Information-Theoretic Approach to Non-Local Correlations

Serge Massar
(Université Libre de Bruxelles, Belgium)

with J. Barrett, N. Linden,
S. Pironio, S. Popescu, D. Roberts

Plan:

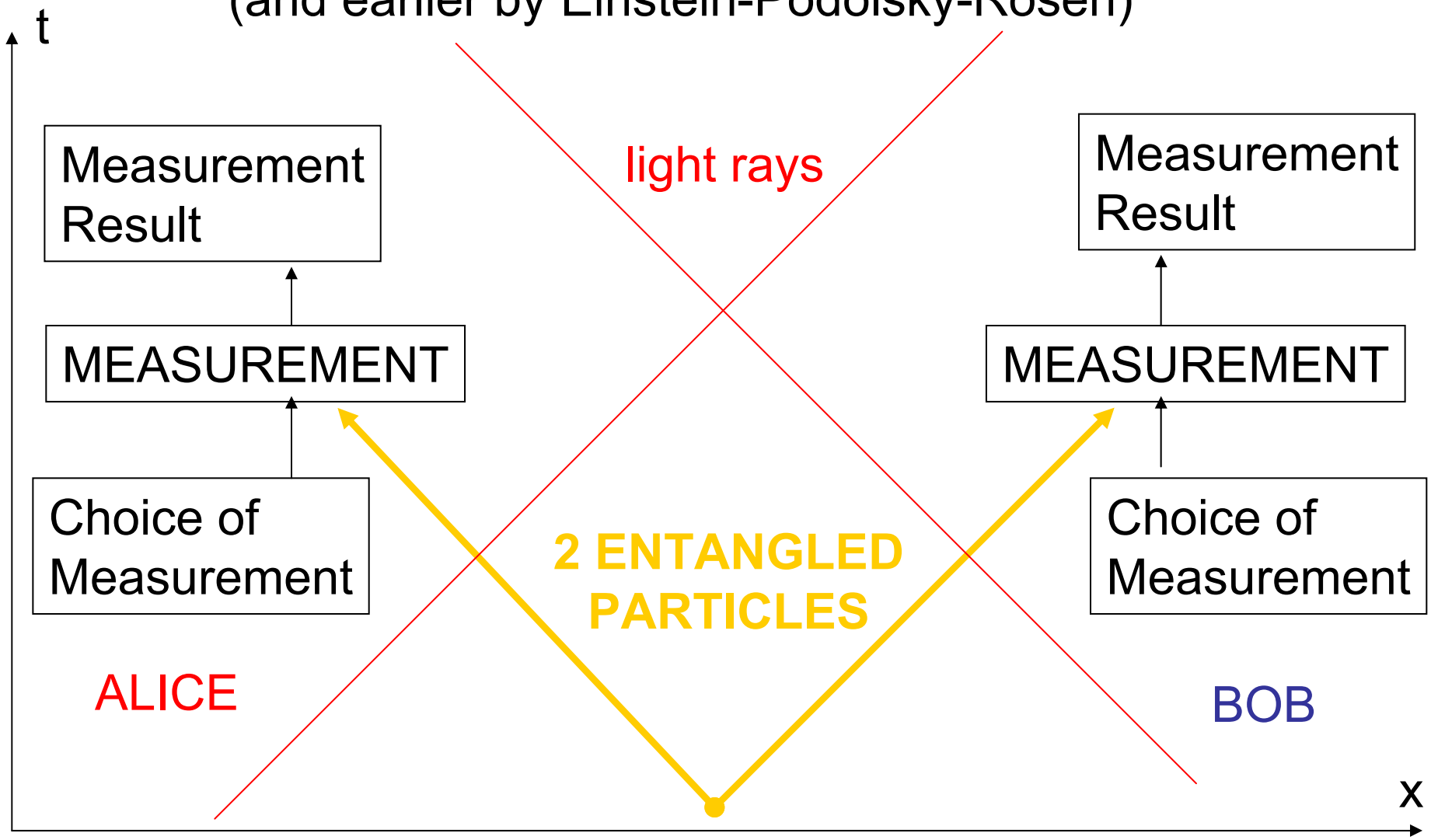
-What is non locality?

-Geometry of non local correlations.

-Non local correlations as information theoretical resources.

Situation Considered by Bell

(and earlier by Einstein-Podolsky-Rosen)



Alice and Bob's measurements are causally disconnected

Quantum Non Locality

Input-Output relation characterized by probabilities P(a,b|x,y)

More Generally: "Bipartite Machines" characterized by input-output relation P(a,b|x,y)

What kind of bipartite machines can exist ?

- Signaling machines: a=y ; b=x (Alice's output tells her about Bob's input)
- No signaling machines: the statistics of Alice's output a tell her nothing about Bob's input:
  - P(a|xy) is independent of y, and similarly for Bob
- Local machines:
  - Local deterministic machines
    - a = f(x) ; b=g(y) (for instance a=x ; b=0)
  - Local hidden variable machines:

    the parties choose before hand what local deterministic machine they are going to use.

A simple no signaling machine x,y=0,1 and a,b=0,1

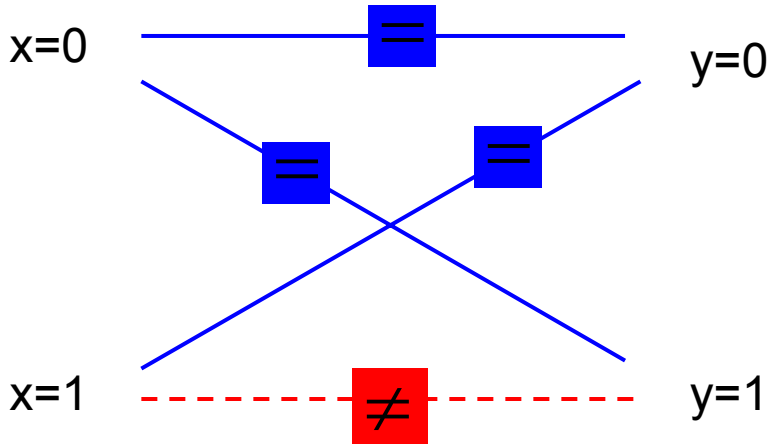
(introduced by Popescu and Rohrlich)

Definition:

- a=b if x or y is equal to zero
- a different from b if x=1 and y=1
- a and b are completely random

Or more synthetically: $a + b \bmod 2 = x.y$

Or graphically:



Local machines versus quantum mechanics versus no signaling machines

- if the inputs x and y are equally probable:
- a local machine (with shared randomness) can satisfy this relation with probability 75%
- quantum correlations can satisfy it with probability 85% (= ½+√½)

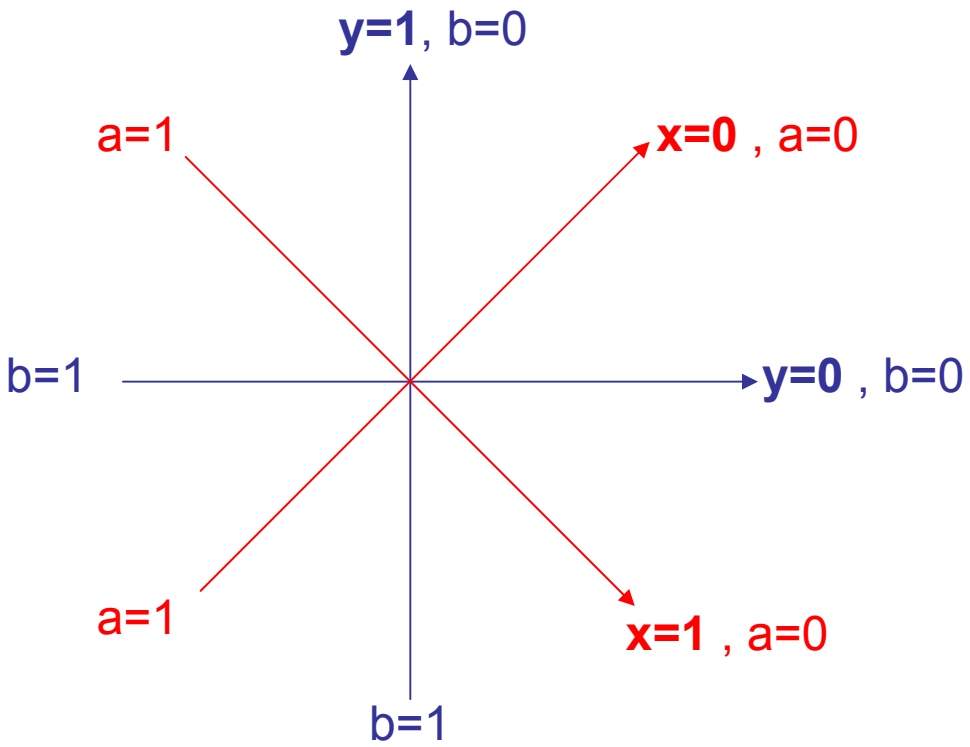
  (Clauser-Horne-Shimony-Holtz)
- physically possible no signaling machines could satisfy this relation with probability 100%
- why don't they?

- Element of answer (Wim van Dam):
  - The perfect machines a+b=x.y allow one to solve all bipartite communication complexity problems with one bit of output with a single bit of communication.

    $\rightarrow$the hierarchy of communication complexity collapses

How do the quantum correlations work?

ALICE and Bob share the state |0>|0> +|1>|1>.
Hence if they measure in the same basis their results will be perfectly correlated. In general the correlations are proportional to cos of the angle between the measurement bases. They measure in the bases:



Why are the Popescu-Rohrlich correlations a+b mod 2 = x.y so important?

→Understand the geometry of non local correlations:

- Correlations are characterized by the probability distributions P(a,b|x,y)
- What conditions do these probability distributions obey?

1) Positivity: $P(a,b|x,y) \geq 0$
2) Normalisation: $\sum_{ab} P(a,b|x,y) = 1$
3) No signalling:

   -Alice cannot learn about Bob's input:

   $\sum_{b} P(a,b|x,y)$ independent of y

   -Bob cannot learn about Alice's input:

   $\sum_{a} P(a,b|x,y)$ independent of x

Thus the non local correlations belong to a **POLYTOPE**.

It lives in the space defined by normalization (2) and no signaling (3).

The facets of the polytope are given by positivity (1).

What are the extremal points of the non-local polytope?

binary case: x,y,a,b=0,1: only two kinds of extremal points:

- 16 local deterministic strategies:
  - $a=f(x)=\alpha x+\beta \bmod 2$ $\quad \alpha,\beta=0,1$
  - $b=g(y)=\gamma y+\delta \bmod 2$ $\quad \gamma,\delta=0,1$
- 8 Popescu-Rohrlich correlations:
  - $a+b \bmod 2 = xy + \alpha x + \beta y + \gamma \bmod 2$

Local transformations

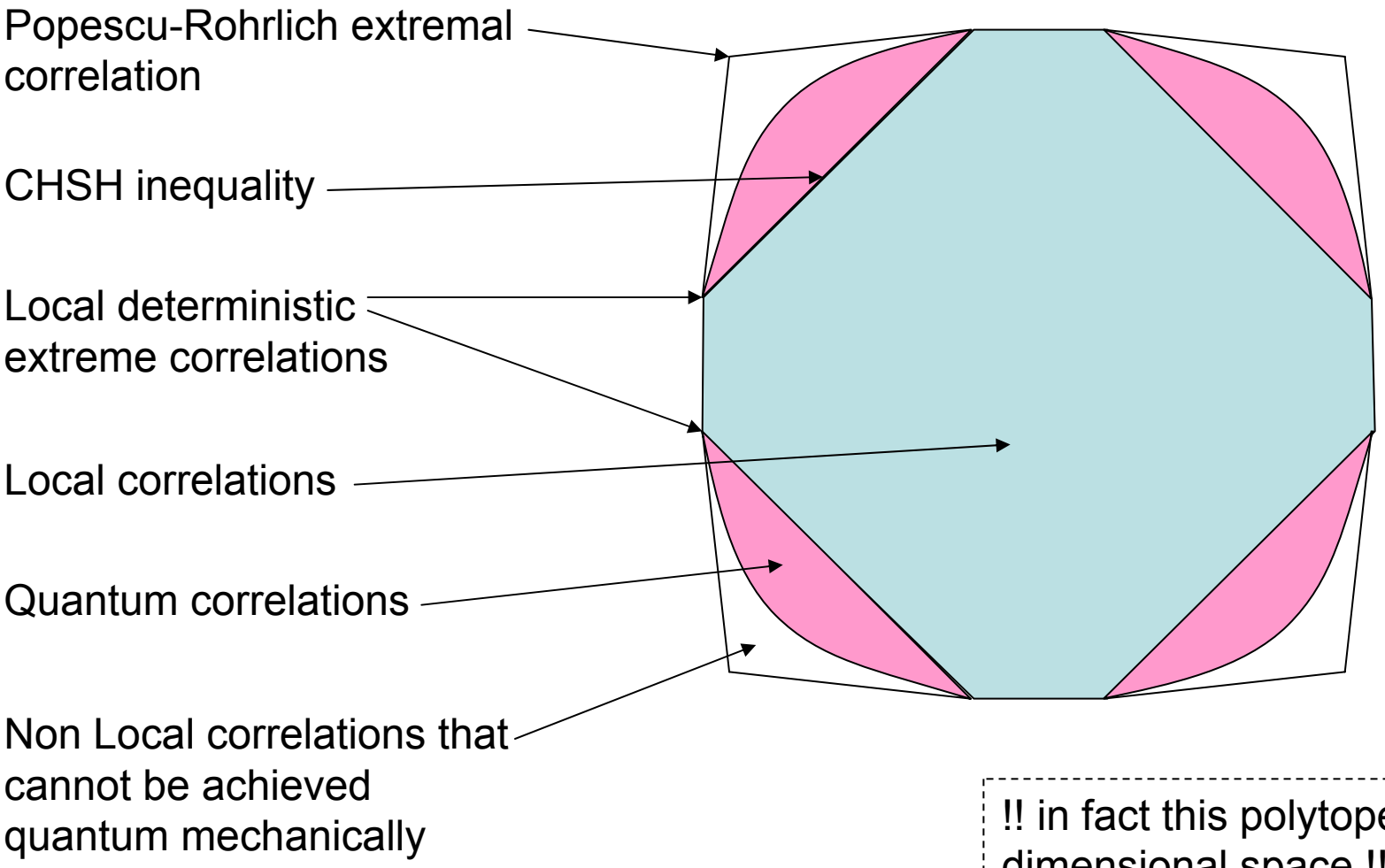
Local transformations that Alice can carry out:

- she can flip her input: $x \rightarrow x + 1$;
- she can flip her output: $a \rightarrow a + 1$;
- she can flip her output conditional on her input: $a \rightarrow a + x$

Hence up to local transformations by both parties there are only 2 kinds of extremal points:

  - local deterministic: $a=0$ & $b=0$
  - non local: $a+b=xy$

Geometry of the space of Non Local Correlations:



!! in fact this polytope lives in an 8 dimensional space !!

Convex Combinations

- Any non local correlation can be realized as a convex combination of the extremal points.
  - Convex combinations can be implemented using shared randomness.
- The local correlations are those that can be realized classically without communication.
  - They are convex combinations of the local deterministic strategies.
  - To realize such convex combinations the parties use shared randomness.
  - The space of local correlations is bounded by *Bell inequalities.*
  - In the present case these are the Clauser-Horne-Shimony-Holt (CHSH) inequalities.
- Each CHSH inequality points towards a single non local extremal point.

What happens when one changes the number of settings? the number of outputs? the number of parties?

- For two parties, two settings (x,y=0,1), d outcomes (a,b=0,…,d-1) we have been able to construct ALL the extremal non local correlations (Stefano Pironio).
- Up to local transformations by the parties they are given by:

  $a-b \bmod d' = x.y$

  where a,b=0,…,d'-1 and $1 \leq d' \leq d$

- In this case we know some (maybe all?) the Bell inequalities.
- In this case there is a one to one correspondence between the known Bell inequalities and the extremal points.
- But the Bell inequalities are much more complicated.

  $\rightarrow$The extremal points capture the essence of non locality

Now the fun begins

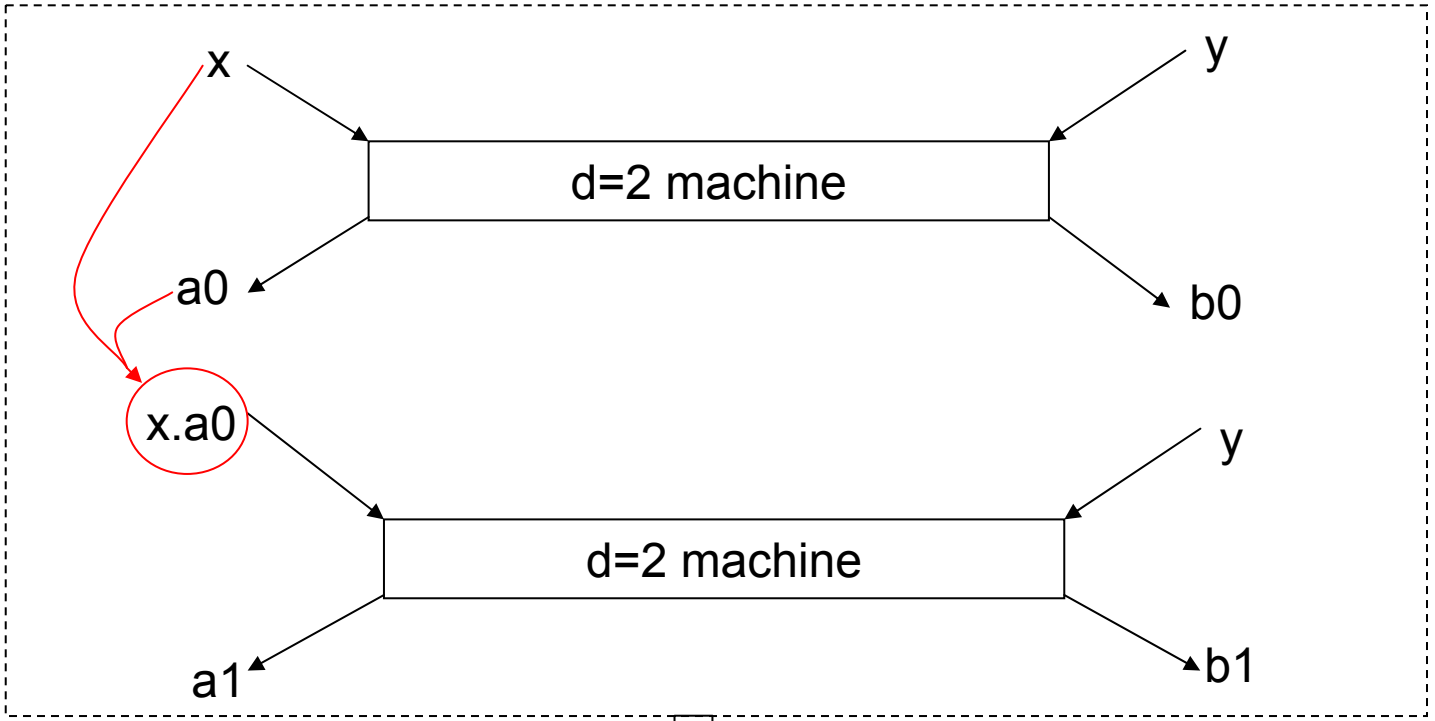
- View non local correlations as information theoretic resources:
- There are different types of non local correlations. Can one interconvert between them?
- Yes:
  - One can interconvert between d=2 and d=4 machines (not reversibly).

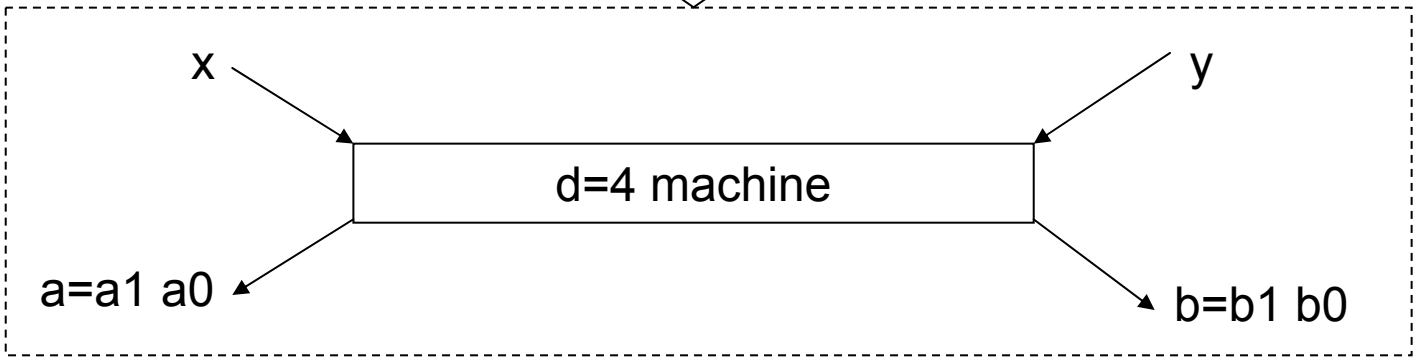
Resources given to the parties

- 1 or many non local machines
- shared randomness
- NO communication

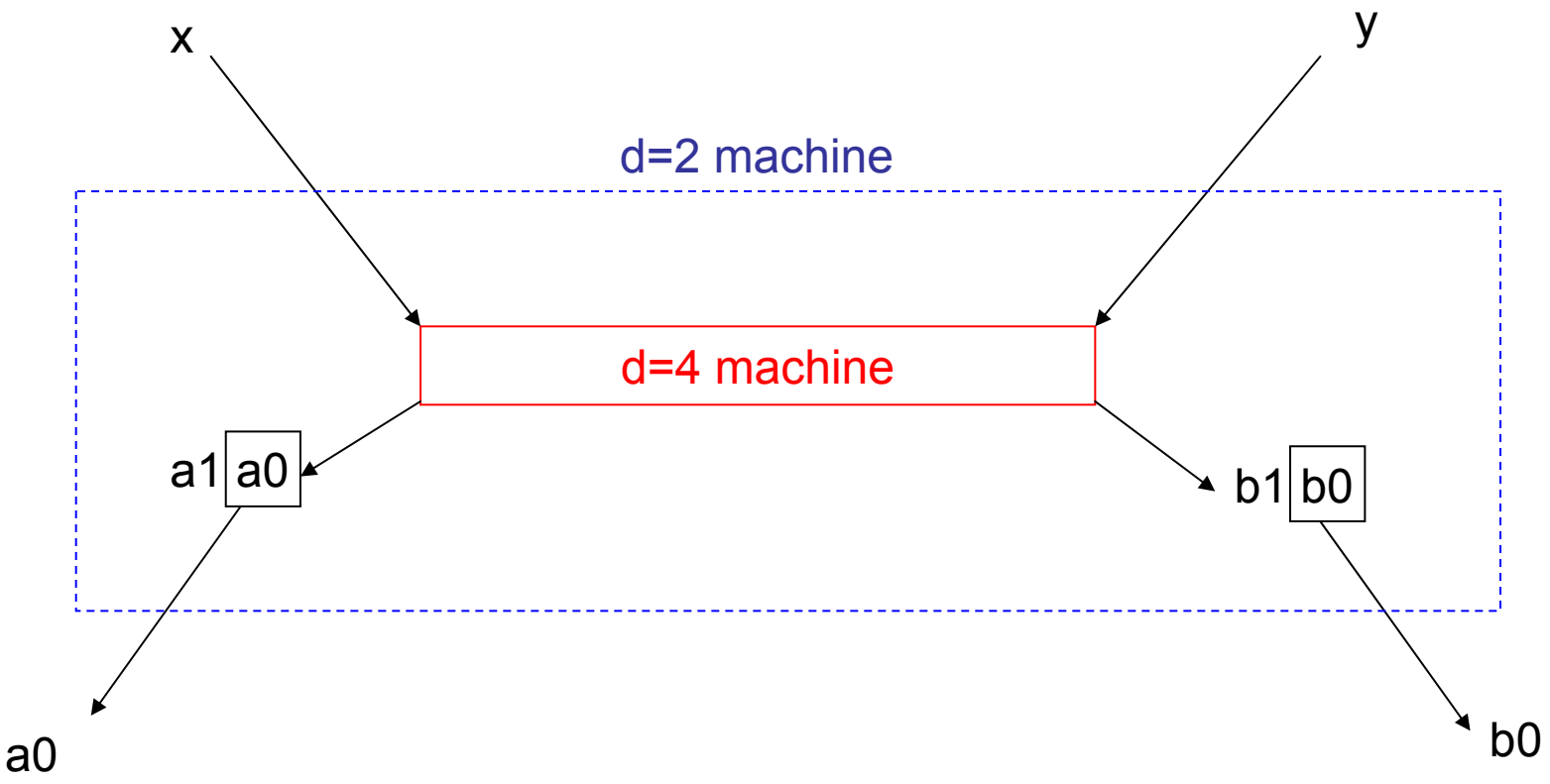
Making a d=4 machine (output written in binary) from a d=2 machine:

The output of one machine times x is used as input of the other machine to realize the carry of addition mod 4.





Making a d=2 machine out of a d=4 machine: use only the least significant bit:



- This can be generalised.
  - one can make a d=2^n machine using n d=2 machines.
  - one can make a d=2 machine from one d=2^n machine.
  - one can convert between k machines of output dimension d and one machine of output dimension d’ with error that decreases as k increases (use the fact that d^n≈d’^m for some n and m).

Interconverting between machines for 2 parties and machines for 3 parties

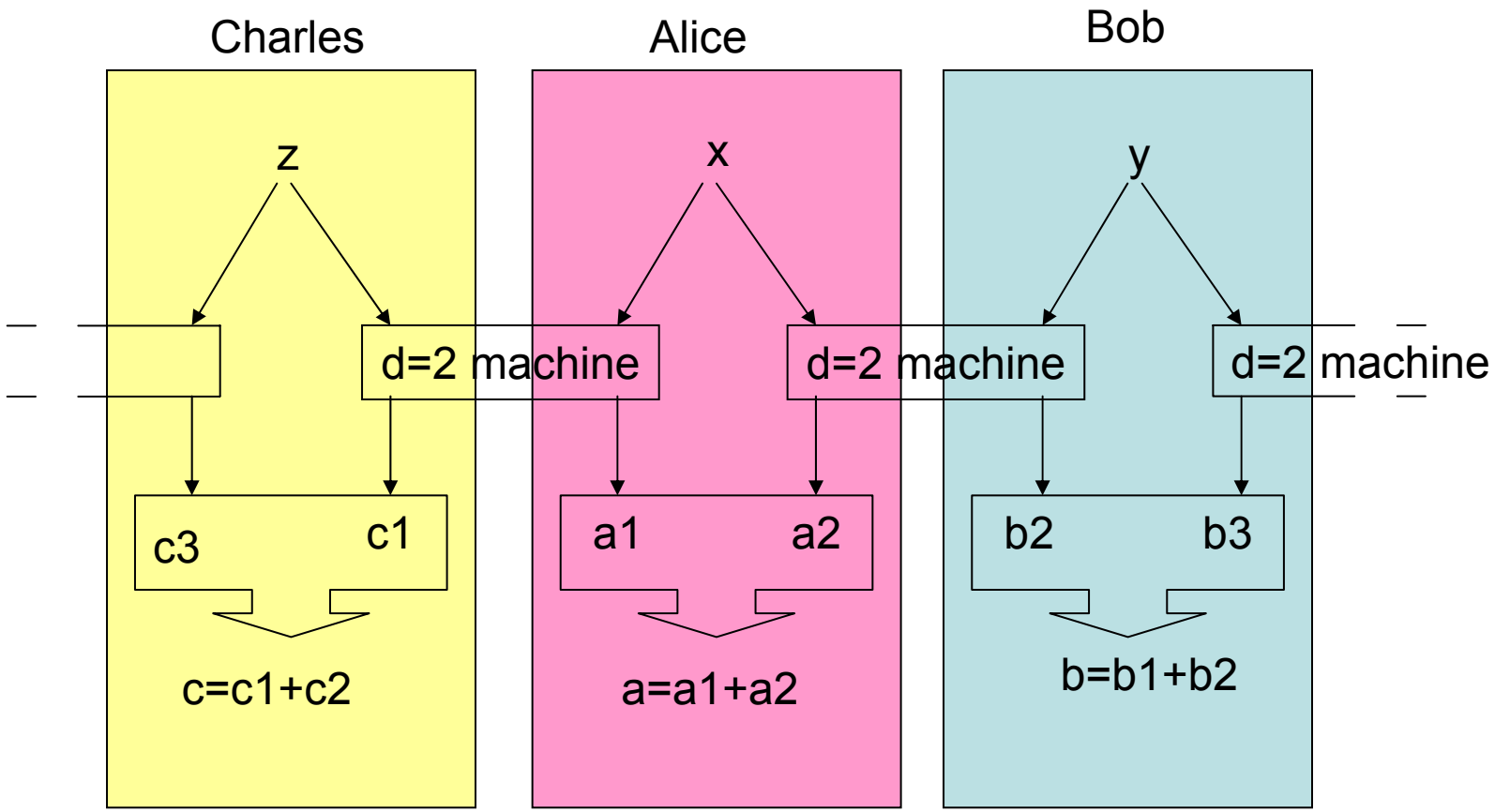
- 3 parties A, B, C
- each party's input is a bit x,y,z =0,1
- each party outputs a bit a,b,c=0,1
- correlations P(a,b,c|x,y,z)
- impose postivity, normalisation, no signalling → (up to local transformations by the parties, and permutations of the parties) 46 inequivalent extremal correlations

- of these 46 extremal correlations, a few have a simple structure:
  1. local deterministic strategies
  2. Popescu-Rohrlich correlations a+b=xy & c=0
  3. a+b+c=xy +yz
  4. a+b+c=xy+yz+zx
  5. a+b+c=xyz

(4 and 5 are related to the GHZ paradox)

- One can make the correlations a+b+c=f(x,y,z) from Popescu-Rohrlich correlations.
- One cannot make Popescu-Rohrlich correlations from the a+b+c=f(x,y,z) correlations.

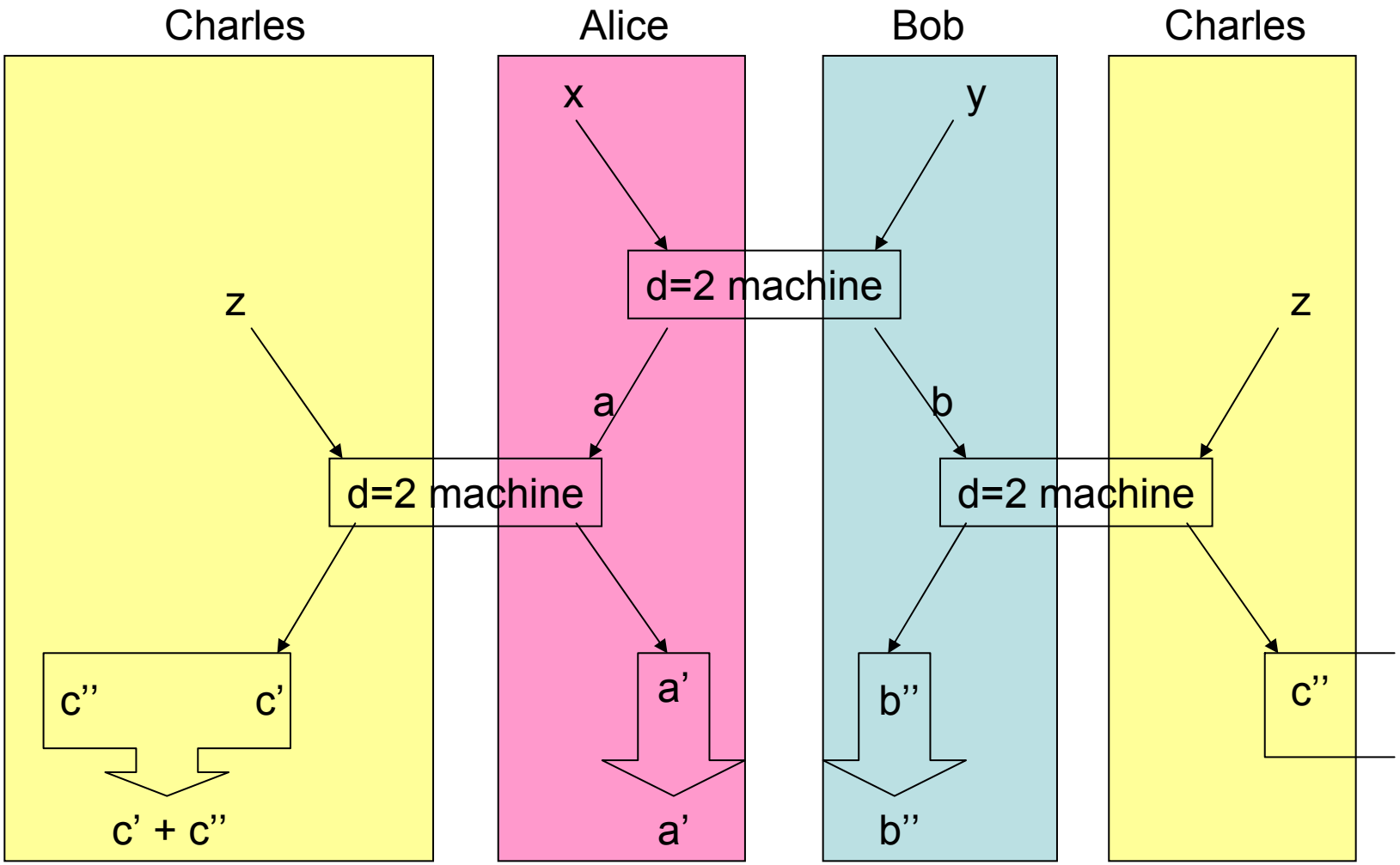
Making the a+b+c=xy+yz+zx machine from three Popescu-Rohrlich machines



a1+c1= xz ; a2+b2= xy ; b3+c3= yz

Hence a + b + c = a1 + a2 + b1 + b2 + c1 + c2 = xy + yz + zx

- the a+b+c=xy+yz machine can be made with 2 Popescu-Rohrlich machines using the same idea.
- what about the a+b+c=xyz machine ?
  - it’s a bit more complicated.

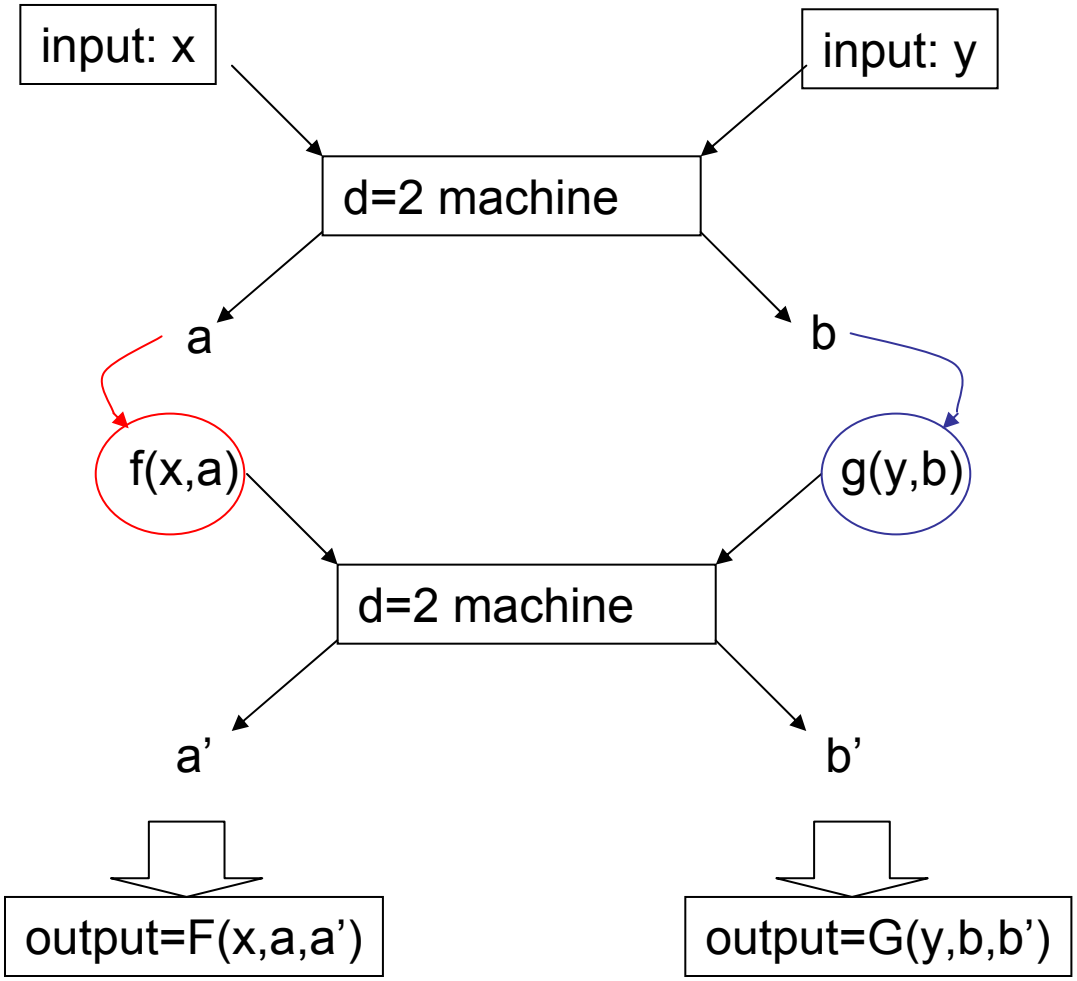


a + b = xy
a' + c' = za ; b'' + c'' = bz
→ a' + b'' + (c' + c'') = (a + b) z = xyz

Open Question 1

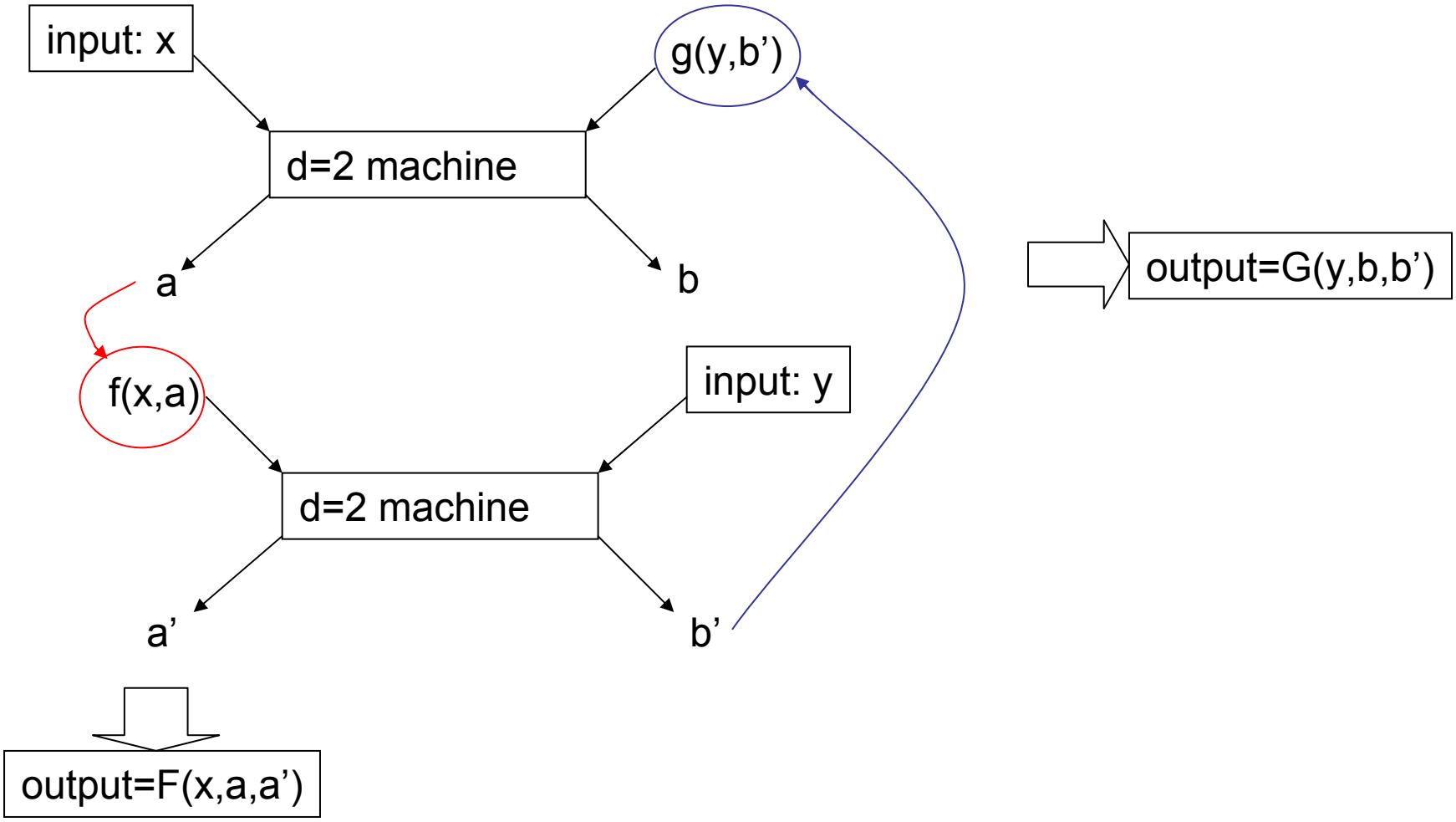
- Are there inequivalent classes of non local correlations?
- Can all extremal non local correlations be made with the Popescu-Rohrlich machine?

What kind of strategies can be used to make new non local correlations from existing machines?



One can use the output of one machine as input for another machine.

But the time ordering need not be the same for both parties!!



- This is possible because of no-signalling:
  - the order in which the parties use the machine cannot transmit information
  - Mathematically:

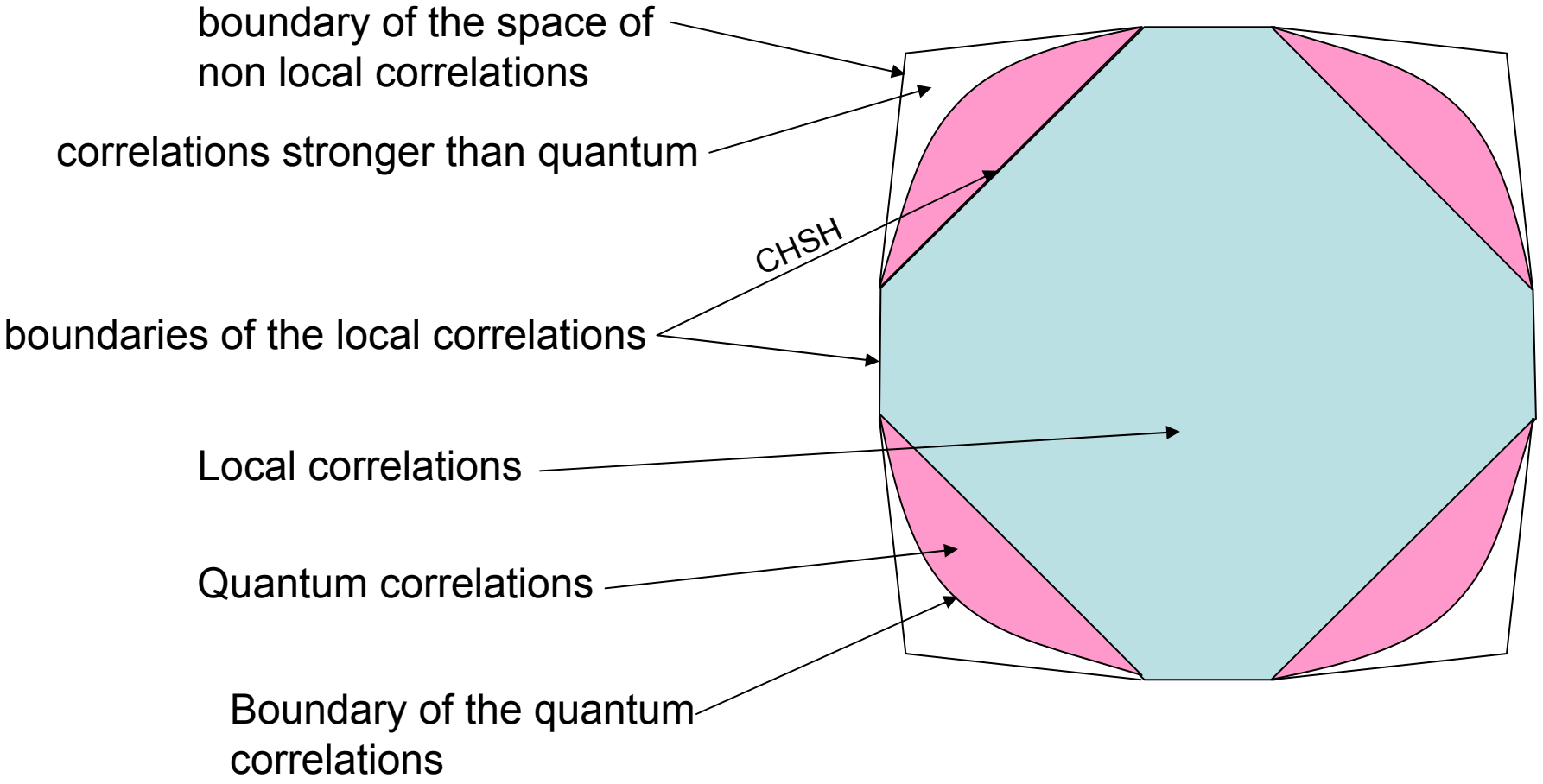
    Bayes and no signaling imply:
    - $P(a,b|x,y)=P(a|b,x,y)P(b|y)$

    $\rightarrow$the machine can first produce Bob's output knowing y, then produce Alice's output knowing b,x,y
    - $P(a,b|x,y)=P(b|a,x,y)P(a|x)$

    $\rightarrow$similarly the machine could first produce Alice's output, then Bob's

Open question 2

- Can one distill noisy non local correlations to make noiseless ones?
  - The operations that should be allowed are local operations and the use of shared randomness.
- Tsirlson (generalized by Popescu & Rorhlich) showed that it is impossible for correlations obtained by measurements on entangled quantum states to violate the CHSH inequality beyond $2\sqrt{1/2}$.



→One cannot distill non local correlations from local ones (Bell)

→One cannot distill correlations stronger than quantum from quantum correlations (Tsirlson)

Is distillation of non local correlations possible?

- Can non local correlations produced by quantum systems be distilled to the Tsirelson bound?
  - if so it would make life easy for experimentators.
- Can non local correlations stronger than quantum mechanics be distilled to the extremal correlations?
  - if so it would explain why quantum mechanics is not maximally non local. Indeed the extremal correlations make communication complexity trivial.

Conclusion

- The talk has been about a classical resource: **non local correlations.**
- They can be viewed as information theoretic resources
  - Different types of these resources are mutually interconvertible.
  - can they be distilled?
- Many new directions for investigation:
  - better understand the geometry of non local correlations.
  - Understand their relation to other information theoretic resources.
  - Understand why quantum correlations are not maximally non local.

Thanks

- Collaborators: J. Barrett, N. Linden, S. Pironio, S. Popescu, D. Roberts
- Funding and Support:
  - Université Libre de Bruxelles (ULB)
  - Belgian National Research Agency (FNRS)
  - Communauté Française de Belgique (ARC)
  - Gouvernement Fédéral Belge (PAI)
  - European Community (project RESQ)