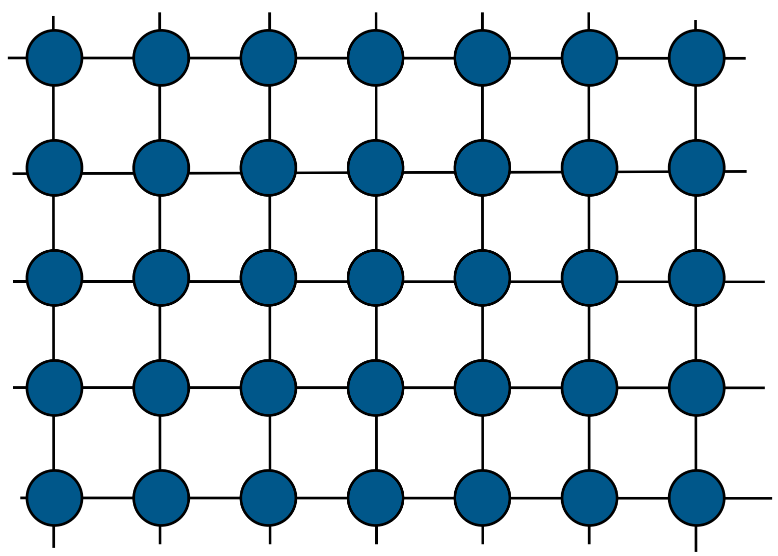
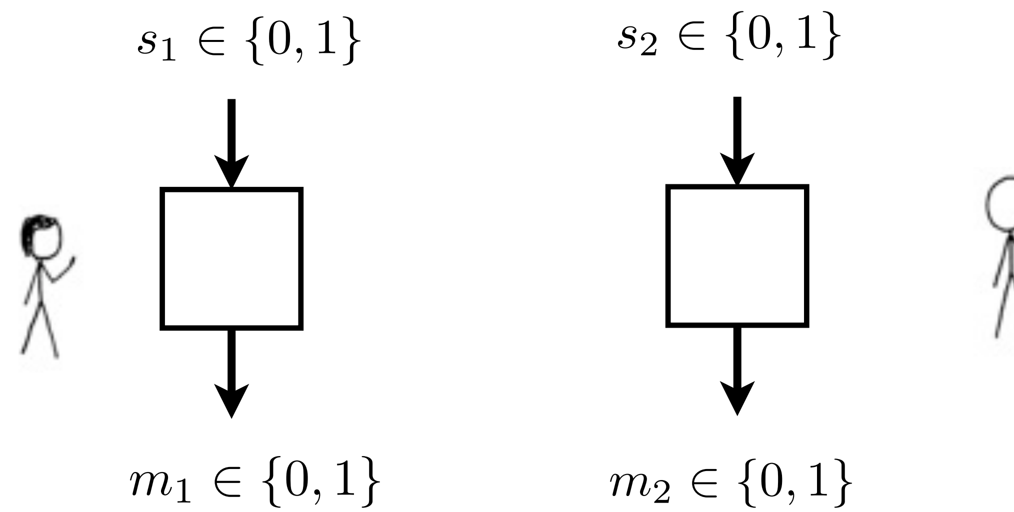
Bell inequalities

for

(*Measurement Based Quantum*) Computation

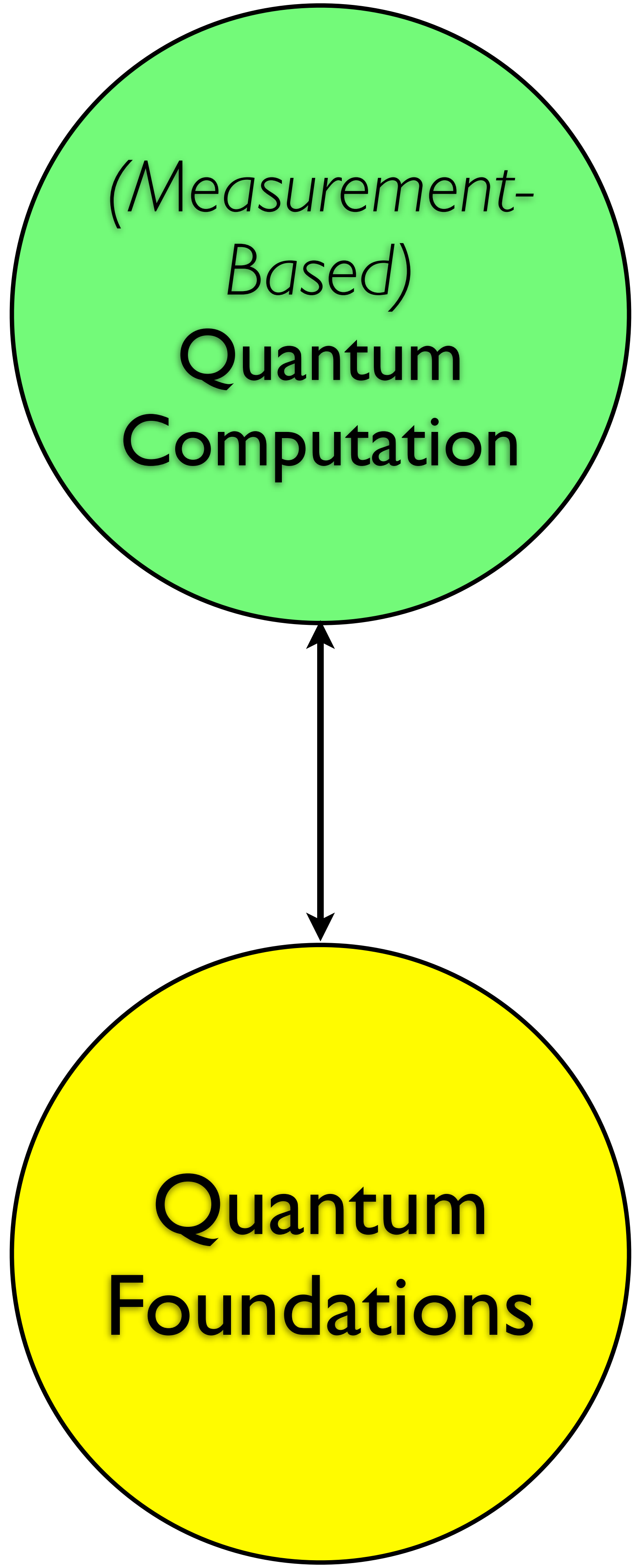




Dan Browne

Dept. of Physics and Astronomy

University College London


(Measurement-Based)
Quantum Computation
Quantum Foundations

Measurement-based quantum computation

Measurement-based quantum computation

- is a model of universal quantum computation.

R. Raussendorf and **H.J. Briegel**, "A one-way quantum computer", PRL 2000.

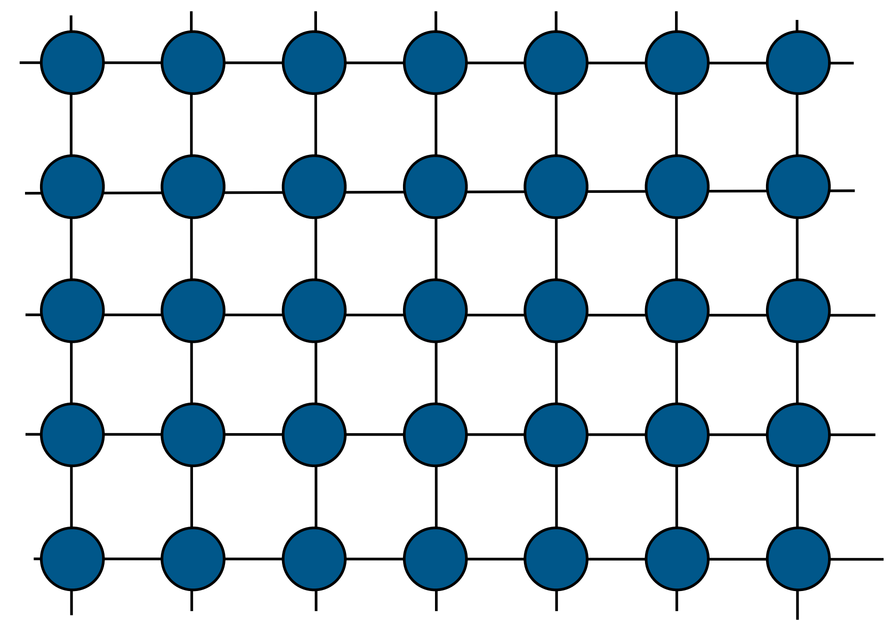
Measurement-based quantum computation

- is a model of universal quantum computation.
  - 1. Create a **special** multi-qubit entangled **state**

R. Raussendorf and **H.J. Briegel**, "A one-way quantum computer", PRL 2000.

Measurement-based quantum computation

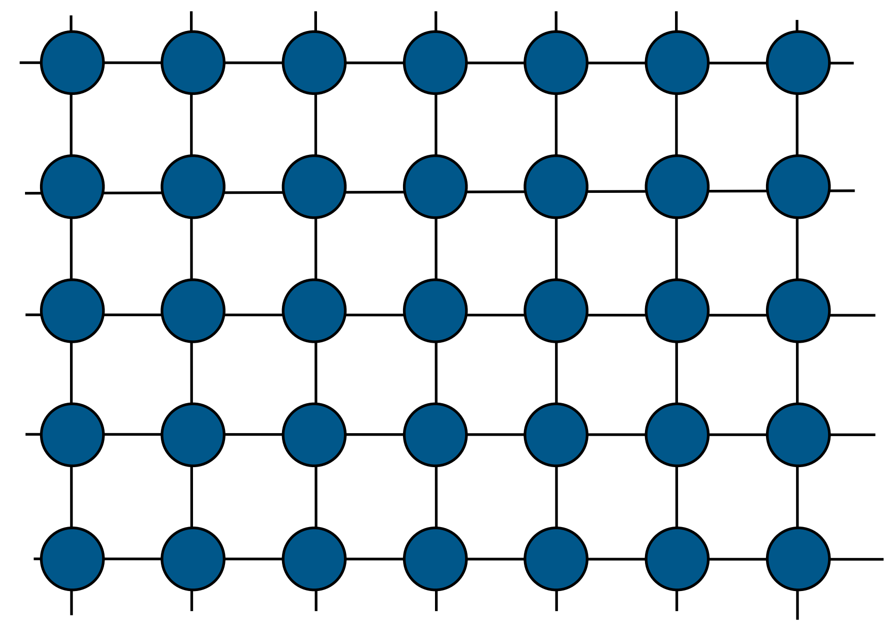
- is a model of universal quantum computation.
  - 1. Create a **special** multi-qubit entangled **state**
    - *e.g. A cluster state*



R. Raussendorf and **H.J. Briegel**, "A one-way quantum computer", PRL 2000.

Measurement-based quantum computation

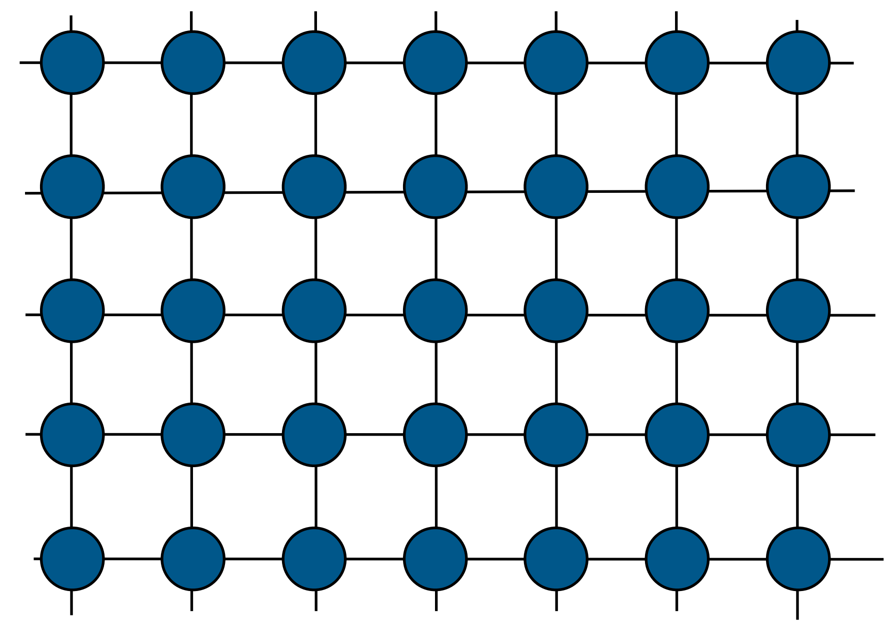
- is a model of universal quantum computation.
  - **1**. Create a **special** multi-qubit entangled **state**
    - *e.g. A cluster state*
  - **2.** Then **measure** qubits **individually**, in certain (**adaptive**) bases, and post-process outcomes.



R. Raussendorf and **H.J. Briegel**, "A one-way quantum computer", PRL 2000.

Measurement-based quantum computation

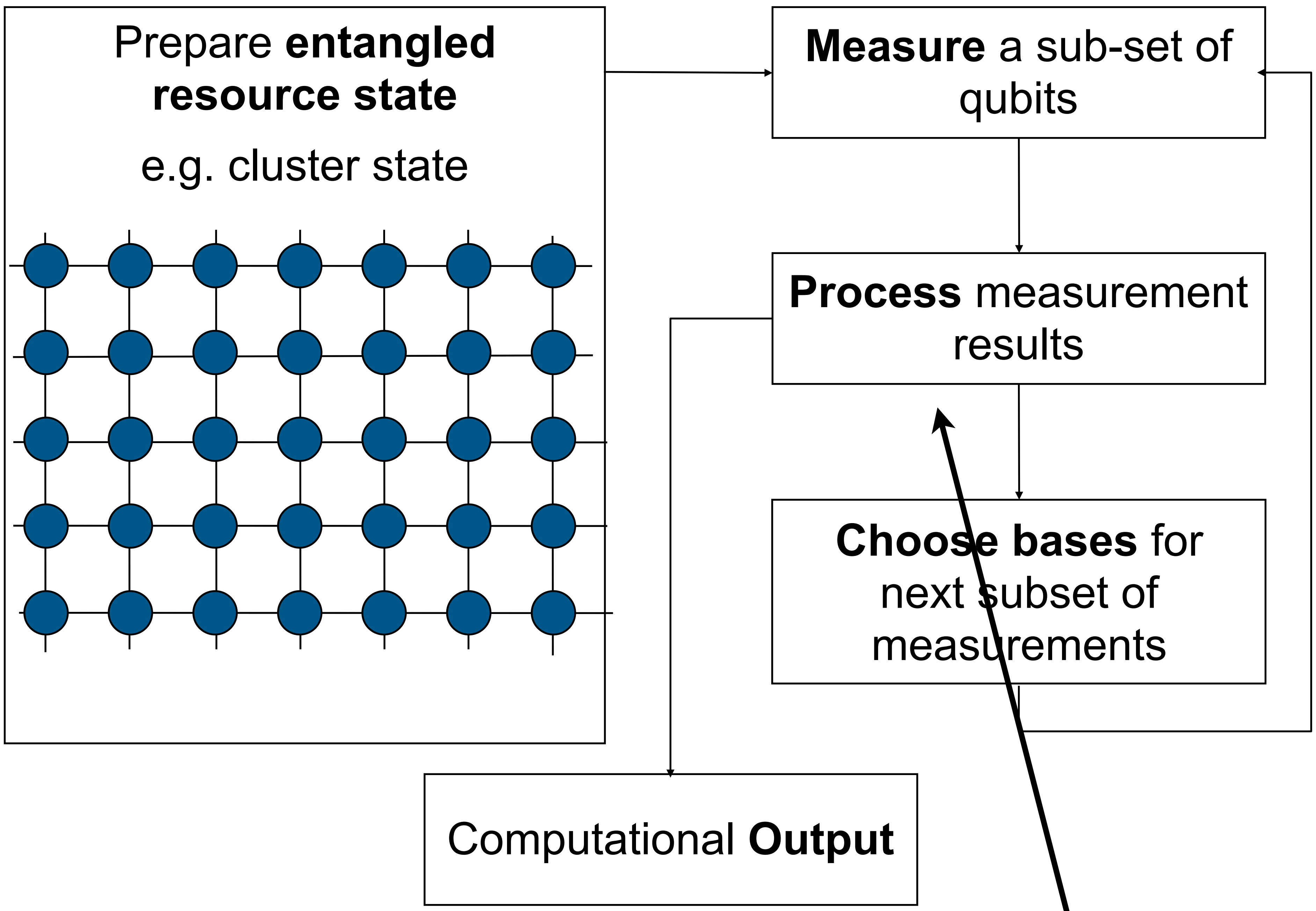
- is a model of universal quantum computation.
  - 1. Create a **special** multi-qubit entangled **state**
    - *e.g. A cluster state*
  - **2.** Then **measure** qubits **individually**, in certain (**adaptive**) bases, and post-process outcomes.



- Via a suitable choice of measurements, **any** quantum computation can be acheived.

R. Raussendorf and **H.J. Briegel**, "A one-way quantum computer", PRL 2000.

Measurement-based quantum computation

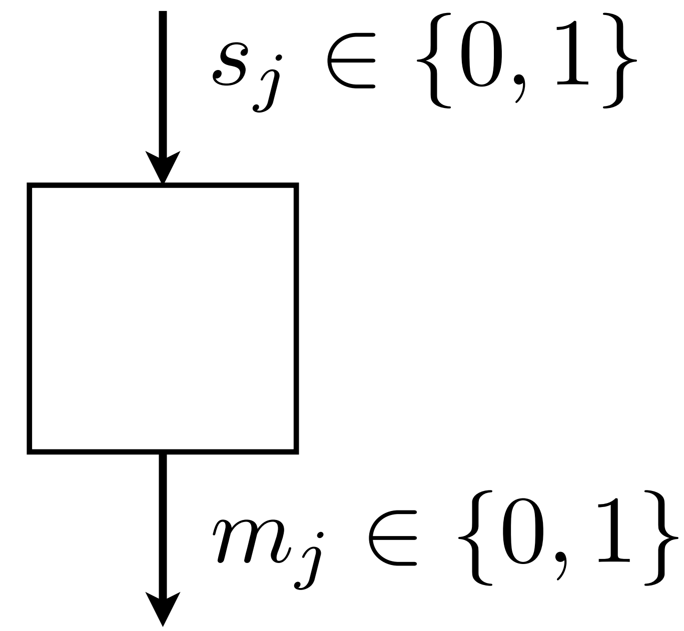


Requires classical "side-computation"

Measurement-based quantum computation

$$\cos\theta_j \; X + \boxed{(-1)^{s_j}} \sin\theta_j \; Y$$

$$+1 \rightarrow 0 \qquad\qquad -1 \rightarrow 1$$



R. Raussendorf, D. E. Browne and **H.J. Briegel,** PRA (2003).

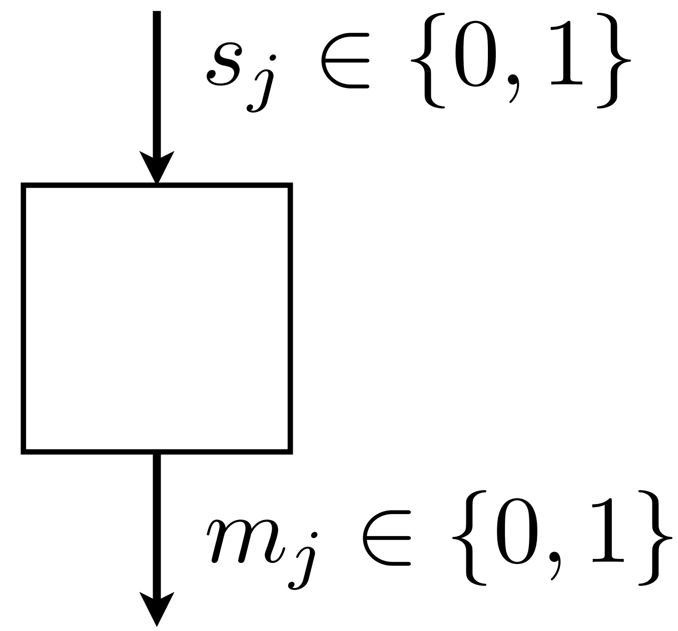
Measurement-based quantum computation

- For a **cluster state** resource it suffices for side-computation to be **linear**.
  - Each measurement is of the form

$$\cos\theta_j \ X + \boxed{(-1)^{s_j}} \sin\theta_j \ Y$$

and meas. outcomes are relabelled

$$+1 \to 0 \qquad -1 \to 1$$



R. Raussendorf, D. E. Browne and **H.J. Briegel,** PRA (2003).

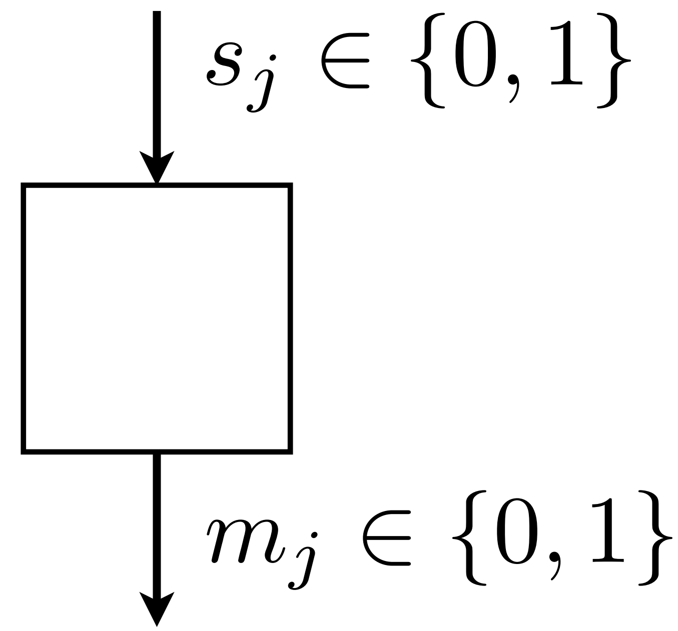
Measurement-based quantum computation

- For a **cluster state** resource it suffices for side-computation to be **linear**.
  - Each measurement is of the form

$$\cos\theta_j \; X + \boxed{(-1)^{s_j}} \sin\theta_j \; Y$$

and meas. outcomes are relabelled

$$+1 \rightarrow 0 \qquad -1 \rightarrow 1$$



- The angle θ_j is **pre-set** and differs for each measurement.

R. Raussendorf, D. E. Browne and **H.J. Briegel,** PRA (2003).

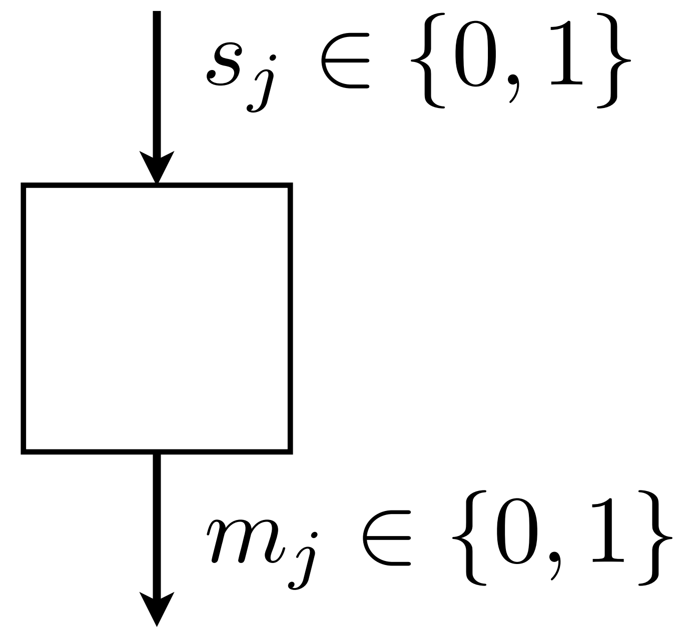
Measurement-based quantum computation

- For a **cluster state** resource it suffices for side-computation to be **linear**.
    - Each measurement is of the form

$$\cos\theta_j \; X + \boxed{(-1)^{s_j}} \sin\theta_j \; Y$$

and meas. outcomes are relabelled

$$+1 \rightarrow 0 \qquad -1 \rightarrow 1$$



- The angle θ_j is **pre-set** and differs for each measurement.
- But bit-value s_j is **calculated on the fly** - and set equal to the **parity** of a sub-set of previous measurement outcomes.

R. Raussendorf, D. E. Browne and **H.J. Briegel,** PRA (2003).

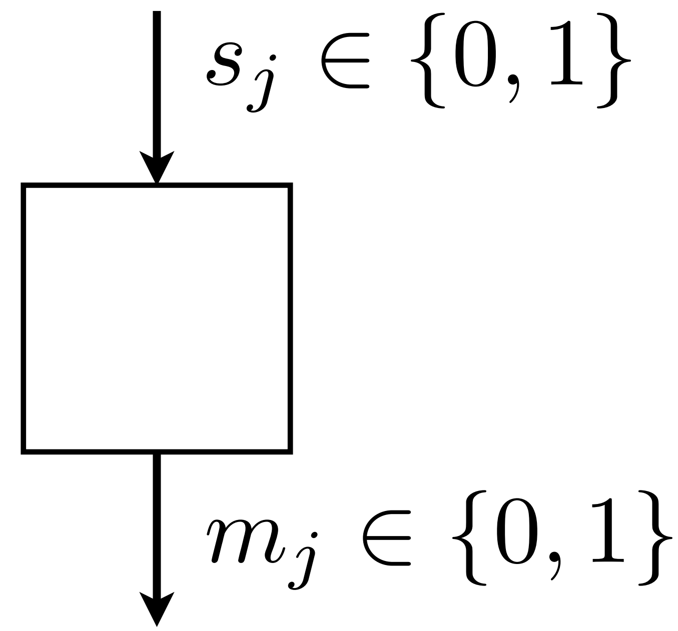
Measurement-based quantum computation

- For a **cluster state** resource it suffices for side-computation to be **linear**.
  - Each measurement is of the form

$$\cos\theta_j \ X + \boxed{(-1)^{s_j}} \sin\theta_j \ Y$$

    and meas. outcomes are relabelled

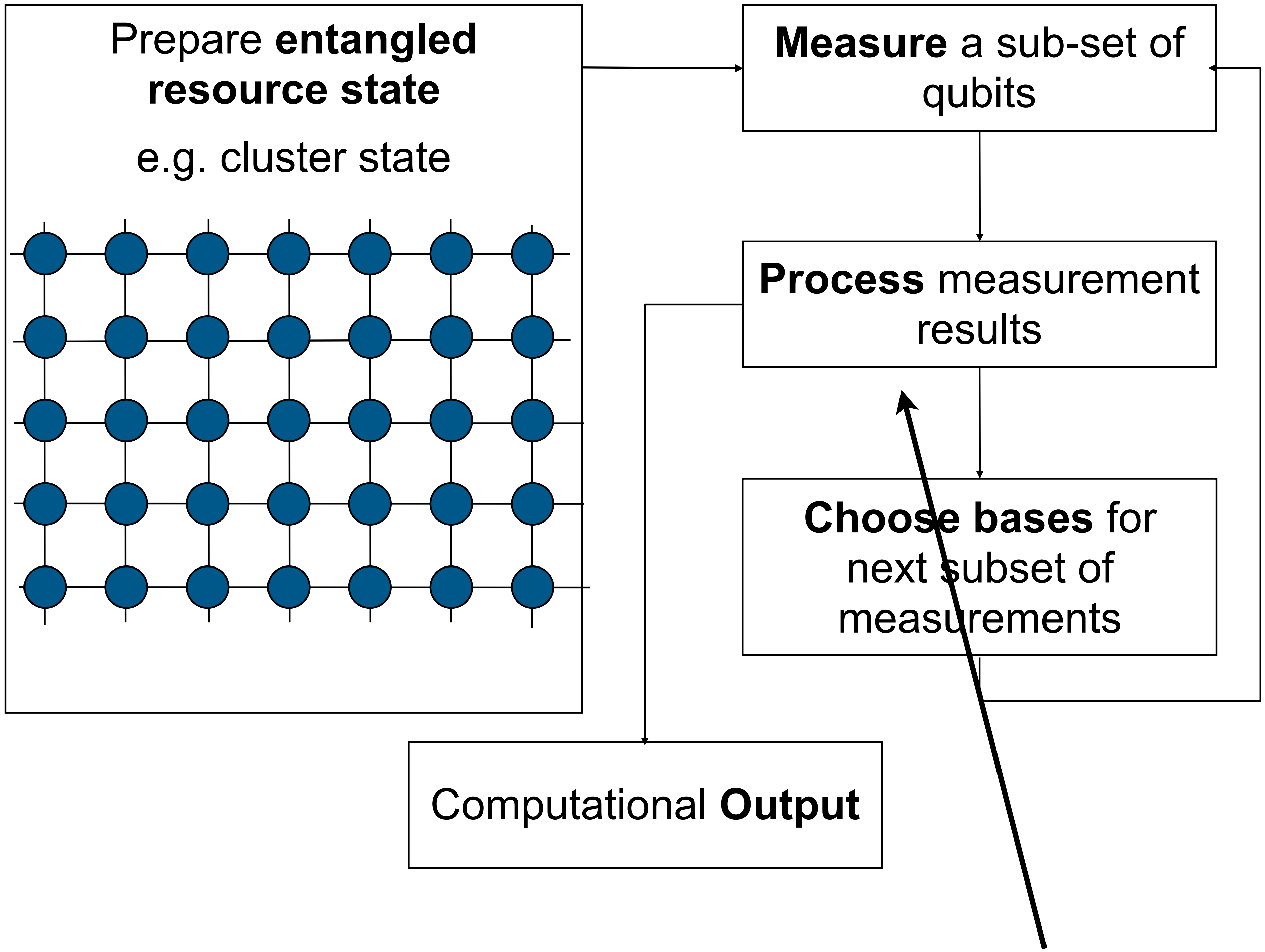
$$+1 \rightarrow 0 \qquad -1 \rightarrow 1$$



- The angle θ_j is **pre-set** and differs for each measurement.
- But bit-value s_j is **calculated on the fly** - and set equal to the **parity** of a sub-set of previous measurement outcomes.
- Final output bits are encoded in the **parity** of a sub-set of the measurement outcomes.

R. Raussendorf, D. E. Browne and **H.J. Briegel,** PRA (2003).

Measurement-based quantum computation



Requires (**linear / XOR**) classical "side-computation"

Bell inequalities

Bell inequalities

Bell inequalities

- Bell inequalities (BIs) express **restrictions** on the **joint probability distributions** for spatially separated measurements in **local hidden variable (LHV) theories**.

CHSH inequality

Setting: $s_1 \in \{0,1\}$ $s_2 \in \{0,1\}$

Outcome: $m_1 \in \{0,1\}$ $m_2 \in \{0,1\}$

- We focus on the **parity** of the outcomes and define:

$$E_{s_1,s_2} = p(m_1 \oplus m_2 = 0|s_1, s_2) - \; p(m_1 \oplus m_2 = 1|s_1, s_2)$$

CHSH inequality

Setting: $s_1 \in \{0,1\}$ $s_2 \in \{0,1\}$

Outcome: $m_1 \in \{0,1\}$ $m_2 \in \{0,1\}$

- We focus on the **parity** of the outcomes and define:

$$E_{s_1,s_2} = p(m_1 \oplus m_2 = 0|s_1, s_2) - p(m_1 \oplus m_2 = 1|s_1, s_2)$$

- and show that for correlations in any LHV theory:

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} \leq 2$$

CHSH inequality

- With **entangled quantum state**, Alice and Bob can violate this inequality, although not exceeding **Tsirelson's bound**:

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} \leq 2\sqrt{2}$$

CHSH inequality

- With **entangled quantum state**, Alice and Bob can violate this inequality, although not exceeding **Tsirelson's bound**:

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} \leq 2\sqrt{2}$$

- A (loophole-free) demonstration of a Bell Inequality violation would **refute** local hidden variable theories.

CHSH inequality

- With **entangled quantum state**, Alice and Bob can violate this inequality, although not exceeding **Tsirelson's bound**:

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} \leq 2\sqrt{2}$$

- A (loophole-free) demonstration of a Bell Inequality violation would **refute** local hidden variable theories.

- The maximal violation (stronger than QM) is achieved by the Popescu-Rohrlich (PR) Box, which acheives

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} = 4$$

B. S. Tsirelson, Lett. Math. Phys. (1980). **S. Popescu** and **D. Rohrlich,** Found. Phys. (1994)

CHSH inequality

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} \leq 2$$

- It is useful to re-express the CHSH Inequality directly in terms of conditional probabilities.

$$E_{s_1,s_2} = p(m_1 \oplus m_2 = 0|s_1, s_2) - p(m_1 \oplus m_2 = 1|s_1, s_2)$$

CHSH inequality

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} \leq 2$$

- It is useful to re-express the CHSH Inequality directly in terms of conditional probabilities.

$$E_{s_1,s_2} = p(m_1 \oplus m_2 = 0|s_1, s_2) - p(m_1 \oplus m_2 = 1|s_1, s_2)$$

- Some simple algebra gives us a very neat representation [1] of the CHSH inequality:

$$\frac{1}{4}\sum_{s_1,s_2} p(m_1 \oplus m_2 = s_1 s_2|s_1 s_2) \leq \frac{3}{4}$$

[1] QIP Folklore: earliest reference I know: Wim Van Dam, PHD Thesis (2000)

CHSH inequality

$$E_{0,0} + E_{0,1} + E_{1,0} - E_{1,1} \leq 2$$

- It is useful to re-express the CHSH Inequality directly in terms of conditional probabilities.

$$E_{s_1,s_2} = p(m_1 \oplus m_2 = 0|s_1, s_2) - p(m_1 \oplus m_2 = 1|s_1, s_2)$$

- Some simple algebra gives us a very neat representation [1] of the CHSH inequality:

$$\frac{1}{4} \sum_{s_1,s_2} p(m_1 \oplus m_2 = s_1 s_2 | s_1 s_2) \leq \frac{3}{4}$$

- Thus we can phrase the CHSH inequality in terms of a **game**.

[1] QIP Folklore: earliest reference I know: Wim Van Dam, PHD Thesis (2000)

CHSH game

- **Rules**:
  - Alice, Bob are given independent bits s_1, s_2 from a uniform distribution.

  - They may not communicate during the game.

- **Aim**:
  - They should each produce a bit m_1, m_2, such that

$$m_1 \oplus m_2 = s_1 s_2$$

$$m_1 \text{ XOR } m_2 = s_1 \text{ AND } s_2$$

- We call games where the desired data is encoded in the **XOR** of measurement outcomes **XOR-games**.

CHSH game

$$\frac{1}{4}\sum_{s_1,s_2} p(m_1+m_2=s_1s_2) \quad \begin{aligned} &\leq \frac{3}{4} && \text{LHV} \\ &\leq \frac{2+\sqrt{2}}{4} \approx 0.85 && \text{Quantum} \\ &= 1 && \text{PR Box} \end{aligned}$$

CHSH game

- **CHSH inequalities** bound the mean success probability of the game.

$$\frac{1}{4}\sum_{s_1,s_2} p(m_1 + m_2 = s_1 s_2)$$

	$\leq \frac{3}{4}$	LHV
	$\leq \frac{2+\sqrt{2}}{4} \approx 0.85$	Quantum
	$= 1$	PR Box

CHSH game

- **CHSH inequalities** bound the mean success probability of the game.

$$\frac{1}{4}\sum_{s_1,s_2} p(m_1 + m_2 = s_1 s_2) \quad \begin{array}{ll} \leq \frac{3}{4} & \text{LHV} \\ \leq \frac{2+\sqrt{2}}{4} \approx 0.85 & \text{Quantum} \\ = 1 & \text{PR Box} \end{array}$$

- The **GHZ paradox** can also be related to a very **similar game**.

GHZ correlation

$$|\psi\rangle = |001\rangle + |110\rangle$$

(uniquely) satisfies:

$$\left.\begin{aligned} X \otimes X \otimes X|\psi\rangle &= |\psi\rangle \\ X \otimes Y \otimes Y|\psi\rangle &= |\psi\rangle \\ Y \otimes X \otimes Y|\psi\rangle &= |\psi\rangle \\ \text{which also imply:} & \\ Y \otimes Y \otimes X|\psi\rangle &= -|\psi\rangle \end{aligned}\right\} \text{Correlations in outcomes of local measurements}$$

N. D. Mermin (1990), building on **Greenberger**, et al. (1989)

GHZ correlation

$$|\psi\rangle = |001\rangle + |110\rangle$$

(uniquely) satisfies:

$$X \otimes X \otimes X|\psi\rangle = |\psi\rangle$$
$$X \otimes Y \otimes Y|\psi\rangle = |\psi\rangle$$
$$Y \otimes X \otimes Y|\psi\rangle = |\psi\rangle$$

which also imply:

$$Y \otimes Y \otimes X|\psi\rangle = -|\psi\rangle$$

Correlations in outcomes of local measurements

N. D. Mermin (1990), building on **Greenberger**, et al. (1989)

GHZ correlation

$$|\psi\rangle = |001\rangle + |110\rangle$$

(uniquely) satisfies:

$$X \otimes X \otimes X|\psi\rangle = |\psi\rangle$$

$$X \otimes Y \otimes Y|\psi\rangle = |\psi\rangle$$

$$Y \otimes X \otimes Y|\psi\rangle = |\psi\rangle$$

which also imply:

$$Y \otimes Y \otimes X|\psi\rangle = -|\psi\rangle$$

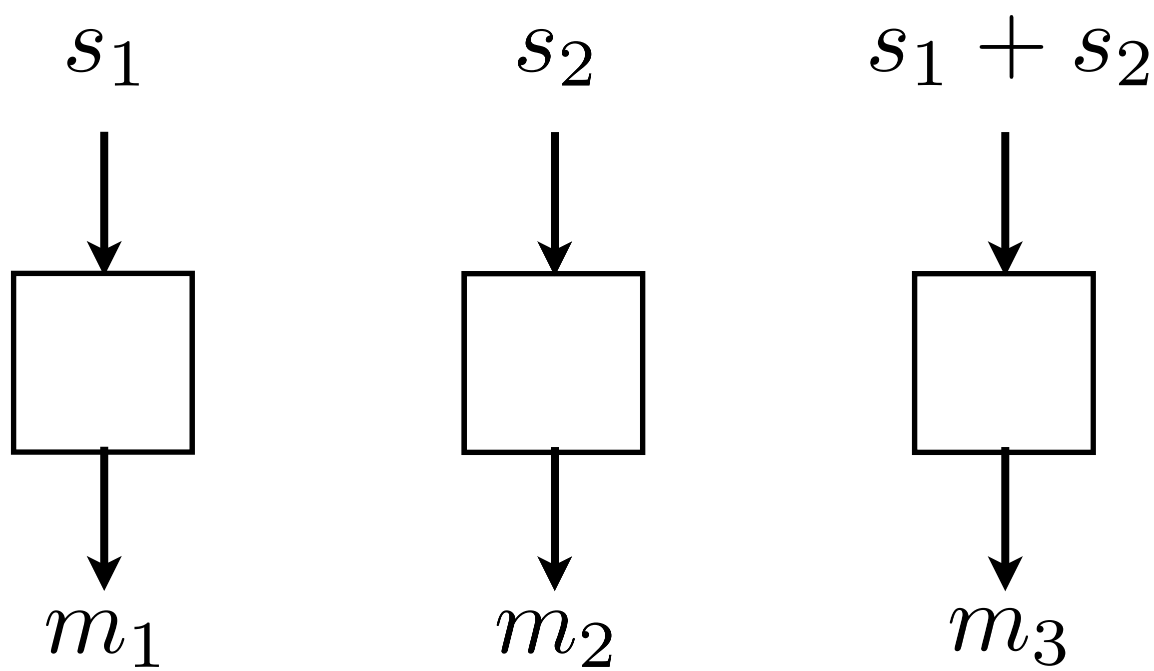
Correlations in outcomes of local measurements

GHZ "Paradox": No **(non-contextual)** real number assignment of **X** and ***Y*** can satisfy all of these.

N. D. Mermin (1990), building on **Greenberger**, et al. (1989)

GHZ "paradox"

- A very **clean** way to express this correlation is to use the **binary notation** introduced above.



$$m_1 \oplus m_2 \oplus m_3 = s_1 s_2$$

- I.e. the correlations "win" an XOR-game, nearly **identical** to the **CHSH game**.

J. Anders and **D. E. Browne** PRL (2009).

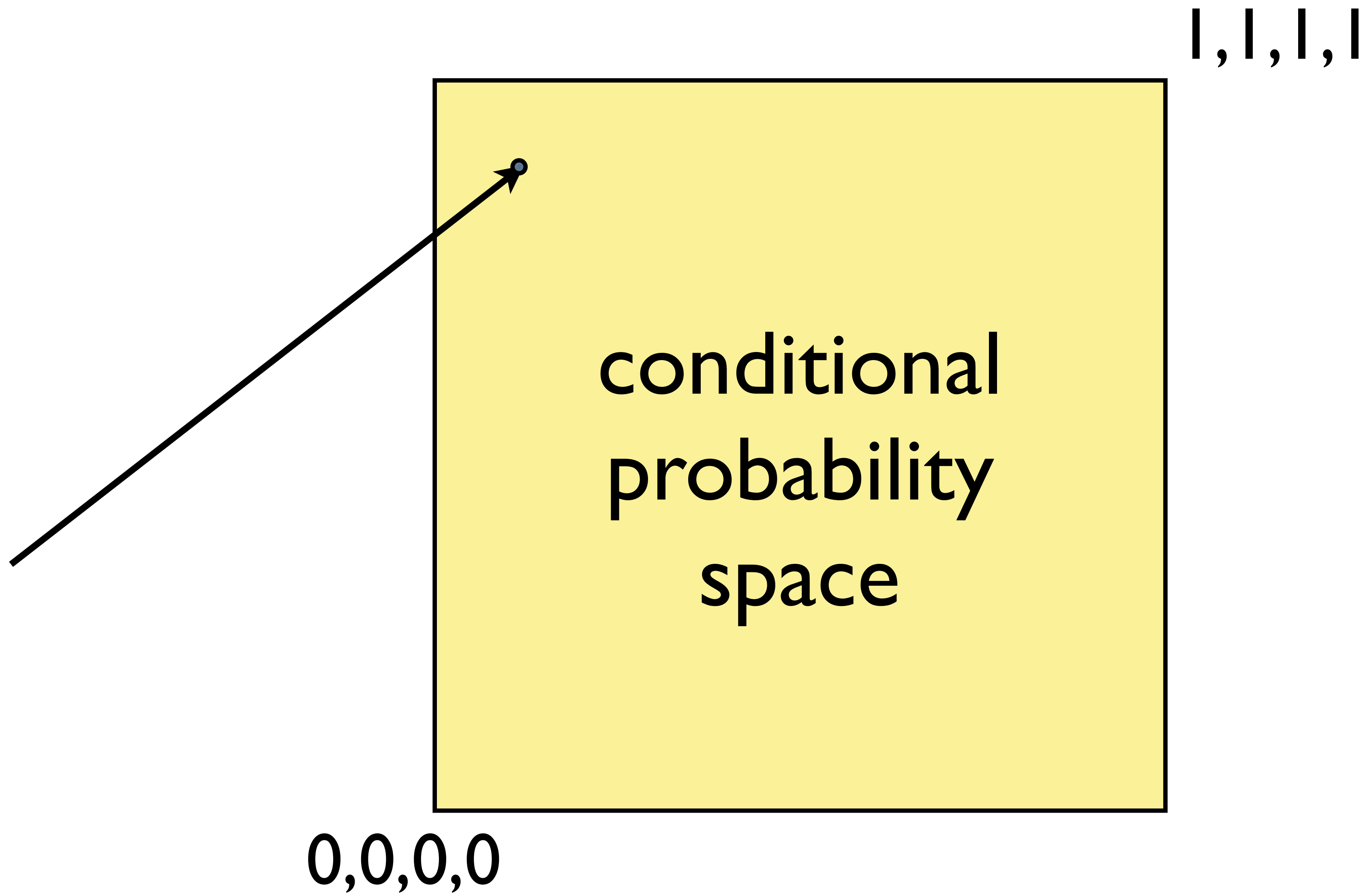
Geometric approach to Bell inequalities

Geometric interpretation of BIs

- Another useful representation of Bell inequalities is to form a **vector** from the **conditional probabilities**.

$$p(s_1, s_2) \equiv p(m_1 \oplus m_2 = 1|s_1, s_2)$$

$$\vec{p} = \begin{bmatrix} p(0,0) \\ p(0,1) \\ p(1,0) \\ p(1,1) \end{bmatrix}$$



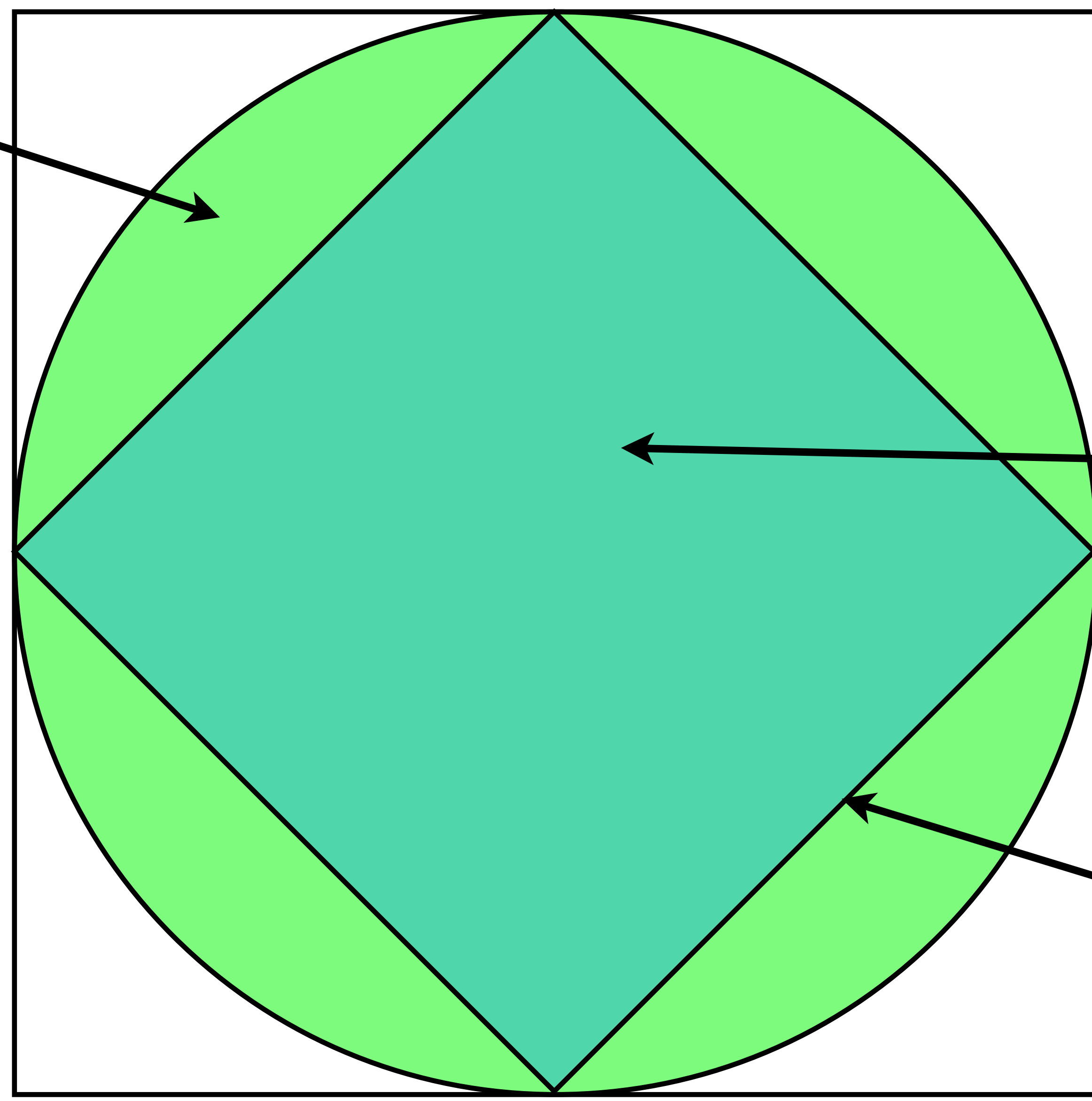
- Each possible set of conditional probabilities is represented a **point** in a **unit hypercube**.

Geometric interpretation of BIs

We can thus classify the regions of conditional probability space (2-D Schematic).

PR Box

Quantum region



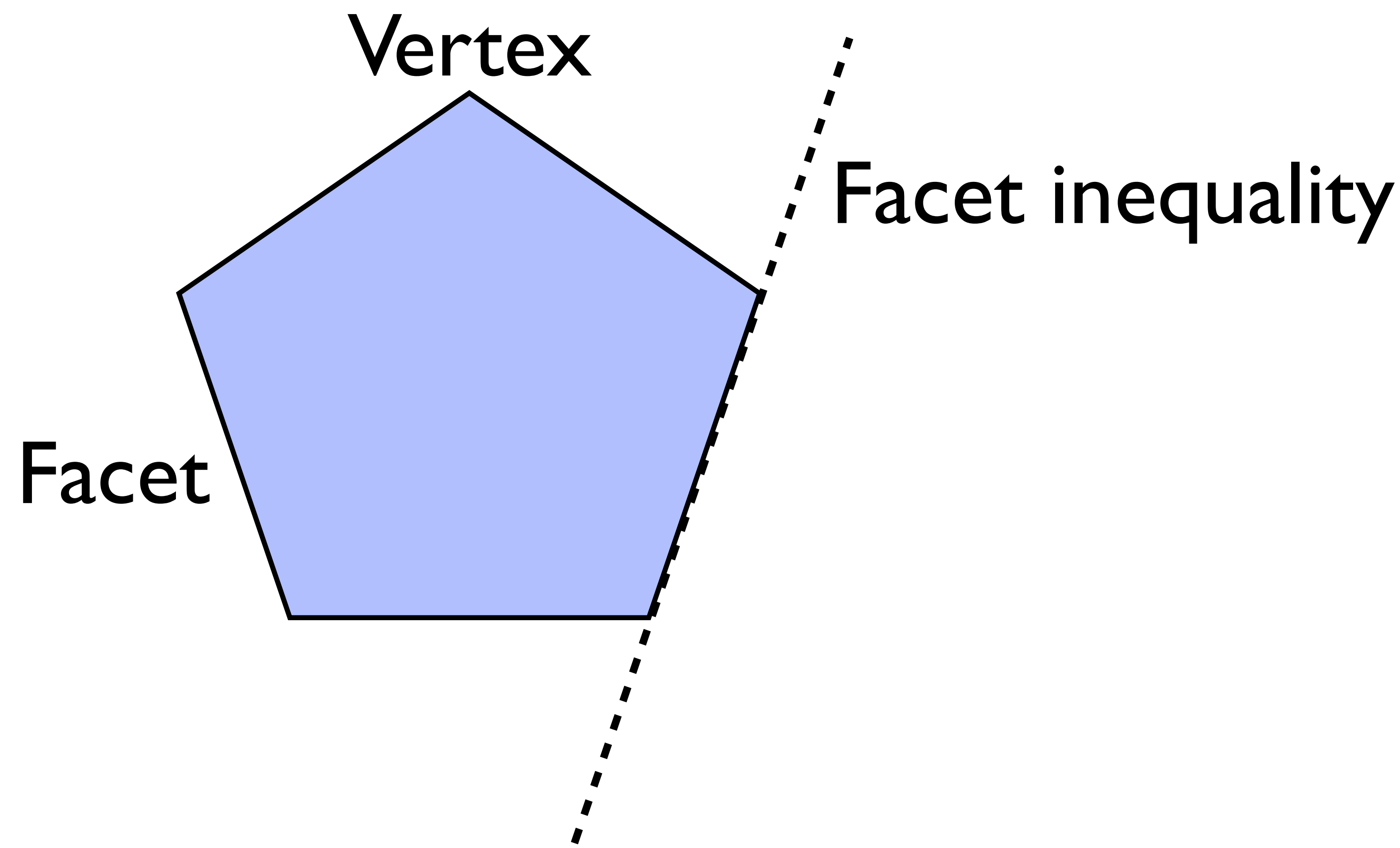
LHV region: "Bell polytope"

Bell inequalities define **facets** of polytope.

Marcel Froissart: Nouvo Cimento (1981), **B.S. Tsirelson**, J. Sov. Math. (1987)

Convex polytopes

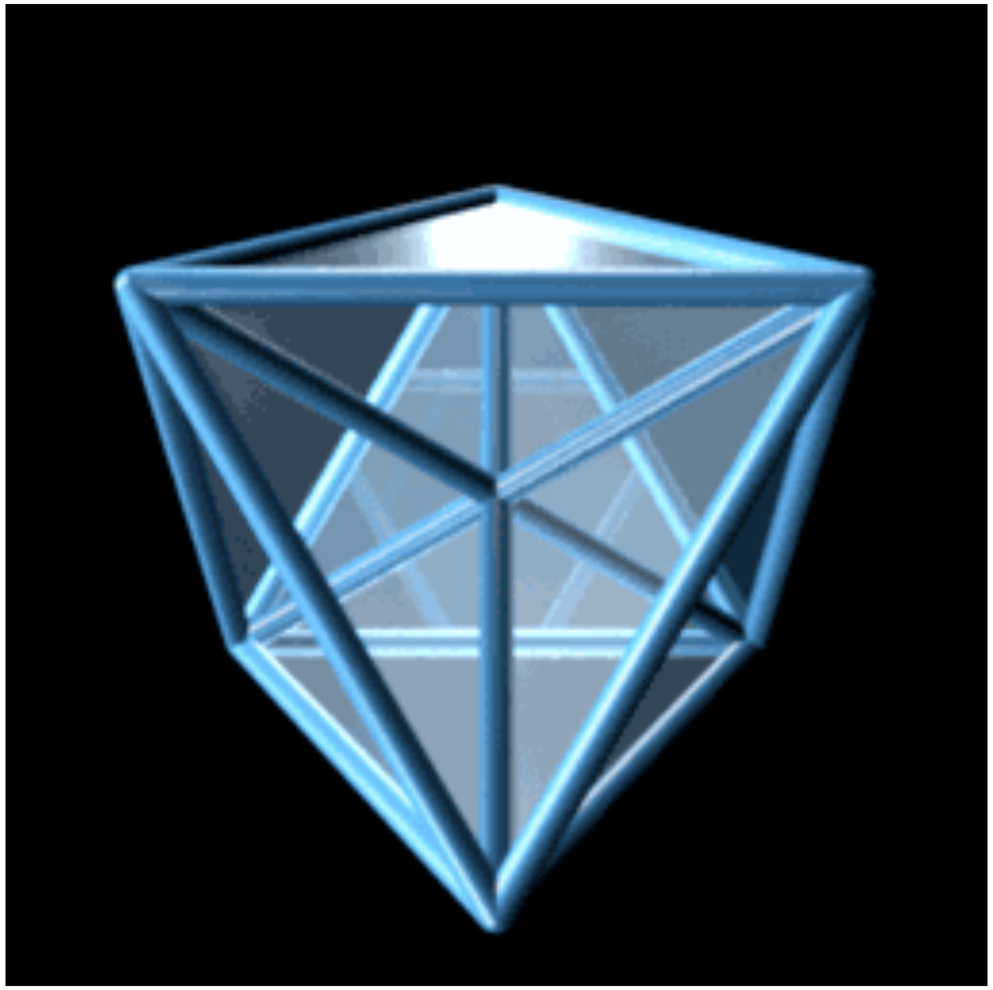
- The **convex hull** of a set of vectors (vertices) in **R^d**.

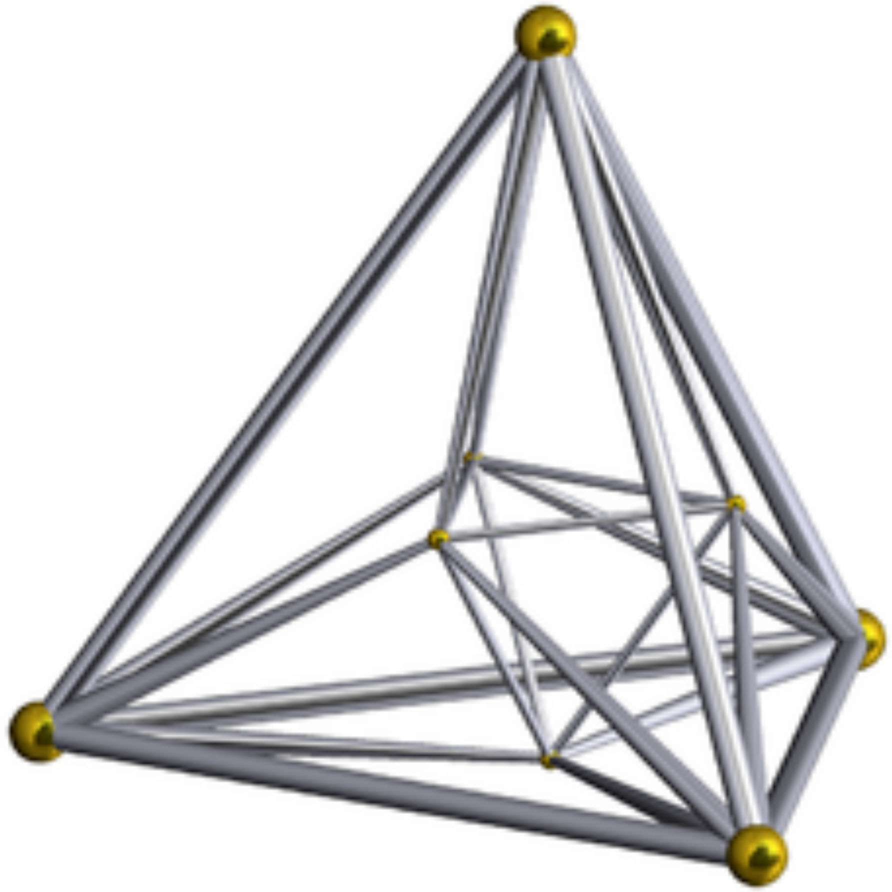


- Generalisation of polygons, polyhedra to higher d.
- May be defined in terms of its **vertices** or its **facets** (as a set of inequalities defining half planes.)

Geometric interpretation of BIs

- The "Bell polytope" represents the region of conditional probabilities allowed in LHV theories.
- It is a **hyper-octahedron.** The facets represent the CHSH inequalities (and normalisation conditions).





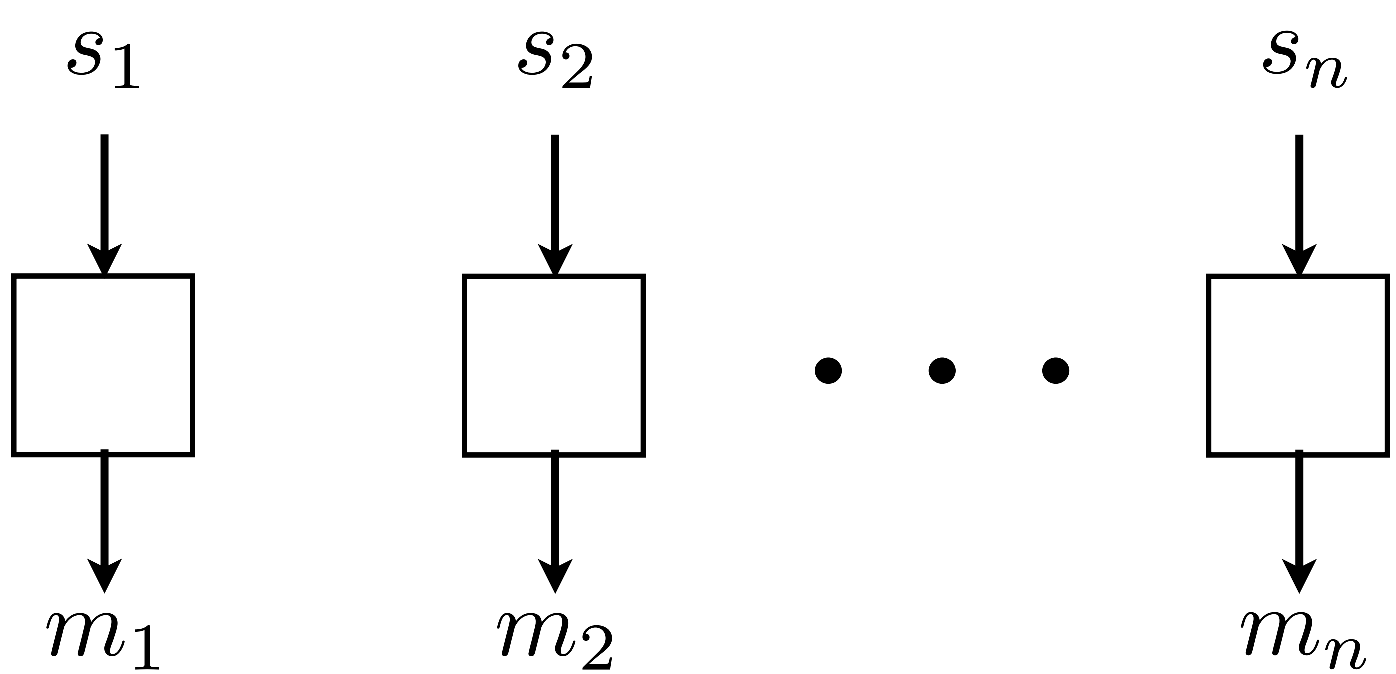
Marcel Froissart: Nouvo Cimento (1981).

Many-party Bell inequalities

Many-party Bell-inequalities

- Werner and Wolf (2001) **generalised** the CHSH setting to **n-parties**.
  - We still keep 2-settings, 2-outputs per meas and consider conditional probs for the XOR of all outputs.

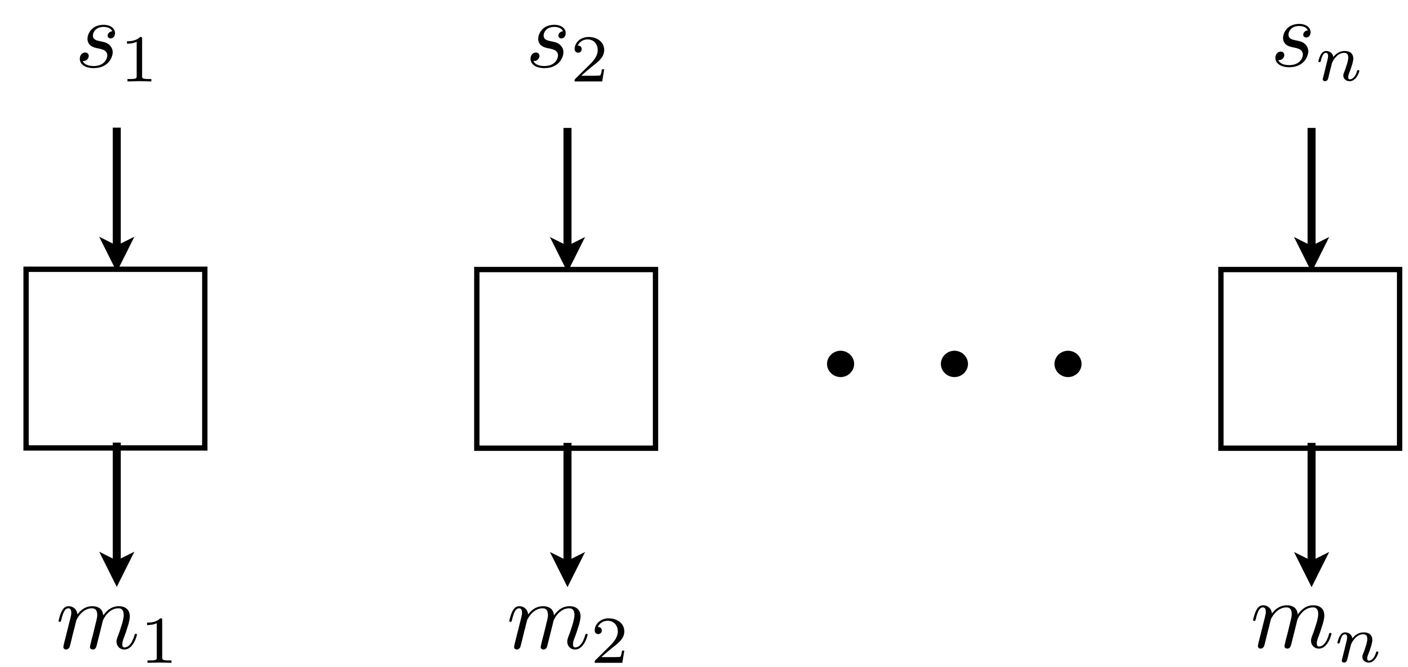
$$M = \sum_j m_j$$



Many-party Bell-inequalities

- Werner and Wolf (2001) **generalised** the CHSH setting to **n-parties**.
  - We still keep 2-settings, 2-outputs per meas and consider conditional probs for the XOR of all outputs.

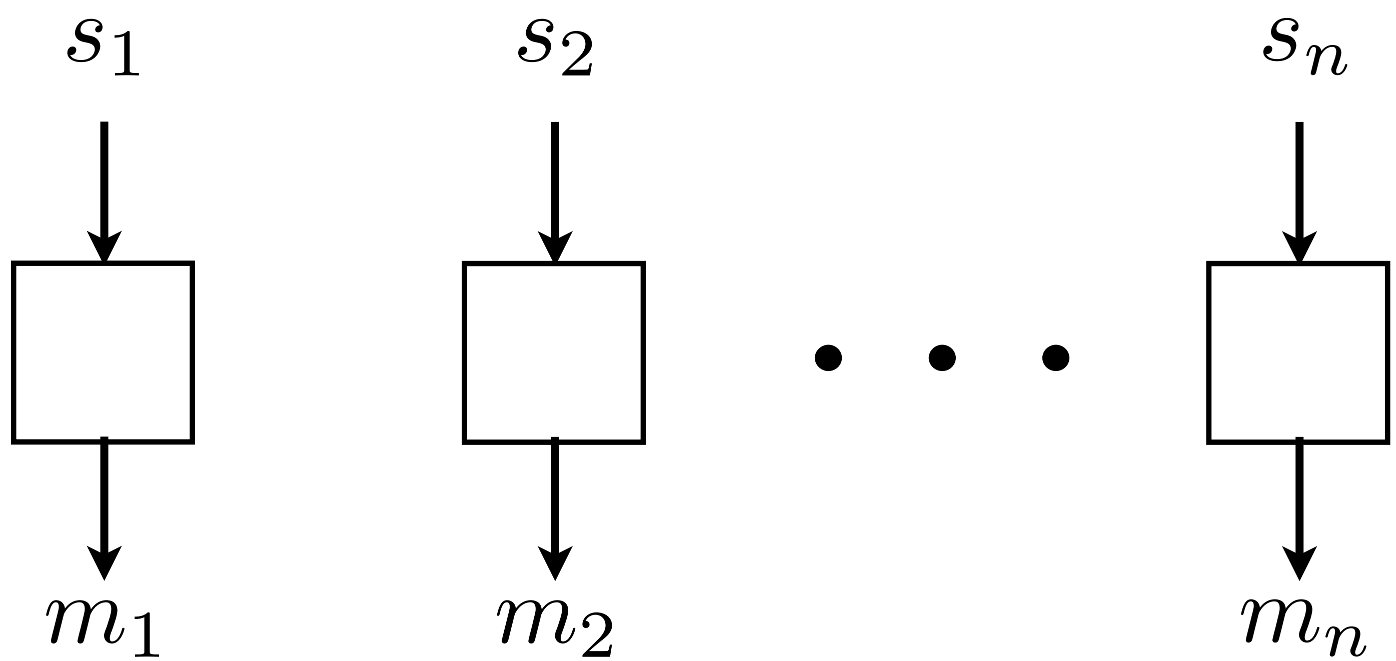
$$M = \sum_j m_j$$



Many-party Bell-inequalities

- Werner and Wolf (2001) **generalised** the CHSH setting to **n-parties**.
  - We still keep 2-settings, 2-outputs per meas and consider conditional probs for the XOR of all outputs.

$$M = \sum_j m_j$$



  - W & W derived the full **n-party Bell polytope** - and found that, for **any n**, it is a **hyper-octahedron** in **2^n** dimensions.

Loopholes in Bell inequality Experiments

Loopholes in Bell Inequality experiments

Loopholes in Bell Inequality experiments

- The beauty of Bell inequalities is that they are **experimentally testable.**

Loopholes in Bell Inequality experiments

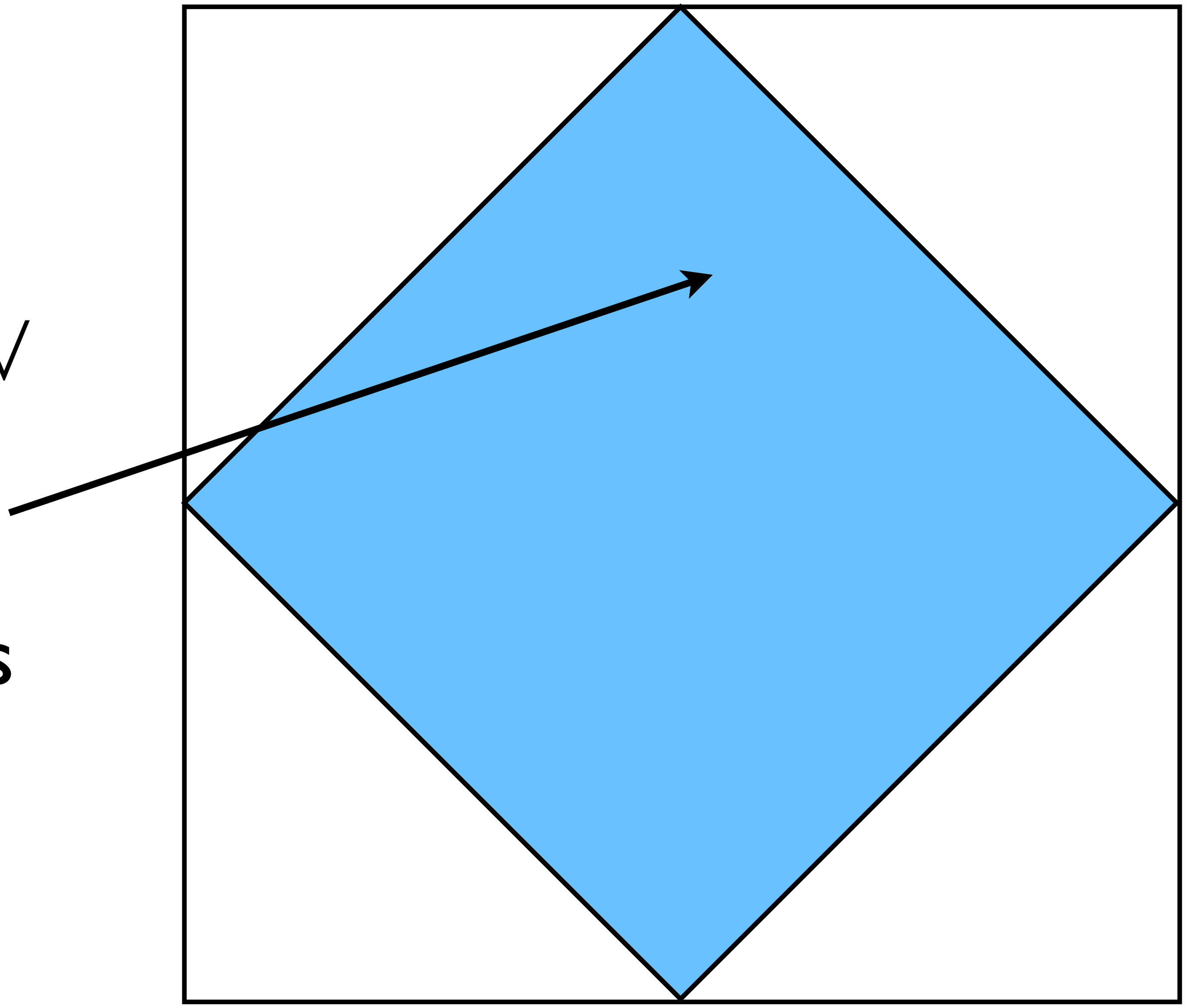
- The beauty of Bell inequalities is that they are **experimentally testable.**
- However, Bell's assumptions are **strict**.
    - **Space-like separated** measurements
    - **Perfect detection efficiency**
    - Measurement settings chosen at **random** (free-will).

Loopholes in Bell Inequality experiments

- The beauty of Bell inequalities is that they are **experimentally testable.**
- However, Bell's assumptions are **strict**.
  - **Space-like separated** measurements
  - **Perfect detection efficiency**
  - Measurement settings chosen at **random** (free-will).
- If these do not hold, then the BIs may not hold - there may be **loopholes**.

Loopholes in Bell Inequality experiments

Loopholes make the LHV region **larger**.

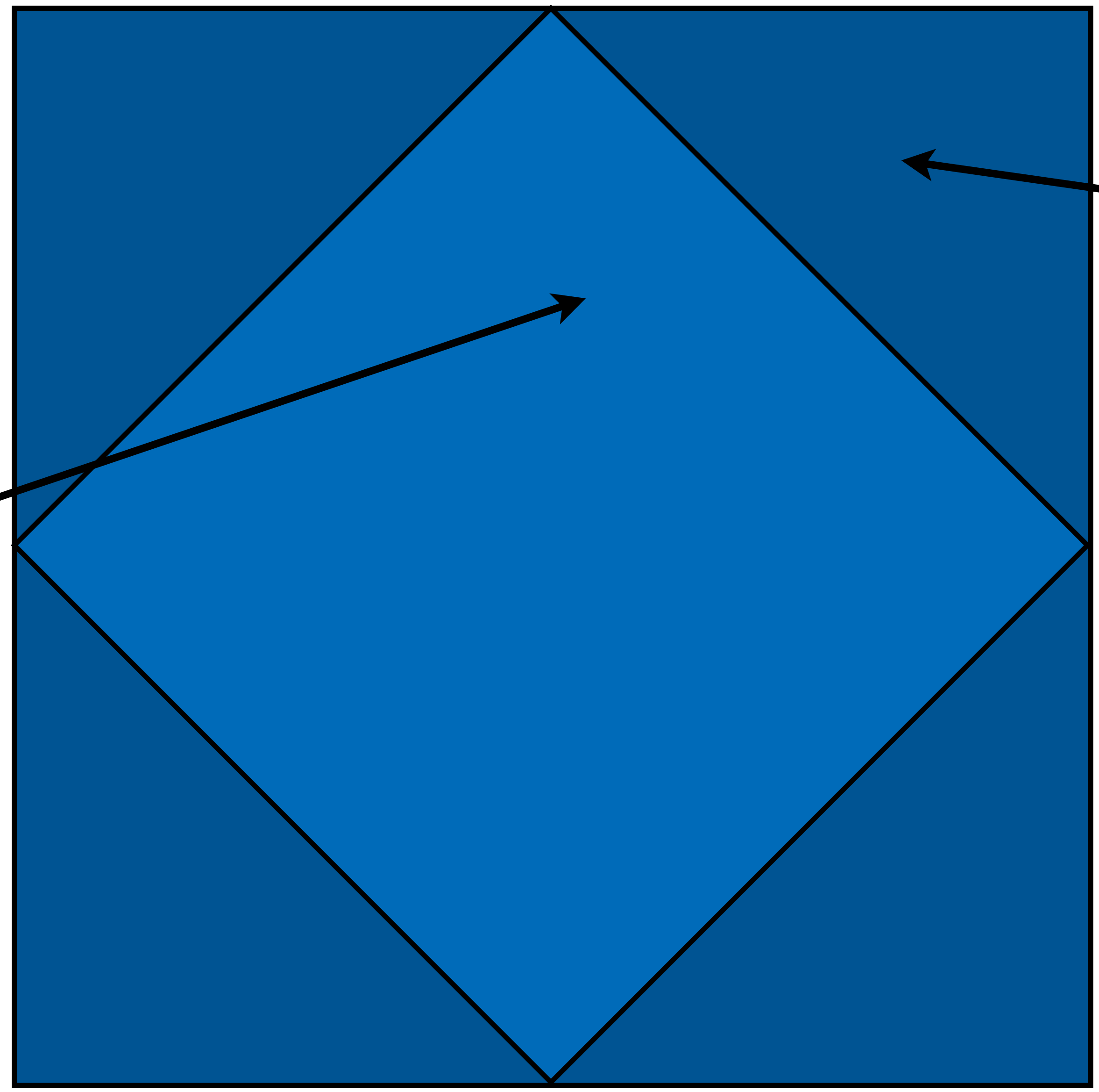


Allowed LHV correlations under **Bell's assumptions**

Loopholes in Bell Inequality experiments

Loopholes make the LHV region **larger**.

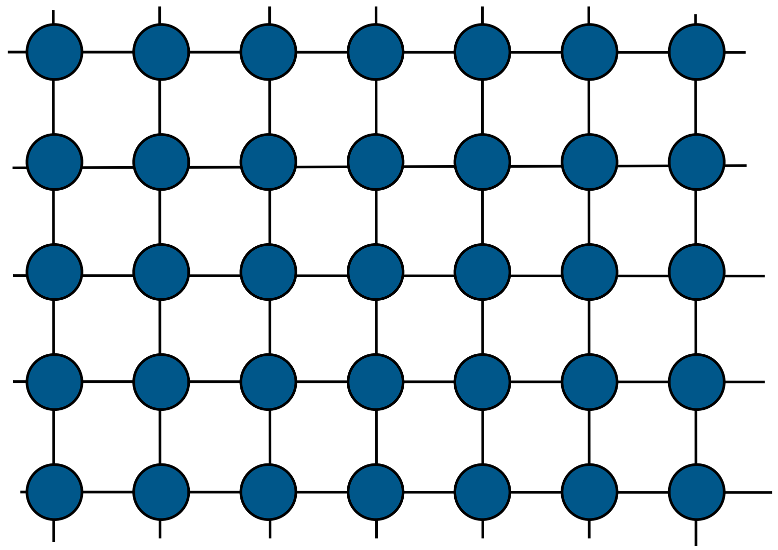
Allowed LHV correlations under **Bell's assumptions**



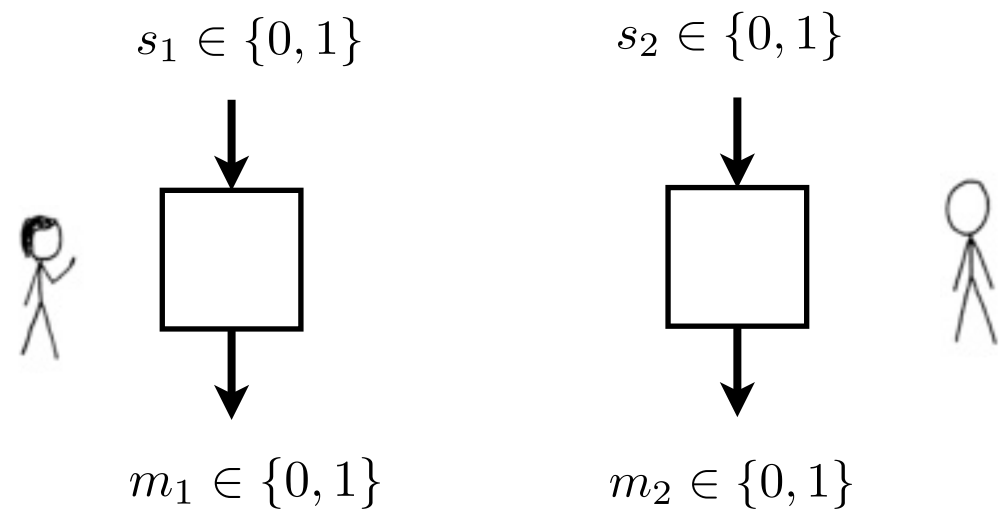
Allowed LHV correlations under **actual experimental conditions**

Bell inequalities
vs
Measurement-Based Quantum Computation

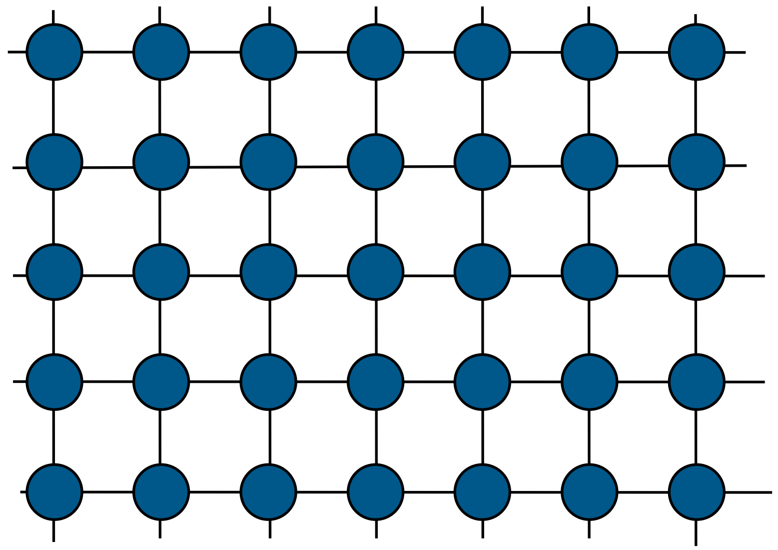
MBQC vs BIs



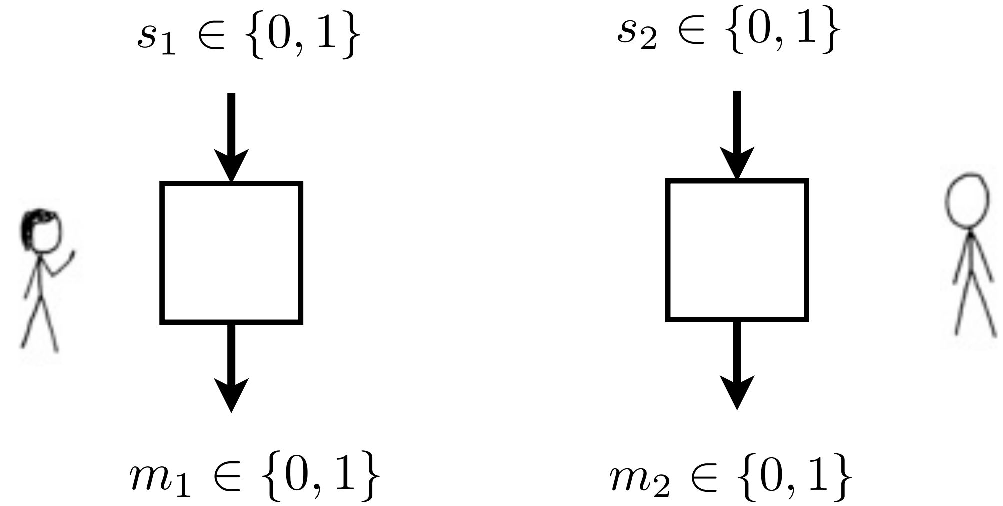
vs



MBQC vs BIs

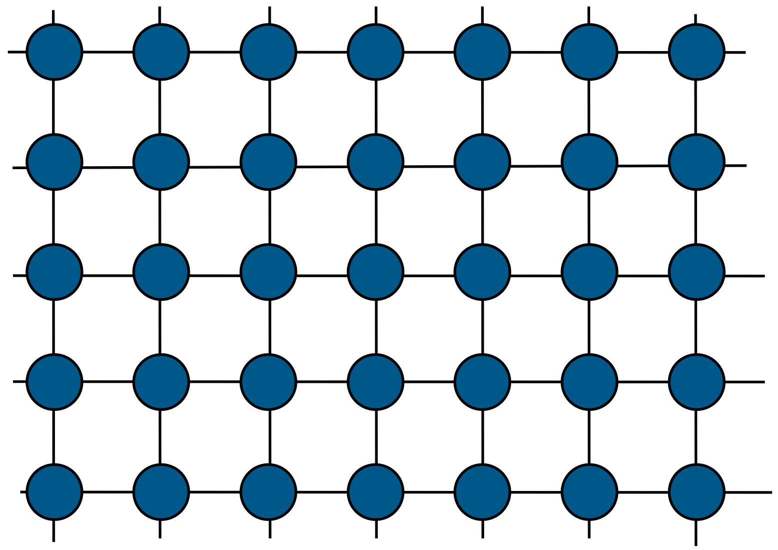


vs

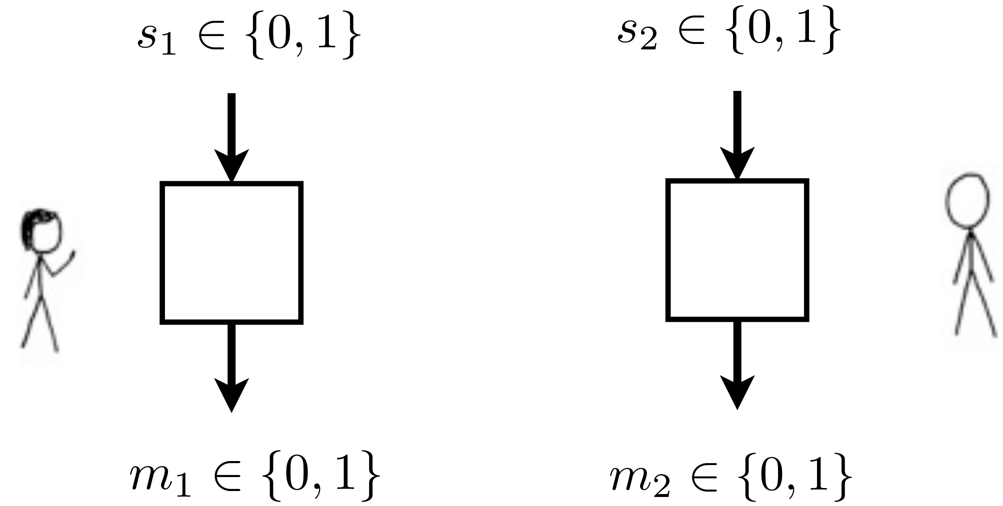


- Both
  - Require (only) **XOR** side-processing to perform computational **game** or **task**.
  - **This task** is **impossible** (non-linear) with **XOR gates** alone (linear gates).

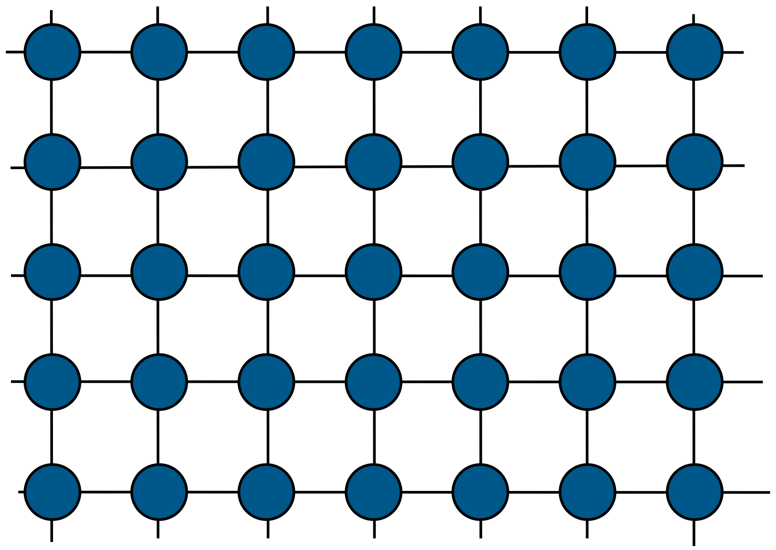
MBQC vs BIs



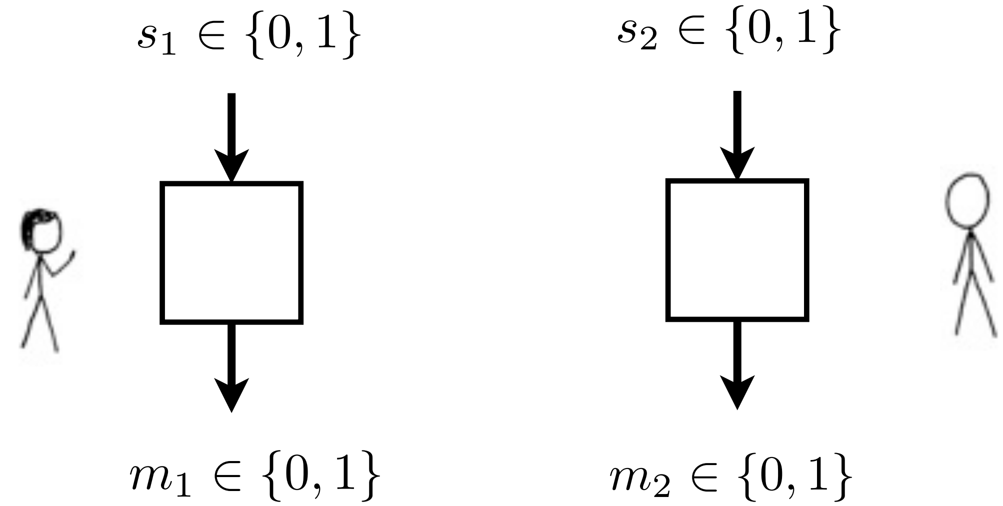
vs



MBQC vs BIs

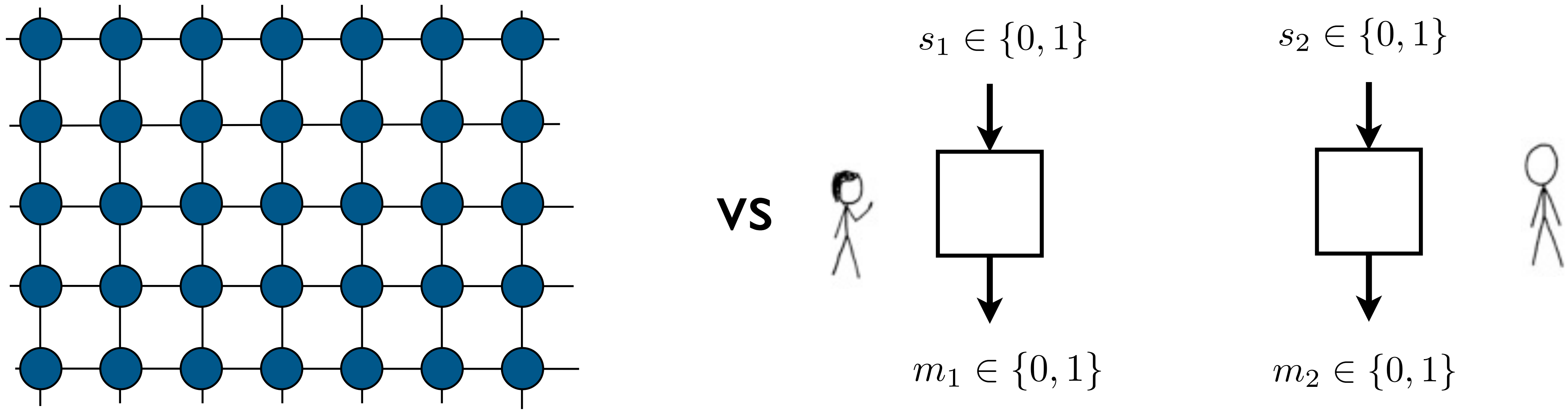


vs



- But
  - MBQC requires **adaptive measurements**, and thus measurements **cannot** be space-like separated.
  - **Spatial separation** is one of the **most important assumptions** in deriving the Bell inequalities.

This talk



- Main result:
  - We will derive an equivalent of the **Bell polytope** for **MBQC**.
    - I.e. Within **LHV theories**, which measurement-based computations can be achieved?
- Main tool:
  - **Polytopes** over **Boolean functions.**

Boolean Functions

Boolean functions

- A **Boolean function** is a map from **n**-bits to a **single** bit.
- Every such function can be represented by a $\mathbf{2^n}$ bit **vector** listing the outputs for each of the $\mathbf{2^n}$ inputs.
- E.g.

$$\vec{f} = \begin{bmatrix} f(0\ldots 00) \\ f(0\ldots 01) \\ f(0\ldots 10) \\ \vdots \\ f(1\ldots 11) \end{bmatrix}$$

- It is convenient to enumerate the Boolean functions as where **j = 1, ..., 2^(2^n)**.

Boolean functions

- A **Boolean function** is a map from **n**-bits to a **single** bit.
- Every such function can be represented by a $\mathbf{2^n}$ bit **vector** listing the outputs for each of the $\mathbf{2^n}$ inputs.
- E.g.

$$\vec{f} = \begin{bmatrix} f(0\ldots00) \\ f(0\ldots01) \\ f(0\ldots10) \\ \vdots \\ f(1\ldots11) \end{bmatrix}$$

- I.e. There **2^(2^n)** Boolean functions.

- It is convenient to enumerate the Boolean functions as where **j = 1, ..., 2^(2^n)**.

Boolean functions

- A **Boolean function** is a map from **n**-bits to a **single** bit.
- Every such function can be represented by a $\mathbf{2^n}$ bit **vector** listing the outputs for each of the $\mathbf{2^n}$ inputs.
- E.g.

$$\vec{f} = \begin{bmatrix} f(0\ldots00) \\ f(0\ldots01) \\ f(0\ldots10) \\ \vdots \\ f(1\ldots11) \end{bmatrix}$$

- I.e. There **2^(2^n)** Boolean functions.

- It is convenient to enumerate the Boolean functions as $f_j(\vec{s})$ where **j = 1, ..., 2^(2^n)**.

Boolean functions

- Every Boolean function may be expressed as a **polynomial** (modulo 2) (known as "algebraic normal form").
- E.g. if input is the bitstring $\vec{s} = s_1 s_2 \ldots s_n$

$$f(s) = a_0 + a_1 s_1 + a_2 s_2 + \cdots + a_{12} s_1 s_2 + \cdots$$

Boolean functions

- Every Boolean function may be expressed as a **polynomial** (modulo 2) (known as "algebraic normal form").
- E.g. if input is the bitstring $\vec{s} = s_1 s_2 \ldots s_n$

$$f(s) = a_0 + a_1 s_1 + a_2 s_2 + \cdots + a_{12} s_1 s_2 + \cdots$$

Boolean functions

- Every Boolean function may be expressed as a **polynomial** (modulo 2) (known as "algebraic normal form").
- E.g. if input is the bitstring $\vec{s} = s_1 s_2 \dots s_n$

$$f(s) = a_0 + a_1 s_1 + a_2 s_2 + \cdots + a_{12} s_1 s_2 + \cdots$$

- In other words, any Boolean function can be expressed as a sequence of **XOR** (add mod 2) and **AND** (multiply) gates.

Boolean functions

- Every Boolean function may be expressed as a **polynomial** (modulo 2) (known as "algebraic normal form").
- E.g. if input is the bitstring $\vec{s} = s_1 s_2 \ldots s_n$

$$f(s) = a_0 + a_1 s_1 + a_2 s_2 + \cdots + a_{12} s_1 s_2 + \cdots$$

- In other words, any Boolean function can be expressed as a sequence of **XOR** (add mod 2) and **AND** (multiply) gates.
- The **degree** of the polynomial is a useful way of classifying Boolean functions.

Linear Boolean functions

- **Linear** Boolean functions are **degree 1** polynomials, and can be most generally written

$$l(s) = a_0 + \sum_{j=1}^{n} a_j s_j \qquad\qquad a_k \in \{0, 1\}$$

Linear Boolean functions

- **Linear** Boolean functions are **degree 1** polynomials, and can be most generally written

$$l(s) = a_0 + \sum_{j=1}^{n} a_j s_j \qquad a_k \in \{0, 1\}$$

Linear Boolean functions

- **Linear** Boolean functions are **degree 1** polynomials, and can be most generally written

$$l(s) = a_0 + \sum_{j=1}^{n} a_j s_j \qquad\qquad a_k \in \{0,1\}$$

- There are thus **2^(n+1)** such functions, which we shall enumerate $l_k(\vec{s})$ where k =1, ..., 2^(n+1).

Linear Boolean functions

- **Linear** Boolean functions are **degree 1** polynomials, and can be most generally written

$$l(s) = a_0 + \sum_{j=1}^{n} a_j s_j \qquad\qquad a_k \in \{0, 1\}$$

- There are thus **2^(n+1)** such functions, which we shall enumerate $l_k(\vec{s})$ where k =1, ..., 2^(n+1).

- All linear functions may be generated via **XOR gates** alone.

Linear Boolean functions

- **Linear** Boolean functions are **degree 1** polynomials, and can be most generally written

$$l(s) = a_0 + \sum_{j=1}^{n} a_j s_j \qquad\qquad a_k \in \{0, 1\}$$

- There are thus **2^(n+1)** such functions, which we shall enumerate $l_k(\vec{s})$ where k =1, ..., 2^(n+1).
- All linear functions may be generated via **XOR gates** alone.
- Linear functions are **closed** under composition.

Linear Boolean functions

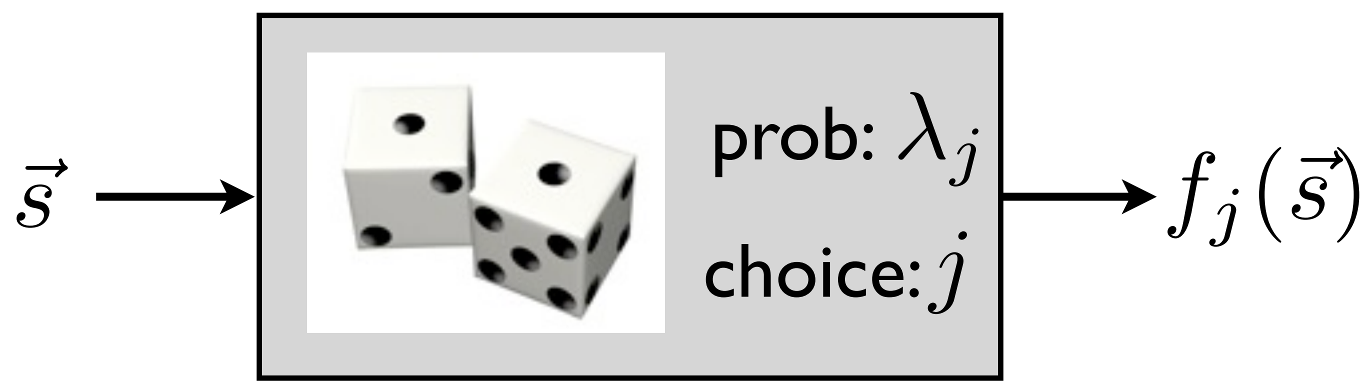
- **Linear** Boolean functions are **degree 1** polynomials, and can be most generally written

$$l(s) = a_0 + \sum_{j=1}^{n} a_j s_j \qquad\qquad a_k \in \{0, 1\}$$

- There are thus **2^(n+1)** such functions, which we shall enumerate $l_k(\vec{s})$ where k =1, ..., 2^(n+1).
- All linear functions may be generated via **XOR gates** alone.
- Linear functions are **closed** under composition.
- In contrast, by composing a quadratic gate (e.g. **NAND**) one can generate **all Booleans**.

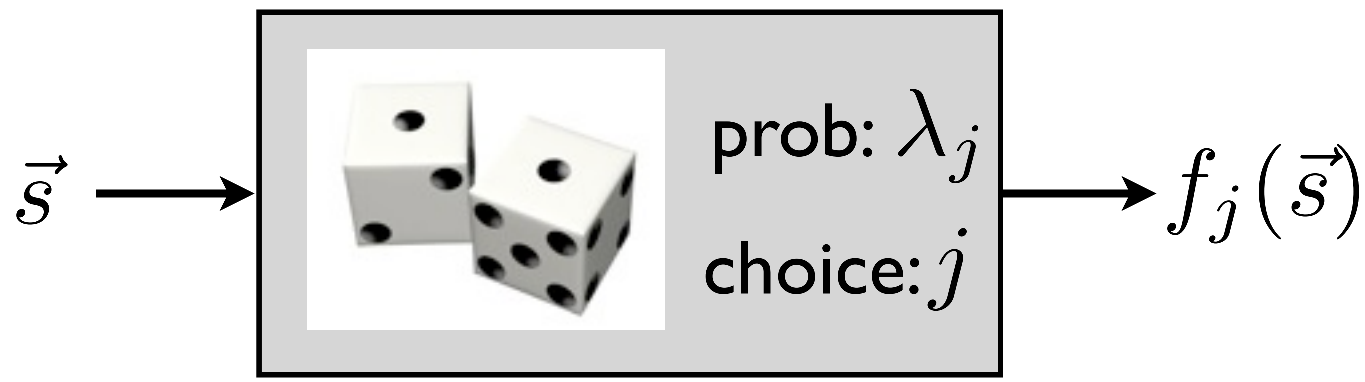
Stochastic Boolean maps

- Consider a **stochastic machine** which, given input string **s**, outputs $f_j(\vec{s})$ with probability λ_j.



Stochastic Boolean maps

- Consider a **stochastic machine** which, given input string **s**, outputs $f_j(\vec{s})$ with probability λ_j.



- The **probability** that the output bit of the machine is **1**, conditional upon the input **s**, is given by:

$$p(1|\vec{s}) = \sum_j \lambda_j p(f_j(\vec{s}) = 1) \qquad \sum_j \lambda_j = 1$$

Stochastic Boolean maps

Stochastic Boolean maps

- We can simplify this expression, due to a **very convenient identity**:

$$p(f_j(\vec{s}) = 1) = f_j(\vec{s})$$

Stochastic Boolean maps

- We can simplify this expression, due to a **very convenient identity**:

$$p(f_j(\vec{s}) = 1) = f_j(\vec{s})$$

- and thus obtain $$p(1|\vec{s}) = \sum_j \lambda_j f_j(\vec{s})$$

Stochastic Boolean maps

- We can simplify this expression, due to a **very convenient identity**:

$$p(f_j(\vec{s}) = 1) = f_j(\vec{s})$$

- and thus obtain $$p(1|\vec{s}) = \sum_j \lambda_j f_j(\vec{s})$$

- or equivalently $$\vec{p} = \sum_j \lambda_j \vec{f_j}$$

Stochastic Boolean maps

- We can simplify this expression, due to a **very convenient identity**:

$$p(f_j(\vec{s}) = 1) = f_j(\vec{s})$$

- and thus obtain $$p(1|\vec{s}) = \sum_j \lambda_j f_j(\vec{s})$$

- or equivalently $$\vec{p} = \sum_j \lambda_j \vec{f}_j$$

- This is a convex combination of real-space vectors and thus a **polytope**, we call it the Boolean **polytope**.

Stochastic Boolean maps

- We can simplify this expression, due to a **very convenient identity**:

$$p(f_j(\vec{s}) = 1) = f_j(\vec{s})$$

- and thus obtain $$p(1|\vec{s}) = \sum_j \lambda_j f_j(\vec{s})$$

- or equivalently $$\vec{p} = \sum_j \lambda_j \vec{f}_j$$

- This is a convex combination of real-space vectors and thus a **polytope**, we call it the Boolean **polytope**.

- Geometrically, it is a **unit 2^n** d. **hypercube**.

The Linear Polytope

$\vec{s} \longrightarrow$

prob: λ_j

choice: j

$\longrightarrow l_j(\vec{s})$

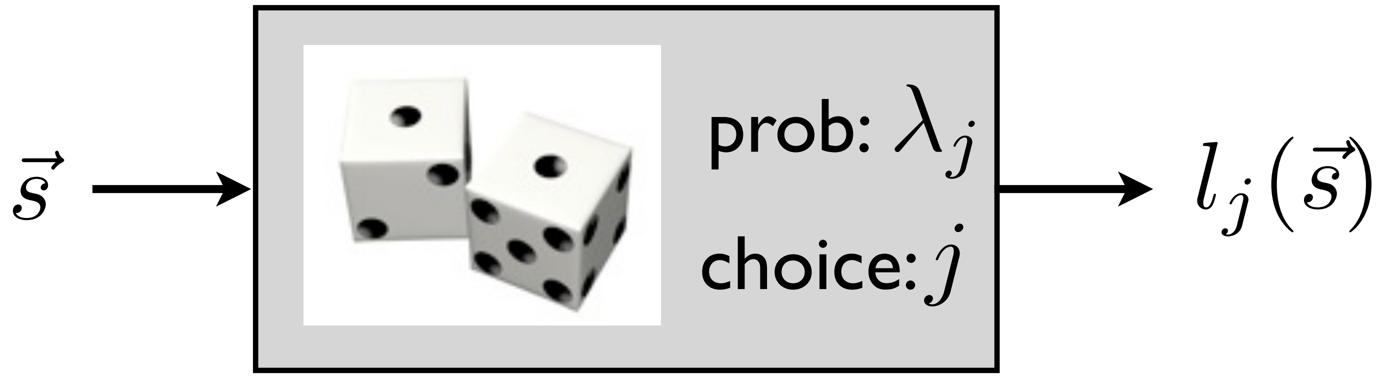
The Linear Polytope

- Consider now a stochastic machine which can **only** implement **linear functions**:

$\vec{s} \longrightarrow$  prob: λ_j choice: j $\longrightarrow l_j(\vec{s})$

The Linear Polytope

- Consider now a stochastic machine which can **only** implement **linear functions**:

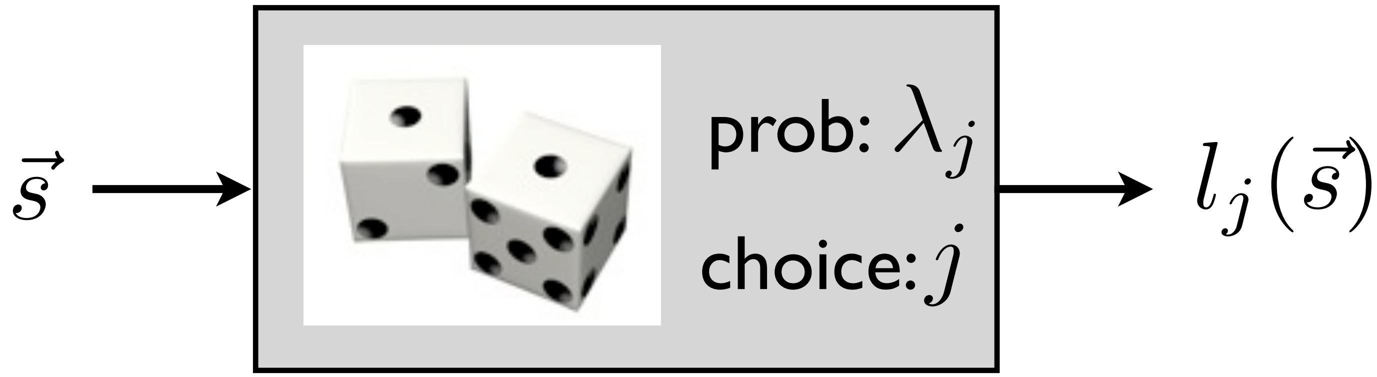


- The output probability of a linear stochastic machine lies in the **2^(n+1)** vertex **polytope**:

$$\vec{p} = \sum_{j=1}^{2^{n+1}} \lambda_j \vec{l_j}$$

The Linear Polytope

- Consider now a stochastic machine which can **only** implement **linear functions**:



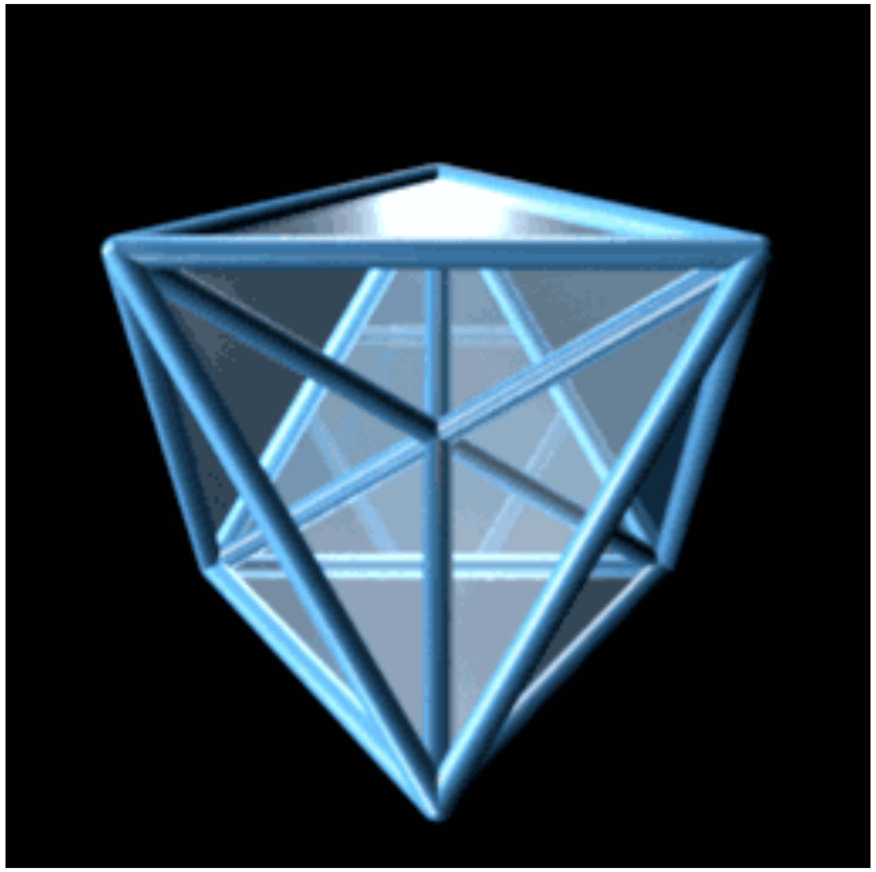
- The output probability of a linear stochastic machine lies in the **2^(n+1)** vertex **polytope**:

$$\vec{p} = \sum_{j=1}^{2^{n+1}} \lambda_j \vec{l_j}$$

- We shall call this the (n-bit) **linear polytope**.

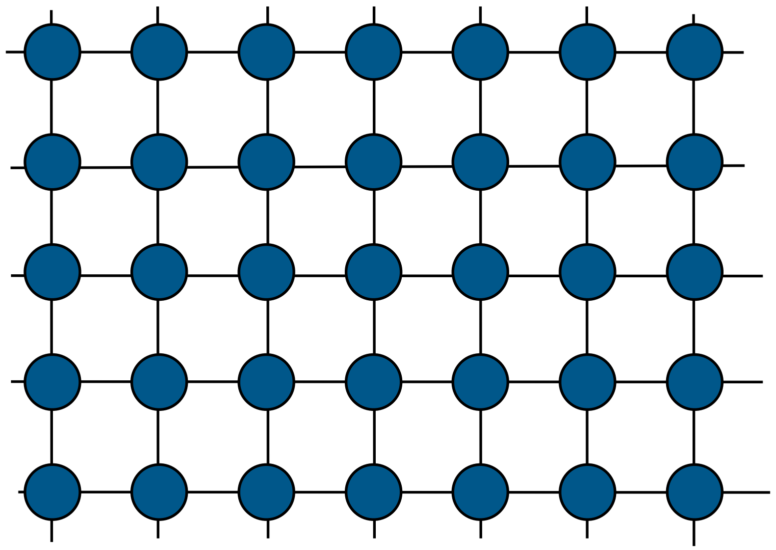
The linear polytope

- We can **classify** the **linear polytope** using standard techniques.
- It has **2^(n+1)** vertices in a **2^n** dimensional space.
- Can show that it is a **hyper-octahedron**.

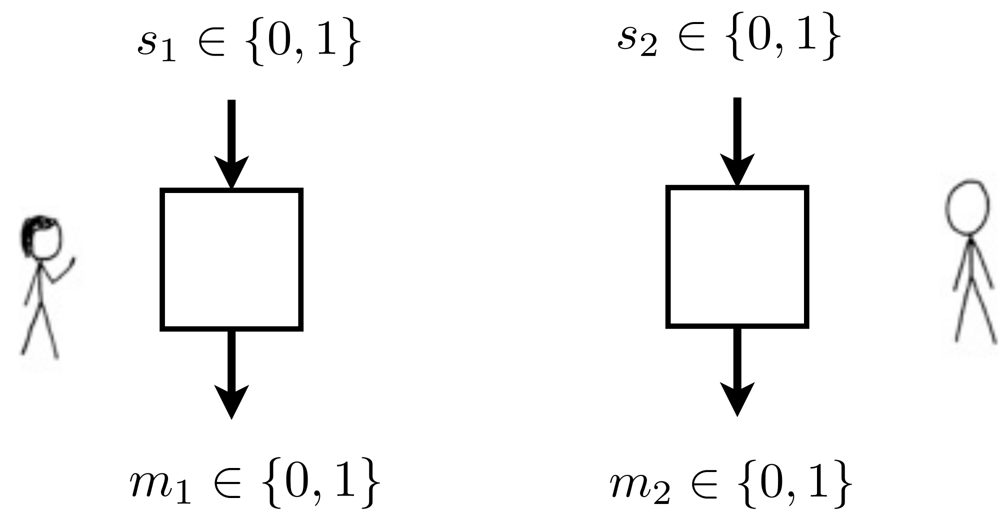


Bell inequalities for MBQC

Bell inequalities for MBQC

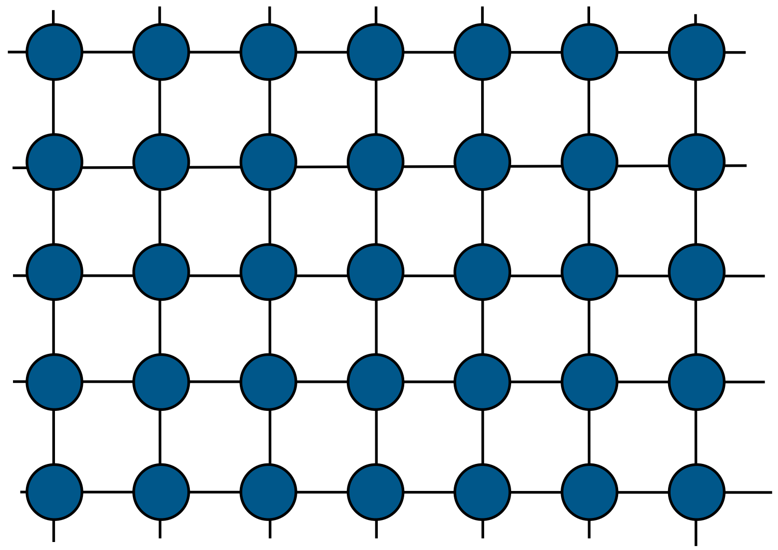


vs

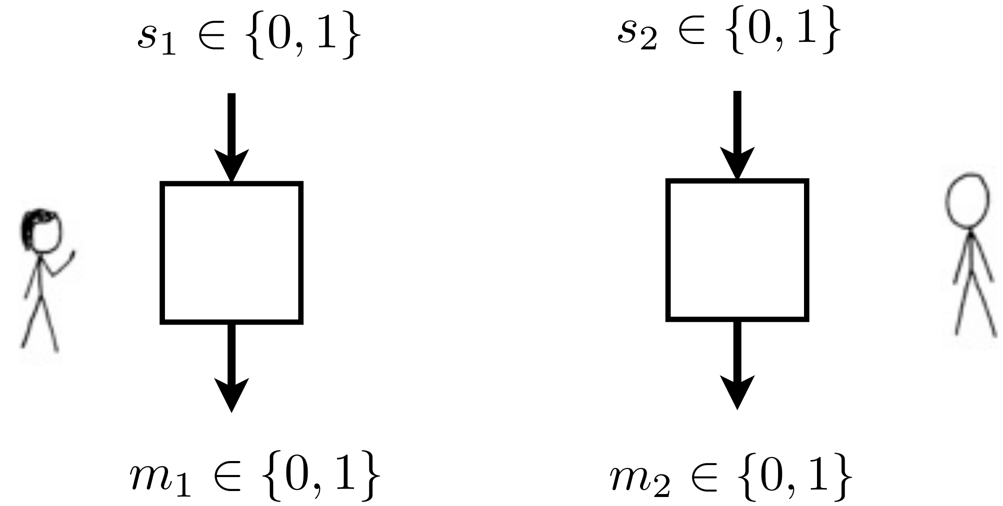


- Let us ask a "**Bell inequality**" type question for **MBQC**:
    - Using the correlations from a **LHV** theory, within an MBQC setting **what computations** can we achieve?

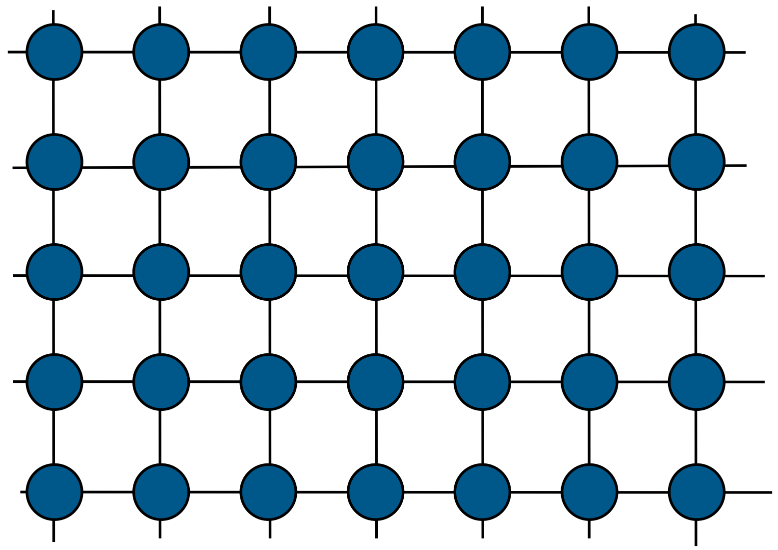
Bell inequalities for MBQC



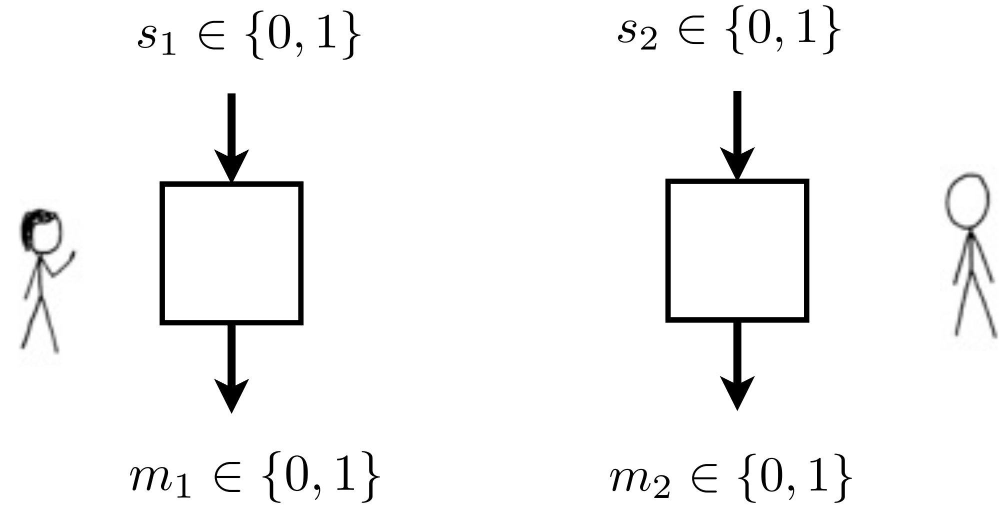
vs



Bell inequalities for MBQC

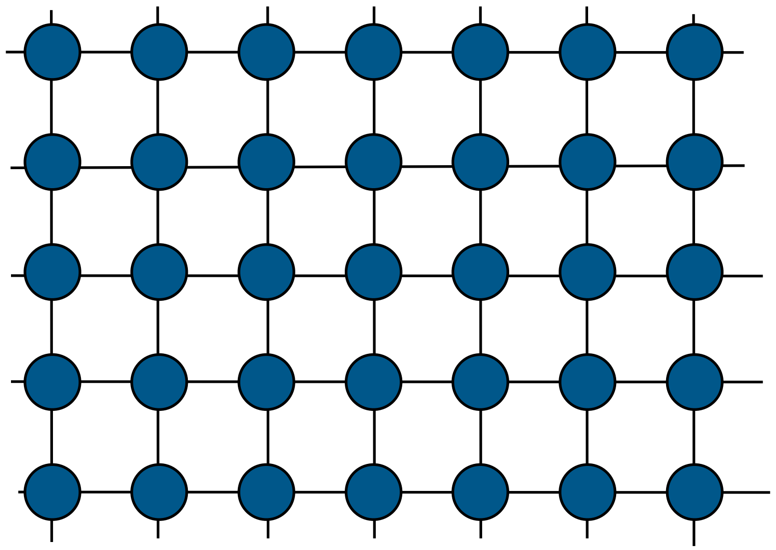


vs

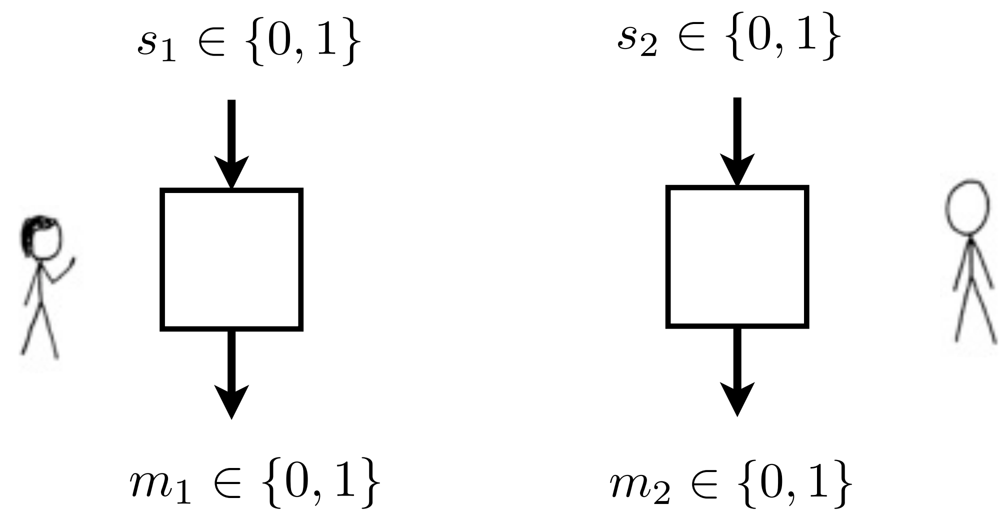


- If we allow **side computation** to be **universal**, we could access the **full Boolean polytope** with side computation alone.

Bell inequalities for MBQC

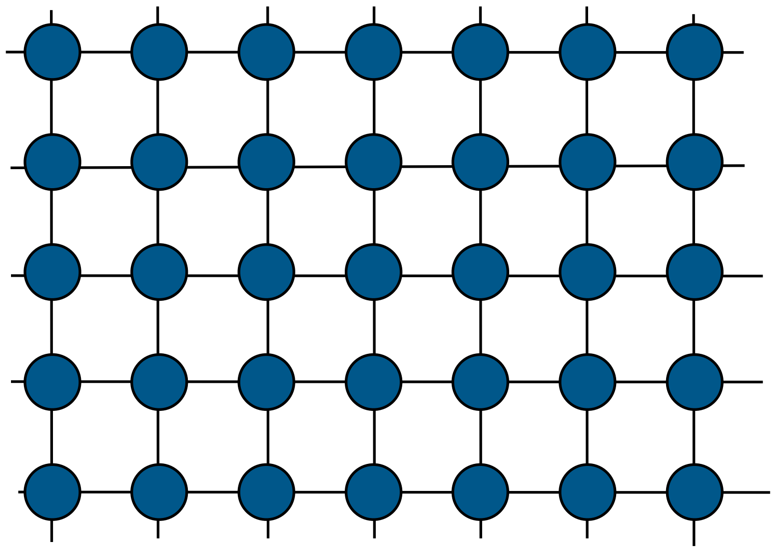


vs

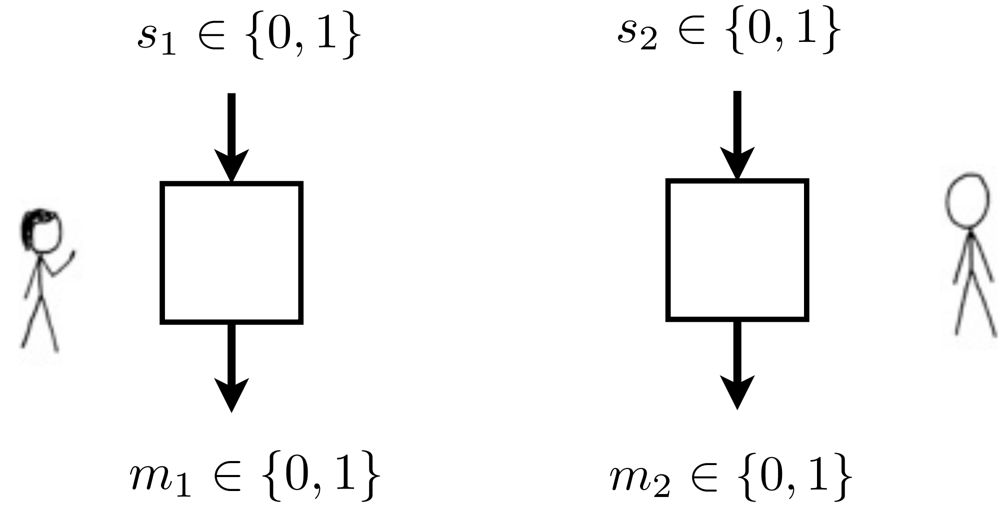


- If we allow **side computation** to be **universal**, we could access the **full Boolean polytope** with side computation alone.
  - For our question to make sense we make the following **key assumption**:

Bell inequalities for MBQC



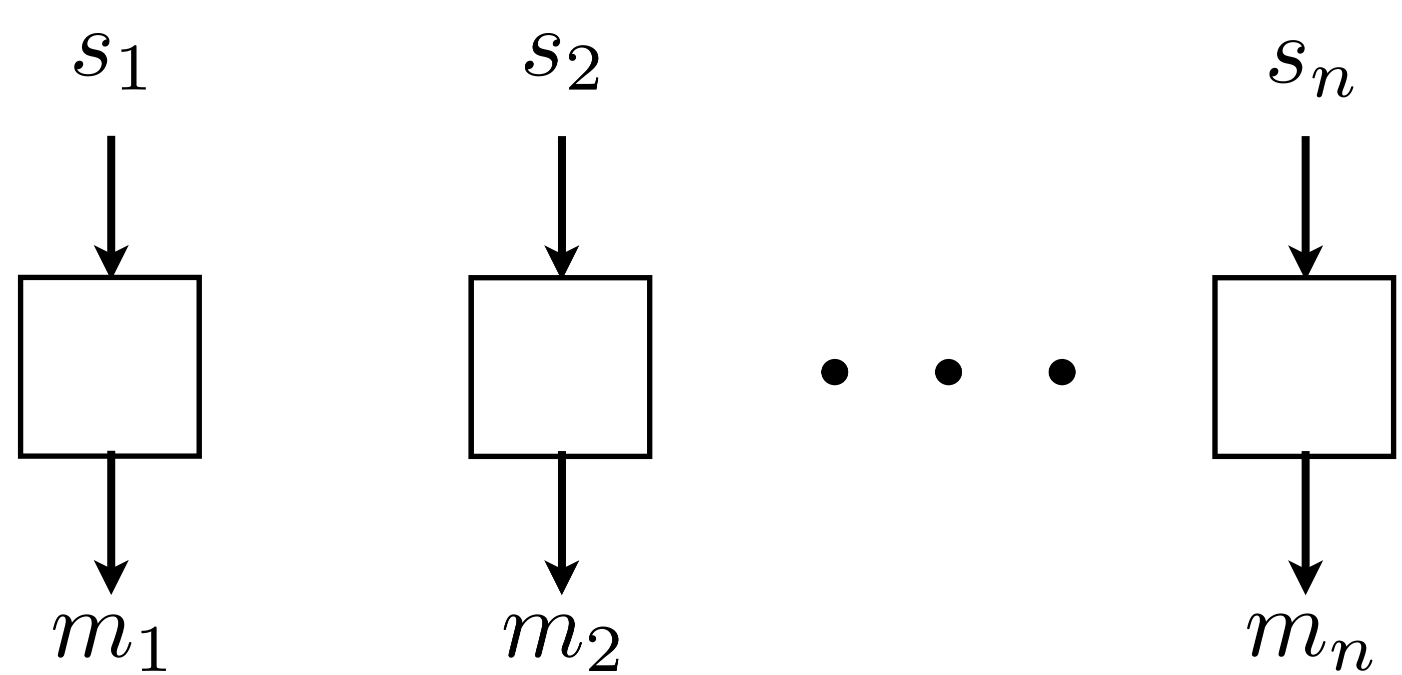
vs



- If we allow **side computation** to be **universal**, we could access the **full Boolean polytope** with side computation alone.
  - For our question to make sense we make the following **key assumption**:
  - Side-computation will be **solely linear**.

Bell inequalities for MBQC

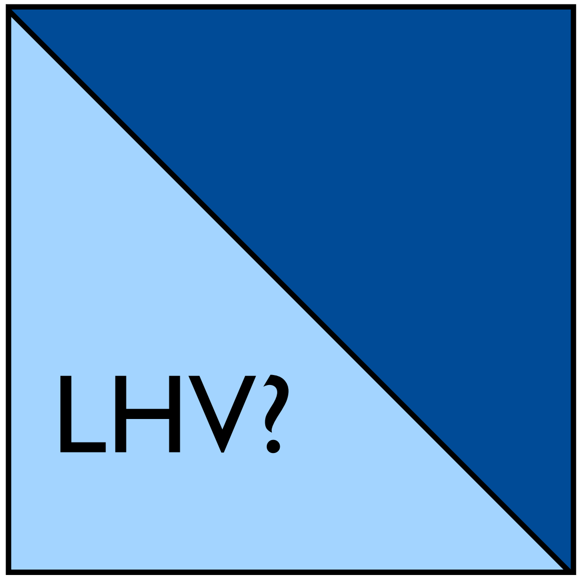
- To simplify further, let's initially adopt the precise **CHSH** (Werner-Wolf) setup.
  - **Spatially separated parties** with independent inputs.
  - Output of computation encoded in the **XOR** of all outcome bits.



$$M = \sum_j m_j$$

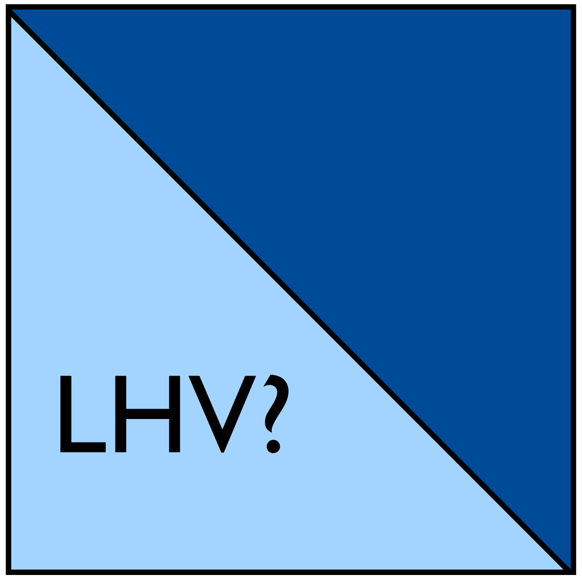
Bell inequalities for MBQC

- What computations $M(\vec{s})$ can this setup perform?
- LHV model may be **stochastic** and thus the computations may include **stochastic maps** - allowed computations will form a **region** of the **Boolean polytope**.



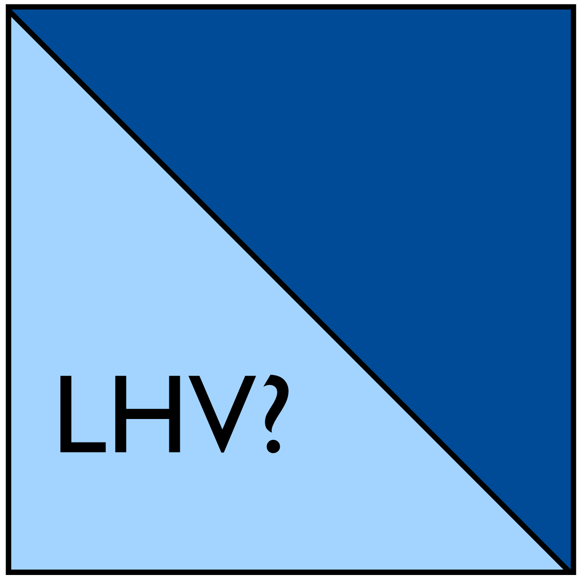
Bell inequalities for MBQC

- What computations $M(\vec{s})$ can this setup perform?
- LHV model may be **stochastic** and thus the computations may include **stochastic maps** - allowed computations will form a **region** of the **Boolean polytope**.



Bell inequalities for MBQC

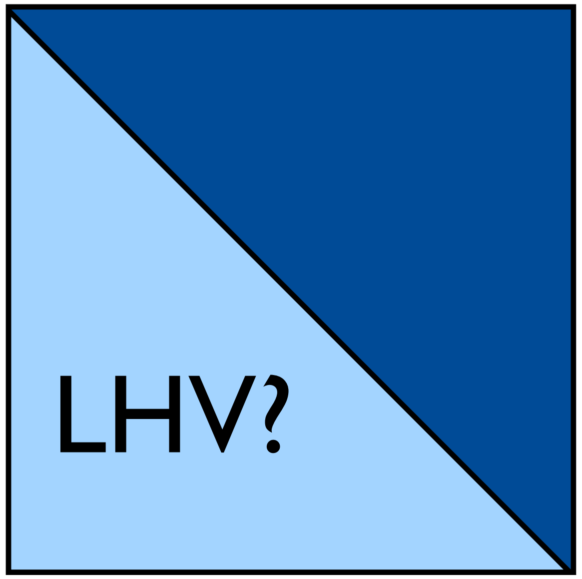
- What computations $M(\vec{s})$ can this setup perform?
- LHV model may be **stochastic** and thus the computations may include **stochastic maps** - allowed computations will form a **region** of the **Boolean polytope**.



- Randomness arises in LHV theories by **random assignment** of the **hidden variables**.

Bell inequalities for MBQC

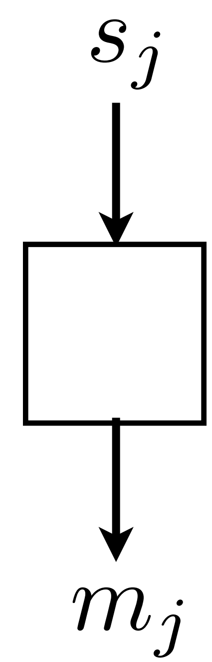
- What computations $M(\vec{s})$ can this setup perform?
- LHV model may be **stochastic** and thus the computations may include **stochastic maps** - allowed computations will form a **region** of the **Boolean polytope**.



- Randomness arises in LHV theories by **random assignment** of the **hidden variables**.
- Hence, this region will be a **convex polytope**, whose vertices correspond to the **deterministic computations**.

Bell inequalities for MBQC

- First let us consider a **single box**.



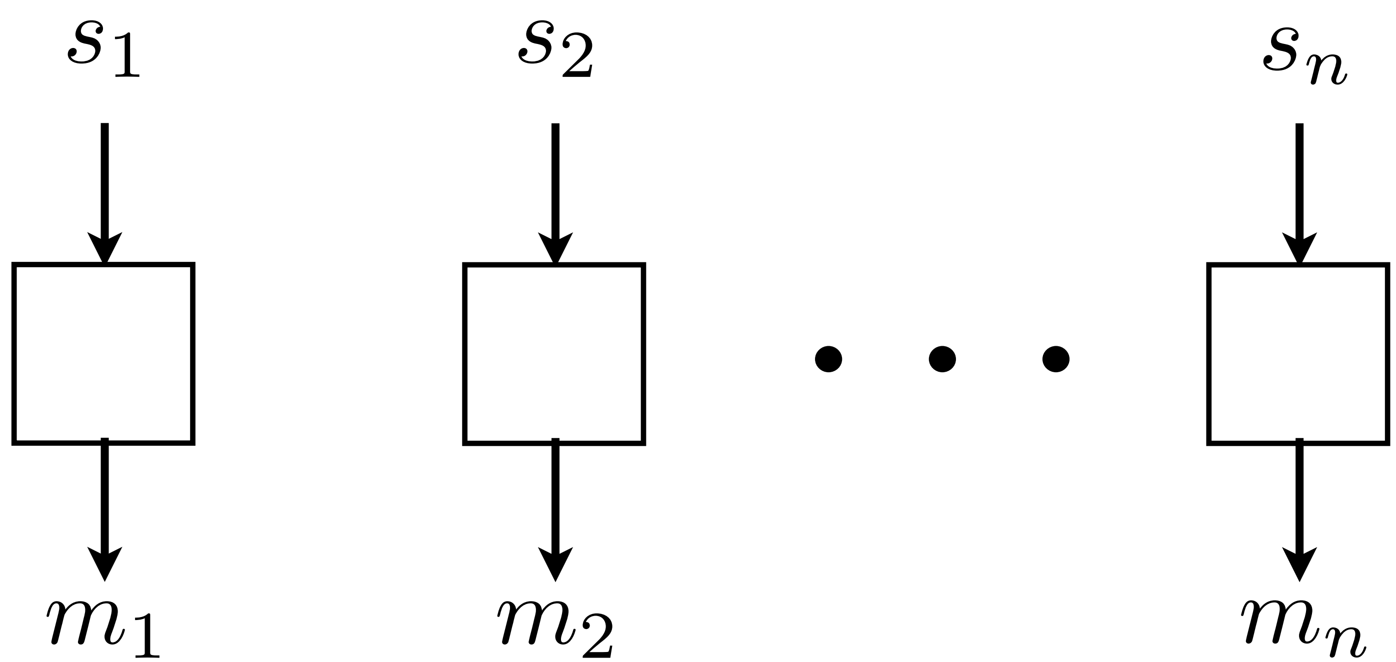
- The most general deterministic relationships between output and input can be written:

$$m_j = a_j + b_j m_j \qquad a_j \in \{0,1\} \qquad b_j \in \{0,1\}$$

- I.e. there are **only 4 1-bit** to **1-bit** functions.

Bell inequalities for MBQC

- If we associates bit **a**$_j$ and **b**$_j$ with each box, the most general expression for the output XOR bit $M(\vec{s})$ is



$$M = \sum_j m_j = \sum_j a_j + \sum_j b_j s_j$$

$$M = a + \sum_j b_j s_j$$

Bell inequalities for MBQC

$$M(\vec{s}) = a + \sum_j b_j s_j$$

Bell inequalities for MBQC

$$M(\vec{s}) = a + \sum_j b_j s_j$$

- We see

Bell inequalities for MBQC

$$M(\vec{s}) = a + \sum_j b_j s_j$$

- We see
  - this is **linear** in s,

Bell inequalities for MBQC

$$M(\vec{s}) = a + \sum_j b_j s_j$$

- We see
  - this is **linear** in s,
  - by suitable choice of $\mathbf{a}_j$ and $\mathbf{b}_j$
    all 2^(n+1) **linear functions** can be achieved.

Bell inequalities for MBQC

$$M(\vec{s}) = a + \sum_j b_j s_j$$

- We see
  - this is **linear** in s,
  - by suitable choice of **a_j** and **b_j** **all** 2^(n+1) **linear functions** can be achieved.
- Hence the full range of computations achievable by LHV correlations with XOR on the outcomes

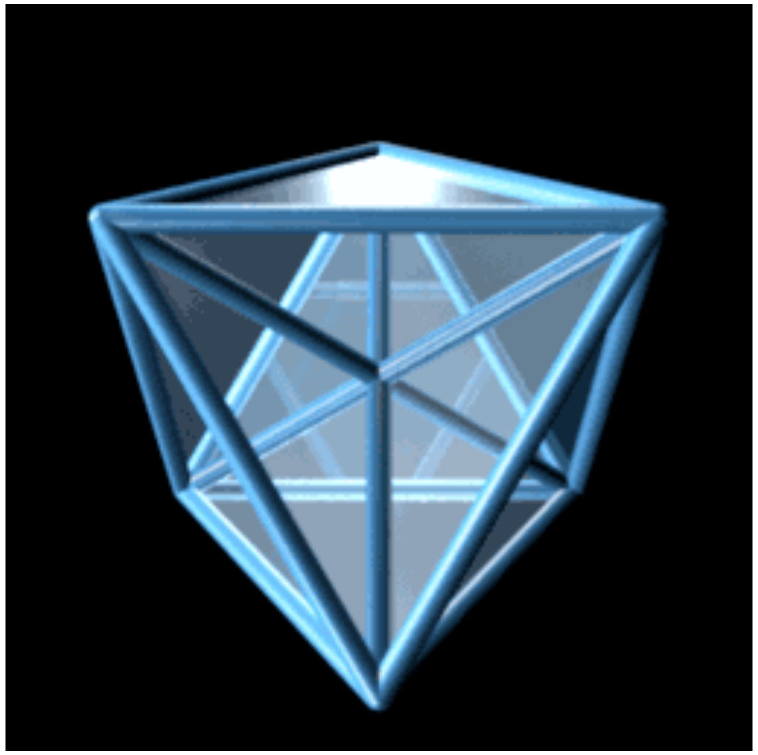
Bell inequalities for MBQC

$$M(\vec{s}) = a + \sum_j b_j s_j$$

- We see
  - this is **linear** in s,
  - by suitable choice of $\mathbf{a_j}$ and $\mathbf{b_j}$ **all** 2^(n+1) **linear functions** can be achieved.

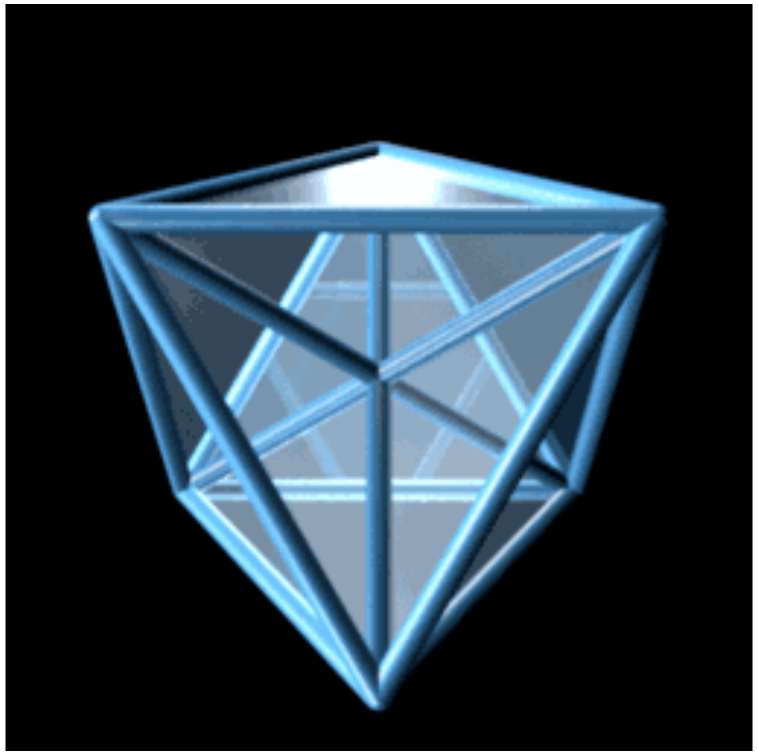
- Hence the full range of computations achievable by LHV correlations with XOR on the outcomes
  - is the **Linear Polytope**.

The linear polytope vs the Werner Wolf polytope



The linear polytope vs the Werner Wolf polytope

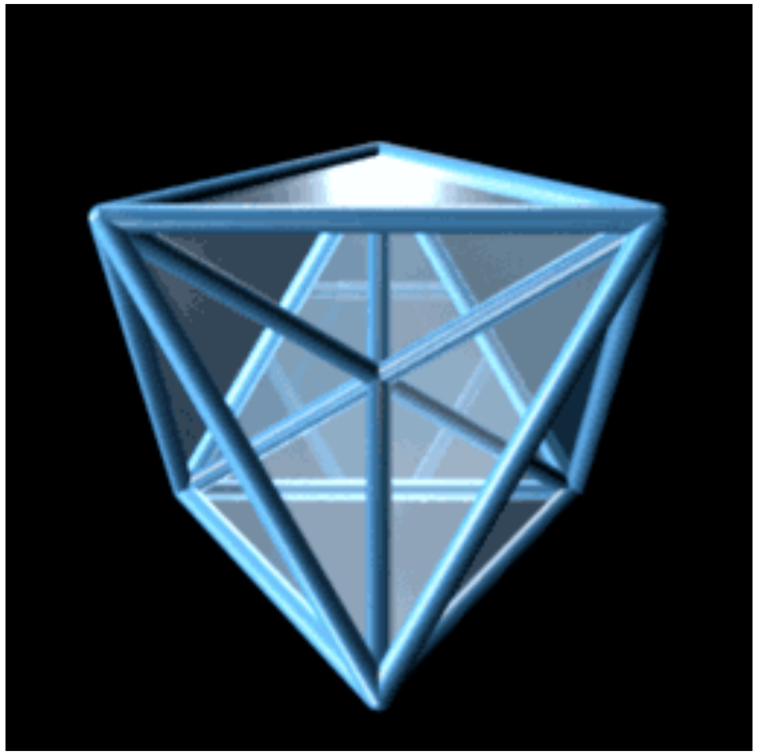
- The **linear polytope** is a **hyper-octahedron** with 2^(n+1) vertices.
- The **Werner-Wolf** polytope is a **hyper-octahedron** with 2^(n+1) vertices.



- Are they the **same polytope?**

The linear polytope vs the Werner Wolf polytope

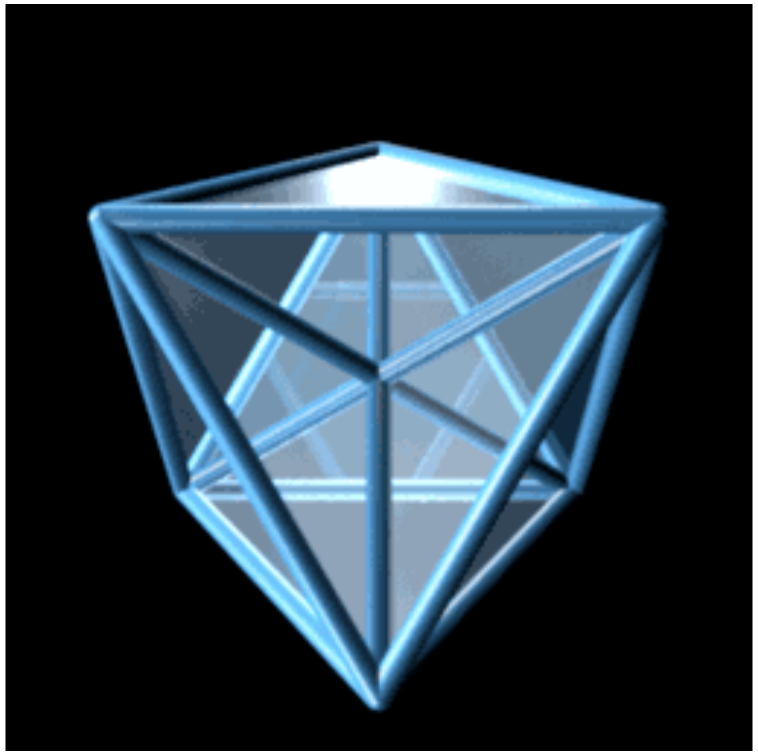
- The **linear polytope** is a **hyper-octahedron** with 2^(n+1) vertices.
- The **Werner-Wolf** polytope is a **hyper-octahedron** with 2^(n+1) vertices.



- Are they the **same polytope?**
- **Yes!** In fact, the derivation above is essentially a line-by-line recasting of Werner and Wolf (2001).

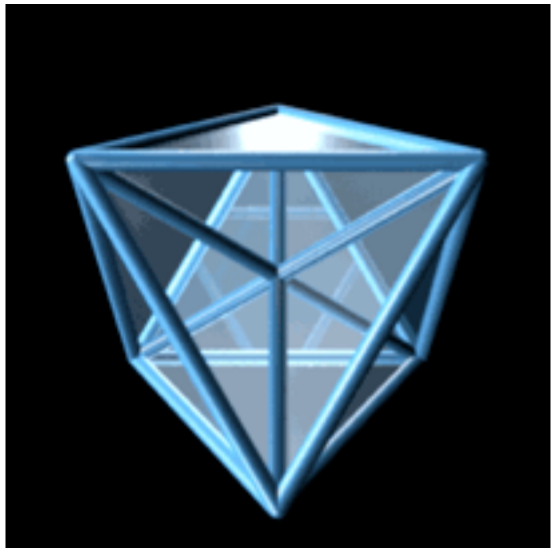
The linear polytope vs the Werner Wolf polytope

- The **linear polytope** is a **hyper-octahedron** with 2^(n+1) vertices.
- The **Werner-Wolf** polytope is a **hyper-octahedron** with 2^(n+1) vertices.



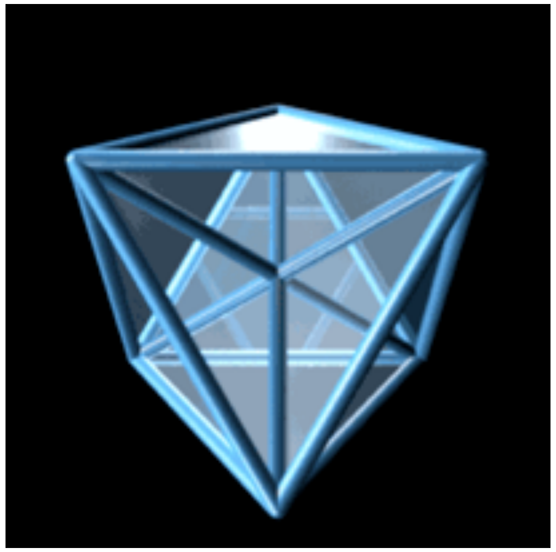
- Are they the **same polytope?**
- **Yes!** In fact, the derivation above is essentially a line-by-line recasting of Werner and Wolf (2001).
- Our derivation is a **computational reformulation** of the traditional Bell inequalities.

Bell inequalities for MBQC



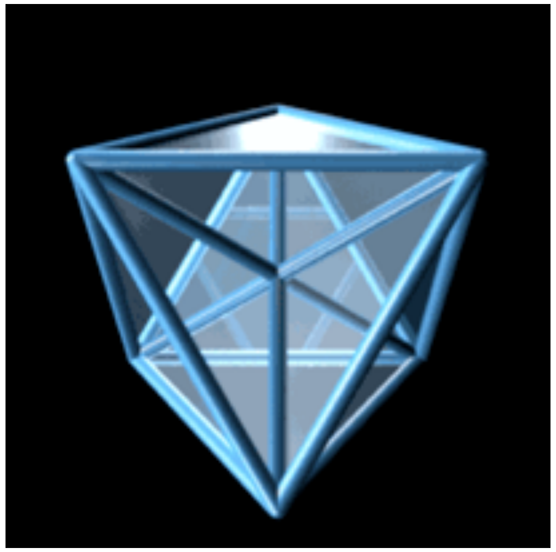
- So is this a **failure**?

Bell inequalities for MBQC



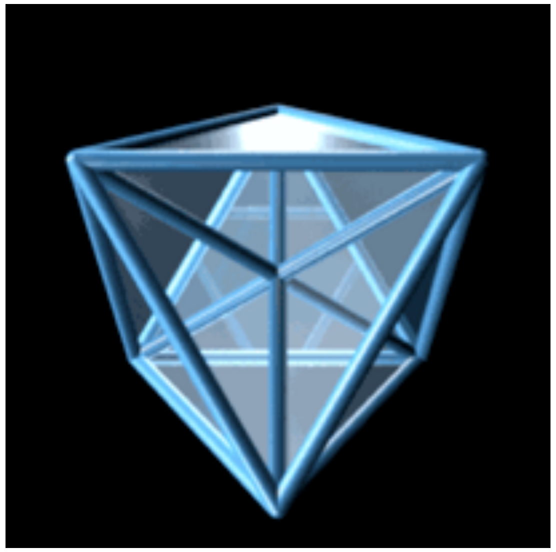
- So is this a **failure**?
  - We have reproduced a **10-year old** result.

Bell inequalities for MBQC



- So is this a **failure**?
  - We have reproduced a **10-year old** result.
  - We have failed to derive Bell inequalities relevant to standard MBQC since that utilises **adaptive measurements.**

Bell inequalities for MBQC



- So is this a **failure**?
  - We have reproduced a **10-year old** result.
  - We have failed to derive Bell inequalities relevant to standard MBQC since that utilises **adaptive measurements.**
- However, sometimes **new representations** give **new insights**....

Loopholes and linearity

- Our Bell polytope is the polytope of **linear functions**.

Loopholes and linearity

- Our Bell polytope is the polytope of **linear functions**.
- Recall that a "**loophole**" is any experimental imperfection which **enlarges** the LHV region.

Loopholes and linearity

- Our Bell polytope is the polytope of **linear functions**.
- Recall that a "**loophole**" is any experimental imperfection which **enlarges** the LHV region.
- Since the LHV region is the **linear polytope**, and since linear functions are **closed under composition**.

Loopholes and linearity

- Our Bell polytope is the polytope of **linear functions**.
- Recall that a "**loophole**" is any experimental imperfection which **enlarges** the LHV region.
- Since the LHV region is the **linear polytope**, and since linear functions are **closed under composition**.
  - Introducing **extra linear computation** will never introduce a **loophole**!

Loopholes and linearity

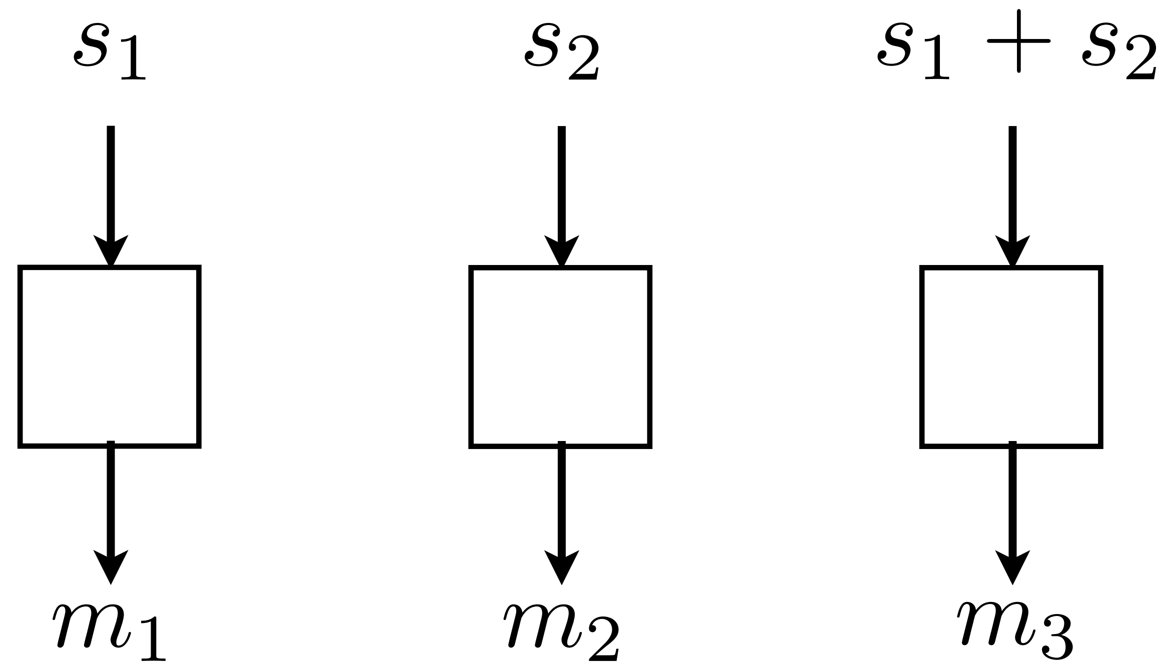
- Our Bell polytope is the polytope of **linear functions**.
- Recall that a "**loophole**" is any experimental imperfection which **enlarges** the LHV region.
- Since the LHV region is the **linear polytope**, and since linear functions are **closed under composition**.
  - Introducing **extra linear computation** will never introduce a **loophole**!
  - **All known loopholes** must be associated with some **non-linear** computation.

Loopholes and linearity

- Our Bell polytope is the polytope of **linear functions**.
- Recall that a "**loophole**" is any experimental imperfection which **enlarges** the LHV region.
- Since the LHV region is the **linear polytope**, and since linear functions are **closed under composition**.
    - Introducing **extra linear computation** will never introduce a **loophole**!
    - **All known loopholes** must be associated with some **non-linear** computation.
- This allows us to **weaken** our **assumptions** and derive the same Bell inequalities.

An example: pre-processing in GHZ

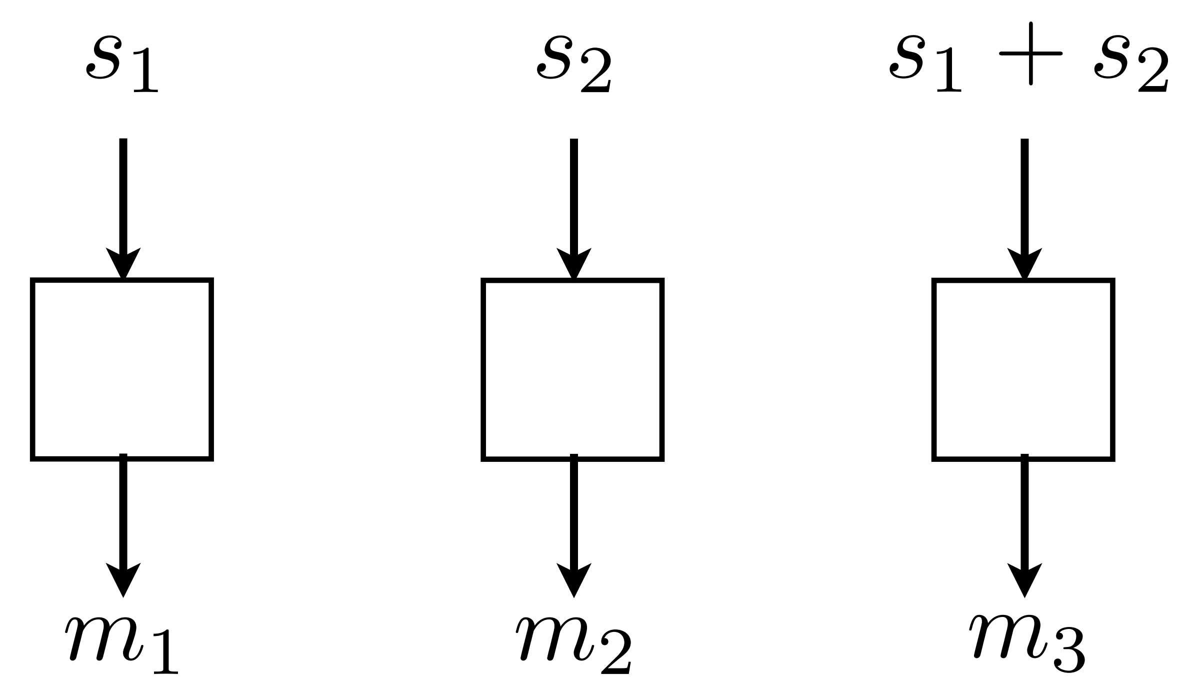
- Notice the third input **depends** upon the other two!



$$m_1 \oplus m_2 \oplus m_3 = s_1 s_2$$

An example: pre-processing in GHZ

- Notice the third input **depends** upon the other two!

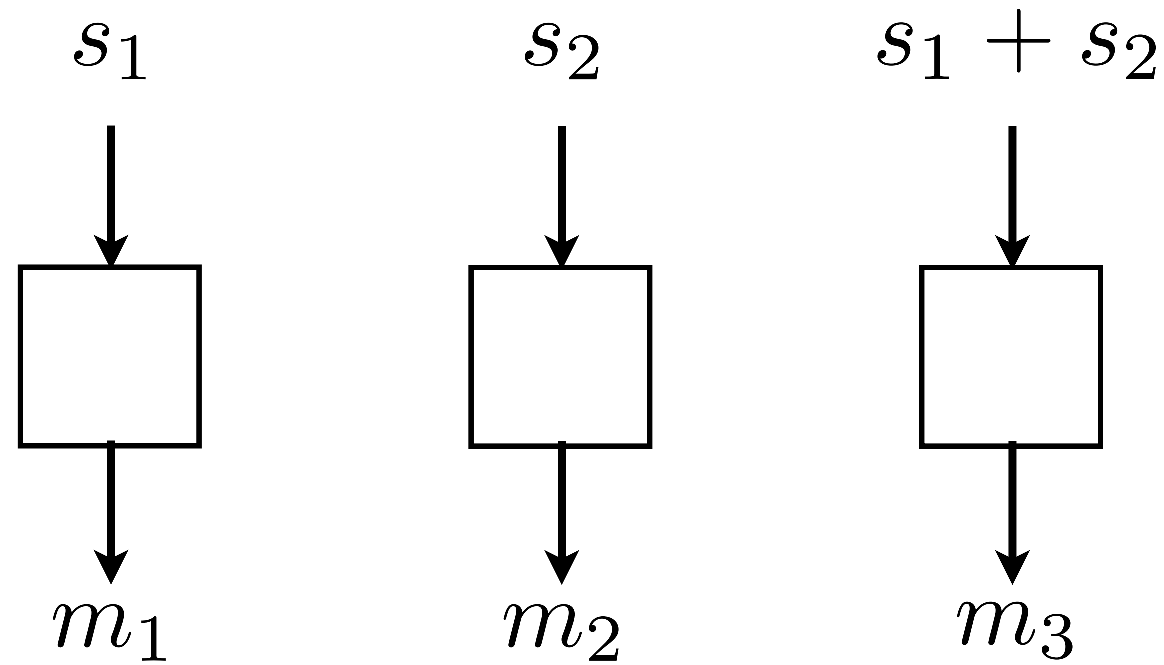


$$m_1 \oplus m_2 \oplus m_3 = s_1 s_2$$

- Why does this not induce a **loophole**?

An example: pre-processing in GHZ

- Notice the third input **depends** upon the other two!

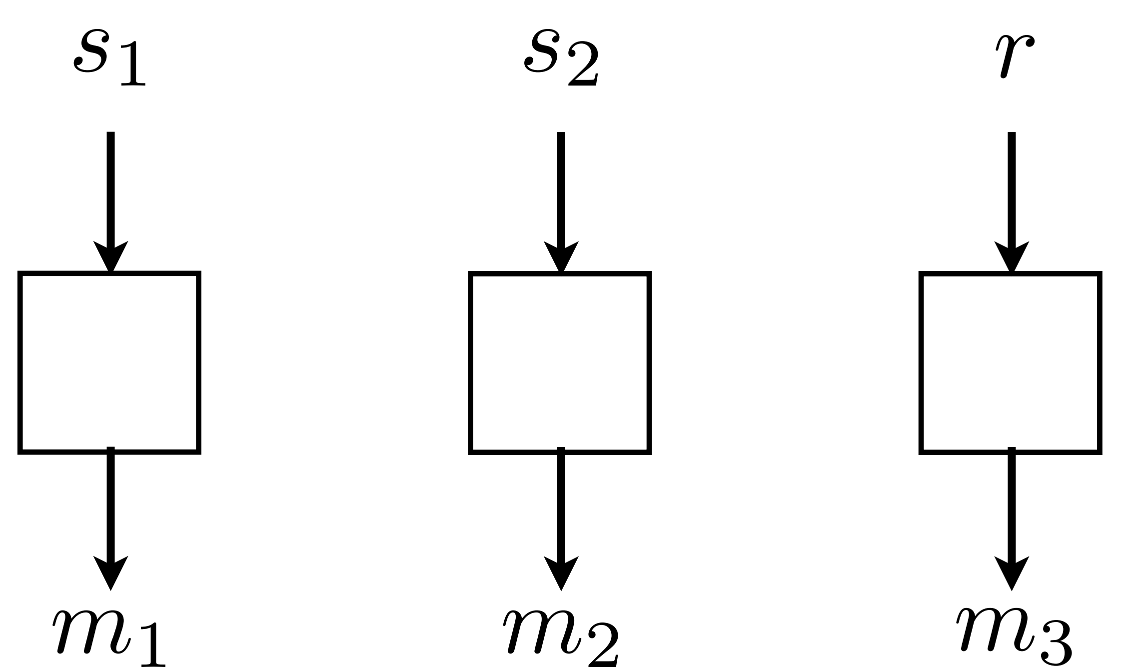


$$m_1 \oplus m_2 \oplus m_3 = s_1 s_2$$

- Why does this not induce a **loophole**?
- In an experiment, we **simulate** the dependency using **post-selection**.

An example: GHZ

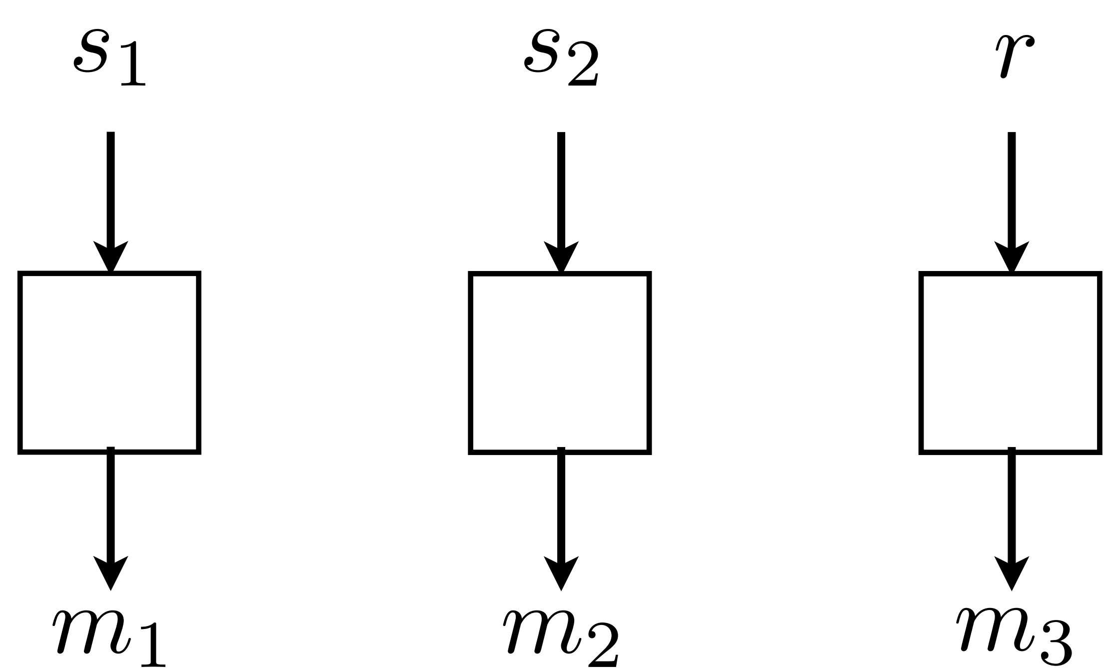
- In an experimental test of GHZ, the third input is set at random.



- We then **post-select** our data, and only keep data where $r = s_1 + s_2$.

An example: GHZ

- In an experimental test of GHZ, the third input is set at random.

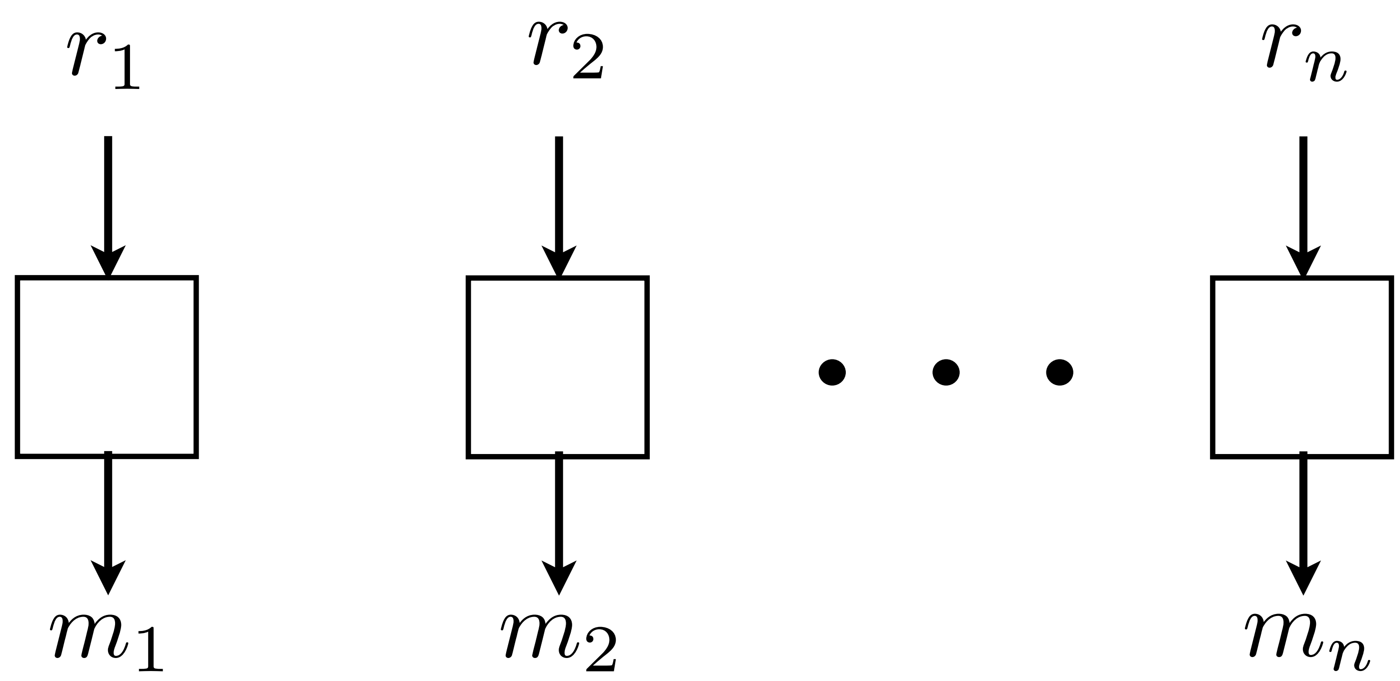


- We then **post-select** our data, and only keep data where $r = s_1 + s_2$.
- Does this induce a **detection loop-hole**? No, it doesn't...

Linear measurement post-selection

- Consider a more general setting. Let us set all inputs to n measurements as n uniformly random bits.

$$M = a + \sum_j b_j r_j$$



- Let s be the input bit-string (provided by a referee, say).
- We can post-select data such that each $\mathbf{r_j}$ is a **linear** function of the bits in **s**.

Linear measurement post-selection

- **Observation:** This post-selection **does not** induce a loophole.
- **Reason**: closure of linear maps under composition.

Linear measurement post-selection

- **Observation:** This post-selection **does not** induce a loophole.
- **Reason**: closure of linear maps under composition.

$$M = a + \sum_j b_j r_j$$

Linear measurement post-selection

- **Observation:** This post-selection **does not** induce a loophole.
- **Reason**: closure of linear maps under composition.

$$M = a + \sum_j b_j r_j$$

- **M** is linear in $\mathbf{r_j}$. The $\mathbf{r_j}$'s are linear in s. Hence M is linear in s.

Linear measurement post-selection

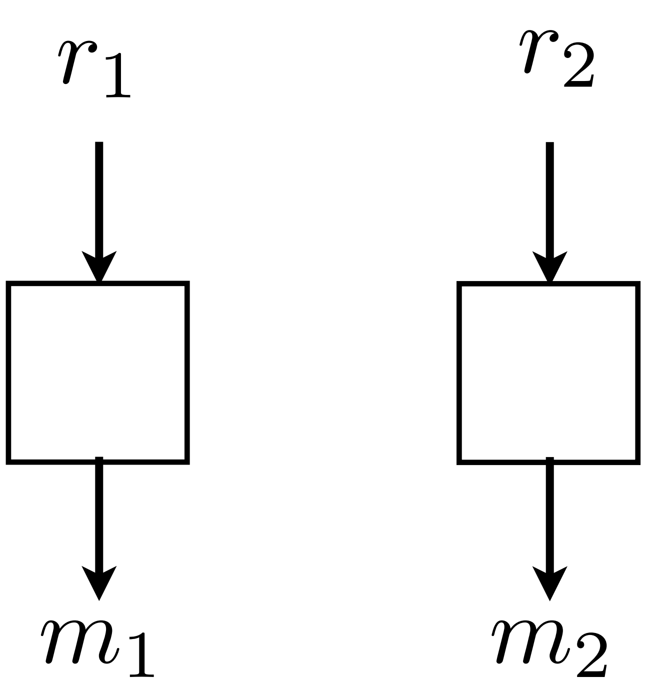
- **Observation:** This post-selection **does not** induce a loophole.
- **Reason**: closure of linear maps under composition.

$$M = a + \sum_j b_j r_j$$

- **M** is linear in $\mathbf{r_j}$. The $\mathbf{r_j}$'s are linear in s. Hence M is linear in s.
- **M** remains inside the **linear polytope** and **no loopholes** are induced - the LHV region is **no larger** than before.

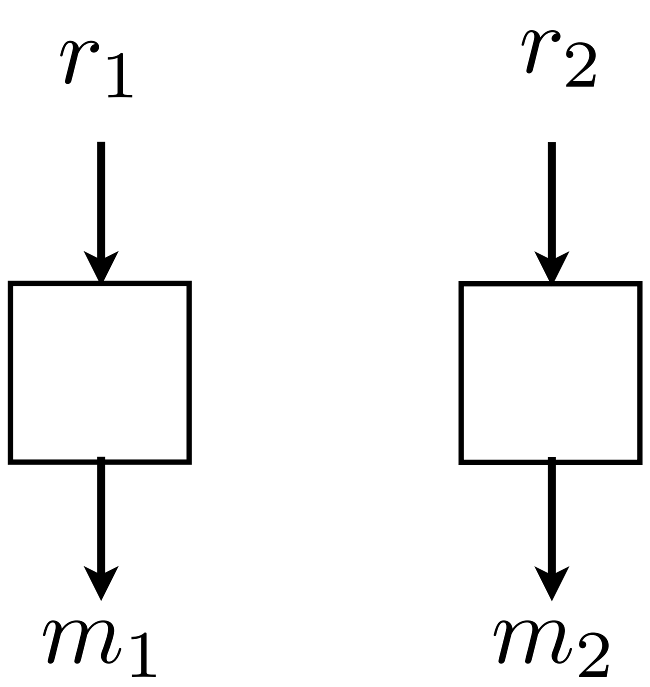
Linear measurement post-selection

- But we can go **further**.



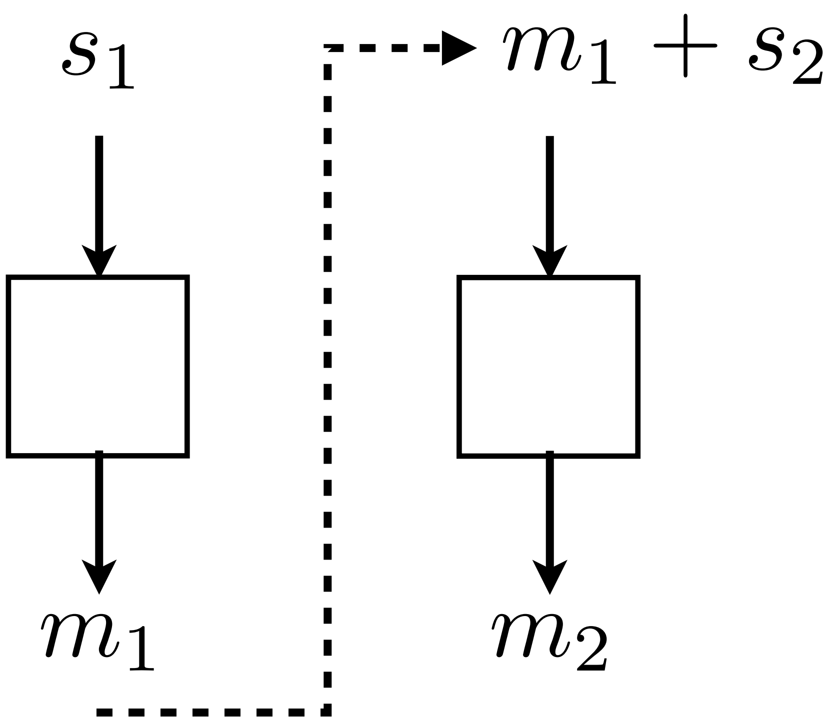
Linear measurement post-selection

- But we can go **further**.
- By the same reasoning, we can post-select **r** to be a linear function in **both** s and the measurement **output bits m$_j$**.



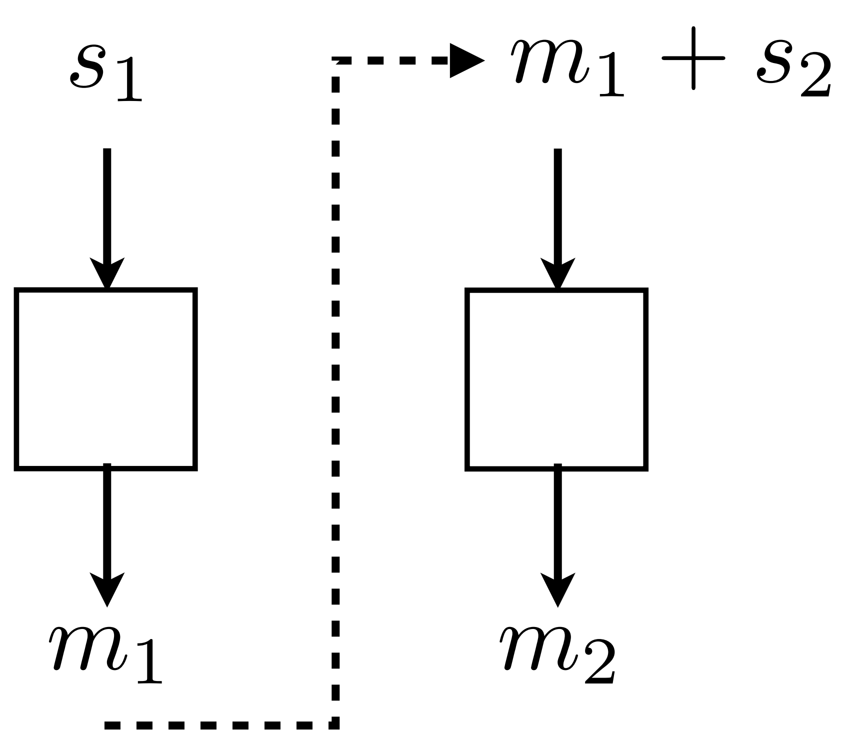
Linear measurement post-selection

- But we can go **further**.
- By the same reasoning, we can post-select **r** to be a linear function in **both** s and the measurement **output bits m**$_j$.



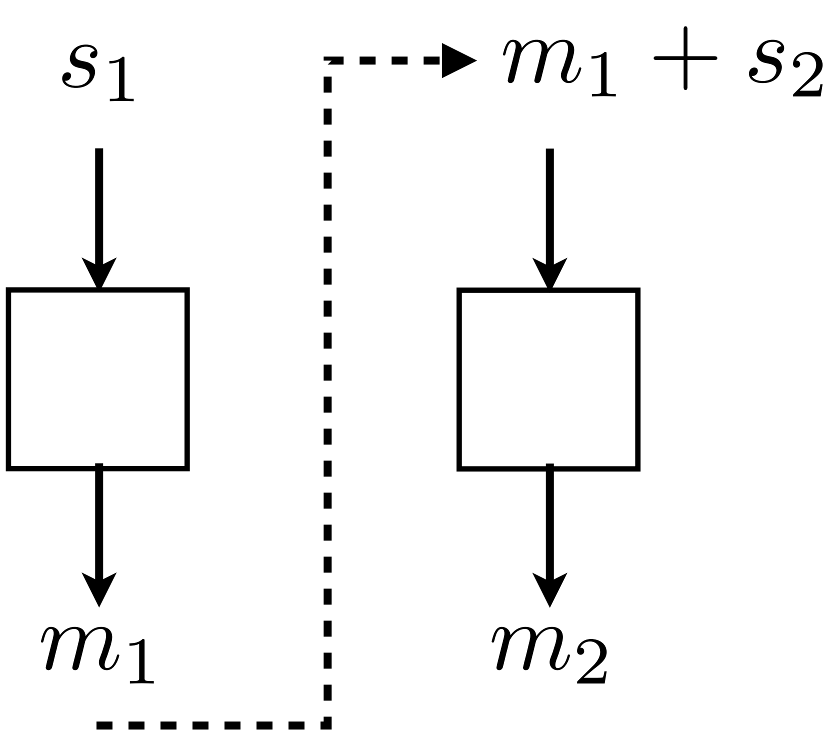
Linear measurement post-selection

- But we can go **further**.
- By the same reasoning, we can post-select **r** to be a linear function in **both** s and the measurement **output bits m**$_j$.
- Since **m**$_j$ are linear in **r**, **M** will remain within the linear polytope!



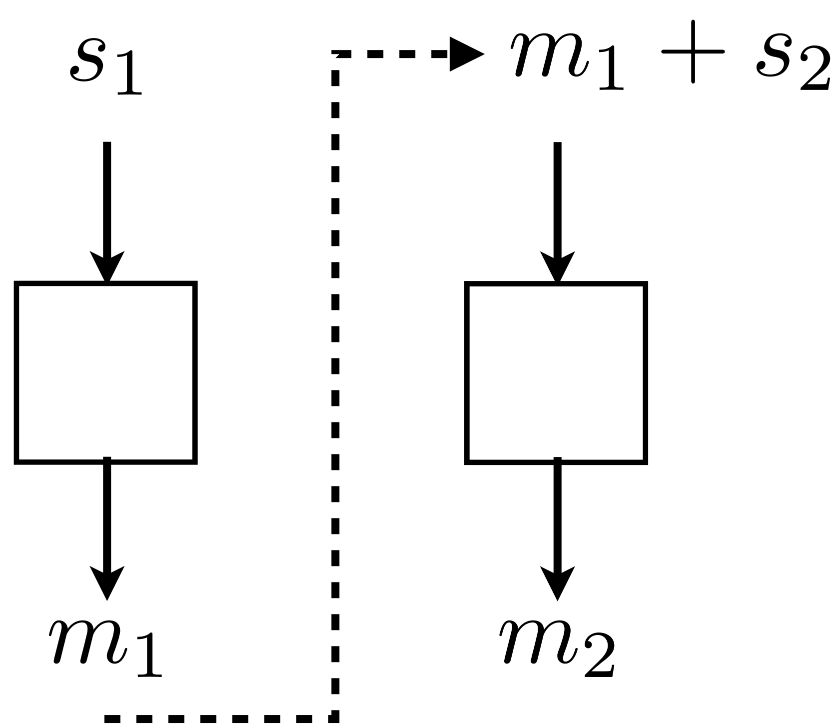
Linear measurement post-selection

- But we can go **further**.
- By the same reasoning, we can post-select **r** to be a linear function in **both** s and the measurement **output bits m_j**.
- Since **m_j** are linear in **r**, **M** will remain within the linear polytope!
- This allows us to simulate **linearly adaptive** measurements,



Linear measurement post-selection

- But we can go **further**.
- By the same reasoning, we can post-select **r** to be a linear function in **both** s and the measurement **output bits** $\mathbf{m}_j$.
- Since $\mathbf{m}_j$ are linear in **r**, **M** will remain within the linear polytope!
- This allows us to simulate **linearly adaptive** measurements,



- And the linear polytope will **still** describe all LHV correlations.

Computational Bell inequalities

Computational Bell Inequalities

- We can use these observations to **generalise** the traditional Bell inequalities.

Computational Bell Inequalities

- We can use these observations to **generalise** the traditional Bell inequalities.
- A **computational Bell inequality** is a facet of the polytope of **Boolean stochastic maps** achieved in any LHV theory
  - On a random **m-bit** input string **s**
  - Given **n 2-setting, 2-outcome** space-like separated measurements
  - With post-selection of measurement settings which are a linear function of input data and other measurement outcomes (**simulated linear adaptivity**)
  - And arbitrary **linear** pre- and post-computation.

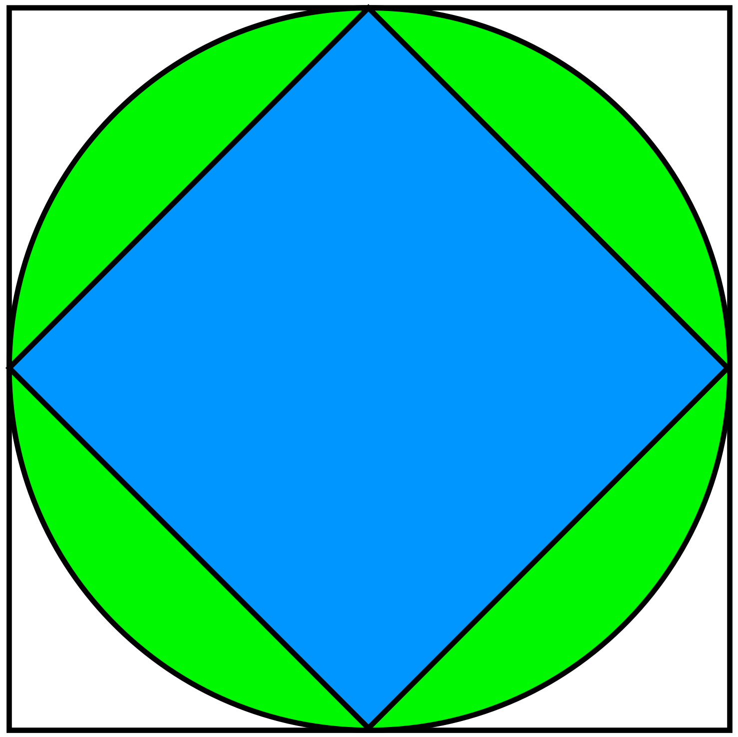
Computational Bell Inequalities

- The "Computational Bell inequalities" are easy to characterise.
- For **n ≥ m** they are facets of the m-bit **linear polytope**.

- Setting **n = m** and **forbidding post-selection**, we recover the traditional definition of CHSH inequalities.

From LHV to Quantum Correlations

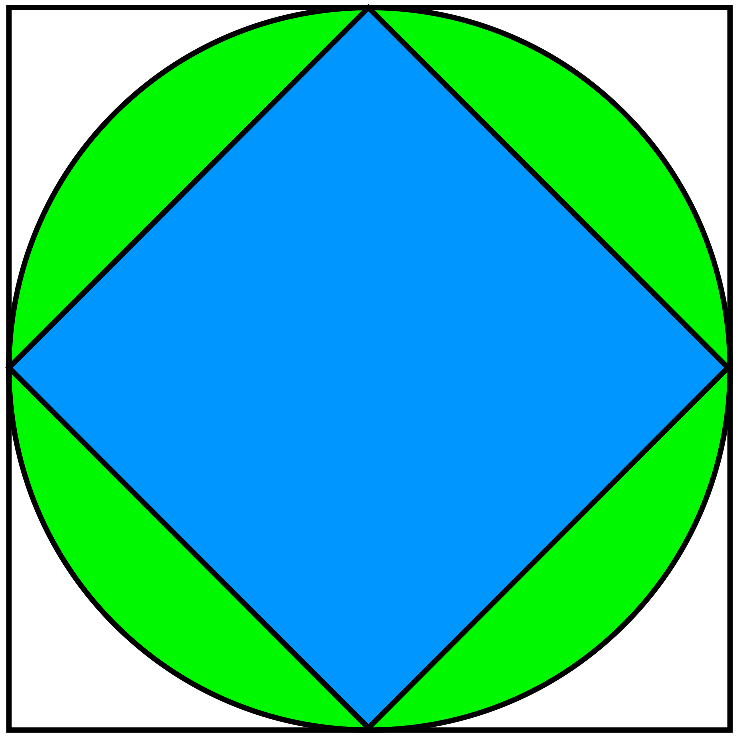
- A significant strand of Bell inequality research has been to characterise the **set** of conditional probabilities / stochastic maps allowed within **Quantum Mechanics**.



[1] Known as **Tsirelson - Landau - Masanes** region.

From LHV to Quantum Correlations

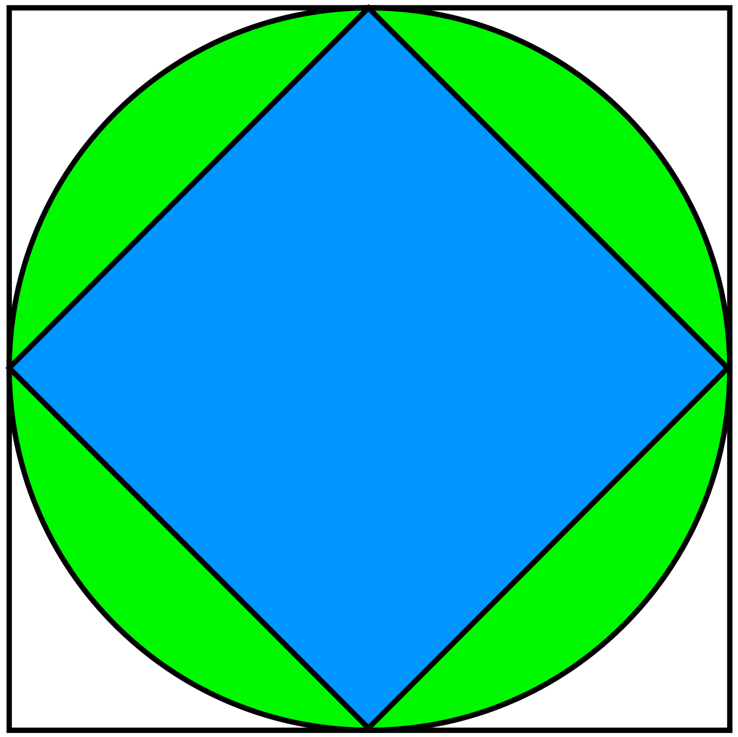
- A significant strand of Bell inequality research has been to characterise the **set** of conditional probabilities / stochastic maps allowed within **Quantum Mechanics**.
- Usually **only non-adaptive** measurements are considered.



[1] Known as **Tsirelson - Landau - Masanes** region.

From LHV to Quantum Correlations

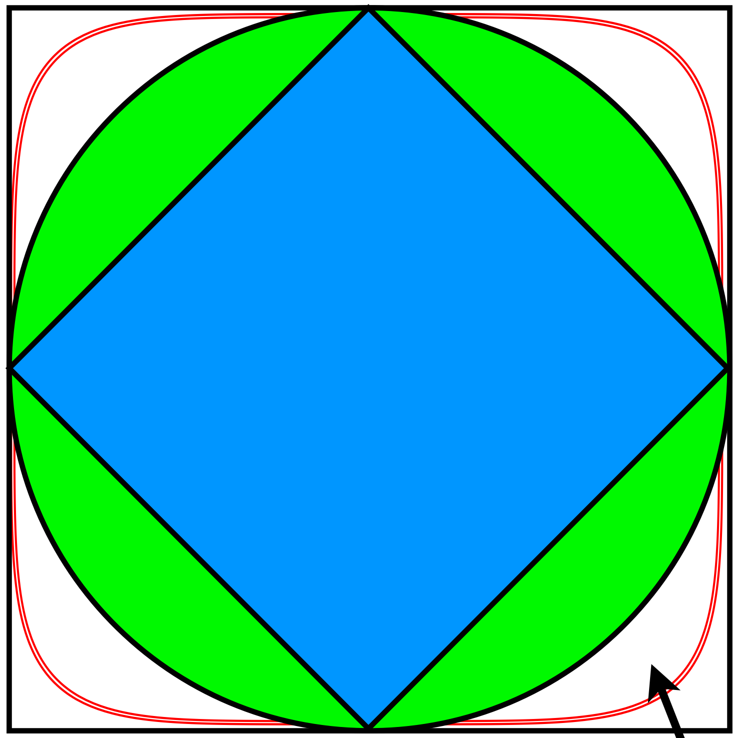
- A significant strand of Bell inequality research has been to characterise the **set** of conditional probabilities / stochastic maps allowed within **Quantum Mechanics**.
- Usually **only non-adaptive** measurements are considered.
- But in our new framework, we can also allow **extra parties,** and simulated **linear adaptive measurement**.



[1] Known as **Tsirelson - Landau - Masanes** region.

From LHV to Quantum Correlations

- A significant strand of Bell inequality research has been to characterise the **set** of conditional probabilities / stochastic maps allowed within **Quantum Mechanics**.
- Usually **only non-adaptive** measurements are considered.
- But in our new framework, we can also allow **extra parties,** and simulated **linear adaptive measurement**.
- Do these enlarge the **quantum region**?

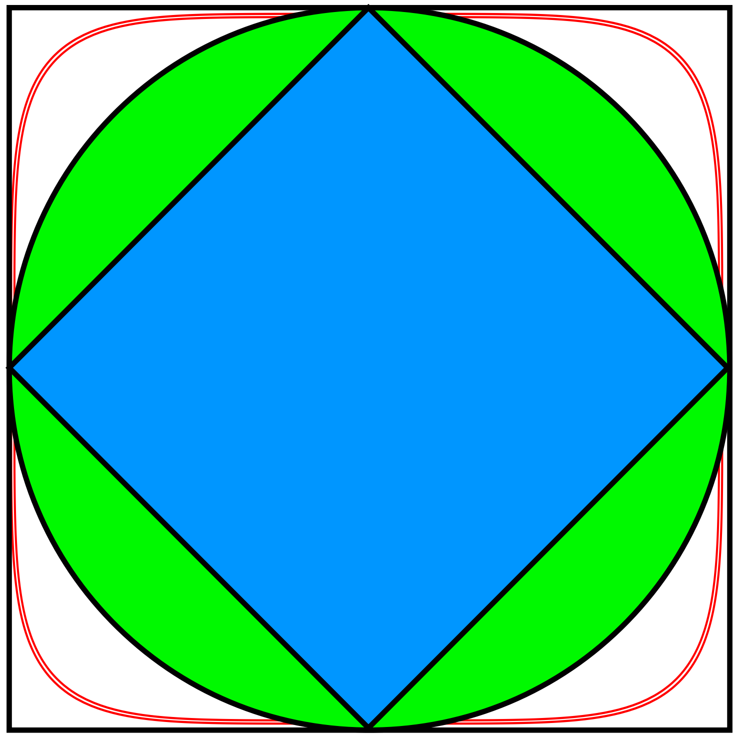


A bigger quantum set?

[1] Known as **Tsirelson - Landau - Masanes** region.

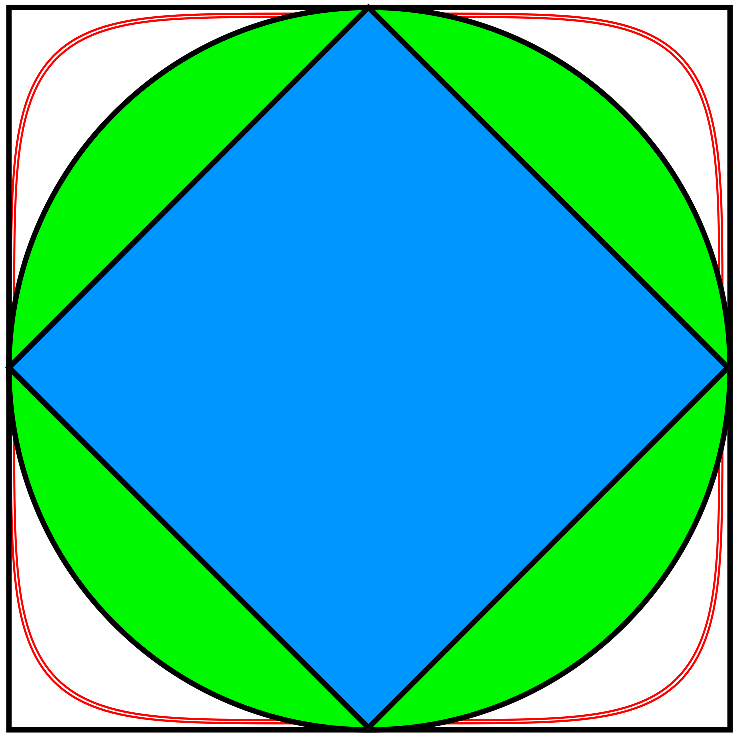
From LHV to Quantum Correlations

- Yes!
- For a fixed **n**,
  - Allowing **extra parties**
  - Allowing **linear post-selection** (simulated adaptivity).
- can **increase** the quantum region.



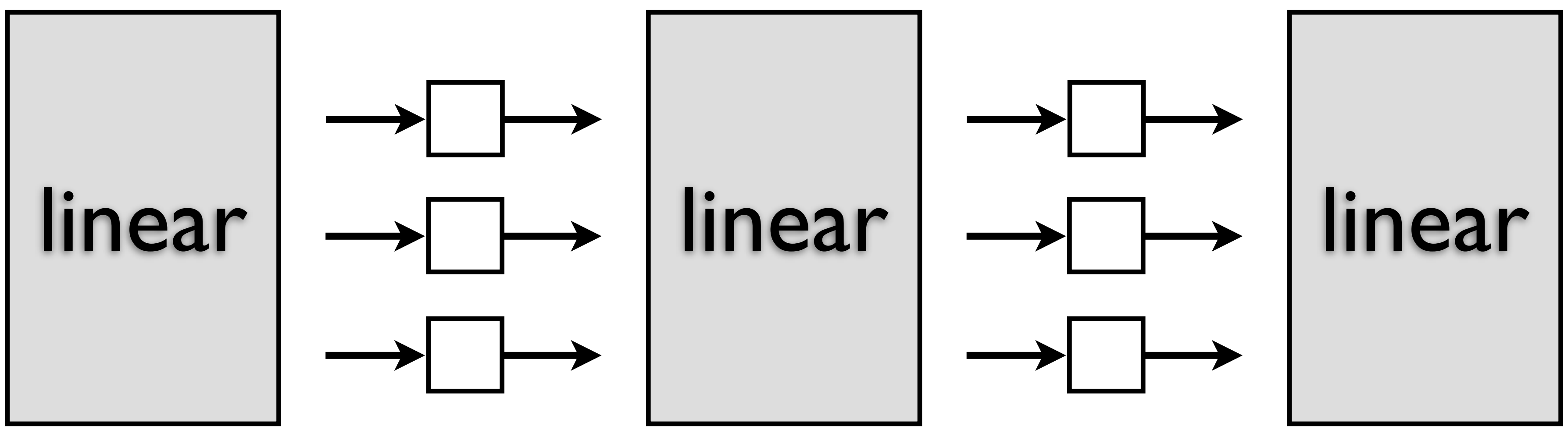
From LHV to Quantum Correlations

- Yes!
- For a fixed **n**,
  - Allowing **extra parties**
  - Allowing **linear post-selection** (simulated adaptivity).
- can **increase** the quantum region.
- This can provide a **greater degree of violation** of Bell Inequalities than in the standard setting.



Quantum correlations with adaptive measurements

- For example, if we limit the number of parties to 6.
  - With linear adaptive measurement we can access the deterministic 3-bit **AND** function.
    - The triple product $\mathbf{s_1 s_2 s_3}$ of input bits $\mathbf{s_1}$, $\mathbf{s_2}$, $\mathbf{s_3}$.



  - With **no adaptivity**, deterministic computation of this function is **impossible** with only 6 measurements [1].

[1] In **Hoban** et al (2010 - arxiv next week) we show that 2^(n-1) qubits are required to acheive an n-bit AND deterministically with no adaptivity.

Summary

- We derived Bell inequalities from the perspective of measurement-based quantum computation.

Summary

- We derived Bell inequalities from the perspective of measurement-based quantum computation.
  - This allowed us to characterise all 2-setting, 2-output Bell inequalities in terms of the **linear Boolean polytope**.

Summary

- We derived Bell inequalities from the perspective of measurement-based quantum computation.
  - This allowed us to characterise all 2-setting, 2-output Bell inequalities in terms of the **linear Boolean polytope**.
  - And made it clear that **extra linear computations** (including simulated adaptivity) do **not** lead to loopholes.

Summary

- We derived Bell inequalities from the perspective of measurement-based quantum computation.
  - This allowed us to characterise all 2-setting, 2-output Bell inequalities in terms of the **linear Boolean polytope**.
  - And made it clear that **extra linear computations** (including simulated adaptivity) do **not** lead to loopholes.
- This enables one to consider a **richer structure** of quantum correlations in the context of BIs (including the **adaptive measurements** arising in **MBQC**) which we are only starting to investigate.

Summary

- We derived Bell inequalities from the perspective of measurement-based quantum computation.
    - This allowed us to characterise all 2-setting, 2-output Bell inequalities in terms of the **linear Boolean polytope**.
    - And made it clear that **extra linear computations** (including simulated adaptivity) do **not** lead to loopholes.
- This enables one to consider a **richer structure** of quantum correlations in the context of BIs (including the **adaptive measurements** arising in **MBQC**) which we are only starting to investigate.
- Are Bell inequality violations more about **non-linearity** than **non-locality**...?

Acknowledgements

- Joint work with members of my UCL group
  - Matty Hoban, Janet Anders, Earl Campbell and Klearchos Loukopoulos.
- These ideas benefitted from discussions with Robert Raussendorf, Robert Spekkens, Miguel Navascues, Akimasa Miyake, Robin Blume-Kohout Debbie Leung and many others...

- **References**

  - R. Werner and M. Wolf, Phys. Rev. A 64 32112 (2001)
  - J. Anders and D. E. Browne, Phys. Rev. Lett. (2009)
  - M. J. Hoban, E.T. Campbell, K. Loukopoulos, D.E. Browne, "Non-adaptive measurement-based quantum computation and multi-party Bell inequalities", arxiv very very soon.
  - M. J. Hoban and D. E. Browne, Bell inequalities and adaptive measurements, arxiv soon.

The Leverhulme Trust

EPSRC Pioneering research and skills

National Research Foundation
Prime Minister's Office, Republic of Singapore