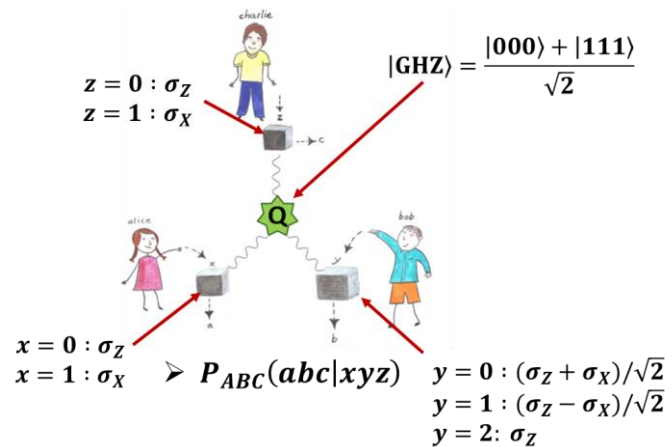


Foundations: Some past works

Experimentalist

Detective

- Master standard Quantum Theory
- Construct a **concrete experiment**



- Obtains **experimental results** (statistics)

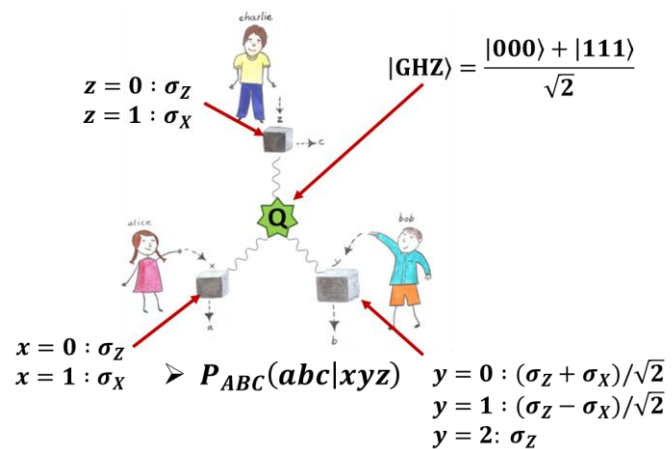
$$\langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle = 2,$$

$$\langle A_0 B_0 \rangle^{C_1=1} + \langle A_0 B_1 \rangle^{C_1=1} + \langle A_1 B_0 \rangle^{C_1=1} - \langle A_1 B_1 \rangle^{C_1=1} = 2\sqrt{2}$$

Foundations: Some past works

Experimentalist

- Master standard Quantum Theory
- Construct a **concrete experiment**



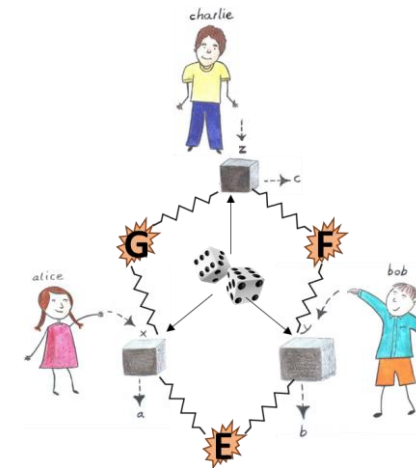
- Obtains **experimental results** (statistics)

$$\langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle = 2,$$

$$\langle A_0 B_0 \rangle^{C_1=1} + \langle A_0 B_1 \rangle^{C_1=1} + \langle A_1 B_0 \rangle^{C_1=1} - \langle A_1 B_1 \rangle^{C_1=1} = 2\sqrt{2}$$

Detective

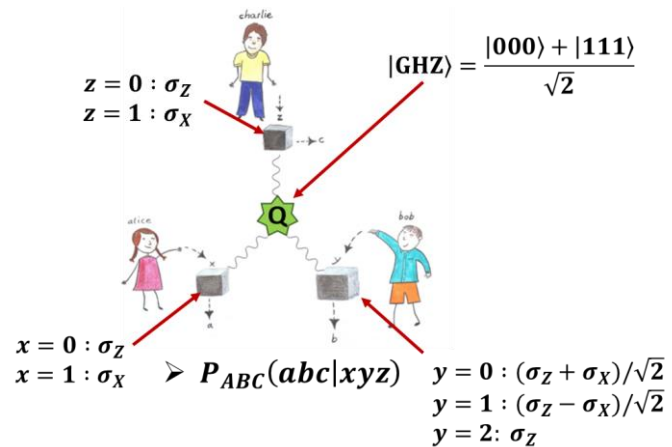
- Believes in bipartite « crazy » sources and shared randomness



Foundations: Some past works

Experimentalist

- Master standard Quantum Theory
- Construct a **concrete experiment**



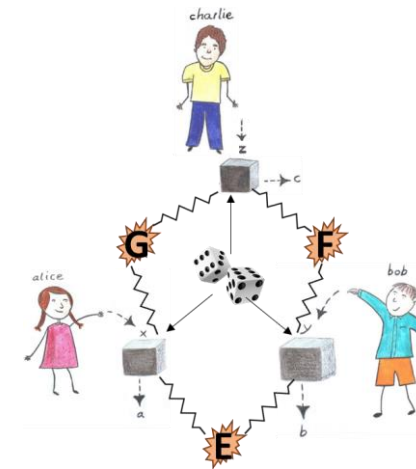
- Obtains **experimental results** (statistics)

$$\langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle = 2,$$

$$\langle A_0 B_0 \rangle^{C_1=1} + \langle A_0 B_1 \rangle^{C_1=1} + \langle A_1 B_0 \rangle^{C_1=1} - \langle A_1 B_1 \rangle^{C_1=1} = 2\sqrt{2}$$

Detective

- Believes in bipartite « crazy » sources and shared randomness



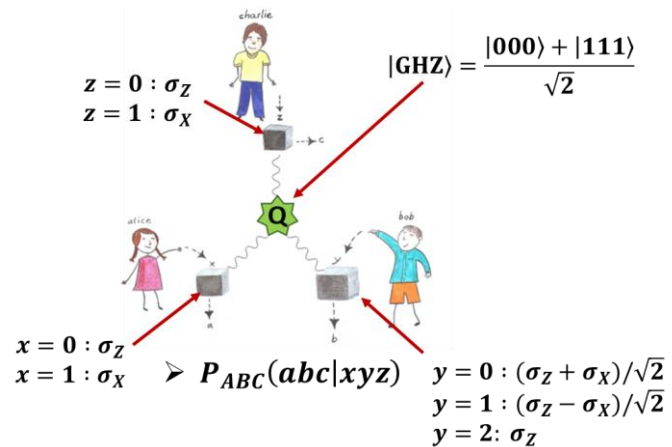
- If the crazy sources satisfy causality and can be duplicated in independent copies:

- Do Inflation

Foundations: Some past works

Experimentalist

- Master standard Quantum Theory
- Construct a **concrete experiment**



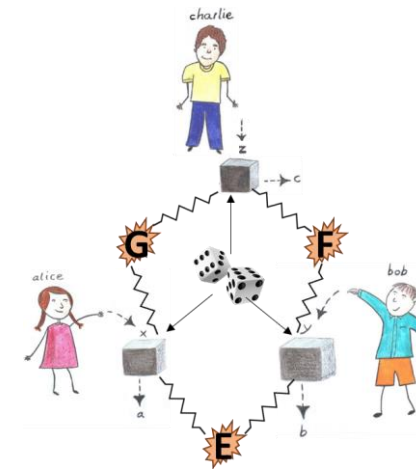
- Obtains **experimental results** (statistics)

$$\langle A_0 B_2 \rangle + \langle B_2 C_0 \rangle = 2,$$

$$\langle A_0 B_0 \rangle^{C_1=1} + \langle A_0 B_1 \rangle^{C_1=1} + \langle A_1 B_0 \rangle^{C_1=1} - \langle A_1 B_1 \rangle^{C_1=1} = 2\sqrt{2}$$

Detective

- Believes in bipartite « crazy » sources and shared randomness

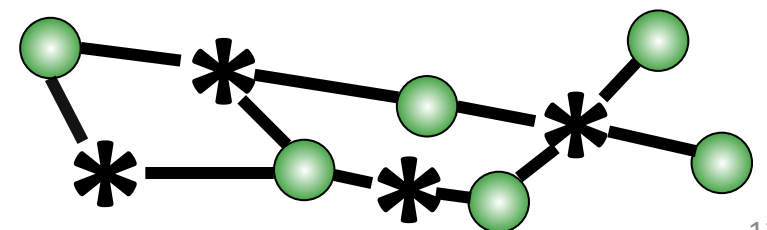
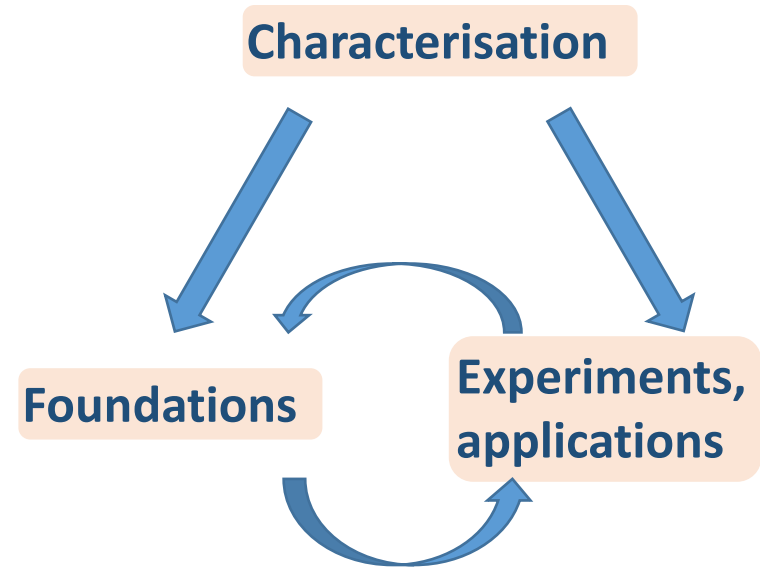
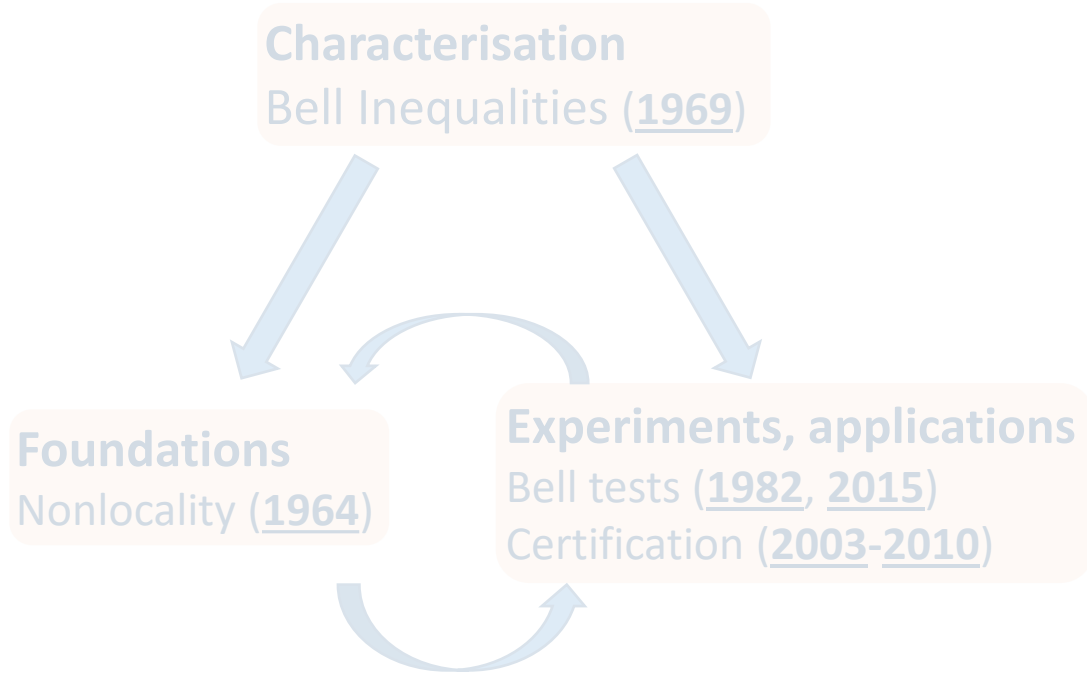


- If the crazy sources satisfy causality and can be duplicated in independent copies:

- Do Inflation

- **Detective explanation must fail**

Causal network quantum correlations



Foundations: ongoing and future goals

Alternative Theory

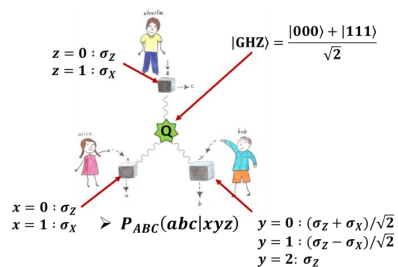
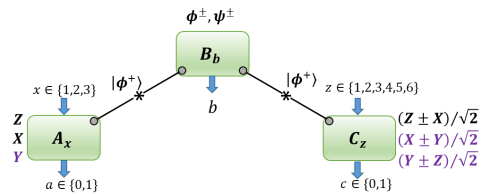
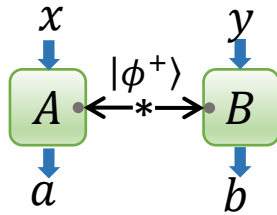
Classical physics

\mathbb{R} – quantum theory

Generalised bipartite entanglement

More?

Incompatibility



...

Reconstruct QIT from its correlations?

- Bell theorem excludes LHV models
- \mathbb{R} – quantum theory excluded
- Generalised bipartite entanglement excluded

Foundations: ongoing and future goals

Alternative Theory

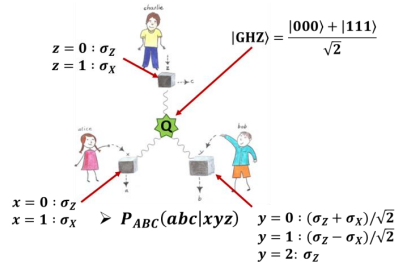
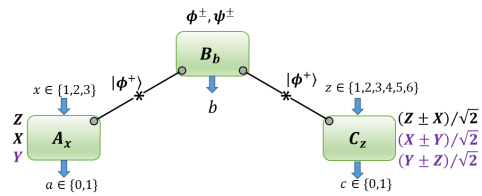
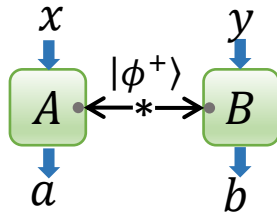
Classical physics

\mathbb{R} – quantum theory

Generalised bipartite entanglement

More?

Incompatibility



...

Reconstruct QIT from its correlations?

- Bell theorem excludes LHV models
 - \mathbb{R} – quantum theory excluded
 - Generalised bipartite entanglement excluded
- Exclude more ?
- **Characterise Quantum Information Theory from its correlations?**