Title: Quantum Tasks in Relativistic Spacetime

Date: Feb 04, 2019 03:30 PM

URL: http://pirsa.org/19010072

Abstract: In this talk I will set out two new contributions to the study of operational tasks in a relativistic quantum setting. First, I will present a generalisation of the task known as â€˜summoning,â€™ in which an unknown quantum state is supplied to an agent and must be returned at a specified point when a corresponding call is made. I will show that when this task is generalised to allow for more than one call to be made, an apparent paradox arises: the extra freedom makes it strictly harder to complete the task. Second, I will describe a quantum generalisation of the classic cryptographic task known as â€˜zero-knowledge-proving.â€™ I will show that there exists no perfectly secure quantum relativistic protocol for this task, and I will then set out a protocol which is conjectured to be close to optimal in security for this task. These results have practical applications for distributed quantum computing and cryptography and also interesting implications for our understanding of relativistic quantum information and its localisation in spacetime.

Quantum Tasks in Relativistic Spacetime

Emily Adlam
January 2019

Outline

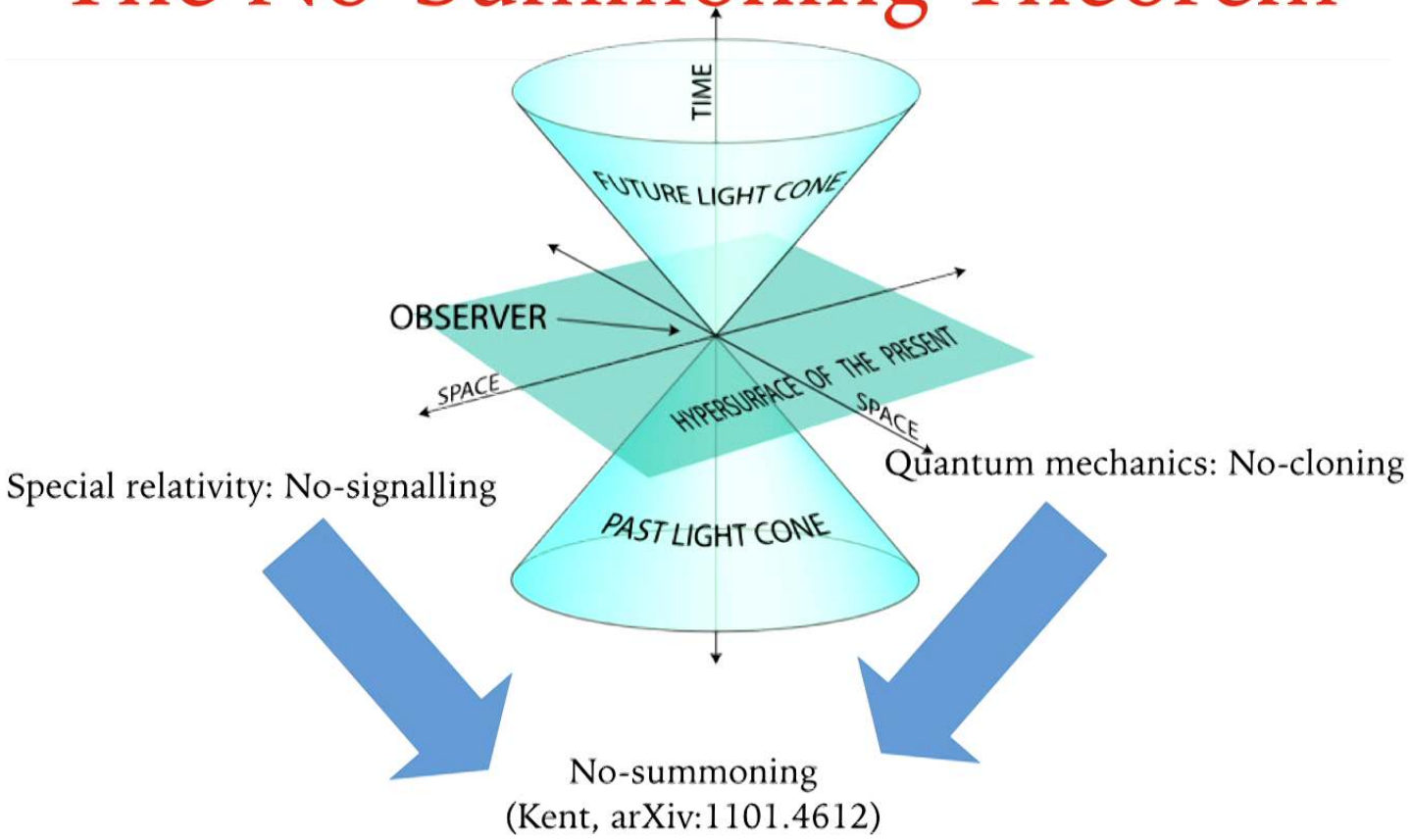
Quantum Paradox of Choice

- The No-Summoning Theorem
- Hayden-May generalisation
- Summoning with unrestricted calls
- Discussion

Zero-Knowledge Proving

- Motivation: Zero-knowledge proofs
- Definition: KCEKQS
- No-go theorems
- New proposed protocol
- Discussion

The No-Summoning Theorem



Special relativity: No-signalling

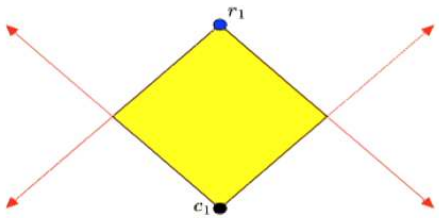
Quantum mechanics: No-cloning

No-summoning
(Kent, arXiv:1101.4612)

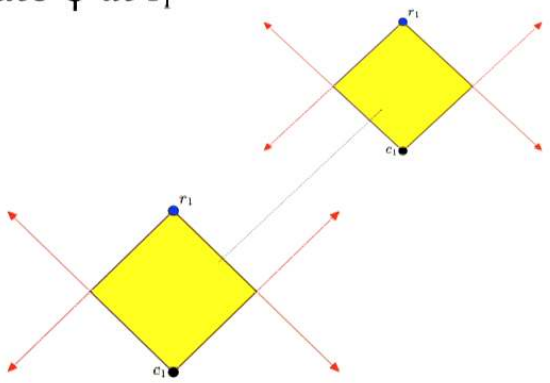
World line" by SVG version: K. Aainsqatsi at en.wikipediaOriginal PNG version: Stib at en.wikipedia - Transferred from en.wikipedia (Original text : self-made). Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:World_line.svg#/media/File:World_line.svg

The No-Summoning Theorem: Hayden and May

- A summoning task is defined by a *start point* s and a set of *call-response pairs* $\{ (c_i, r_i) \}$
- Alice is given a quantum system in some unknown state ψ at s.
- A call is made at exactly one call point c_i. If a call is made at point c_i, then Alice must return a quantum system in state ψ at r_i



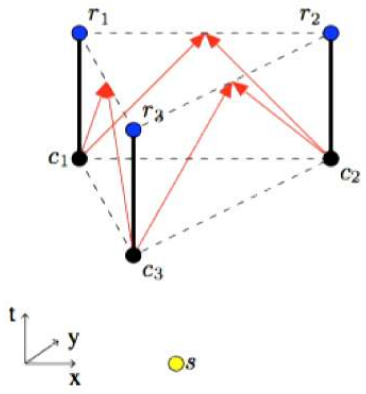
Causal diamond for (c_1, r_1)



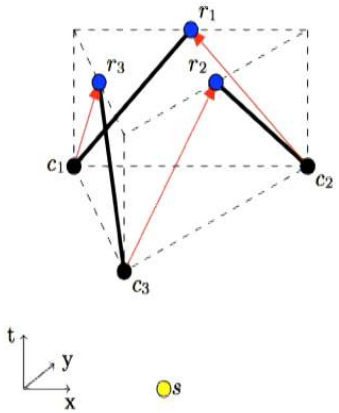
Causally related causal diamonds

The No-Summoning Theorem: Hayden and May

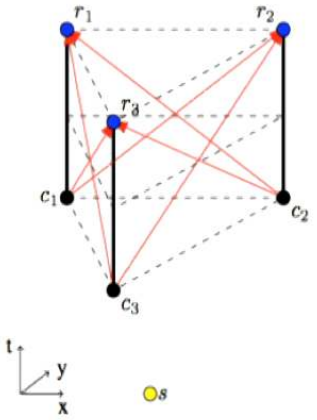
Theorem: A given summoning task is possible if and only if every response point r_i is in the future lightcone of the start point and every pair of causal diamonds D_i and D_j are causally related
(Hayden and May, arXiv:1210.0913)



Impossible



Possible

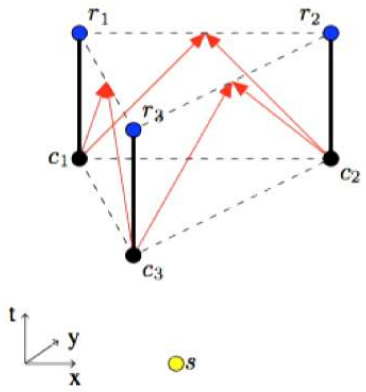


Possible

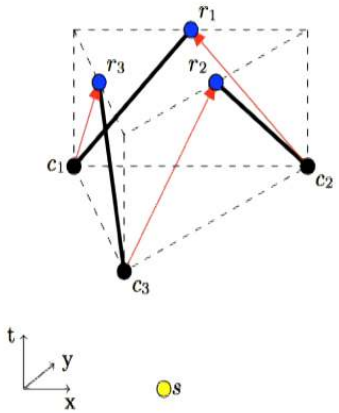
Summoning with Unrestricted Calls

Theorem: Summoning with unrestricted calls is possible if and only if:

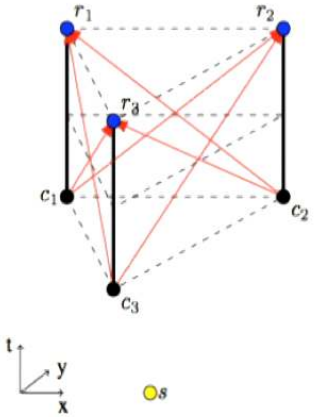
- Every response point is in the future lightcone of the start point
- For any subset K of the call-response pairs, there is at least one pair $\{c_x, r_x\}$ in K such that r_x is in the future lightcone of the call point of every pair in K.



Impossible



Impossible!



Possible

Interpretation

'We fully characterize which regions of spacetime can all hold the same quantum information … this provides a simple and complete description of where and when a qubit can be located in spacetime, revealing a remarkable variety of possibilities'

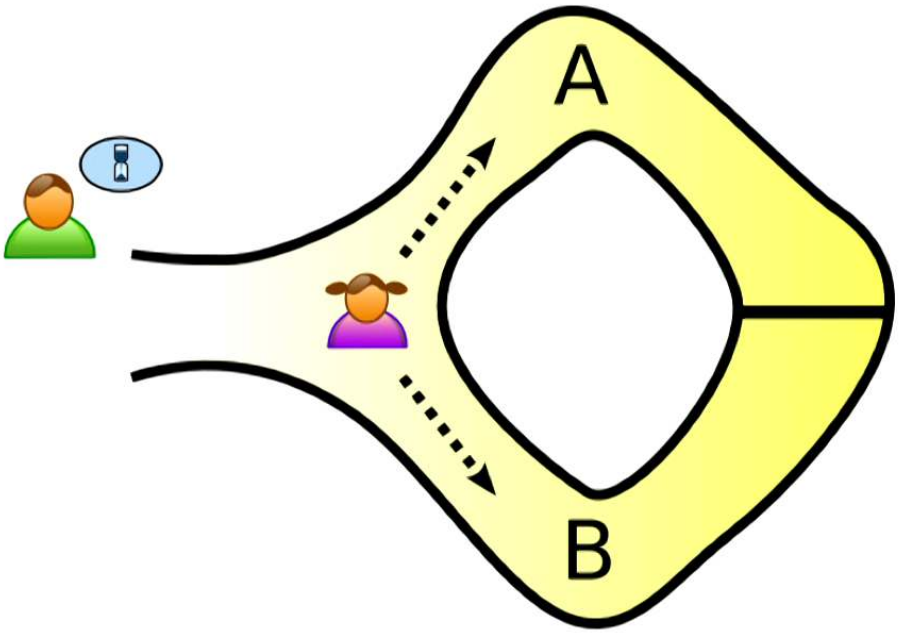
(Hayden and May)

'This is the essence of teleportation: a quantum state is transferred from one place to another: not copied to the other place, but moved to that place.'

(Horodecki et al)

Zero-Knowledge Proofs

- Soundness
- Completeness
- Zero-knowledge



Zero-knowledge proofs of knowledge of a quantum state

- Horodecki, Horodecki and Horodecki *quant-ph/0010048*
- No-go theorem: zero-knowledge, completeness and soundness are incompatible
  - Non-relativistic context only
  - Assumes that Bob keeps the system and performs a measurement
  - Does not allow relaxation of the security requirements

(Relativistic) Knowledge-concealing proofs

A protocol in which Alice performs actions to convince Bob that she knows the quantum state η of some system Q_B in Bob's possession, such that the following three conditions are satisfied, where ε and χ can be made arbitrarily small in the limit as some variable parameter of the protocol becomes large:

Soundness: If Alice knows nothing about the state η, and the states η are drawn uniformly at random from the Hilbert space for Q_B, then for any strategy employed by Alice, the probability that the proof is accepted is less than or equal to ε_S.

Completeness: If Alice knows η and performs the protocol correctly, and the states η are drawn uniformly at random from the Hilbert space for Q_B, with probability at least $1 - \varepsilon_C$ the proof is accepted by Bob.

Knowledge-concealing: If Φ is Bob's best guess for η after the protocol, then the average value of $|\langle \Phi | \eta \rangle|^2$ is less than or equal to ε_K

New no-go theorems

No assumptions about the form of the protocol, covering relativistic context, considering possible relaxations

- **Zero-knowledge:** There exists no non-trivial protocol for proving knowledge of a quantum state which is perfectly zero-knowledge
- **Completeness vs soundness:** In any protocol for proving knowledge of a quantum state of dimension d, we must have $\varepsilon_S/(1 - \varepsilon_C) \geq 1/d$

Quantum Bob-to-Alice

- Bob prepares N quantum systems in states chosen uniformly at random.
- Bob randomly permutes these systems together with the system Q_B, assigns them all indices from 1 to N + 1, and gives them to Alice
- Alice chooses a projective measurement P consisting of d projectors, one of which is $|\eta\rangle\langle\eta|$. She performs P on all of the N + 1 systems that Bob has given to her and forms a set containing up to q indices which correspond to systems for which her measurement obtained the outcome $|\eta\rangle\langle\eta|$. (If she obtained this outcome more than q times, she randomly chooses a subset of size q from the relevant indices)
- Alice performs q relativistic bit commitments committing her to all of the indices in the set C. Each bit commitment is set up so that Alice can commit either to one of the indices in {1, 2 ... N} or to a dummy index
- Bob tells Alice the index that he assigned to Q_B
- If the index that Bob announces is one of the indices in C, Alice unveils her commitment to that index.
- If Alice unveils a commitment that matches the index associated with Q_B, Bob accepts Alice's proof.

Analysis

- We assume that Kent's secure relativistic bit commitment protocol remains secure under parallel repetition
- For a system of dimension d, if we choose $\varepsilon_S = 1/d$, we can obtain $\varepsilon_C \to 0$ in the limit of large N
- Bob's information gain goes to zero in the limit of large dimension d

Quantifying Knowledge

- Fidelity squared: $|<\Phi|\ \eta>|^2$
  - Good measure of Bob's ability to produce copies and predict outcomes
  - Question about different probabilistic decompositions of the same density matrix
    - e.g. Uniform distribution over all states vs +X or -X with equal probability