Playing (non-local) games with operator spaces

David Pérez-García
UCM - ICMAT Madrid

12 April 2019

STRUCTURE OF THE TALK

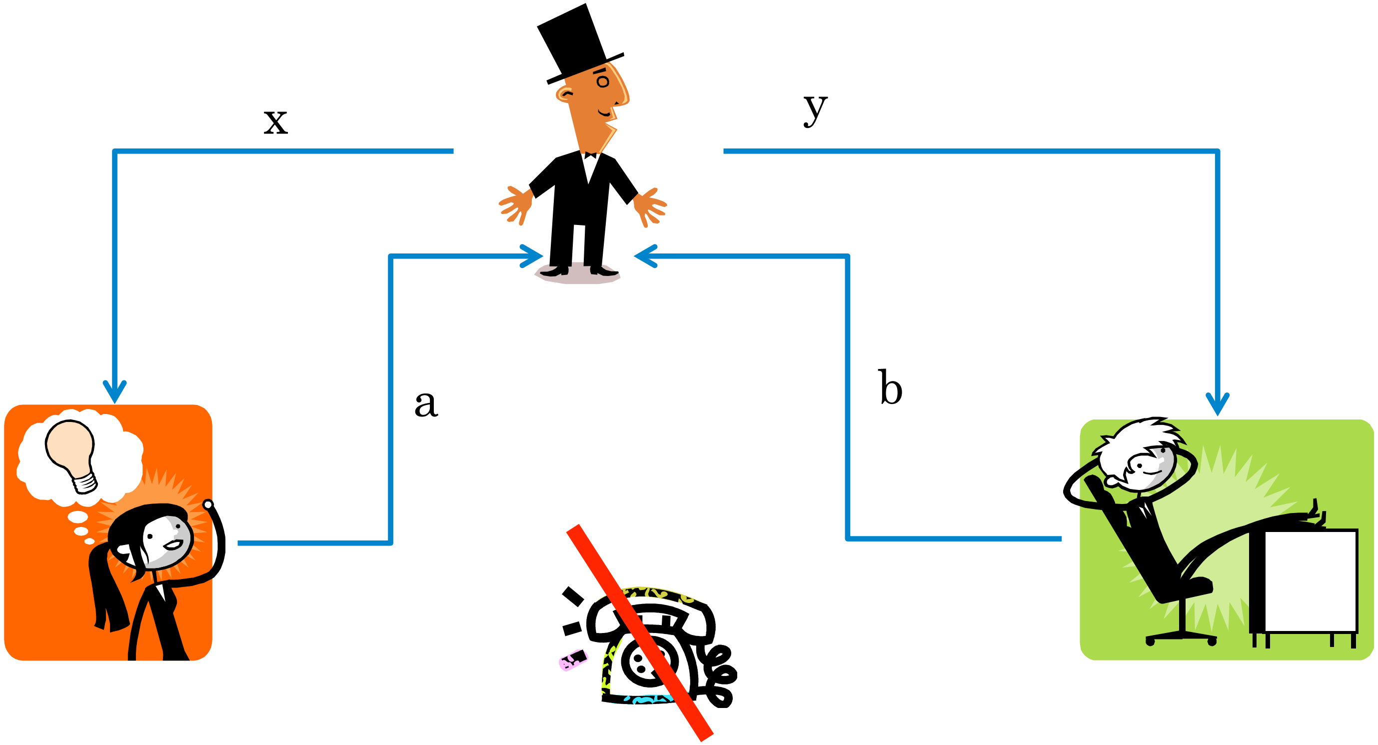
- The object under study: Non-local games
- Examples. Why are they important?
  - Complexity theory I. Innaproximability results.
  - Complexity theory II. Parallel computation.
  - Position based cryptography.
  - Certifiable random number generation.
  - … …
- Where are the maths?
  - Our contribution. Operator Spaces.

- Based on joint works (2008-2019) with T. Cooney, M Junge, A.M. Kubicki, C. Palazuelos, I. Villanueva, M.M. Wolf.

Non-local games

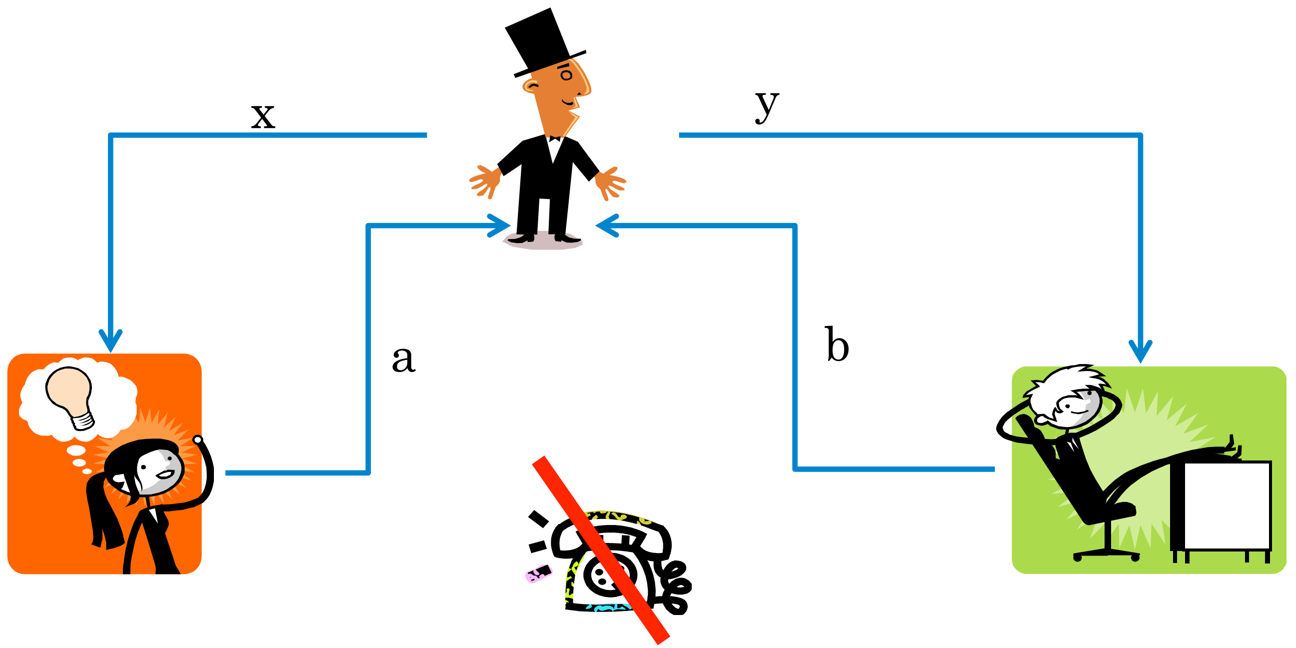
NON-LOCAL GAMES

1. A set of possible **questions** for Alice and Bob (denoted by **x,y** resp.).
2. A known **probability** distribution for the questions.
3. A known **boolean function V(x,y,a,b)** which decides, based on questions and answers **a,b,** whether they win (=1) or lose (=0) the game.
4. A **limitation in the communication** between Alice and Bob.

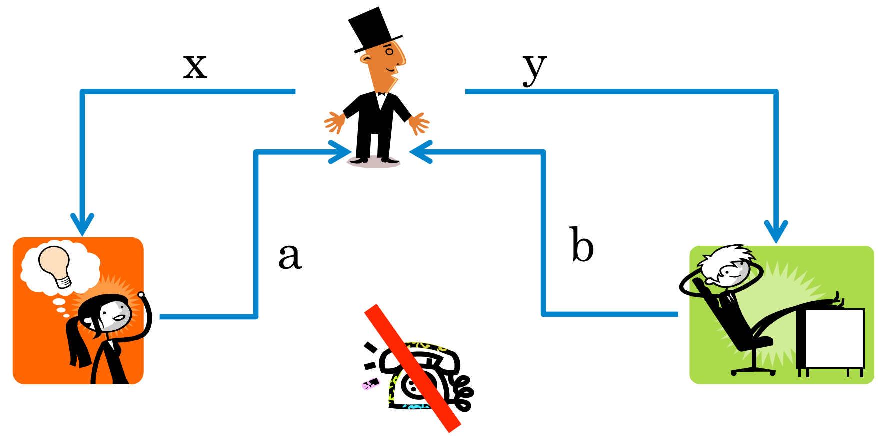


Non-local games

The **value of the game** is the largest probability of wining the game while optimizing over the possible strategies of Alice and Bob.
It is assumed that Alice and Bob have free communication BEFORE the game to coordinate an strategy .
Hence strategies can involve **shared randomness (classical value of the game)** or **quantum entanglement (quantum value of the game)** depending on the resources of Alice and Bob.



Non-local games



What is an strategy?

A probability distribution p(ab|xy)

Which are the possible strategies in the classical case?

$$p(ab|xy)=\sum_{\lambda} q(\lambda) p_A(a|x\lambda) p_B(b|y\lambda)$$

And in the quantum one?

$$p(ab|xy)=tr\left(\rho E_a^x F_b^y\right)$$

$$\rho \in S(H)$$

$$E_a^x, F_b^y \geq 0$$

$$\sum_a E_a^x = Id_H, \forall x$$

$$\sum_b F_b^y = Id_H, \forall y$$

$$[E_a^x, F_b^y] = 0.$$

EXAMPLES.
Innaproximability

EXAMPLES.
INNAPROXIMABILITY RESULTS

Theorem *(PCP theorem (Arora et al., 92)+ Parallel repetition (Raz, 94)):*

Unless P=NP, given e>0 and a game with the promise that the value is 1 or <e, there cannot exist a polynomial algorithm to decide which is the case.

Examples. Innaproximability results

It is the mother of most innaproximability results. For instance:

Theorem (Hastad, 1999):
Unless P=NP, given e>0 and a polynomial algorithm to determine the MAX-CLIQUE of a graph, there exist graphs of n vertices for which

$$\frac{\text{MAX-CLIQUE}}{\text{output of the algorithm}} = n^{1-e}$$

Note that MAX-CLIQUE is always less or equal than n (!!)
The same result is true for the CHROMATIC NUMBER.

EXAMPLES. INNAPROXIMABILITY RESULTS

Connection with non-local games. Via LABEL-COVER.

Given a bipartite graph $(V = U \cup W, E)$

A set of colors Σ

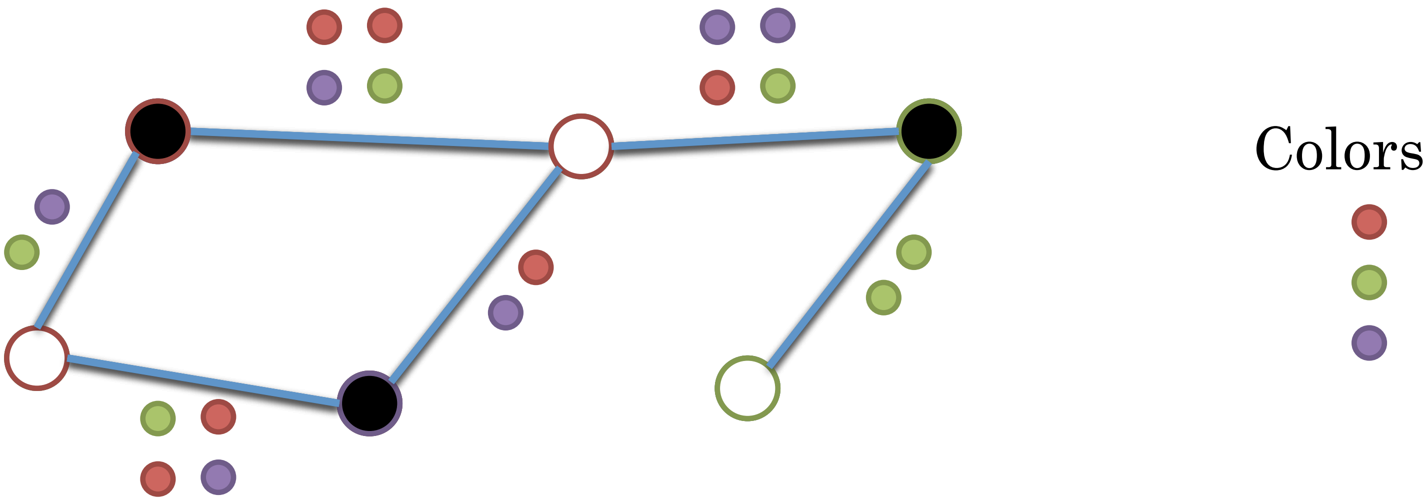
And a set of valid configurations for each edge

$$\forall e = (u, w) \in E, \quad C_e : \Sigma \times \Sigma \to \{\text{valid}, \text{invalid}\}$$

Find a coloring of the graph which maximizes the number of edges with a valid configuration.

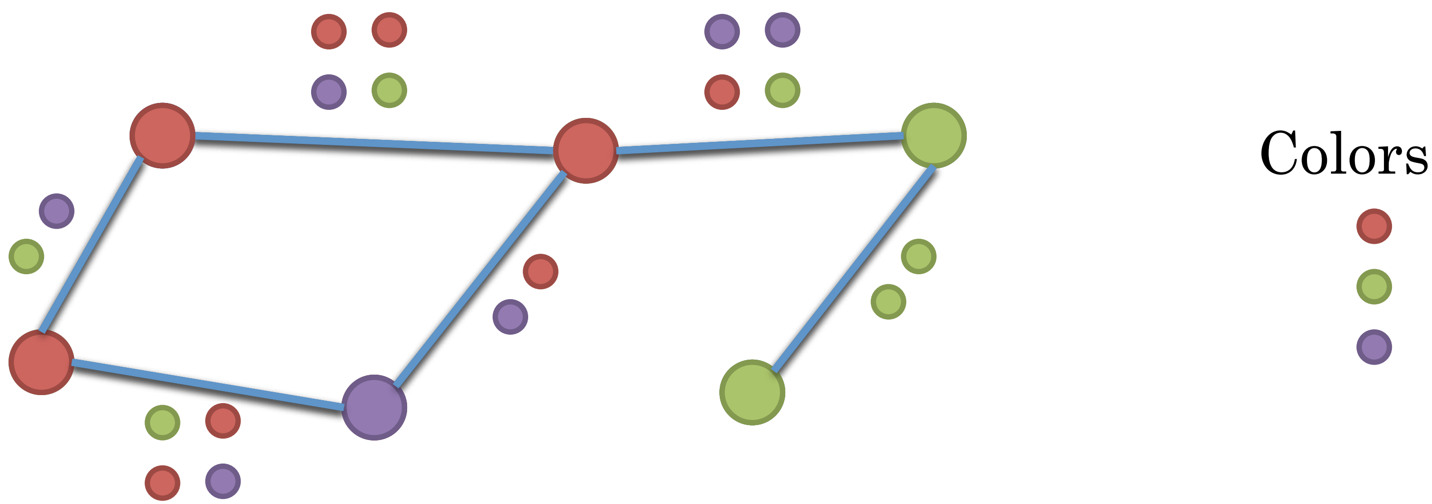
Examples. Inaproximability results

Connection with non-local games. Via LABEL-COVER.



EXAMPLES.
INAPROXIMABILITY RESULTS

Connection with non-local games. Via LABEL-COVER.



Solution to LABEL-COVER = 5

EXAMPLES. INNAPROXIMABILITY RESULTS

Connection with non-local games. Via LABEL-COVER.

Given an instance of LABEL-COVER, we define a non-local game by:

Questions = edges (the vertex from U to Alice and from W to Bob) with uniform probability.

Answers = colors to the vertices.

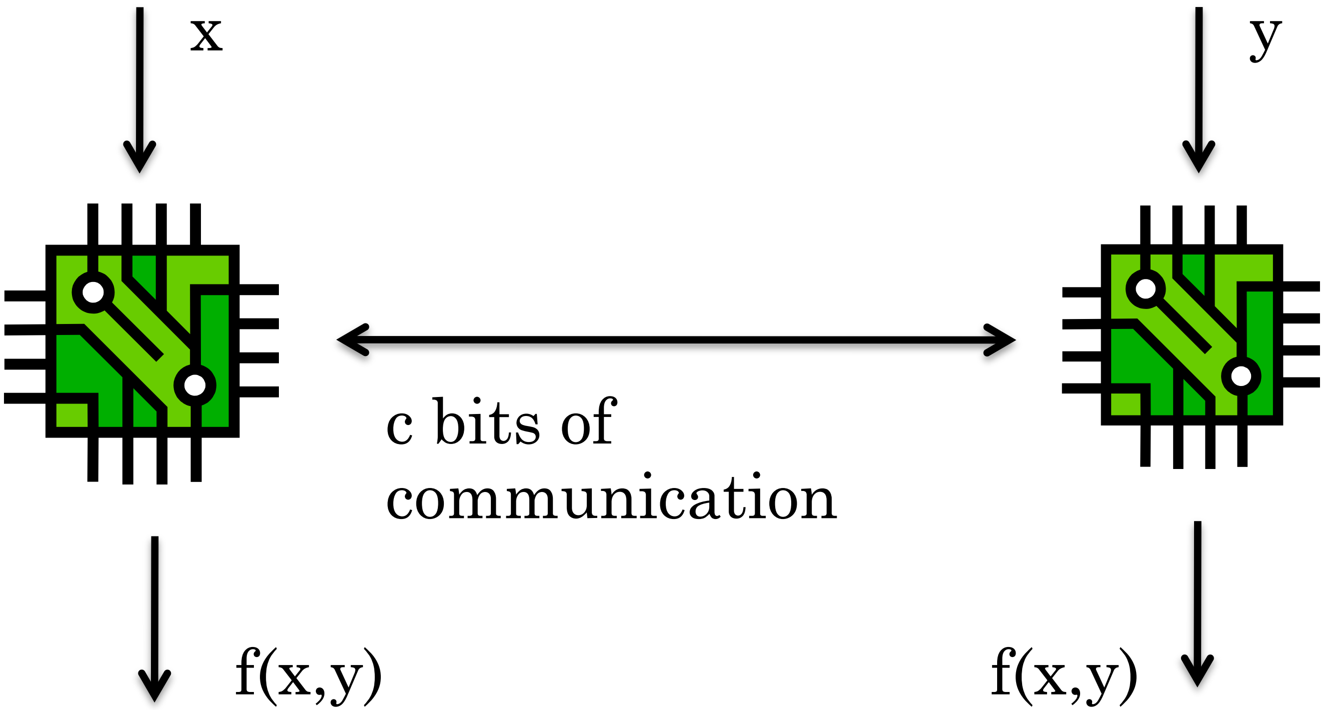
They win the game if they give a valid coloring for the edge which is asked. Then:

Value of the game * number of edges = LABEL-COVER

Examples. Parallel computation

Examples.
Parallel computation

Given a boolean function f(x,y), minimize c in:

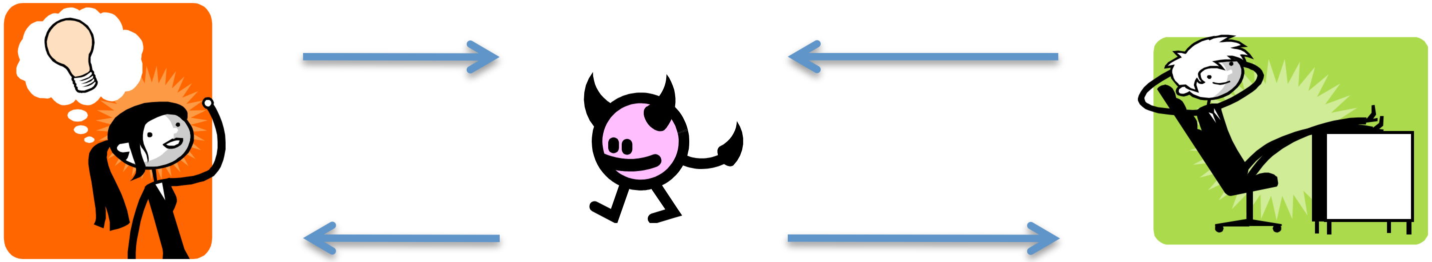


Examples. Position based cryptography.

(Chandran et al, 2009)

Examples.
Position based cryptography

The man-in the middle attack

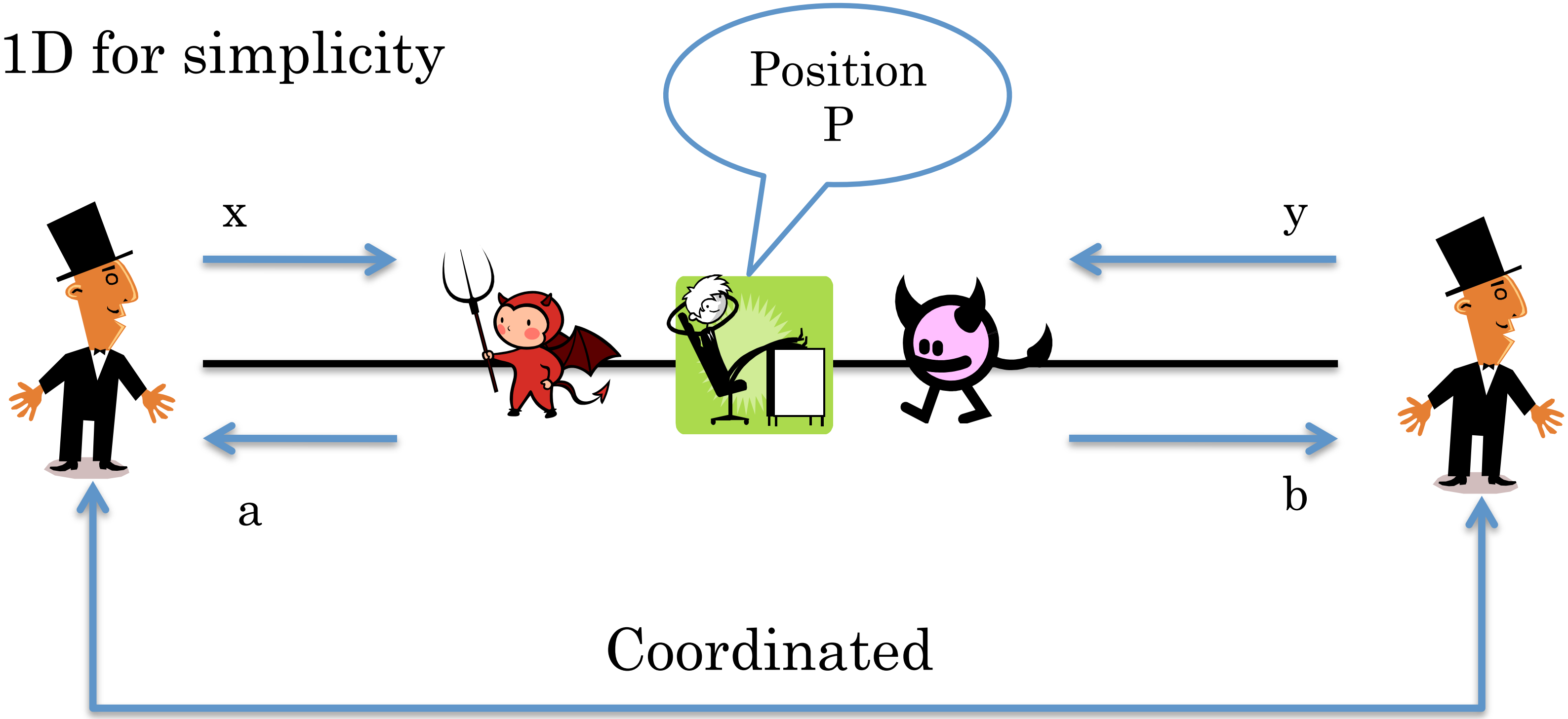


It seems there cannot be a solution to this problem.

There could be one. Authentication based on position.

EXAMPLES.
POSITION BASED CRYPTOGRAPHY

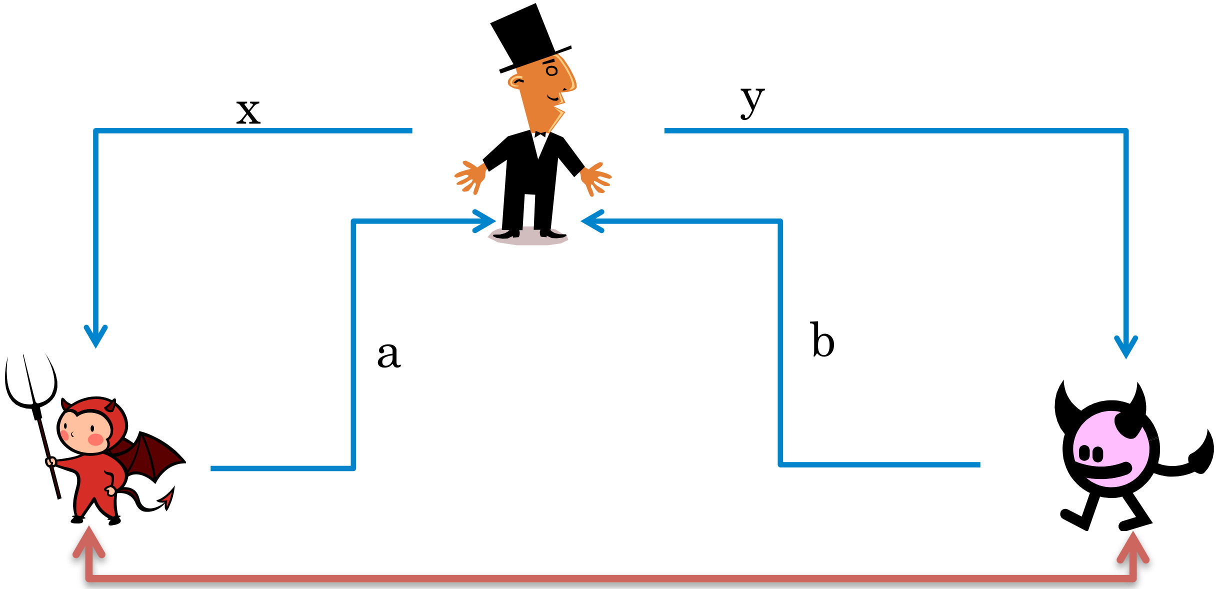
1D for simplicity



AIM: That only someone in position P could answer with probability 1 to the challenge.
→ Solution to the man-in-the-middle problem.

Examples.
Position based cryptography

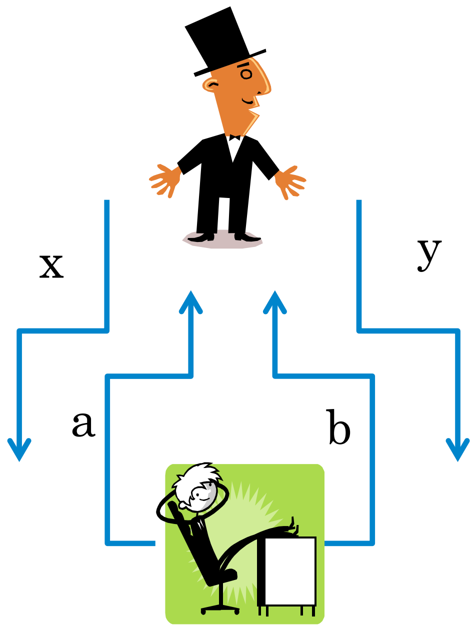
Relation with non-local games. Since the verifiers act coordinated, we can assume there is just one of them. Based on answering times, we have:



Communication "independent-one-way"

Examples.
Position based cryptography

Hence, the aim is to find a challenge which can be won always with arbitrary communication (all classical challenges are like that) but not with “independent-one-way” communication.



The honest case is the one of arbitrary communication, since there is only a single prover.

Examples.
Position based cryptography

This is impossible classically. Both models of communication are the same. To see it, just copy and send the received question.

In the quantum case (with no entanglement) it is indeed possible (Buhrman et al., 2010). The key idea lies on the fact that it is NOT possible to copy quantum states by the NO-CLONING theorem.

Question: Is it also possible when a polynomial amount of entanglement is allowed?

Partial answers (Beigi et al., Burhman et al, 2011, Tomamichael et al 2013):
LINEAR = YES, EXPONENTIAL = NO.

Examples. Random number generation

Example.
Random number generation

The New York Times
Expect the World®

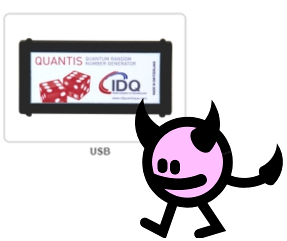
(September 2013) But internal memos leaked by a former N.S.A. contractor, Edward Snowden, suggest that the N.S.A. generated one of the random number generators used in a 2006 N.I.S.T. Standard - called the Dual_EC-DRBG standard – which contains a back door for the N.S.A.

USB

EXAMPLE.
RANDOM NUMBER GENERATION

PROBLEM: How to construct an apparatus which **<u>generates</u>** perfect random numbers (and hence secret) in a certifiable way?

00111010100101010 1….
.

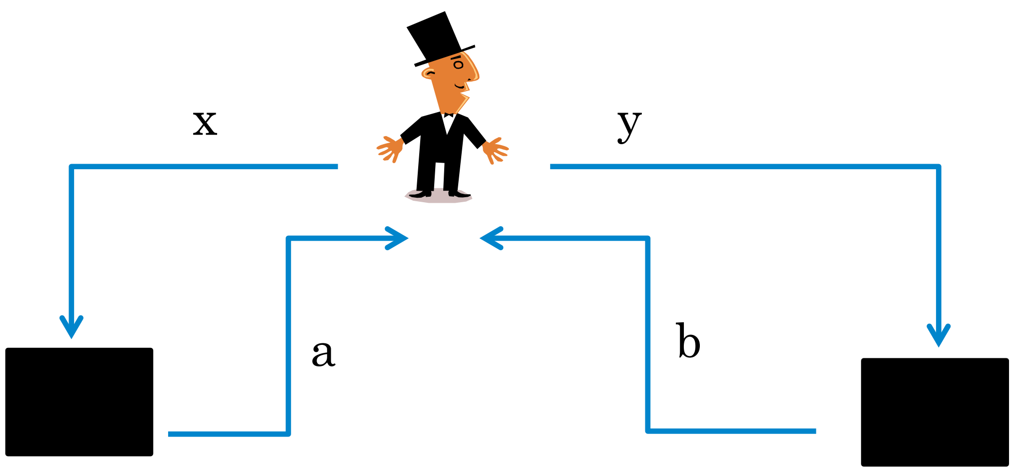


could have a copy of 001110101001010101…..

But in quantum mechanics copying is not allowed !!!

Example.
Random number generation

Theorem (Pironio et al., Colbeck et al., 2010):
If (after many rounds in the game) one gets a value strictly larger than the classical one, there is a classical post-processing of the outputs a, b which produces numbers which are perfectly random and secret.



Example.
Random number generation

Comments:

One needs a small random seed to run the algorithm.

Done even experimentally !!

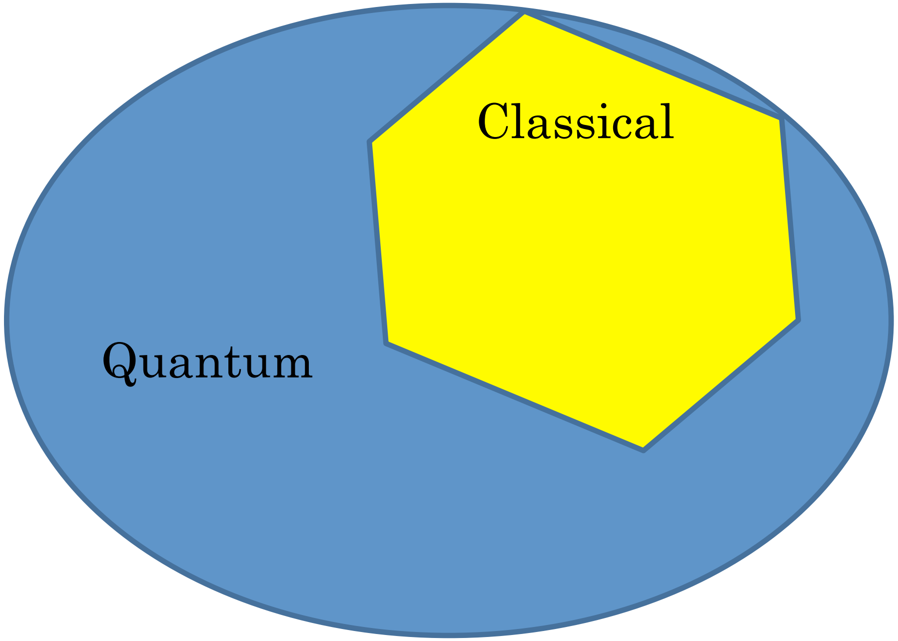
Improved later by many authors (e.g. Miller et al. and Chung et al, 2014).

1. The initial seed is allowed to be only very weakly random and secret.
2. The size of the final random string is exponential on the size of the seed.
3. All steps are robust and efficient

Example. Random number generation

The key is, hence, the existence of quantum strategies which are NOT classical. This guarantees an intrinsic randomness.

$p(ab|xy)$

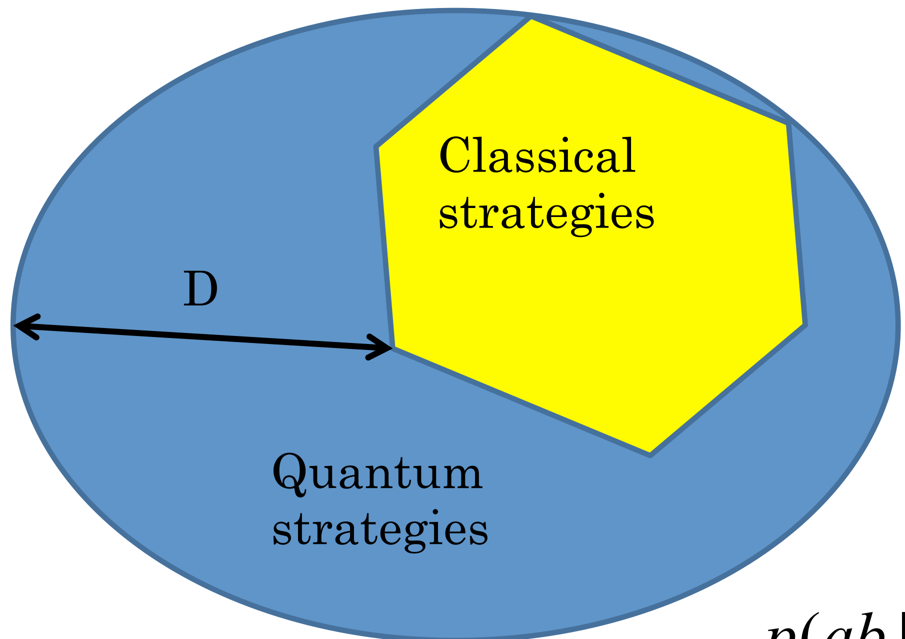


Our contribution

The problems we want to attack.
Games with classical questions/answers

How large can D be?

$$D = \max \frac{\text{quantum value}}{\text{classical value}}$$



$p(ab \mid xy)$

Estimate D.

Parameters:

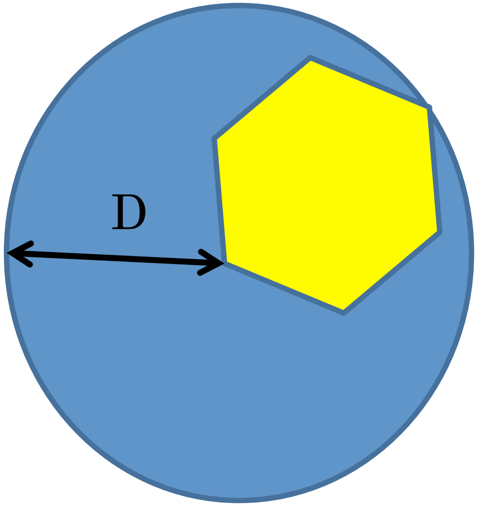
Number of questions = N

Number of answers = M

Size (dimension) of the quantum system = d

Operational interpretation of D

$$D = \frac{1+p}{1-p}, p \in [0,1]$$



Where p is the maximum (classical) noise that a quantum strategy can withstand before getting classical.

D also related to the amount of saving in communication (parallel computing) by using quantum resources.

It is hence desirable to have a large D. How does D scale with the parameters N,M, d?

MAIN THEOREM 1:

Theorem (Junge, Palazuelos, Pérez-García, Villanueva, Wolf, CMP+PRL 2010).
D can be arbitrarily large, This requires:
N= D^2
M= EXP(D)
d= D^2

Later improvements

Theorem (Junge, Palazuelos, 2011).
N= D^2, M= D^2, d= D^2

Theorem (Buhrman et al, 2011).
N= D, M= EXP(D), d= D.

Theorem (Junge, Oikhberg, Palazuelos, 2016).
N= D, M= D^8, d= D

The problems we want to attack. Games with quantum questions/answers

Complexity theory:

How hard is it to estimate the value of a quantum game?

Position based crypto (and other Q-protocols)

If we play a game n times in parallel and we want to win all n times. Does the probability of doing it decreases exponentially with n? (parallel repetition theorem)

Is exponential entanglement needed to break position based crypto protocols?

MAIN THEOREM 2:

Theorem (Cooney, Junge, Palazuelos, Pérez-García, CC 2014). For *rank-one* quantum games

There is a parallel repetition theorem for the value with one-way communication.
There is no perfect parallel repetition for the value with no communication.

The value with one-way communication can be computed efficiently.
The value with no communication can be approximated efficiently up to (multiplicative) constant 4.

Proved independently by Regev and Vidick (similar proof)

MAIN THEOREM 3:

Theorem (Kubicki, Palazuelos, Pérez-García, PRL 2019).

There exists a quantum game so that in the "independent one-way" communication scenario has value 1 but any "universal" strategy requires exponential entanglement.

"Universal" means that in the second round of the optimal strategy, the operations made by Alice and Bob do not depend on the concrete question they receive.

All known attacks to position based crypto are universal.

The tools: Operator spaces

Operator Spaces

An operator space is a complex vector space E with a sequence of norms defined on $M_n(E)$ such that:

$$\|a \oplus b\|_{n+m} = \max\{\|a\|_n, \|b\|_m\}$$

$$\|axb\|_n \leq \|a\|_{M_{nm}} \cdot \|x\|_m \cdot \|b\|_{M_{mn}}$$

Given a C*-algebra, there exists a unique norm which makes $M_n(A)$ a C*-algebra. With these norms, A is an operator space.

Operator spaces

In particular: $\ell_\infty^k = (C^k, \| \ \|_{\max})$

Given $x = \sum_i A_i \otimes e_i \in M_n \otimes \ell_\infty^k = M_n(\ell_\infty^k)$

$$\|x\|_n = \max_i \|A_i\|$$

Operator spaces

The morphisms in this category are the completely bounded maps:

$$u : E \to F, \|u\|_{cb} = \sup_n \|u_n\|$$

$$u_n = 1_n \otimes u : M_n(E) \to M_n(F)$$

CB(E,F) is an operator space via

$$M_n(CB(E,F)) \approx CB(E, M_n(F))$$

In particular E* is an operator space

Connection with classical non-local games

Theorem (Junge, Palazuelos, Pérez-García, Villanueva, Wolf, 2010).
Given a non-local game $T_{ab}^{xy} = \pi(x,y)V(x,y,a,b)$

The classical value is given (with the order a,x,b,y) by the norm:

$$B(B(\ell_\infty^M,\ell_\infty^N),B(\ell_\infty^M,\ell_\infty^N)^*)$$

The quantum value, by the norm:

$$CB(CB(\ell_\infty^M,\ell_\infty^N),CB(\ell_\infty^M,\ell_\infty^N)^*)$$

Connection with rank-one quantum games

Theorem (Cooney, Junge, Palazuelos, Perez-Garcia, 2014).

Any rank-one quantum game can be associated with a map

$$T : M_n \to M_n^*$$

So that the quantum value of the game is exactly

$$\|T\|_{cb}^2$$

CONNECTION WITH POSITION BASED CRYPTOGRAPHY

Theorem (Kubicki, Palazuelos, Perez-Garcia, 2019).

There exists a family of quantum games so that "universal" winning strategies correspond exactly to completely contractive maps (contractive for cb-norm)

$$T : M_n^* \to M_N$$

that are Banach space embeddings (n = size of the game, N = dimension of entanglement)

Take home message

Operator Spaces are the natural mathematical framework to analyze non-local games.

Take home message

Operator Spaces are the natural mathematical framework to analyze non-local games.

1. D. Pérez-García, M.M. Wolf, C. Palazuelos, I. Villanueva, M. Junge, **Unbounded violations of Bell inequalities**, Comm. Math. Phys. 279, 455 (2008)
2. M. Junge, C. Palazuelos, D. Pérez-García, I. Villanueva, M.M. Wolf, **Operator Space theory: a natural framework for Bell inequalities**, Phys. Rev. Lett. 104, 170405 (2010).
3. M. Junge, C. Palazuelos, D. Pérez-García, I. Villanueva, M.M. Wolf, **Unbounded violations of bipartite Bell Inequalities via Operator Space theory**, Comm. Math. Phys. 300, 715–739 (2010).
4. T. Cooney, M. Junge, C. Palazuelos, D. Pérez-García, **Rank-one quantum games**, Computational Complexity, 2014.
5. A.M. Kubicki, C. Palazuelos, D. Pérez-García, **Resource quantification of the no-programming theorem**, Phys. Rev. Lett. 2019 (to appear).