

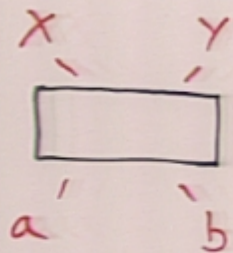
Title: Super-quantum correlations and linear dynamics

Date: Jul 22, 2005 10:15 AM

URL: <http://pirsa.org/05070117>

Abstract:

A PR box...



$$X, Y, a, b \in \{0, 1\}$$

$$a \oplus b = XY$$
$$\Pr(a=0) = 1/2$$
$$\Pr(b=0) = 1/2$$

Super-quantum!

$$\text{CHSH} = 4$$

Isirelson
 $\Rightarrow$ quantum correlations $\leq 2\sqrt{2}$

PR: Why does quantum mechanics
not allow these correlations?

van Dam:

If Alice and Bob share enough
PR boxes, they can solve the inner
product problem in communication
complexity with 1 bit communication

(Compare quantum - need n bits)

→ can solve any problem in
communication complexity with
constant communication

PR: Why does quantum mechanics
not allow these correlations?

van Dam:

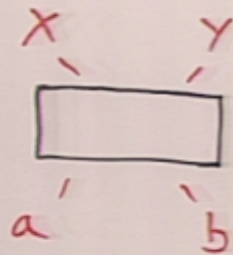
If Alice and Bob share enough
PR boxes, they can solve the inner
product problem in communication
complexity with 1 bit communication

(Compare quantum - need n bits)

→ can solve any problem in
communication complexity with
constant communication

A framework for non-signalling linear theories

A in ...



$$X, Y, a, b \in \{0, 1\}$$

$$a \oplus b = XY$$

$$\Pr(a=0) = 1/2$$

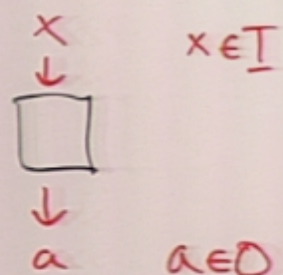
$$\Pr(b=0) = 1/2$$

Super-quantum!

$$\text{CHSH} = 4$$

Isirelson
 $\Rightarrow$ quantum correlations $\leq 2\sqrt{2}$

A single system

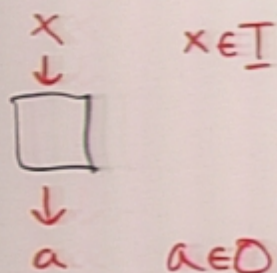


$$\underline{p} = \left(\begin{array}{c} \Pr(a=0 | x=0) \\ \Pr(a=1 | x=0) \\ \vdots \\ \hline \Pr(a=0 | x=1) \\ \Pr(a=1 | x=1) \\ \vdots \\ \hline \vdots \end{array} \right) \left\{ \begin{array}{l} \Sigma = 1 \\ \\ \Sigma = 1 \end{array} \right.$$

State defined by vector of probabilities for outputs given inputs.

Other measurements will be possible.
Think of the 'inputs' as fiducial measurements.

A single system

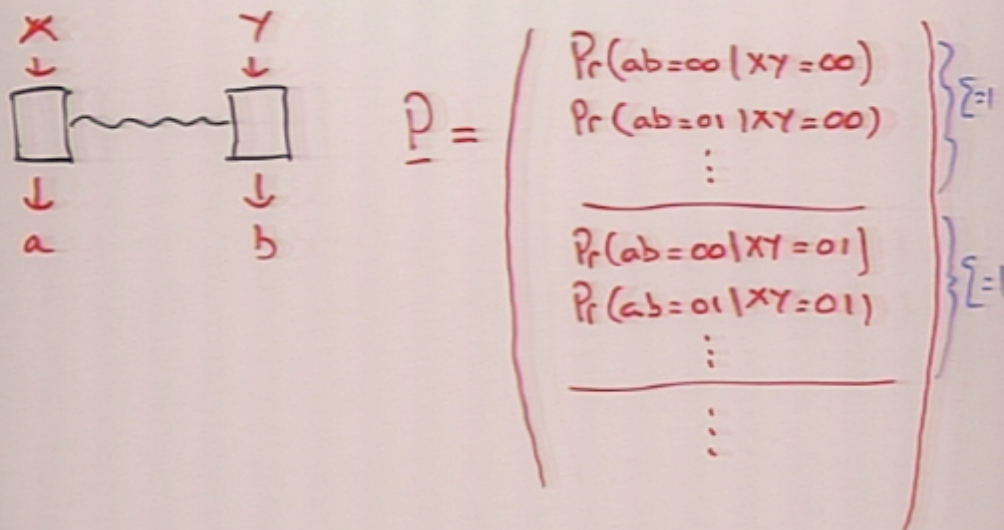


$$\underline{P} = \left(\begin{array}{c} \Pr(a=0 | x=0) \\ \Pr(a=1 | x=0) \\ \vdots \\ \hline \Pr(a=0 | x=1) \\ \Pr(a=1 | x=1) \\ \vdots \\ \hline \vdots \end{array} \right) \left\{ \begin{array}{l} \Sigma = 1 \\ \\ \Sigma = 1 \end{array} \right.$$

State defined by vector of probabilities for outputs given inputs.

Other measurements will be possible.
Think of the 'inputs' as fiducial measurements.

Bipartite systems



NB We will always assume that states are non-signalling. This places linear constraints on P .

NB Assumption. State is completely determined by correlations between outcomes of local measurements.

Measurement

- Yes/no measurement ---

$$P(\text{yes}) = \underline{R} \cdot \underline{P}$$

Must have $0 \leq \underline{R} \cdot \underline{P} \leq 1 \quad \forall \underline{P} \in S,$

where S is set of allowed states.

- If
$$\left. \begin{aligned} 0 \leq \underline{R}_1 \cdot \underline{P} &\leq 1 \\ 0 \leq \underline{R}_2 \cdot \underline{P} &\leq 1 \\ 0 \leq (\underline{R}_1 + \underline{R}_2) \cdot \underline{P} &\leq 1 \end{aligned} \right\} \forall \underline{P} \in S,$$

Then $\underline{R}_1, \underline{R}_2$ can represent different outcomes of a single measurement (of effects in QM)

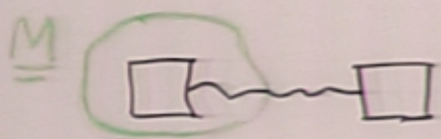
- System destroyed on measurement.

Transformations

$$\underline{P} \rightarrow \underline{P'} = \underline{\underline{M}} \cdot \underline{P}$$

Must have $\underline{P'} \in S \quad \forall \underline{P} \in S.$

Consider...



How define action of $\underline{\underline{M}}$ on joint system?

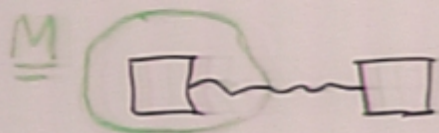
Stipulate that $\underline{\underline{M}}$ commutes with distant measurements.

Transformations

$$\underline{P} \rightarrow \underline{P'} = \underline{M} \cdot \underline{P}$$

Must have $\underline{P'} \in S \quad \forall \underline{P} \in S.$

Consider...



How define action of $\underline{M}$ on joint system?

Stipulate that $\underline{M}$ commutes with distant measurements.

Why linearity?

With non-linear transformations...

- Can in general distinguish
 $\underline{P} = p \underline{P}_1 + (1-p) \underline{P}_2$ from
 $\underline{P} = q \underline{P}_3 + (1-q) \underline{P}_4$.

So $\underline{P}$ is not a complete description.

- This in turn will in general allow signalling in those theories with non-local correlations.
- More bluntly, all Hell breaks loose (probable solution of NP-complete problems in poly time etc).

meaning
With non-linear transformations...

- Can in general distinguish

$$\underline{P} = p \underline{P}_1 + (1-p) \underline{P}_2 \text{ from}$$

$$\underline{P} = q \underline{P}_3 + (1-q) \underline{P}_4.$$

So $\underline{P}$ is not a complete description.

- This in turn will in general allow signalling in those theories with non-local correlations.
- More bluntly, all Hell breaks loose (probable solution of NP-complete problems in polytime etc).

Specify a factory as follows

- i) Specify allowed types of system.
How many inputs/outputs?
- ii) For each allowed type, specify
set of allowed P.
Will be convex in interesting cases.
- iii) Allow all R, M consistent with

$$0 \leq \underline{R} \cdot \underline{P} \leq 1 \quad \forall \underline{P} \in S$$

$$\underline{M} \cdot \underline{P} \in S \quad \forall \underline{P} \in S$$

Interesting Examples

- All types allowed.
All non-signalling $\mathcal{P}$ allowed.
Call this Generalised Non-Signalling Mechanics (GNSM).
- All types allowed.
For single system, any $\mathcal{P}$ allowed.
Multi-partite states must be local.
Call this Generalised Local Mechanics (GLM).
- Variant of QM.
States must be locally quantum
but allow arbitrary multi-partite states.
(Howard's Mechanics)
- QM.
- Classical probabilistic theory.

These theories all have the following properties

- Non-signalling states, linear dynamics, State determined by local measurements.

Apart from the classical theory they have

- Non-commuting measurements, measurement disturbs the system, fuzzy joint measurements of non-commuting observables, no cloning.

QNSM

- Key distribution (Ekert style)
- Communication complexity trivial
- Can't do teleportation! (Bristol group)
- Bit commitment

CLM

- Key distribution (BB84 style)
- Oblivious transfer, bit commitment.

These
properties

owing

- Non-signalling states, linear dynamics, State determined by local measurements.

Apart from the classical theory they have

- Non-commuting measurements, measurement disturbs the system, fuzzy joint measurements of non-commuting observables, no cloning.

QNSM

- Key distribution (Ekert style)
- Communication complexity trivial
- Can't do teleportation! (Bristol group)
- Bit commitment unclear

CLM

- Key distribution (BB84 style)
- Oblivious transfer, bit commitment.

Non-commuting measurements,
 Apart from the classical theory they have

- Non-commuting measurements, measurement disturbs the system, fuzzy joint measurements of non-commuting observables, no cloning.

QNSM

- Key distribution (Ekert style)
- Communication complexity trivial
- Can't do teleportation! (Bristol group)
- Bit commitment unclear

CLM

- Key distribution (BB84 style)
- Oblivious transfer, bit commitment.

Single system dynamics in QM and GZM

Consider the simplest non-trivial single system

$$\begin{array}{c} x \\ \downarrow \\ \square \\ \downarrow \\ z \\ \downarrow \\ a \end{array} \quad x, a \in \{0,1\}$$

Set of states is a square ...



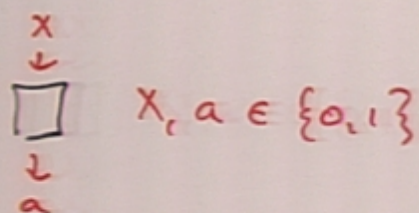
Interpret $x=0$ σ_z -measurement
 $x=1$ σ_x -measurement
QM states $\rightarrow$ circle.

Allowed transformations must take
square $\rightarrow$ square.

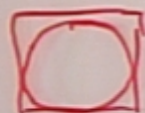


Single system dynamics in GNSM and GZM

Consider the simplest non-trivial single system

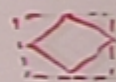
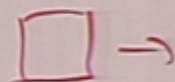
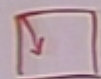


Set of states is a square...



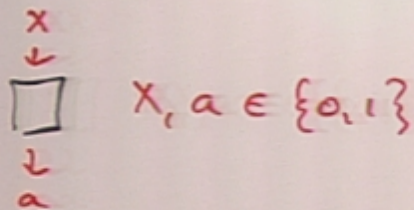
Interpret $x=0$ σ_z -measurement
 $x=1$ σ_x -measurement
QM states $\rightarrow$ circle.

Allowed transformations must take
square $\rightarrow$ square.

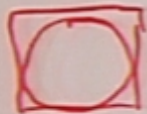


and QLM

Consider the simplest non-trivial single system



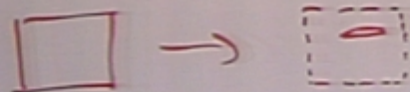
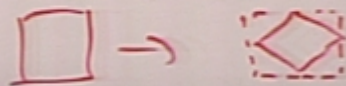
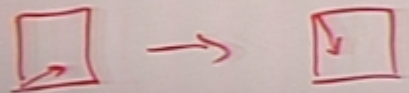
Set of states is a square...



Interpret $x=0$ σ_z -measurement
 $x=1$ σ_x -measurement

QM states $\rightarrow$ circle.

Allowed transformations must take
square $\rightarrow$ square.

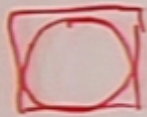


and QLM

Consider the simplest non-trivial single system

x
 $\downarrow$
 $\square$ $x, a \in \{0, 1\}$
 $\downarrow$
 a

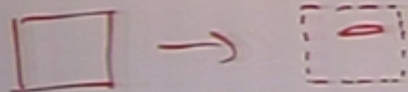
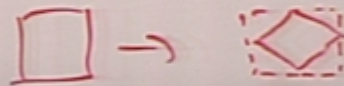
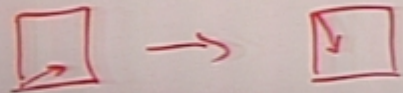
Set of states is a square...



Interpret $x=0$ σ_z -measurement
 $x=1$ σ_x -measurement

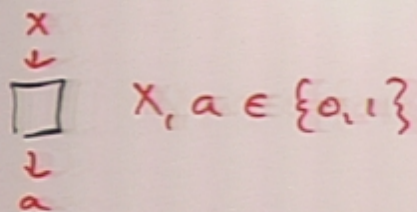
QM states $\rightarrow$ circle.

Allowed transformations must take
square $\rightarrow$ square.

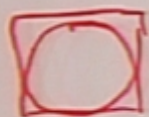


and QLM

Consider the simplest non-trivial single system



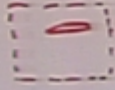
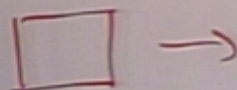
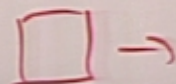
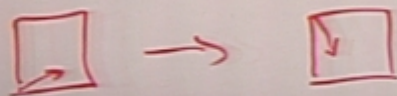
Set of states is a square...



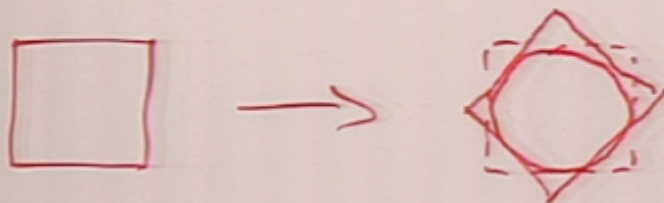
Interpret $x=0$ σ_z -measurement
 $x=1$ σ_x -measurement

QM states $\rightarrow$ circle.

Allowed transformations must take square $\rightarrow$ square.



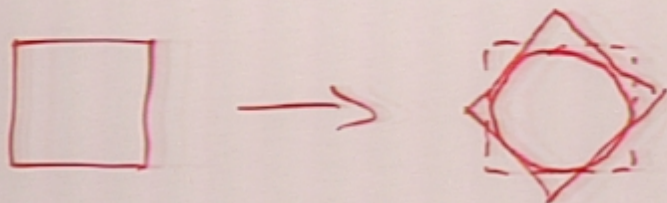
Rotate 45°



Not allowed!

But allowed in qm...

Rotate 45°



Not allowed!

But allowed in qm...

General idea

Expanding set of allowed states
tends to restrict set of allowed
measurements / transformations.

Why no teleportation in QASM?

Required Bell-basis measurement
not properly defined on the
PR box states.

General Idea

Expanding set of allowed states
tends to restrict set of allowed
measurements / transformations.

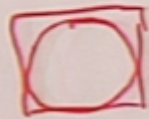
Why no teleportation in GNSM?

Required Bell-basis measurement
not properly defined on the
PR box states.

System

$$\begin{array}{c} \square \\ \downarrow \\ a \end{array} \quad x \in \{0,1\}$$

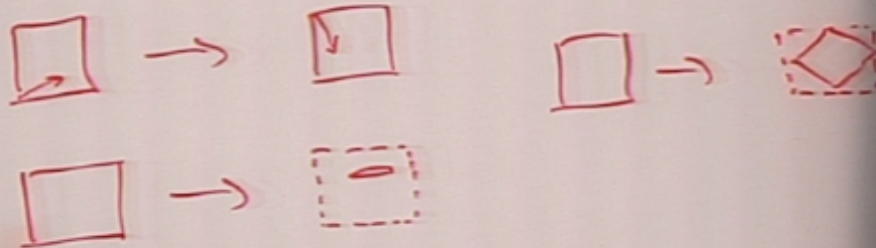
Set of states is a square ...



Interpret $x=0$ σ_z -measurement
 $x=1$ σ_x -measurement

QM states $\rightarrow$ circle.

Allowed transformations must take
square $\rightarrow$ square.



S_i

GNSM, GLM is trivial

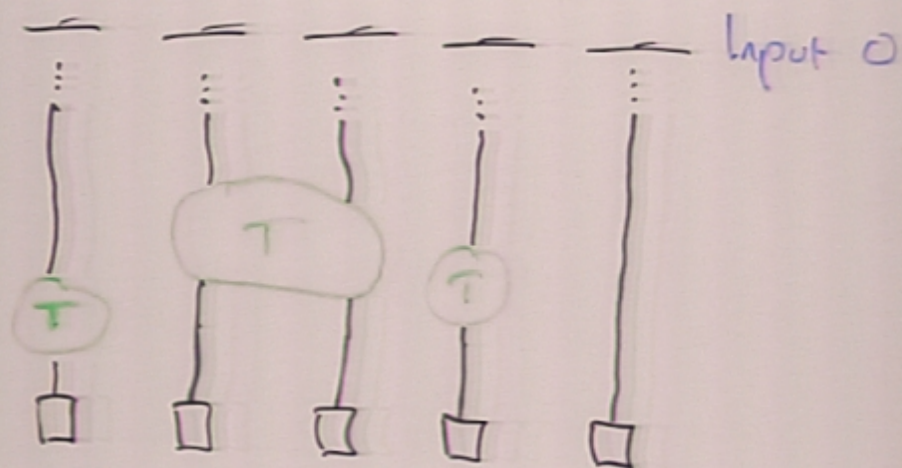
Theorem

Consider a single system in GNSM or GLM with n fiducial measurements (inputs) with K outcomes each.

An allowed transformation is trivial in the following sense. It can always be performed passively by (a convex combination of) relabellings of inputs and outputs.

Computation

Define a circuit model in the obvious way...



Computation in GHM

No better than classical.

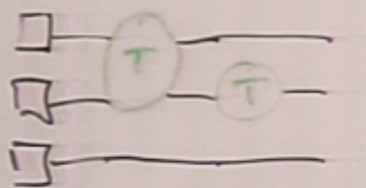
Computation in GNSM

Conjecture no better than classical.

(depends on whether there are
non-trivial joint transformations
on multi-partite systems.)

A weir consequence in QASM

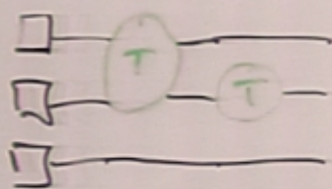
- Start with n single systems prepared in a standard state (e.g. output 0 for all inputs).
- Perform transformations corresponding to some computation



- Much later, can determine result of computation evaluated on any input (but not all inputs!)
- Do this by inputting $x=0,1$ into each system

A weird consequence in QASM

- Start with n single systems prepared in a standard state (e.g. output 0 for all inputs).
- Perform transformations corresponding to some computation



- Much later, can determine result of computation evaluated on any input (but not all inputs!)
- Do this by inputting $x=0,1$ into each system or measuring

A speculation

In this framework, there is a tradeoff between allowed states and allowed dynamics, with corresponding implications for the information processing possibilities of any given theory.

Is QM "optimal" in some sense?