Title: Randomness amplification

Date: May 10, 2011 04:10 PM

URL: http://pirsa.org/11050053

Abstract: I will discuss what we know about creating randomness within physics. Although quantum theory prescribes completely random outcomes to particular processes, could it be that within a yet-to-be-discovered post-quantum theory these outcomes are predictable? We have recently shown that this is not possible, using a very natural assumption. In the present talk, I will discuss some recent progress towards relaxing this assumption, providing arguably the strongest evidence yet for truly random processes in our world.

Free Randomness Amplification

Roger Colbeck (Perimeter Institute)
Based on work with Renato Renner
and ideas in arXiv:1005.5173
10th May 2011

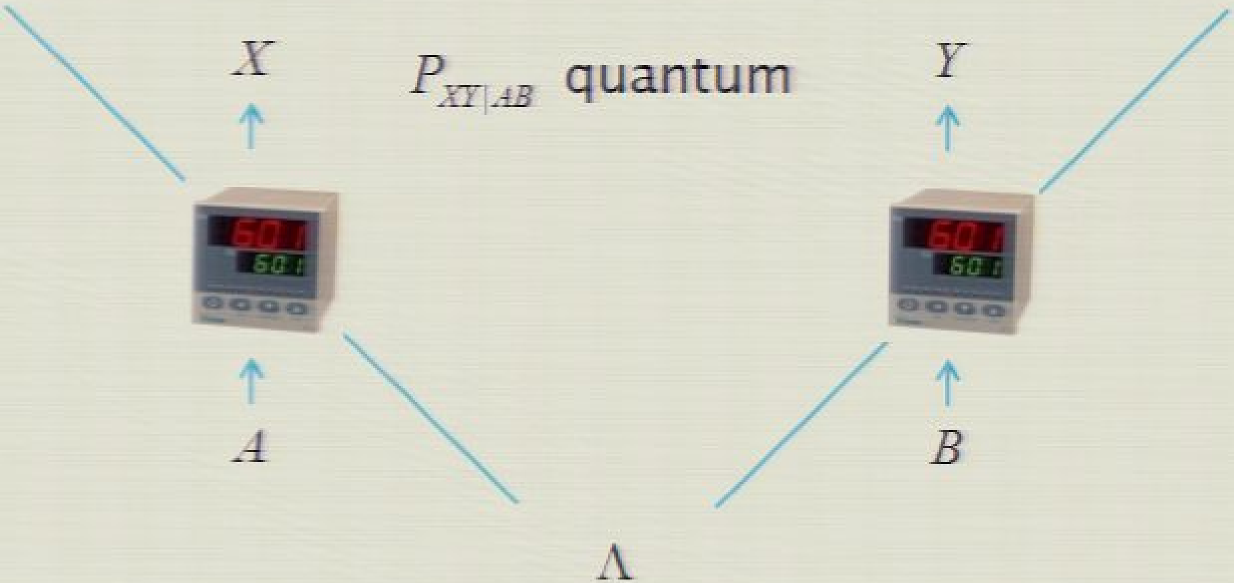
Are there fundamentally random processes?

- Classical theory: no
  - All randomness can be attributed to lack of knowledge
  - An all-knowing observer could predict the future time evolution of the entire universe
- Quantum theory: yes
  - For example, measure a $|+\rangle$ state in the $\{|0\rangle, |1\rangle\}$ basis

Can we really be sure?

- Quantum randomness led EPR to question the completeness of quantum theory and inspired the search for hidden variable models to explain the apparently random outcomes
- For some quantum experiments, it is easy to explain the random outcomes via hidden variables
- However, Bell later showed that no local hidden variable model can explain the outcomes of certain measurements on a maximally entangled pair.

Bell's theorem



- It cannot be that X and Y are functions of the locally accessible parameters, i.e. we cannot have $P_{X|A\Lambda} \in \{0,1\}$ and $P_{Y|B\Lambda} \in \{0,1\}$

Is that enough?

- Bell's theorem doesn't guarantee perfect randomness in the outcomes: it only says there is no way to predict the outcomes perfectly (some randomness in outcomes)

- Bell's theorem is based on certain assumptions:
  - Locality
  - Free measurement settings

The assumption of free measurement settings is sufficient

- It turns out that the assumption that the measurement settings are free alone is sufficient to conclude that the outcomes of measurements on EPR pairs are completely unpredictable.

- See "Quantum Theory cannot be extended", arXiv:1005.5173

Is that enough?

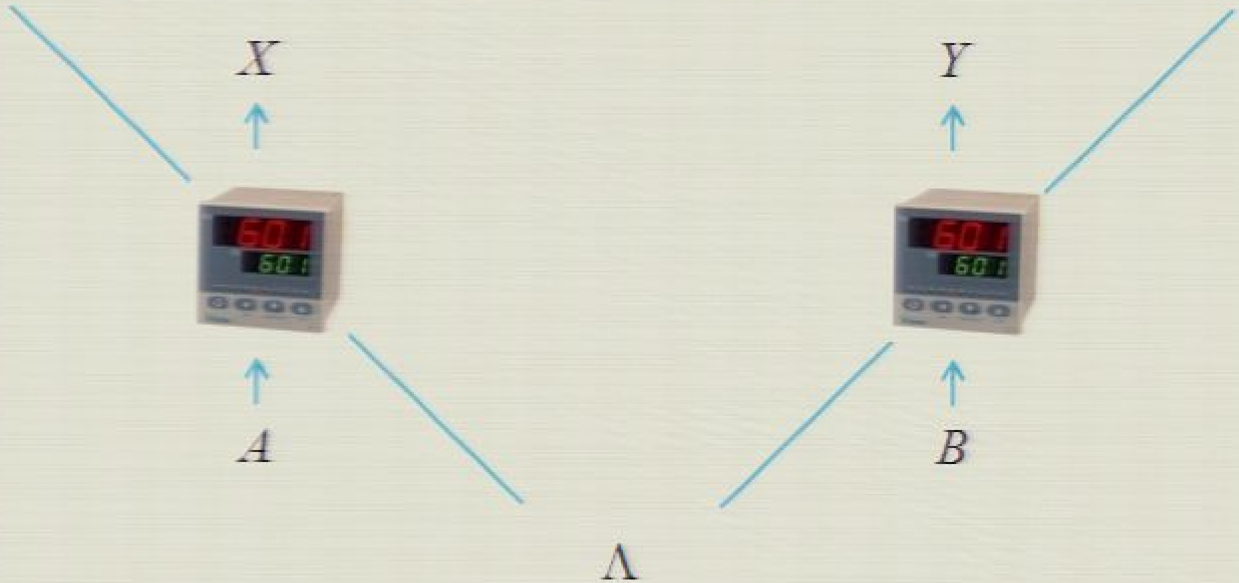
- Bell's theorem doesn't guarantee perfect randomness in the outcomes: it only says there is no way to predict the outcomes perfectly (some randomness in outcomes)

- Bell's theorem is based on certain assumptions:
  - Locality
  - Free measurement settings

The assumption of free measurement settings is sufficient

- It turns out that the assumption that the measurement settings are free alone is sufficient to conclude that the outcomes of measurements on EPR pairs are completely unpredictable.
- See “Quantum Theory cannot be extended”, arXiv:1005.5173

The assumption of free measurement settings is sufficient



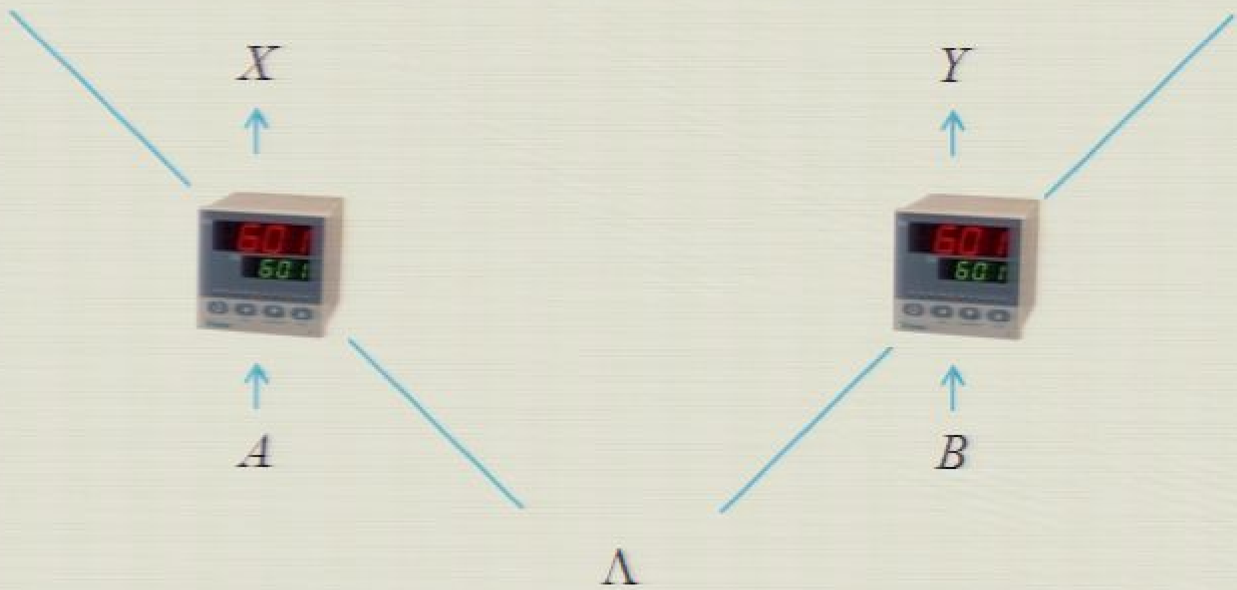
- $P_{A|BY\Lambda} = P_A$, $P_{B|AY\Lambda} = P_B$ and quantum correlations imply $P_{X|A\Lambda} = P_{\overline{X}}$
  (where $P_{\overline{X}}$ denotes the uniform distribution on X)

The assumption of free measurement settings is sufficient

- It turns out that the assumption that the measurement settings are free alone is sufficient to conclude that the outcomes of measurements on EPR pairs are completely unpredictable.

- See “Quantum Theory cannot be extended”, arXiv:1005.5173

The assumption of free measurement settings is sufficient



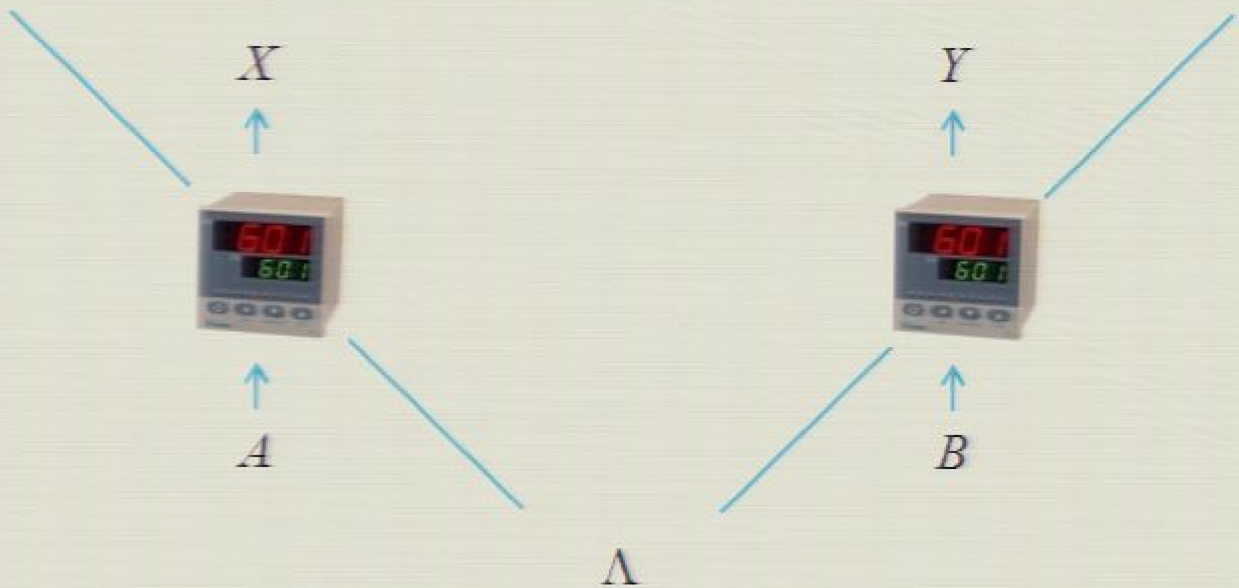
- $P_{A|BY\Lambda} = P_A$, $P_{B|AY\Lambda} = P_B$ and quantum correlations imply $P_{X|A\Lambda} = P_{\overline{X}}$
(where $P_{\overline{X}}$ denotes the uniform distribution on X)

The assumption of free measurement settings is sufficient

- It turns out that the assumption that the measurement settings are free alone is sufficient to conclude that the outcomes of measurements on EPR pairs are completely unpredictable.

- See "Quantum Theory cannot be extended", arXiv:1005.5173

The assumption of free measurement settings is sufficient

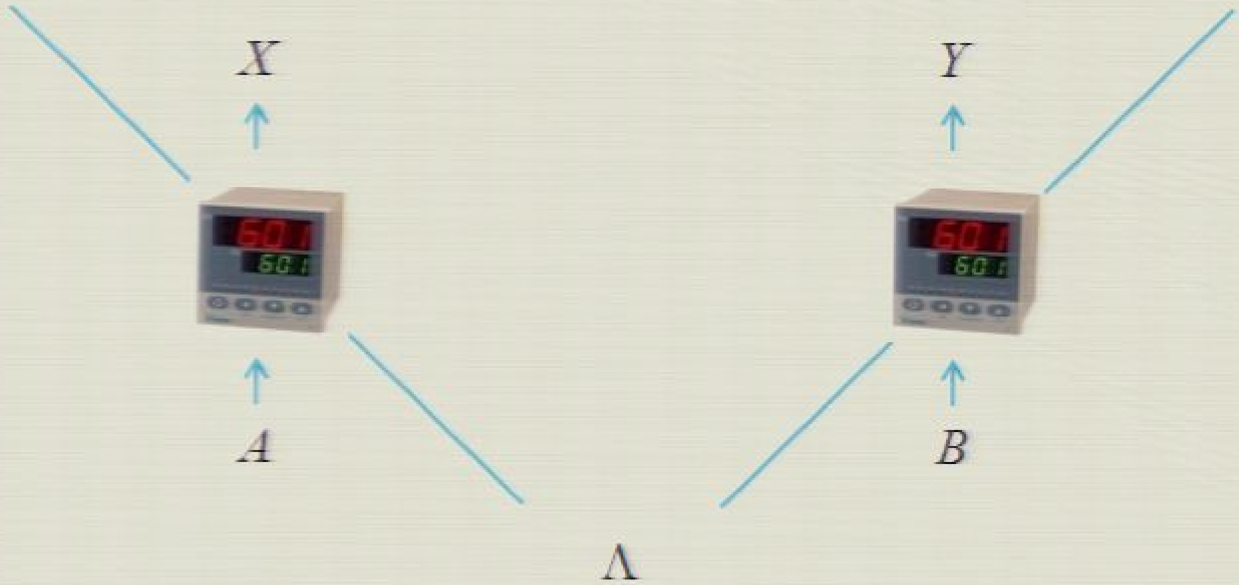


- $P_{A|BY\Lambda} = P_A$, $P_{B|AY\Lambda} = P_B$ and quantum correlations imply $P_{X|A\Lambda} = P_{\overline{X}}$
(where $P_{\overline{X}}$ denotes the uniform distribution on X)

So are there truly random processes?

- For the purpose of arguing for the existence of truly random processes, this is a little unsatisfying, because it says that if the measurement settings are free and random, so are the outcomes.
- Cf Conway and Kochen's "Free Will Theorem": if the experimentalists have free will, then so do the particles.
- Our aim here is to explore the weakening of the free choice assumption.

The assumption of free measurement settings is sufficient

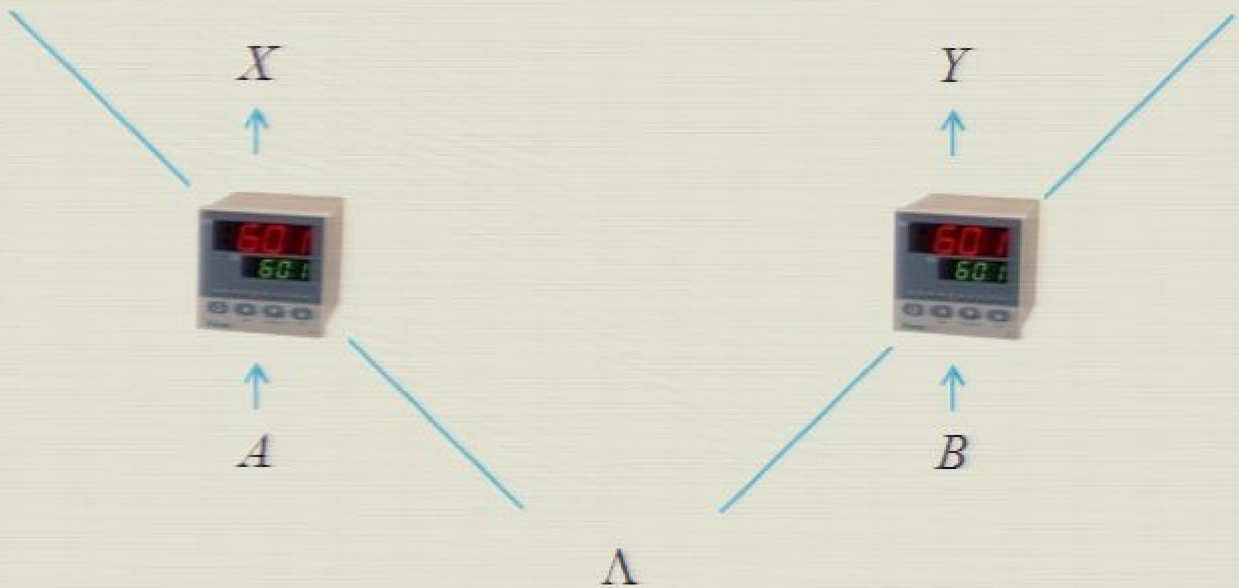


- $P_{A|BY\Lambda} = P_A$, $P_{B|AY\Lambda} = P_B$ and quantum correlations imply $P_{X|A\Lambda} = P_{\overline{X}}$
(where $P_{\overline{X}}$ denotes the uniform distribution on X)

So are there truly random processes?

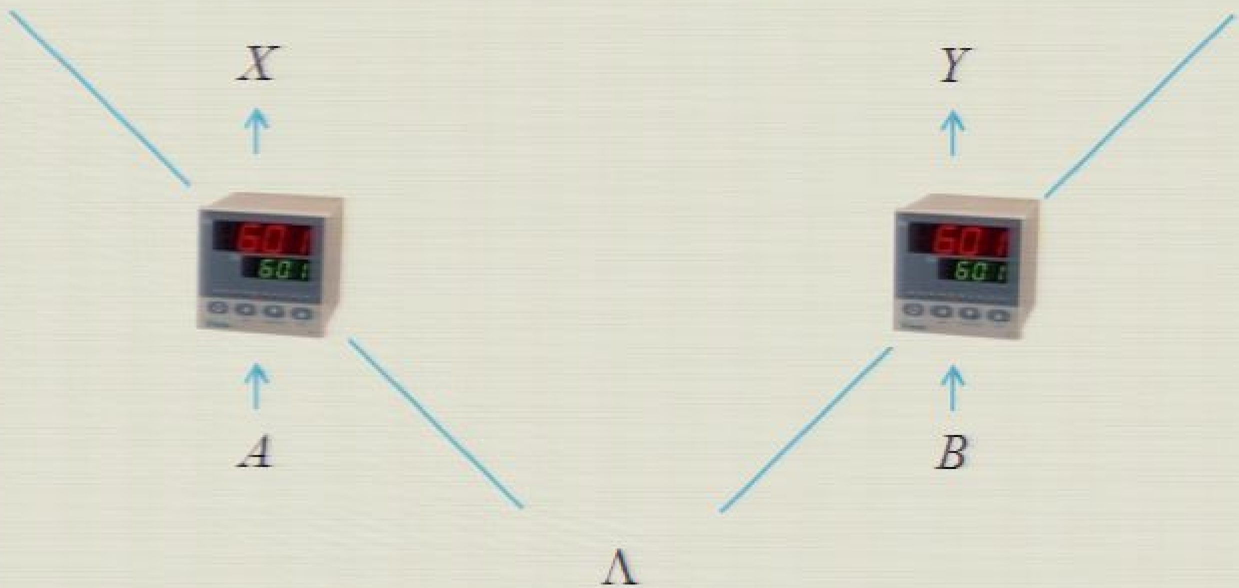
- For the purpose of arguing for the existence of truly random processes, this is a little unsatisfying, because it says that if the measurement settings are free and random, so are the outcomes.
- Cf Conway and Kochen's "Free Will Theorem": if the experimentalists have free will, then so do the particles.
- Our aim here is to explore the weakening of the free choice assumption.

The assumption of free measurement settings is sufficient



- $P_{A|BY\Lambda} = P_A$, $P_{B|AY\Lambda} = P_B$ and quantum correlations imply $P_{X|A\Lambda} = P_{\overline{X}}$
(where $P_{\overline{X}}$ denotes the uniform distribution on X)

The assumption of free measurement settings is sufficient



- $P_{A|BY\Lambda} = P_A$, $P_{B|AY\Lambda} = P_B$ and quantum correlations imply $P_{X|A\Lambda} = P_{\overline{X}}$
(where $P_{\overline{X}}$ denotes the uniform distribution on X)

So are there truly random processes?

- For the purpose of arguing for the existence of truly random processes, this is a little unsatisfying, because it says that if the measurement settings are free and random, so are the outcomes.
- Cf Conway and Kochen's "Free Will Theorem": if the experimentalists have free will, then so do the particles.
- Our aim here is to explore the weakening of the free choice assumption.

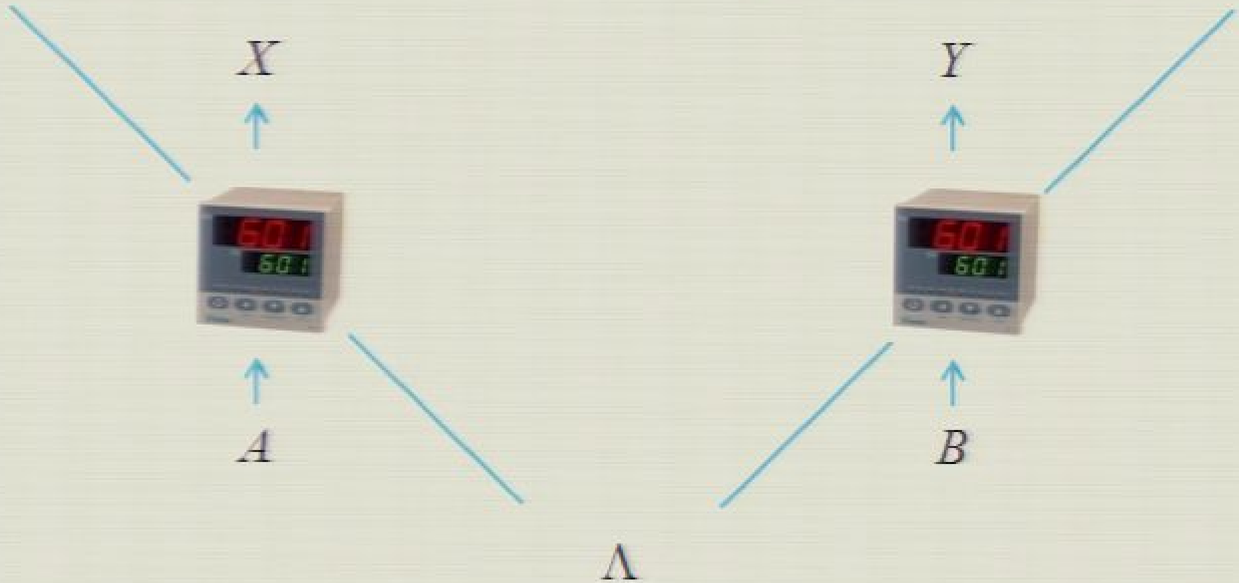
Definitions

- We say that X is perfectly free if it is uncorrelated with anything outside its future lightcone.
- Likewise, X is ε–free if $D(P_{X|\Gamma}, P_{\bar{X}}) \leq \varepsilon$, where Γ is the set of variables outside the future lightcone of X, and D is the variational distance

$$D(P_X, Q_X) = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)|.$$

- Note that if X is a bit, $0 \leq \varepsilon \leq 1/2$

The assumption of free measurement settings is sufficient



- $P_{A|BY\Lambda} = P_A$, $P_{B|AY\Lambda} = P_B$ and quantum correlations imply $P_{X|A\Lambda} = P_{\overline{X}}$

(where $P_{\overline{X}}$ denotes the uniform distribution on X)

Definitions

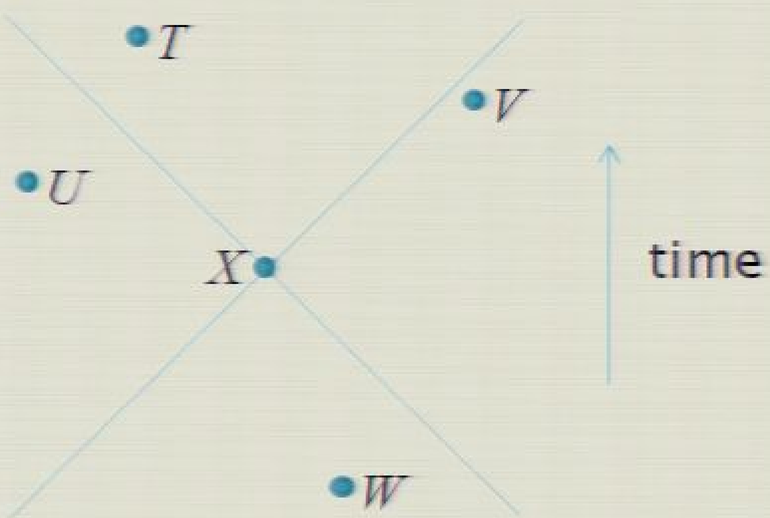
- We say that X is perfectly free if it is uncorrelated with anything outside its future lightcone.
- Likewise, X is ε–free if $D(P_{X|\Gamma}, P_{\bar{X}}) \leq \varepsilon$, where Γ is the set of variables outside the future lightcone of X, and D is the variational distance

$$D(P_X, Q_X) = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)|.$$

- Note that if X is a bit, $0 \leq \varepsilon \leq 1/2$

Definitions

- X is ε–free if $D(P_{X|\Gamma}, P_{\bar{X}}) \leq \varepsilon$, where Γ is the set of variables outside the future lightcone of X.



$U, V, W \in \Gamma$

$T \notin \Gamma$

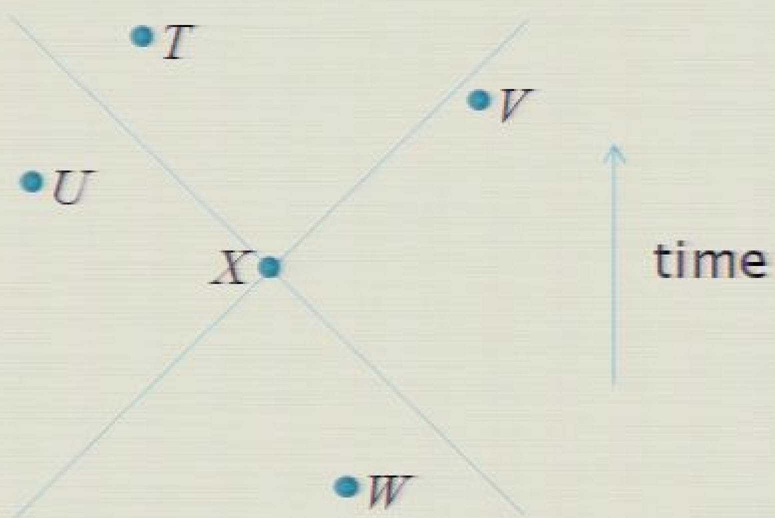
Intuitive idea: X cannot be free if it is correlated with something in its past (in some frame).

Aim

- Free randomness amplification is the task of making ε smaller.
- Ideally, we want to show that ε–free bits can be used to generate bits that are arbitrarily close to perfectly free.
- Main result: this is possible for a range of ε.
- (We do not assume completeness of QM)

Definitions

- X is ε–free if $D(P_{X|\Gamma}, P_{\bar{X}}) \leq \varepsilon$, where Γ is the set of variables outside the future lightcone of X.



$$U, V, W \in \Gamma$$

$$T \notin \Gamma$$

Intuitive idea: X cannot be free if it is correlated with something in its past (in some frame).

Definitions

- We say that X is perfectly free if it is uncorrelated with anything outside its future lightcone.
- Likewise, X is ε–free if $D(P_{X|\Gamma}, P_{\overline{X}}) \leq \varepsilon$, where Γ is the set of variables outside the future lightcone of X, and D is the variational distance

$$D(P_X, Q_X) = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)|.$$

- Note that if X is a bit, $0 \leq \varepsilon \leq 1/2$

Definitions

- We say that X is perfectly free if it is uncorrelated with anything outside its future lightcone.
- Likewise, X is ε–free if $D(P_{X|\Gamma}, P_{\bar{X}}) \leq \varepsilon$, where Γ is the set of variables outside the future lightcone of X, and D is the variational distance

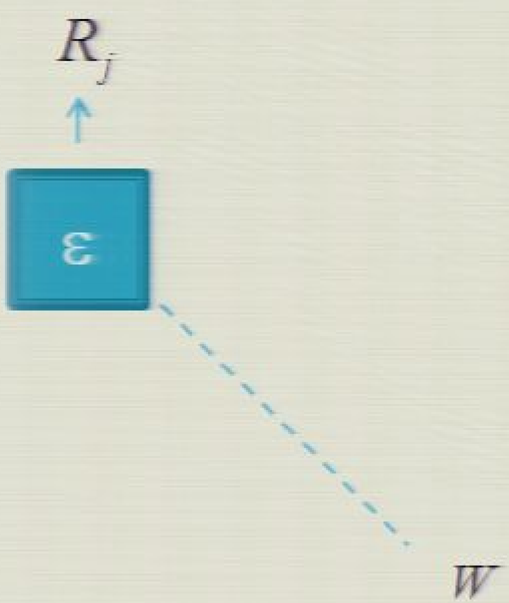
$$D(P_X, Q_X) = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)|.$$

- Note that if X is a bit, $0 \leq \varepsilon \leq 1/2$

Aim

- Free randomness amplification is the task of making ε smaller.
- Ideally, we want to show that ε–free bits can be used to generate bits that are arbitrarily close to perfectly free.
- Main result: this is possible for a range of ε.
- (We do not assume completeness of QM)

Modelling the ε–free sources



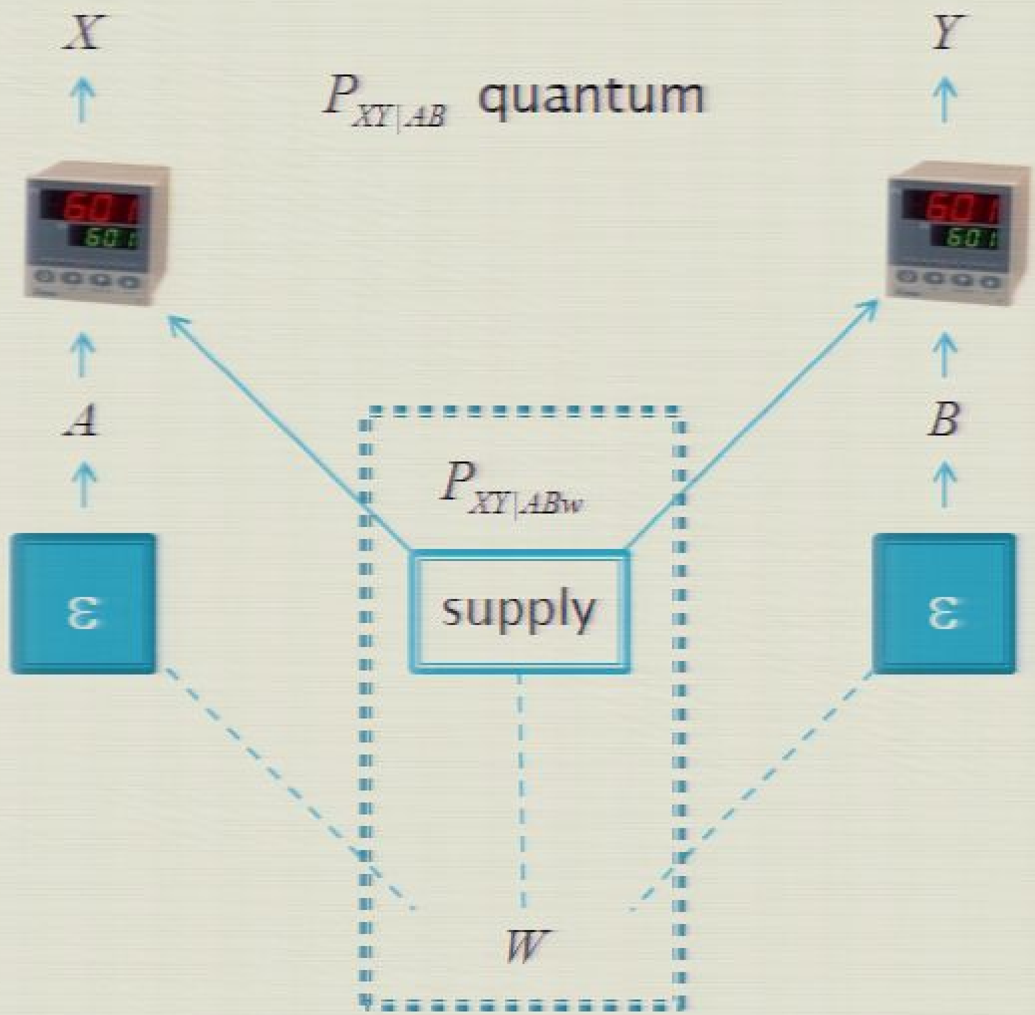
- We use an adversarial model of the sources of bits
- An adversary picks W and the source behaves such that, e.g.

$$P(R_j = 0 | W = 0) = 1/2 + \varepsilon$$

$$P(R_j = 1 | W = 0) = 1/2 - \varepsilon$$

- Note that the adversary can always symmetrize their strategy so that P_{R_j} looks uniform

Adversarial picture



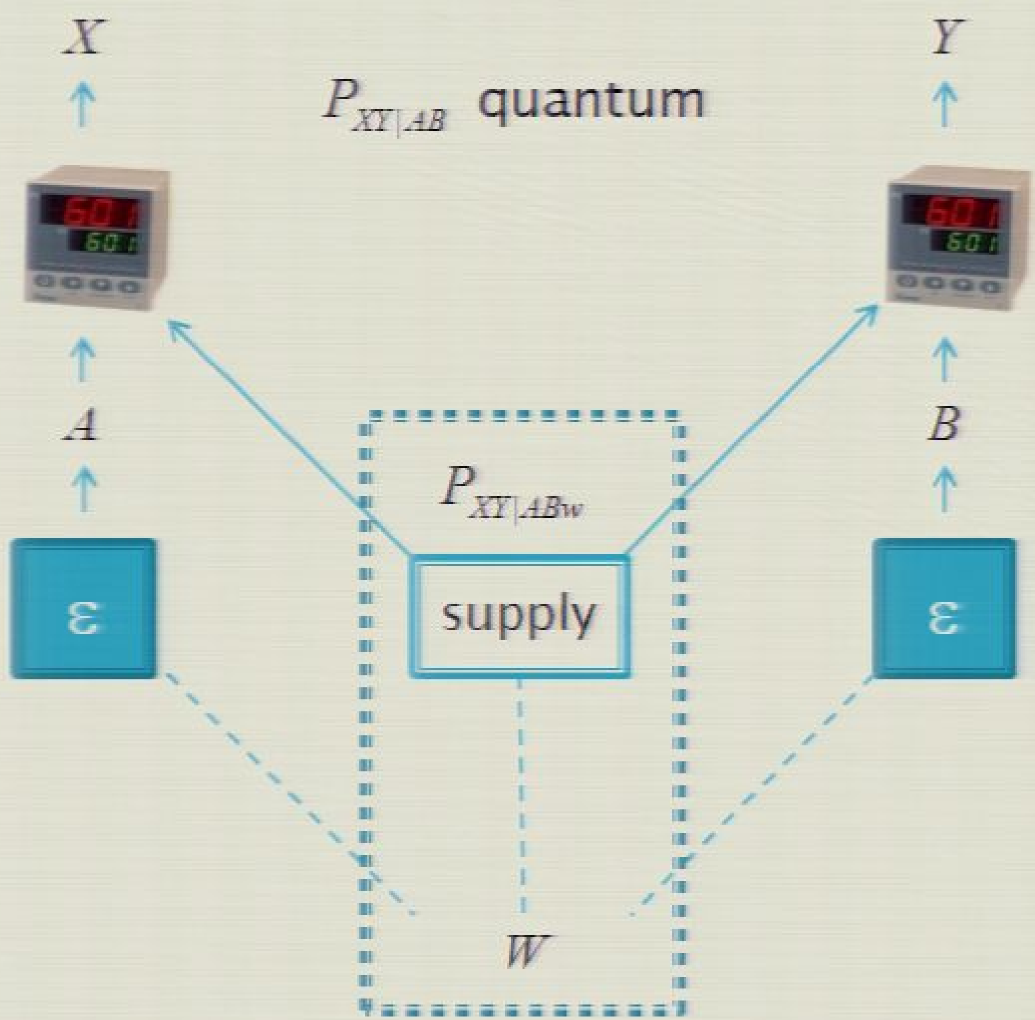
Controlled by adversary

Illustration for bipartite case, but in general there may be more parties.

Adversarial picture

- If W is completely correlated with A and B, then it is easy to recreate any correlations $P_{XY|AB}$ with a deterministic model.
- In order that it is in principle possible for there to be perfectly free bits, $P_{XY|ABw}$ should be non-signalling.

Adversarial picture



Controlled by adversary

Illustration for bipartite case, but in general there may be more parties.

Adversarial picture

- If W is completely correlated with A and B, then it is easy to recreate any correlations $P_{XY|AB}$ with a deterministic model.
- In order that it is in principle possible for there to be perfectly free bits, $P_{XY|ABw}$ should be non-signalling.

Adversarial picture

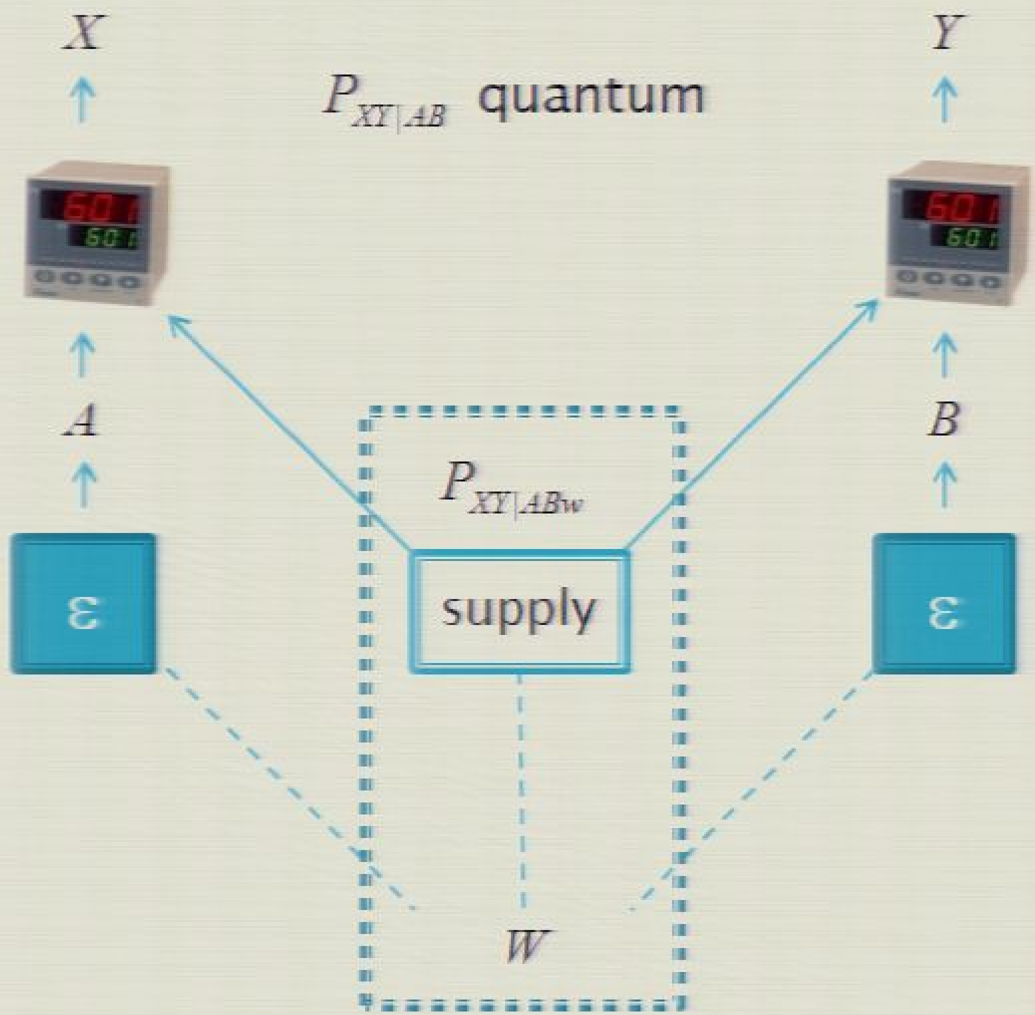


Illustration for bipartite case, but in general there may be more parties.

Controlled by adversary

Adversarial picture

- If W is completely correlated with A and B, then it is easy to recreate any correlations $P_{XY|AB}$ with a deterministic model.
- In order that it is in principle possible for there to be perfectly free bits, $P_{XY|ABw}$ should be non-signalling.

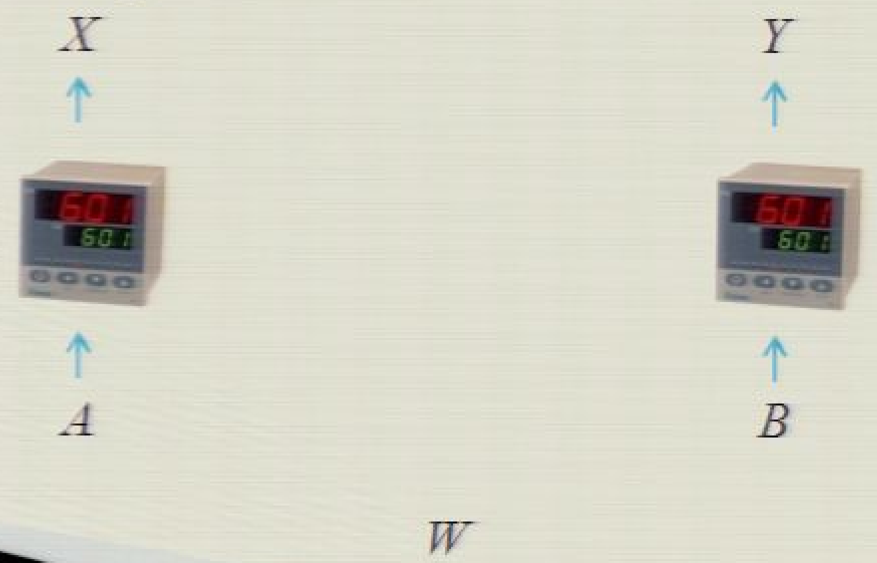
The non-signalling – free choice connection

- Suppose X conveys information about B so that $P_{X|ABw} \neq P_{X|Aw}$, i.e. there is signalling.

- Then it cannot be that $P_{B|AXw} = P_B$, i.e. that B is free.

Adversarial picture

- If W is completely correlated with A and B, then it is easy to recreate any correlations $P_{XY|AB}$ with a deterministic model.
- In order that it is in principle possible for there to be perfectly free bits, $P_{XY|ABw}$ should be non-signalling.



Adversarial picture

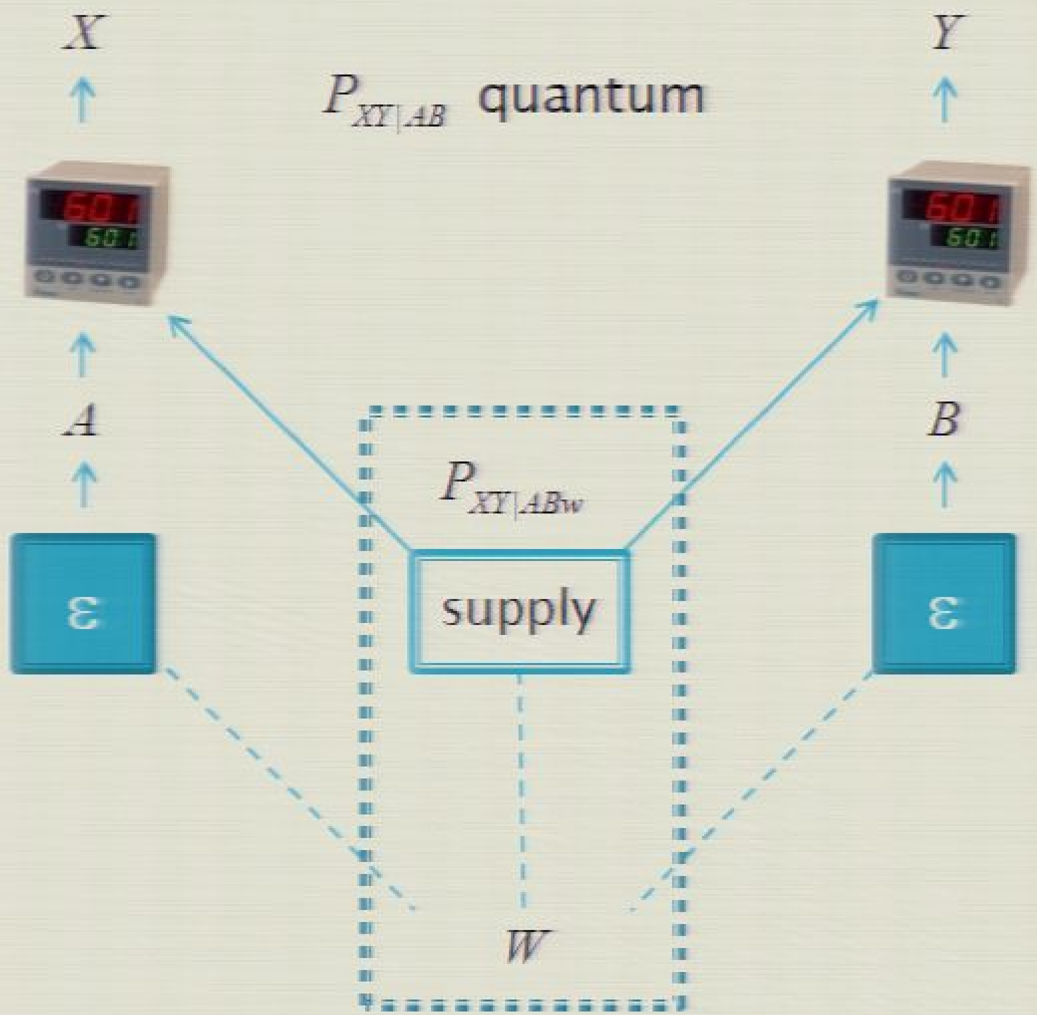


Illustration for bipartite case, but in general there may be more parties.

Controlled by adversary

Adversarial picture

- If W is completely correlated with A and B, then it is easy to recreate any correlations $P_{XY|AB}$ with a deterministic model.
- In order that it is in principle possible for there to be perfectly free bits, $P_{XY|ABw}$ should be non-signalling.

The non-signalling – free choice connection

- Suppose X conveys information about B so that $P_{X|ABw} \neq P_{X|Aw}$, i.e. there is signalling.

- Then it cannot be that $P_{B|AXw} = P_B$, i.e. that B is free.

Positive result

- Technique based on bipartite quantum correlations gives that provided the partially free initial bits are ε–free, for $\varepsilon \leq (1 - \frac{1}{\sqrt{2}})^2 \approx 0.09$, the output bits are arbitrarily free.

- Proof based on chained Bell correlations, whose power for device-independent cryptography was first realized by Barrett, Hardy and Kent (PRL 95, 010503 (2005)).

Adversarial picture

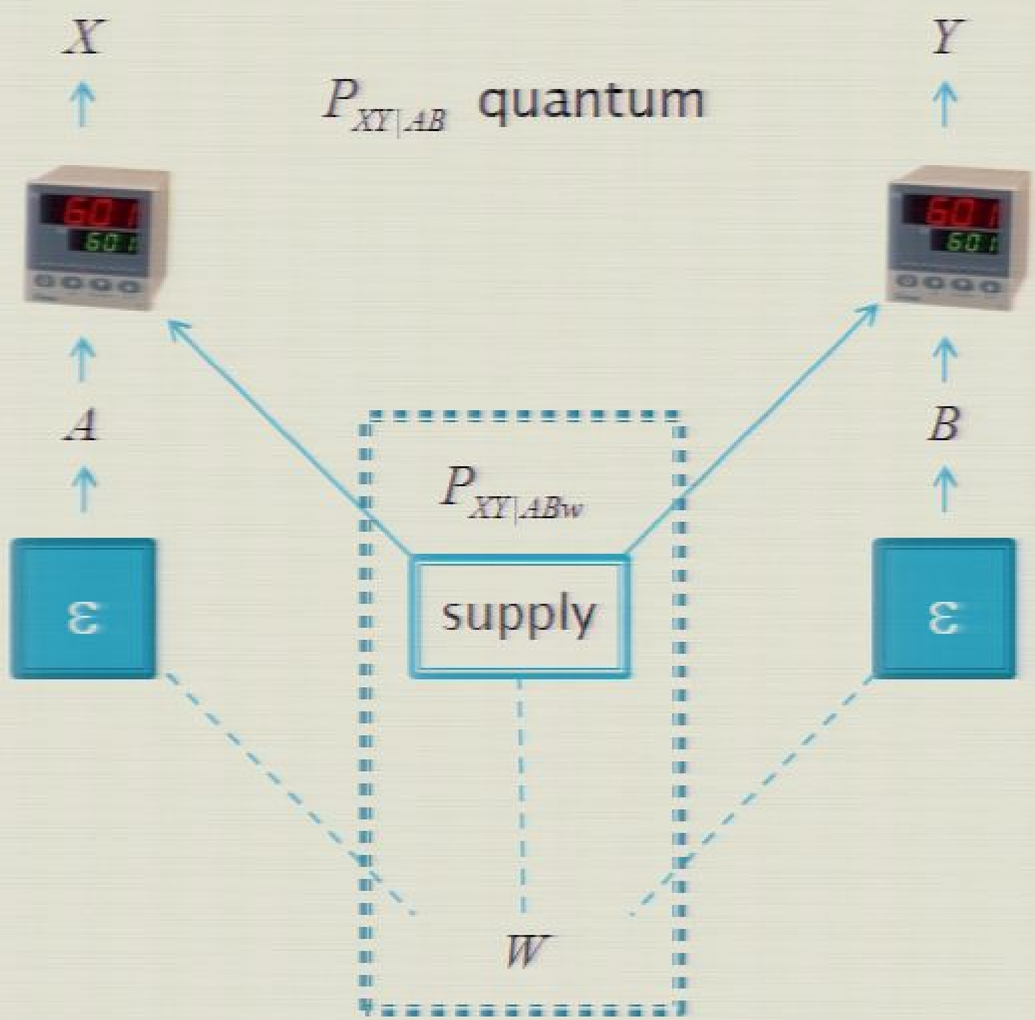


Illustration for bipartite case, but in general there may be more parties.

Controlled by adversary

Positive result

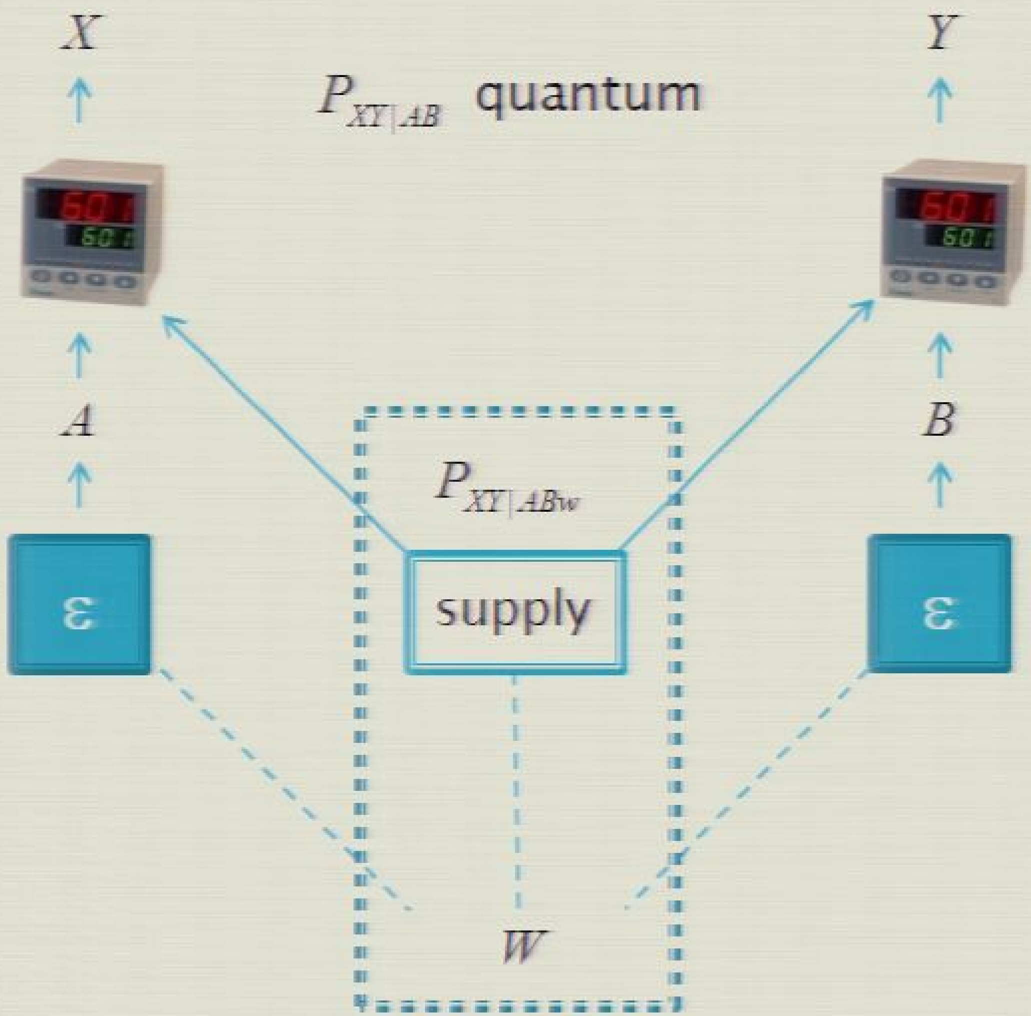
- Technique based on bipartite quantum correlations gives that provided the partially free initial bits are ε–free, for $\varepsilon \leq (1-\frac{1}{\sqrt{2}})^2 \approx 0.09$, the output bits are arbitrarily free.

- Proof based on chained Bell correlations, whose power for device–independent cryptography was first realized by Barrett, Hardy and Kent (PRL 95, 010503 (2005)).

Positive result

- Chained Bell correlations are a family of quantum correlations $P_{XY|AB}$, with the property that X is uncorrelated with any other variables.
- If A and B are not free, then the correlations can look like they have the correct distribution when really they do not.

Positive result



Controlled by adversary

- An adversary can say "given my knowledge of A and B, I can send a different distribution $P_{XY|ABw}$ without being detected"
- With only a small loss of freedom, $\varepsilon \leq 0.09$ the correlations are still strong enough to conclude that X is uncorrelated with any other variables.

Negative result

- Any technique based on these correlations is limited: it can be seen to fail if the partially free sources have $\varepsilon \geq \frac{1}{2}(1-\frac{1}{\sqrt{2}}) \approx 0.15$
- This is the value for which the correlations can be explained by a classical model
- Related to the question "How much free will is required to demonstrate nonlocality?" (see work by Hall (arXiv:1007.5518) and Barrett and Gisin (arXiv:1008.3612)

Extending the result

- Ideally we would like to show that, for any $0 \leq \varepsilon < 1/2$, ε–free bits can be amplified to arbitrarily free ones.

- A hint that higher dimensional systems may allow this comes from the observation that for any $0 \leq \varepsilon < 1/2$, ε–free bits are sufficient to demonstrate nonlocality.

Negative result

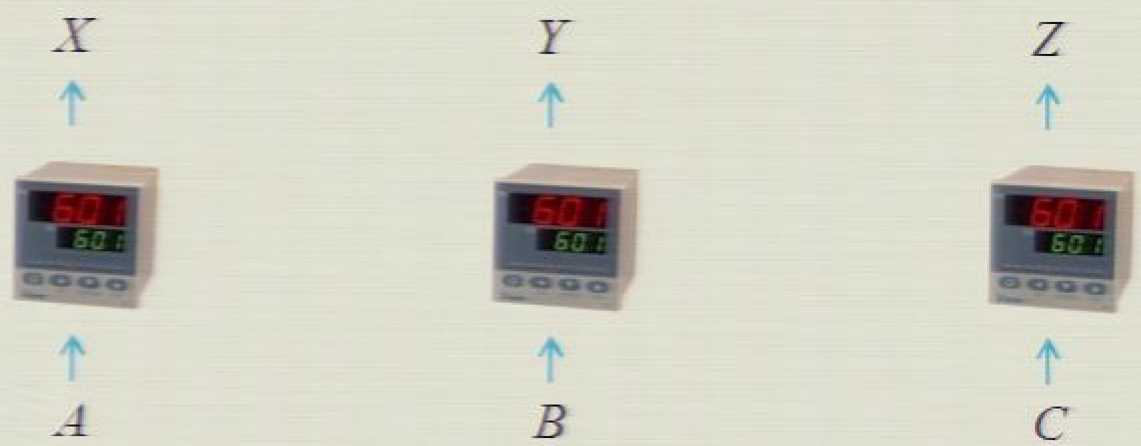
- Any technique based on these correlations is limited: it can be seen to fail if the partially free sources have $\varepsilon \geq \frac{1}{2}(1-\frac{1}{\sqrt{2}}) \approx 0.15$
- This is the value for which the correlations can be explained by a classical model
- Related to the question "How much free will is required to demonstrate nonlocality?" (see work by Hall (arXiv:1007.5518) and Barrett and Gisin (arXiv:1008.3612)

GHZ relations

- Correlations satisfy:

$$x \times y \times z = -1 \quad \text{if} \quad (a,b,c) = (0,0,0)$$

$$x \times y \times z = +1 \quad \text{if} \quad (a,b,c) = (0,1,1), (1,0,1) \text{ or } (1,1,0)$$



$X, Y, Z \in \{+1, -1\}$

$A, B, C \in \{0, 1\}$

- Best classical strategy satisfies 3 of these relations

Verifying nonlocality

- Best classical strategy is to position the unsatisfied relation for the least likely A, B and C.

- Using the ε–free bits to choose A, B and C, the probability of the least likely combination is $(1/2-\varepsilon)^3$.

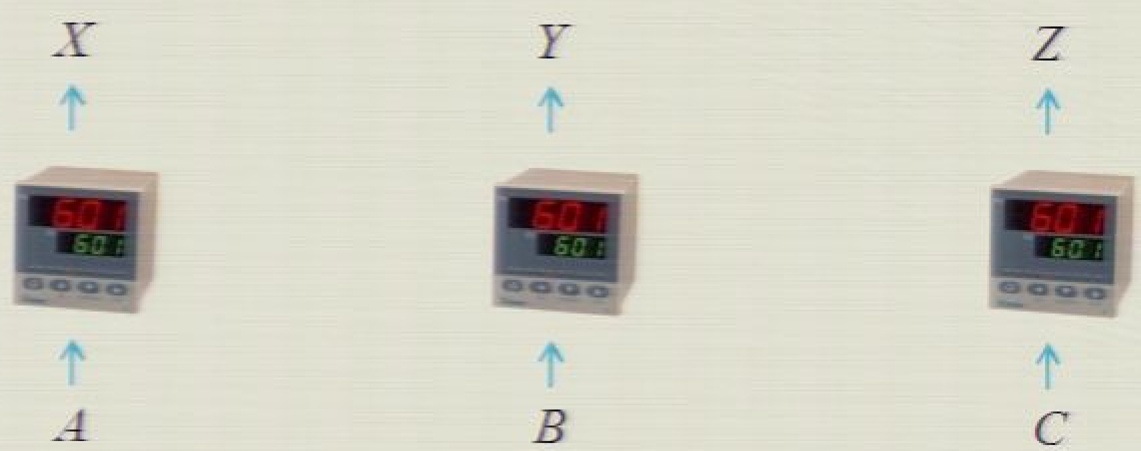
- Hence, for any $\varepsilon < 1/2$, we would be able to detect this with enough measurements

GHZ relations

- Correlations satisfy:

$$x \times y \times z = -1 \quad \text{if} \quad (a,b,c) = (0,0,0)$$

$$x \times y \times z = +1 \quad \text{if} \quad (a,b,c) = (0,1,1), (1,0,1) \text{ or } (1,1,0)$$



$$X, Y, Z \in \{+1, -1\}$$

$$A, B, C \in \{0,1\}$$

- Best classical strategy satisfies 3 of these relations

Verifying nonlocality

- Best classical strategy is to position the unsatisfied relation for the least likely A, B and C.

- Using the ε–free bits to choose A, B and C, the probability of the least likely combination is $(1/2-\varepsilon)^3$.

- Hence, for any $\varepsilon < 1/2$, we would be able to detect this with enough measurements

GHZ relations

- Correlations satisfy:

$$x \times y \times z = -1 \quad \text{if} \quad (a,b,c) = (0,0,0)$$

$$x \times y \times z = +1 \quad \text{if} \quad (a,b,c) = (0,1,1), (1,0,1) \text{ or } (1,1,0)$$

X Y Z $\quad X, Y, Z \in \{+1, -1\}$

A B C $\quad A, B, C \in \{0, 1\}$

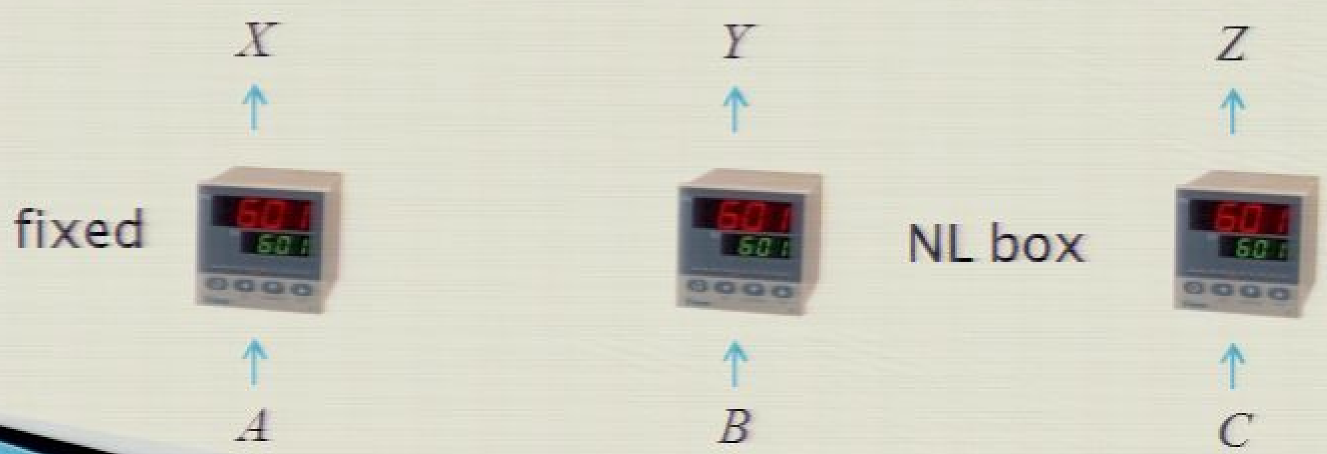
- Best classical strategy satisfies 3 of these relations

Verifying nonlocality

- Best classical strategy is to position the unsatisfied relation for the least likely A, B and C.
- Using the ε–free bits to choose A, B and C, the probability of the least likely combination is $(1/2-\varepsilon)^3$.
- Hence, for any $\varepsilon < 1/2$, we would be able to detect this with enough measurements

Towards an Extension of the result

- Tripartite GHZ correlations provide a good way to demonstrate nonlocality, but their outputs are not guaranteed to be free and random
- In fact, there are non-signalling strategies for which one of the outputs is determined (and hence not free at all)

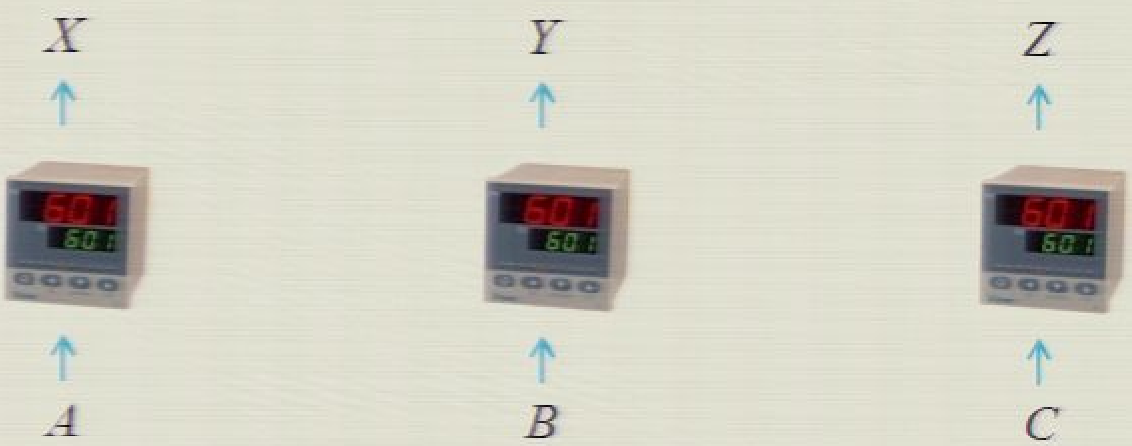


GHZ relations

- Correlations satisfy:

$$x \times y \times z = -1 \quad \text{if} \quad (a,b,c) = (0,0,0)$$

$$x \times y \times z = +1 \quad \text{if} \quad (a,b,c) = (0,1,1), (1,0,1) \text{ or } (1,1,0)$$



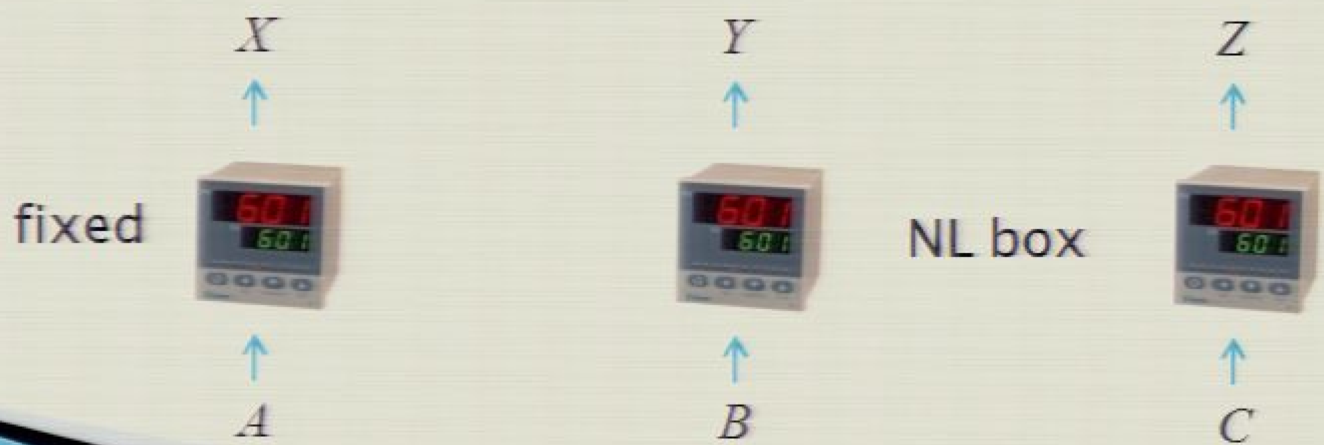
$$X, Y, Z \in \{+1, -1\}$$

$$A, B, C \in \{0,1\}$$

- Best classical strategy satisfies 3 of these relations

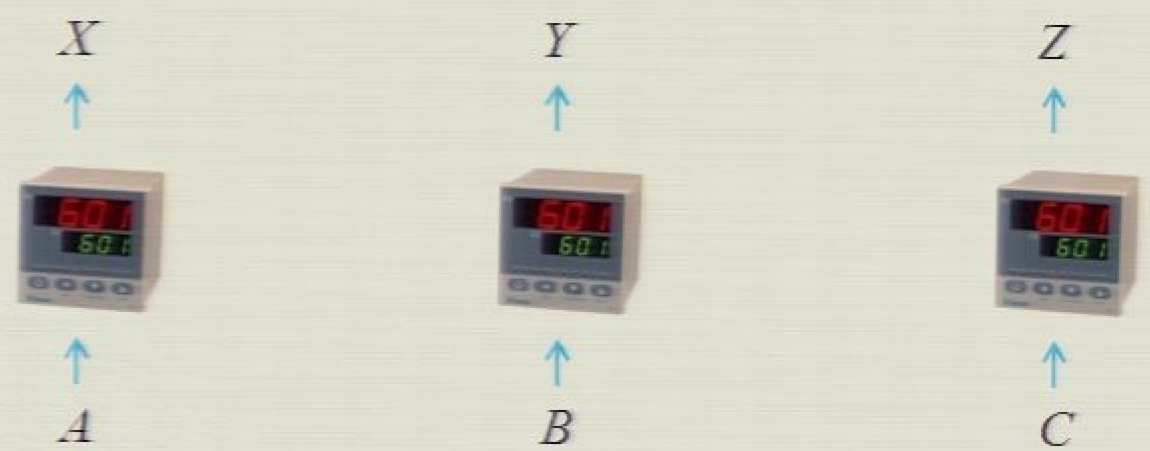
Towards an Extension of the result

- Tripartite GHZ correlations provide a good way to demonstrate nonlocality, but their outputs are not guaranteed to be free and random
- In fact, there are non-signalling strategies for which one of the outputs is determined (and hence not free at all)



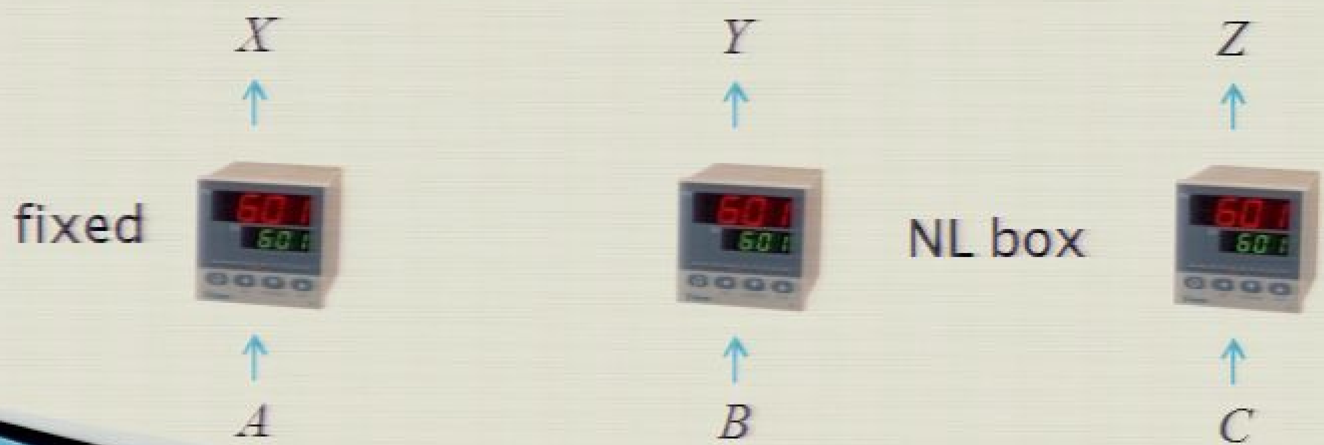
Towards an Extension of the result

- There is also a non-signalling strategy where each output can be correctly guessed with probability 2/3.



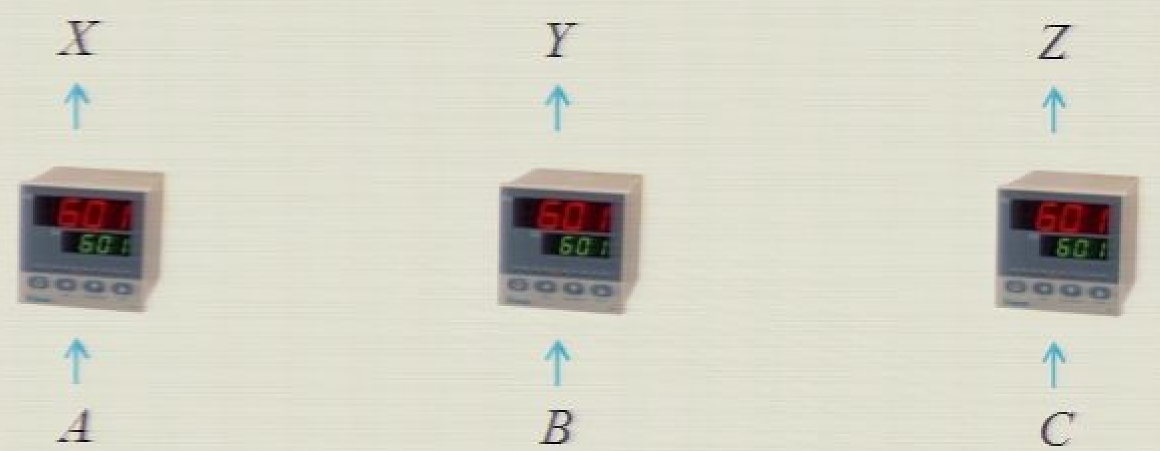
Towards an Extension of the result

- Tripartite GHZ correlations provide a good way to demonstrate nonlocality, but their outputs are not guaranteed to be free and random
- In fact, there are non-signalling strategies for which one of the outputs is determined (and hence not free at all)



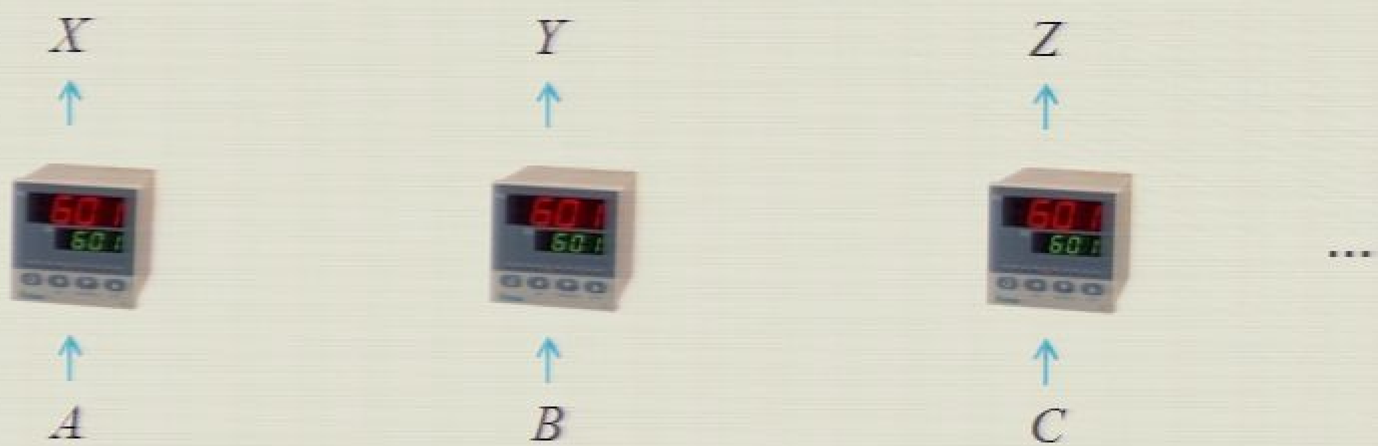
Towards an Extension of the result

- There is also a non-signalling strategy where each output can be correctly guessed with probability 2/3.



Towards an Extension of the result

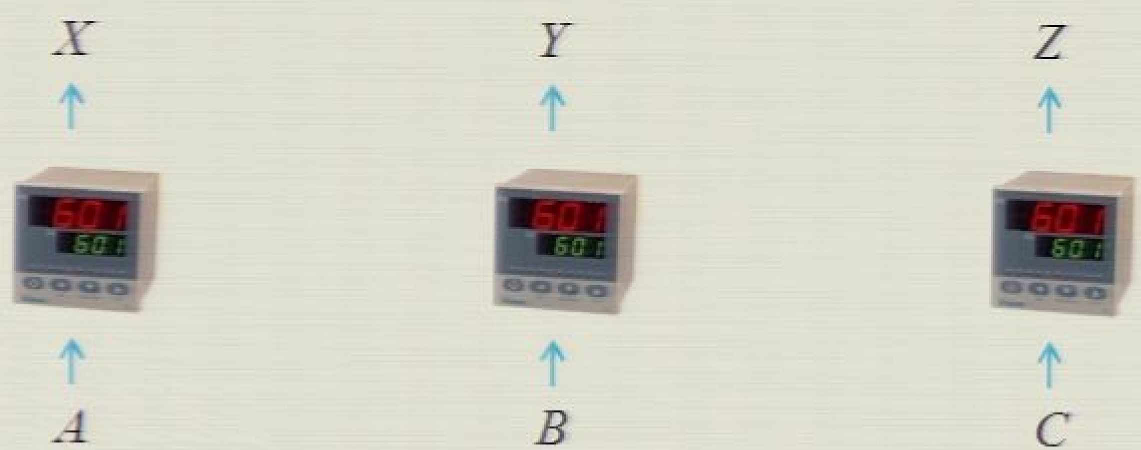
- Speculate that this improves with more systems (M-party GHZ correlations)



- Hope: for large M, any bit picked at random is with high probability very close to perfectly free.

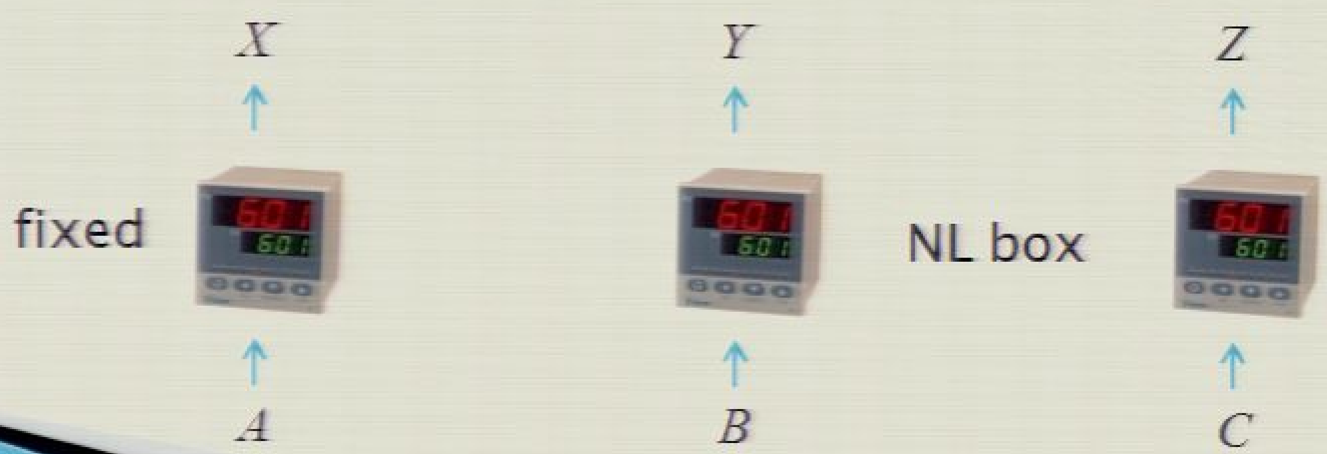
Towards an Extension of the result

- There is also a non-signalling strategy where each output can be correctly guessed with probability 2/3.



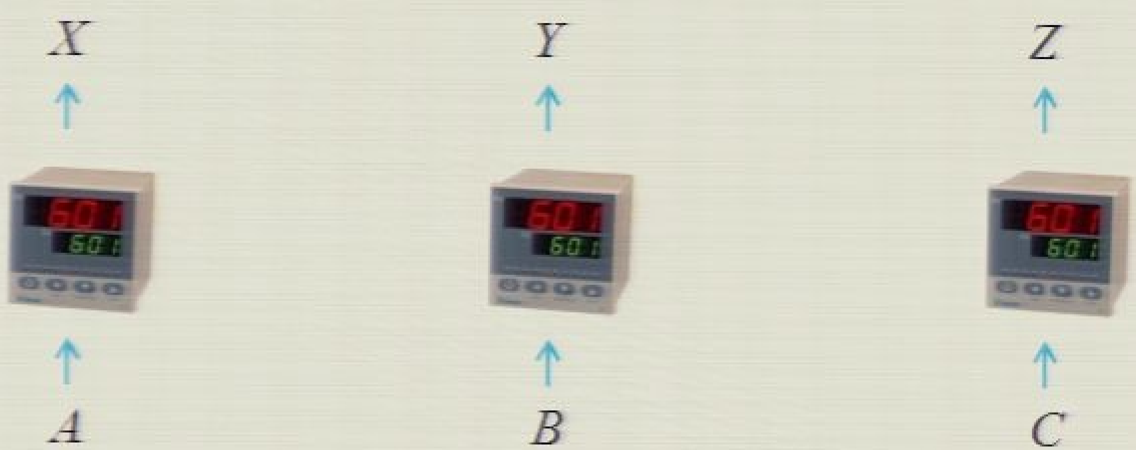
Towards an Extension of the result

- Tripartite GHZ correlations provide a good way to demonstrate nonlocality, but their outputs are not guaranteed to be free and random
- In fact, there are non-signalling strategies for which one of the outputs is determined (and hence not free at all)



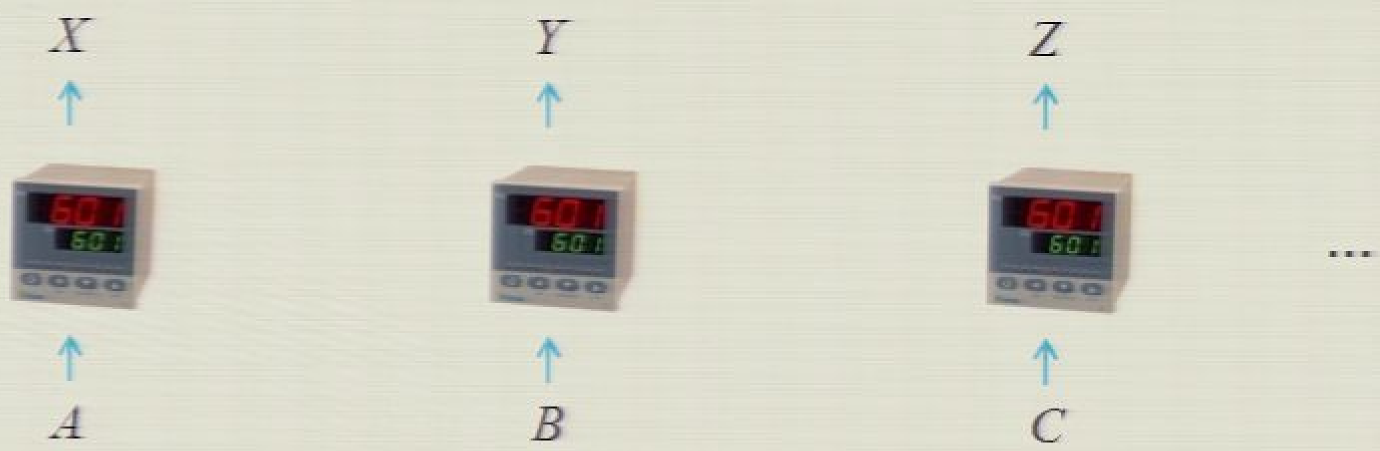
Towards an Extension of the result

- There is also a non-signalling strategy where each output can be correctly guessed with probability 2/3.



Towards an Extension of the result

- Speculate that this improves with more systems (M-party GHZ correlations)



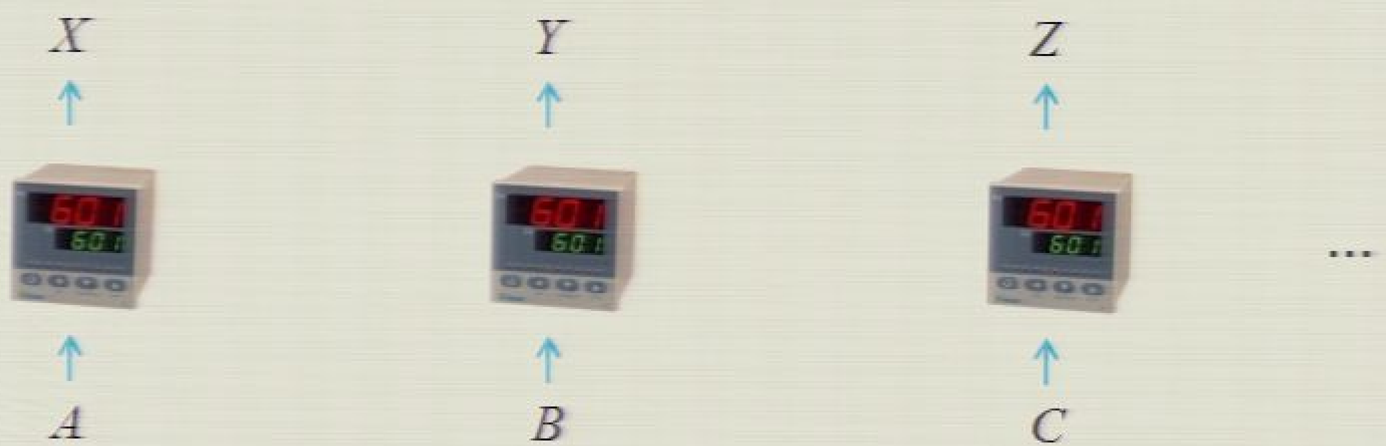
- Hope: for large M, any bit picked at random is with high probability very close to perfectly free.

Summary

- For initial sources with $\varepsilon \leq 0.09$, we can generate arbitrarily free bits.
- Although using chained Bell correlations, we cannot extend this to all ε, we speculate that there exist quantum correlations for which this is possible.
- If so, initial bits with an arbitrarily small amount of freedom would be sufficient to generate free bits.
- Arguably the strongest evidence yet for the existence of truly random processes.

Towards an Extension of the result

- Speculate that this improves with more systems (M–party GHZ correlations)



- Hope: for large M, any bit picked at random is with high probability very close to perfectly free.

Summary

- For initial sources with $\varepsilon \leq 0.09$, we can generate arbitrarily free bits.
- Although using chained Bell correlations, we cannot extend this to all ε, we speculate that there exist quantum correlations for which this is possible.
- If so, initial bits with an arbitrarily small amount of freedom would be sufficient to generate free bits.
- Arguably the strongest evidence yet for the existence of truly random processes.