Hyperbits

Vincent Russo

University of Michigan
Quantum Communication Group

October 13, 2011

Outline

1. Hyperbits
2. Applications
3. Conclusions and Open Problems

Qubits vs. Hyperbits

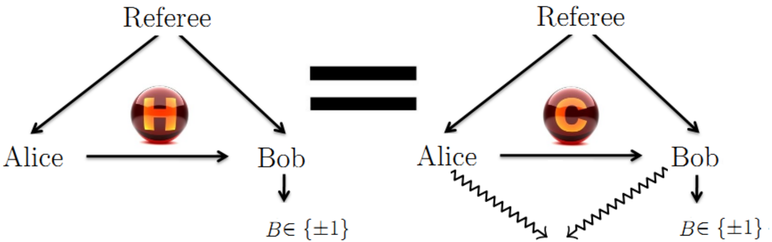
- 3-sphere
- States and measurements represented by 3-dimensional vectors.
- Defined for von Neumann measurements.

- n-sphere
- States and measurements represented by n-dimensional vectors.
- Defined for von Neumann measurements.

Motivations

- Tool to analyze quantum communication protocols.
- Ability to prove stronger form of Information Casuality.
- Application in the security of quantum key distribution against individual attacks.
- Can be used in oblivious transfer, parity oblivious multiplexing, random access codes, etc.

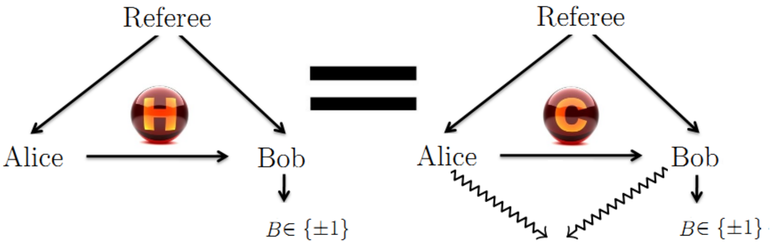
Entanglement and Classical Communication Equivalence



Theorem

Sending one hyperbit is equivalent to sharing any amount of entanglement and sending one classical bit (where Bob outputs only binary answers $B \in \{\pm 1\}$.

Entanglement and Classical Communication Equivalence



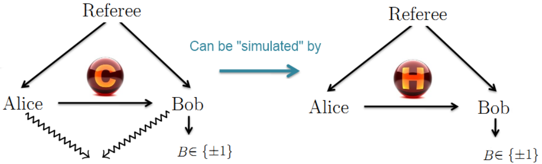
Theorem

Sending one hyperbit is equivalent to sharing any amount of entanglement and sending one classical bit (where Bob outputs only binary answers $B \in \{\pm 1\}$.

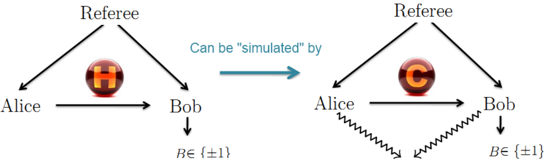
Theorem 1: Proof Approach

Proof.

Step 1:



Step 2:



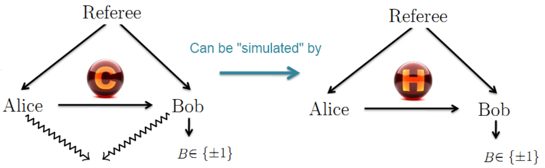
□

- "Simulated" means:
  - Bob's answer in both protocols yields the same expectation value.

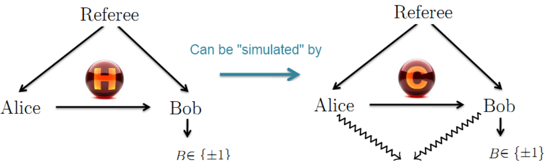
Theorem 1: Proof Approach

Proof.

Step 1:



Step 2:

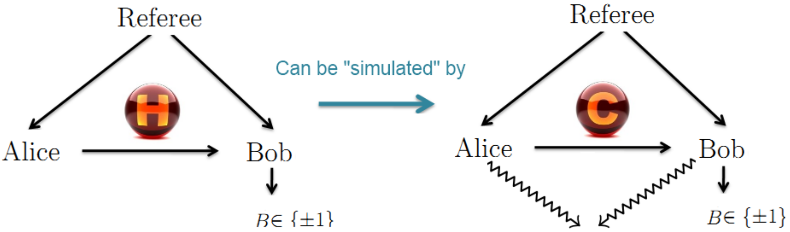


□

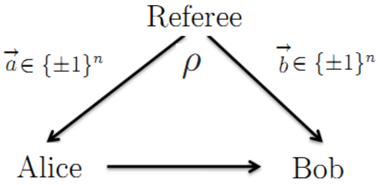
- "Simulated" means:
  - Bob's answer in both protocols yields the same expectation value.

Proof Step 2:

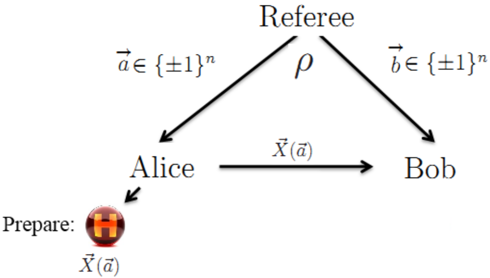
Let's now prove (much easier):



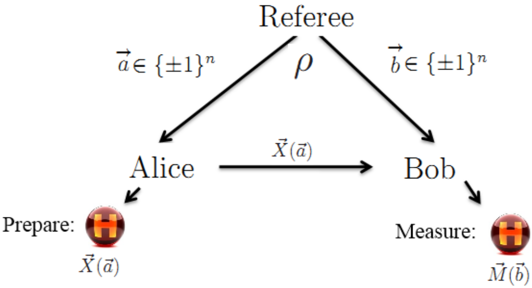
General Strategy



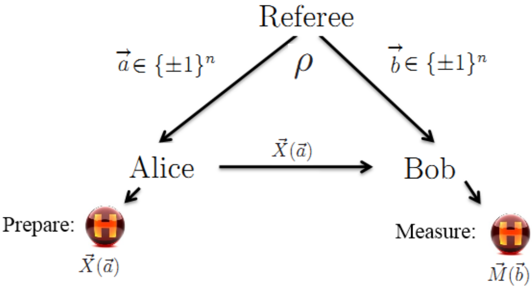
General Strategy



General Strategy



General Strategy



<u>Expectation:</u>

$$\langle B(\vec{a}, \vec{b}) \rangle = \langle \vec{X}(\vec{a}), \vec{M}(\vec{b}) \rangle$$

General Strategy - Tsirelson's Theorem

Theorem

There exists a state and collection of measurements such that:

$$\langle \vec{X}(\vec{a}), \vec{M}(\vec{b}) \rangle = \mathrm{Tr}(\hat{A}_{\vec{a}} \otimes \hat{B}_{\vec{b}} \rho) = \langle AB \rangle$$

Proof.

Bob can simply multiply A and B to obtain the answer with exactly the same expectation. □

General Strategy - Tsirelson's Theorem

Theorem

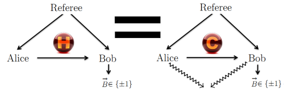
There exists a state and collection of measurements such that:

$$\langle \vec{X}(\vec{a}), \vec{M}(\vec{b}) \rangle = \mathrm{Tr}(\hat{A}_{\vec{a}} \otimes \hat{B}_{\vec{b}} \rho) = \langle AB \rangle$$

Proof.

Bob can simply multiply A and B to obtain the answer with exactly the same expectation. □

Applications

Since we have proven that 

, hyperbits may be used as a tool in numerous contexts:

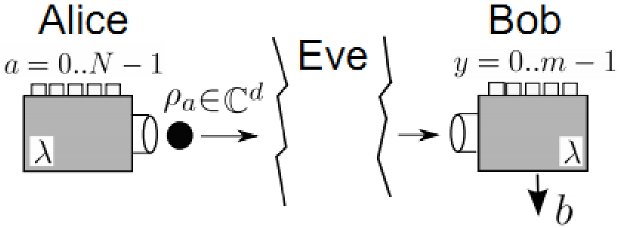
- Communication Complexity
- Quantum Key Distribution (QKD)
- Strengthened Information Casuality
- Random Access Codes
- Oblivious Transfer
- etc.

Application: Quantum Key Distribution

Security of Quantum Key Distribution Against Individual Attacks

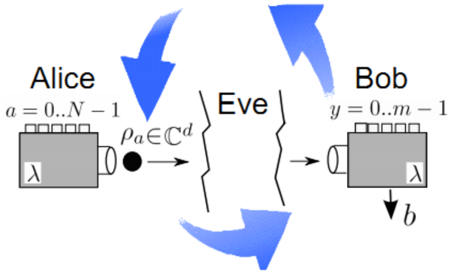
Semi-Device Independent QKD

Alice encodes classical information as quantum states. Bob receives these states, performs a measurement and outputs b.



Semi-Device Independent QKD

Repeat protocol.

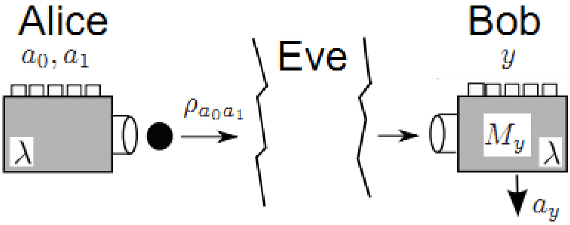


$$P(b|a,y) = tr(\rho_a M_y^b) \tag{1}$$

Probability of Bob finding outcome b conditioned on measurement M_y and state ρ_a.

Semi-Device Independent QKD - Our Scenario

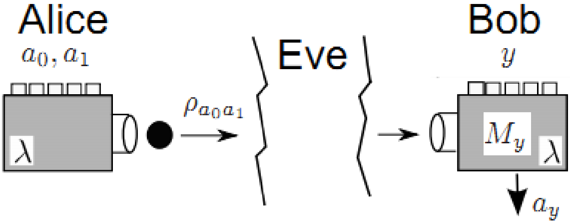
Alice generates random bits $\{a_0, a_1\}$, and sends $\rho_{a_0 a_1}$ to Bob.
Bob's random bit is y, performs measurement M_y, and guesses bit a_y.



Goal: Show security of protocol against Eve can be guaranteed based on its probability distribution.

Semi-Device Independent QKD - Our Scenario

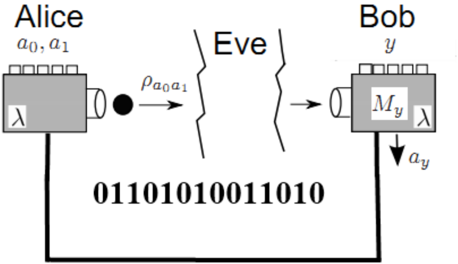
Alice generates random bits $\{a_0, a_1\}$, and sends $\rho_{a_0 a_1}$ to Bob.
Bob's random bit is y, performs measurement M_y, and guesses bit a_y.



Goal: Show security of protocol against Eve can be guaranteed based on its probability distribution.

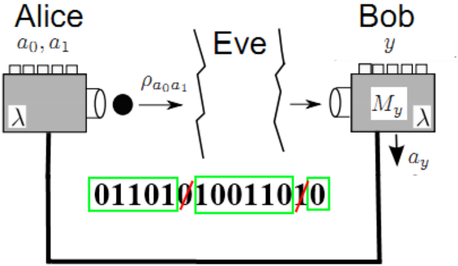
Semi-Device Independent QKD - Security

Compare part of their data on a public channel.



Semi-Device Independent QKD - Security

Toss out bits that don't agree.



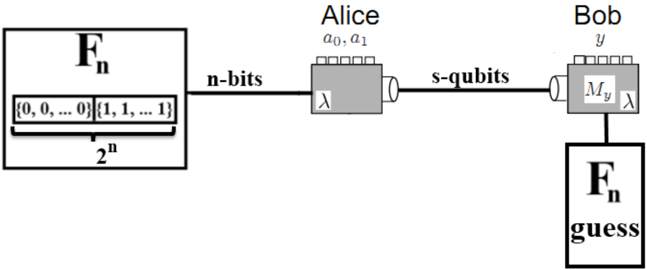
Security is obtained if

$$P_B > \frac{5+\sqrt{3}}{8} \approx 0.8415 \tag{2}$$

Otherwise security has been compromised. Note similarity to CHSH.

Semi-Device Independent QKD - Security Proof

Main Ingredient



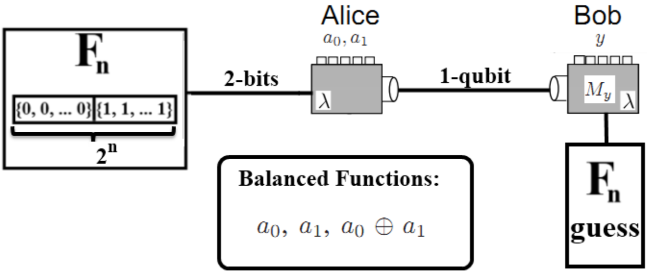
Probability of Bob's success:

König, R. Ph.D. Thesis.

$$P_n \leq \frac{1}{2}\left(1 + \sqrt{\frac{2^s - 1}{2^n - 1}}\right)$$

Semi-Device Independent QKD - Specific Case

Case of interest to us: $n = 2, s = 1$.

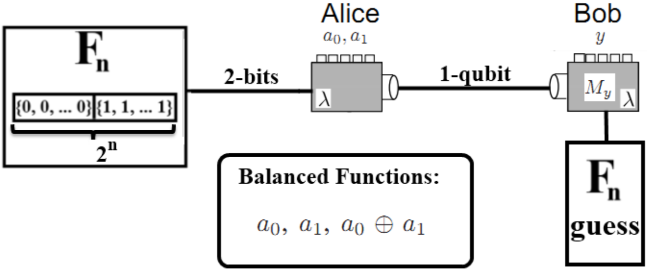


$$P(a_0) + P(a_1) + P(a_0 \oplus a_1) \leq \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

where $P(a_i)$ is the probability of Bob guessing a_i correctly.

Semi-Device Independent QKD - Specific Case

Case of interest to us: $n = 2, s = 1$.



$$P(a_0) + P(a_1) + P(a_0 \oplus a_1) \leq \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

Applications: QKD

Security of QKD against individual attacks.

Prior Inequality

$$P(a_0) + P(a_1) + P(a_0 \oplus a_1) \leq \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

Stronger Inequality

$$E(a_0)^2 + E(a_1)^2 + E(a_0 \oplus a_1)^2 \leq 1$$

Stronger inequality, weaker requirement, same level of security.

Applications: QKD

Security of QKD against individual attacks.

Prior Inequality

$$P(a_0) + P(a_1) + P(a_0 \oplus a_1) \leq \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

Stronger Inequality

$$E(a_0)^2 + E(a_1)^2 + E(a_0 \oplus a_1)^2 \leq 1$$

Stronger inequality, weaker requirement, same level of security.

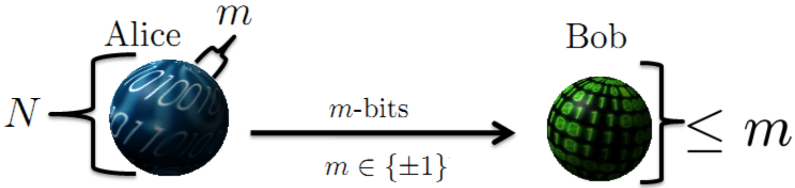
Application: Information Causality

Strengthened Information Causality Result

Information Causality - Description

Definition

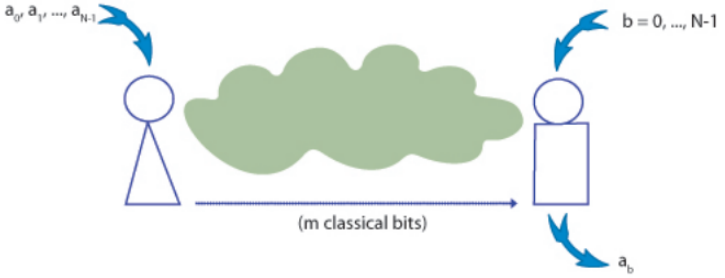
Transmission of m classical bits can cause an information gain of at most m-bits.



M. Pawlowski, T. Paterek, D. Kaszilikowski, V. Scarani, A. Winter, M. Zukowski Information Causality as a Physical Principle Nature, 2009.

Information Causality - Example

Distributed version of random access coding, oblivious transfer, and related communication complexity problems.

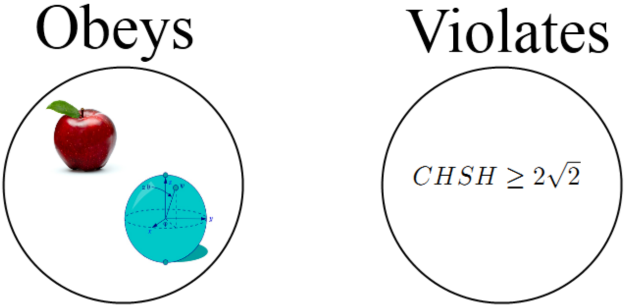


- Alice has N random and independent bits.
- Bob receives a random value b.
- Alice sends Bob m bits. Bob must guess the value of the b^{th} bit in Alice's list, a_b.

Information Causality - Violation

What's the big deal? Consider where information causality is violated.

Classical and quantum physics obey information Causality. CHSH correlations beyond Tsirelson's bound $2\sqrt{2}$ violate.



Information Causality - No Signaling

Previous task is open to producing no-signaling correlations.

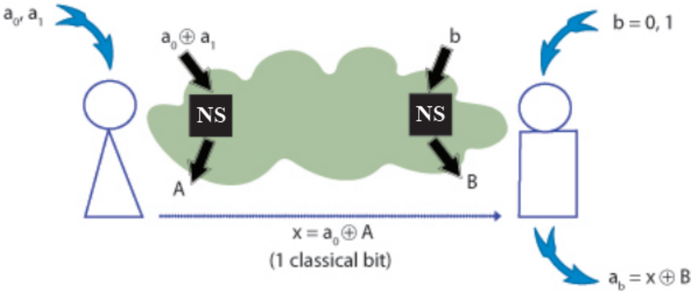
Definition

No-Signaling Box: Hypothetical resource producing no-signaling correlations.

Correlations among either classical or quantum systems.

Information Causality - No Signaling Example

Simplest case where information causality is violated.



Alice receives two bits; sends one to Bob.

Information Causality - Main Contributions

What is Information Causality good for?

1. Classical and quantum theories respect Information Causality.
2. Quantum theory achieves the maximal value of a certain class of Bell inequalities.
3. Any no signaling theory can violate the Bell inequality by more than quantum theory.
4. Can be used as a principle to distinguish physical theories from non-physical ones.

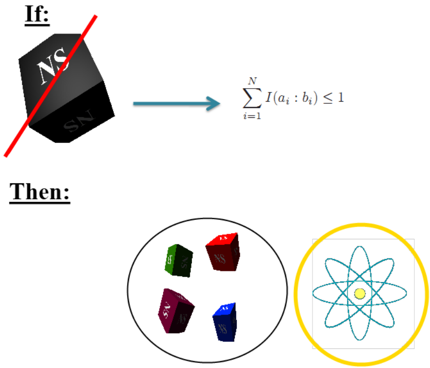
Information Causality - Main Contributions

What is Information Causality good for?

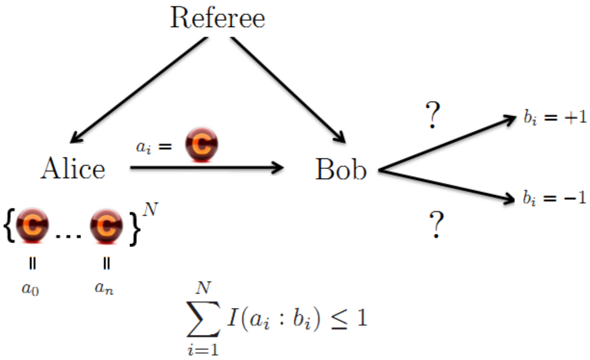
1. Classical and quantum theories respect Information Causality.
2. Quantum theory achieves the maximal value of a certain class of Bell inequalities.
3. Any no signaling theory can violate the Bell inequality by more than quantum theory.
4. Can be used as a principle to distinguish physical theories from non-physical ones.

Information Causality - Main Contributions

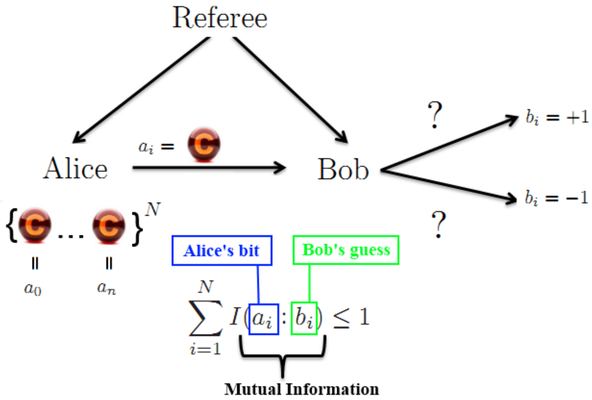
Quantum theory *might* be *the* theory that maximally violates Bell inequalities among all no-signaling theories if no-signaling is replaced by information causality.



Information Causality - Hyperbit Enhancement



Information Causality - Hyperbit Enhancement (continued)



Information Causality - Hyperbit Enhancement (continued)

Theorem

$\sum_{i=1}^{N} I(a_i : b_i) \leq 1$ *holds even if Alice's bits a_i are only pairwise independent.*

Proof.

Proven in Appendix B. Proof uses hyperbits to show that the theorem holds for pairwise independent, uniformly distributed bits a_i □

Significance?

Information Causality - Hyperbit Enhancement (continued)

Theorem

$\sum_{i=1}^{N} I(a_i : b_i) \leq 1$ *holds even if Alice's bits a_i are only pairwise independent.*

Proof.

Proven in Appendix B. Proof uses hyperbits to show that the theorem holds for pairwise independent, uniformly distributed bits a_i □

Significance?

Conclusions – (Recap)

- Introduced hyperbits.
  - Useful for 2-party; 1-bit output communication with unlimited shared entanglement.
- Hyperbits may be substituted for entanglement assisted communication.
  - Cryptography
  - Information Causality

Conclusions – (Recap)

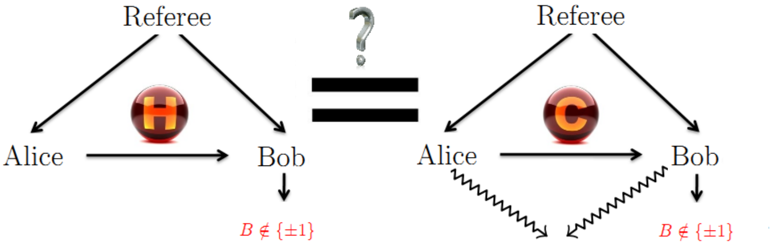
- Introduced hyperbits.
  - Useful for 2-party; 1-bit output communication with unlimited shared entanglement.
- Hyperbits may be substituted for entanglement assisted communication.
  - Cryptography
  - Information Causality

Conclusions – (Recap)

- Introduced hyperbits.
  - Useful for 2-party; 1-bit output communication with unlimited shared entanglement.
- Hyperbits may be substituted for entanglement assisted communication.
  - Cryptography
  - Information Causality

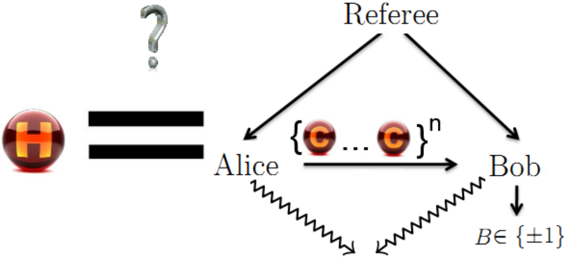
Open Problems

Does Theorem-1 still hold if Bob outputs some $B \notin \{\pm 1\}$?



Open Problems

Generalization of hyperbits that are equivalent to scenario of unlimited entanglement and communication of some fixed number of bits?

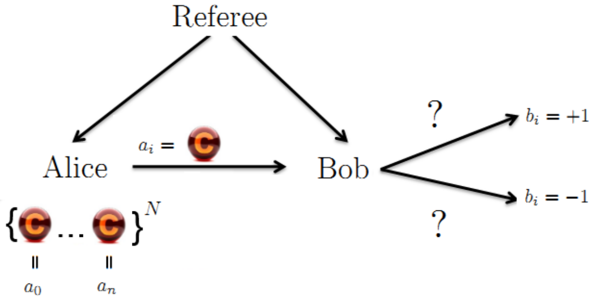


Open Problems - Information Causality

In communication of m bits can be

$$\sum_{i=1}^{N} I(a_i : b_i) \leq 2^m - 1. \tag{3}$$

Is this the maximum? (Likely, but not proven).



Open Problems - Information Causality

1. Are there Bell inequalities for which Information Causality is not enough?
2. Can the argument in the paper be generalized to a large set of Bell inequalities?
   - Right now, only holds for one type of Bell inequality.

"Preprint [PPKSWZ09] cries out for follow up work" – David Bacon.

Questions in regards to "Information Causality as a Physical Principle" [PPKSWZ09] posed by David Bacon on his blog, "The Quantum Pontiff".

Thank You

Thanks!
Questions? / Comments?

(And thanks to Marcin Pawlowski and Andreas Winter on which this content is primarily based [PW11].)

References I

B.S. Tsirelson.
Quantum Analogues of the Bell Inequalities. The Case of Two Spatiall Separated Domains.
Springer

M. Pawlowski, A. Winter.
From Qubits to Hyperbits.
arXiv:1106.2409

M. Pawlowski, N. Brunner.
Semi-Device Independent Security of One-Way Quantum Key Distribution.
arXiv:1103.4105.

References II

M. Pawlowski, T. Paterek, D. Kaszilikowski, V. Scarani, A. Winter, M. Zukowski
Information Causality as a Physical Principle.
Nature

R. Spekkens, D.H. Buzacott, A.J. Keehn, B. Tone, G.J. Pryde
Preparation Contextuality Powers Parity-Oblivious Multiplexing.
PRL 102, 010401.

R. König.
Ph.D. Thesis