Device-Independent Tests of Entropy

Jonatan Bohr Brask

with Rafael Chaves, Nicolas Brunner

Phys. Rev. Lett. 115, 110501 (2015)

FONDS NATIONAL SUISSE
SCHWEIZERISCHER NATIONALFONDS
FONDO NAZIONALE SVIZZERO
SWISS NATIONAL SCIENCE FOUNDATION

Device independence

Testing physical properties from experimental data
without detailed knowledge of the implementation.

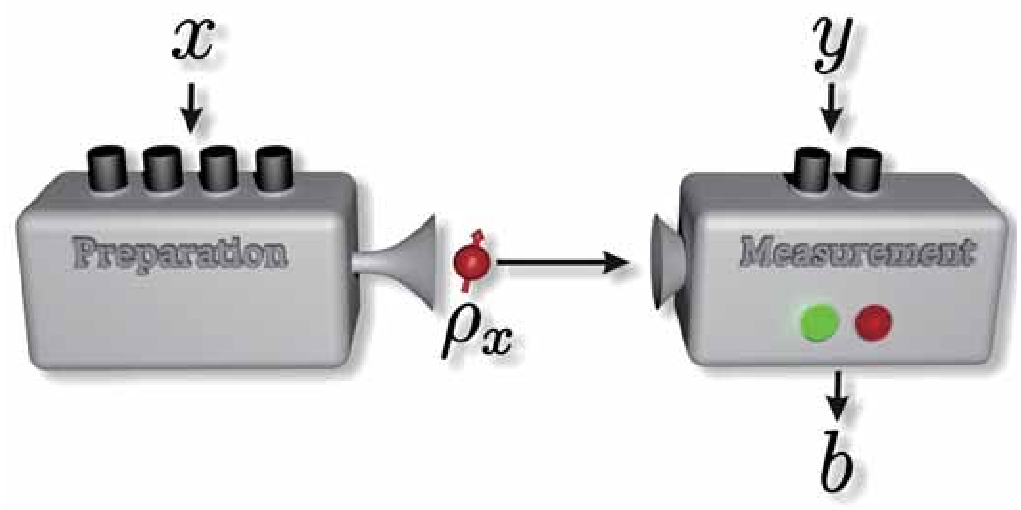
Examples : Bell nonlocality, entanglement, dimension.

Device independence

Testing physical properties from experimental data without detailed knowledge of the implementation.

Examples : Bell nonlocality, entanglement, dimension.

In this talk: message entropy in prepare and measure scenario.



Bound minimal entropy $S(\rho)$

compatible with data $p(b|xy)$

Minimal entropy: *average* communication.

Minimal dimension: *worst case* communication.

Entropy witnesses

Want function of data and a bound such that

$$W(p(b|xy)) > L_s \Rightarrow S(\rho) > s$$

For the average message (we will assume uniform inputs).

$$\rho = \sum_x p(x)\rho_x$$

Diagonal for classical messages so von Neumann → Shannon.

Entropy witnesses

Want function of data and a bound such that

$$W(p(b|xy)) > L_s \Rightarrow S(\rho) > s$$

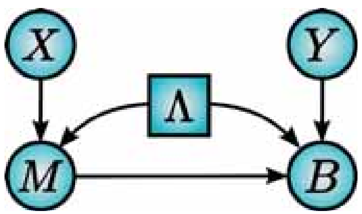
For the average message (we will assume uniform inputs).

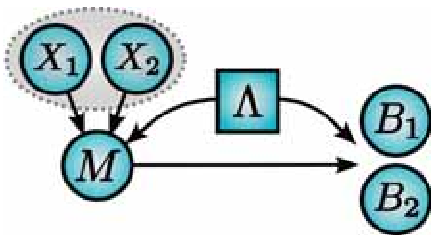
$$\rho = \sum_x p(x)\rho_x$$

Diagonal for classical messages so von Neumann → Shannon.

Causal inference graphs

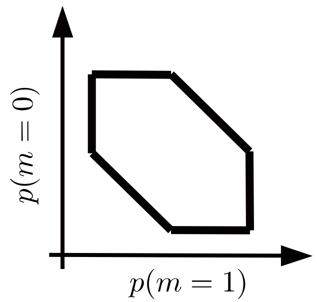
- Very general (arbitrary input/ouput)
- Generally not tight
- Does not distinguish classical/quantum.





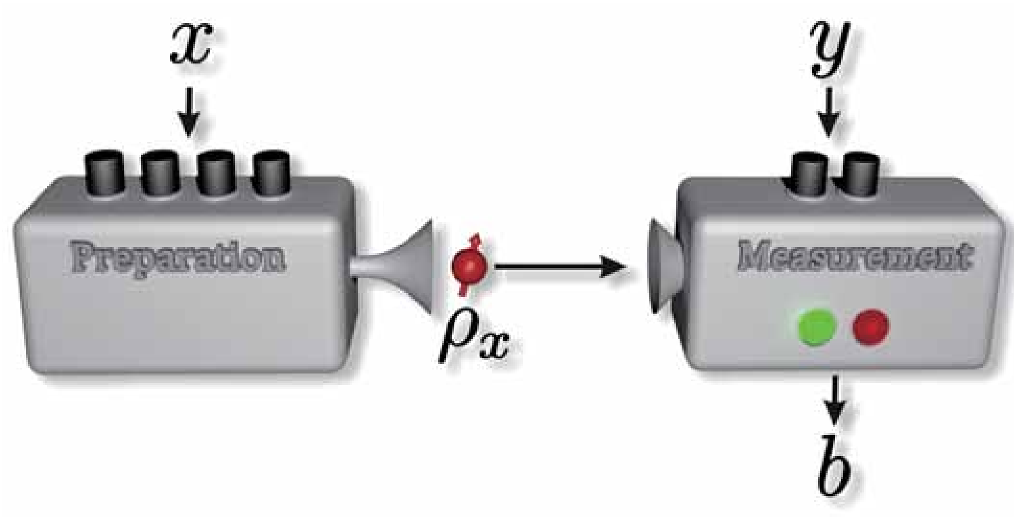
Convex optimisation

- Restricted numbers input/output
- Tight bounds
- Demonstrate quantum advantage.



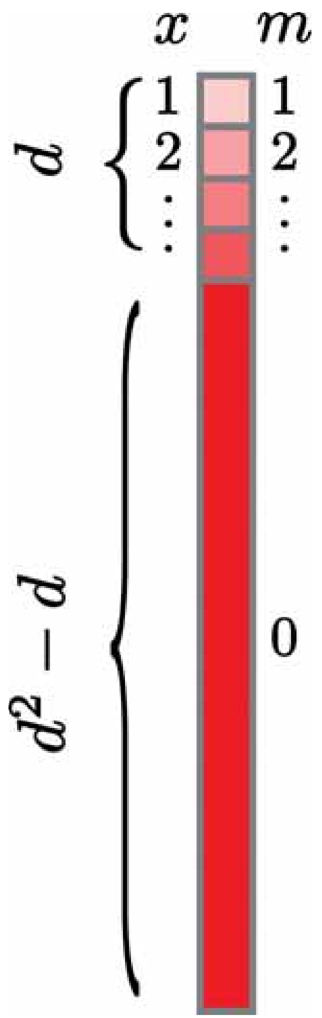
Entropy and dimension are different quantities

Classical strategy for d^2 preparations
and d^2-1 measurements, binary output.



Entropy and dimension are different quantities

Classical strategy for d^2 preparations
and d^2-1 measurements, binary output.



$$p(m) = \frac{1}{d^2} \to 0$$

$$p(m) = \frac{d^2 - d}{d^2} \to 1$$

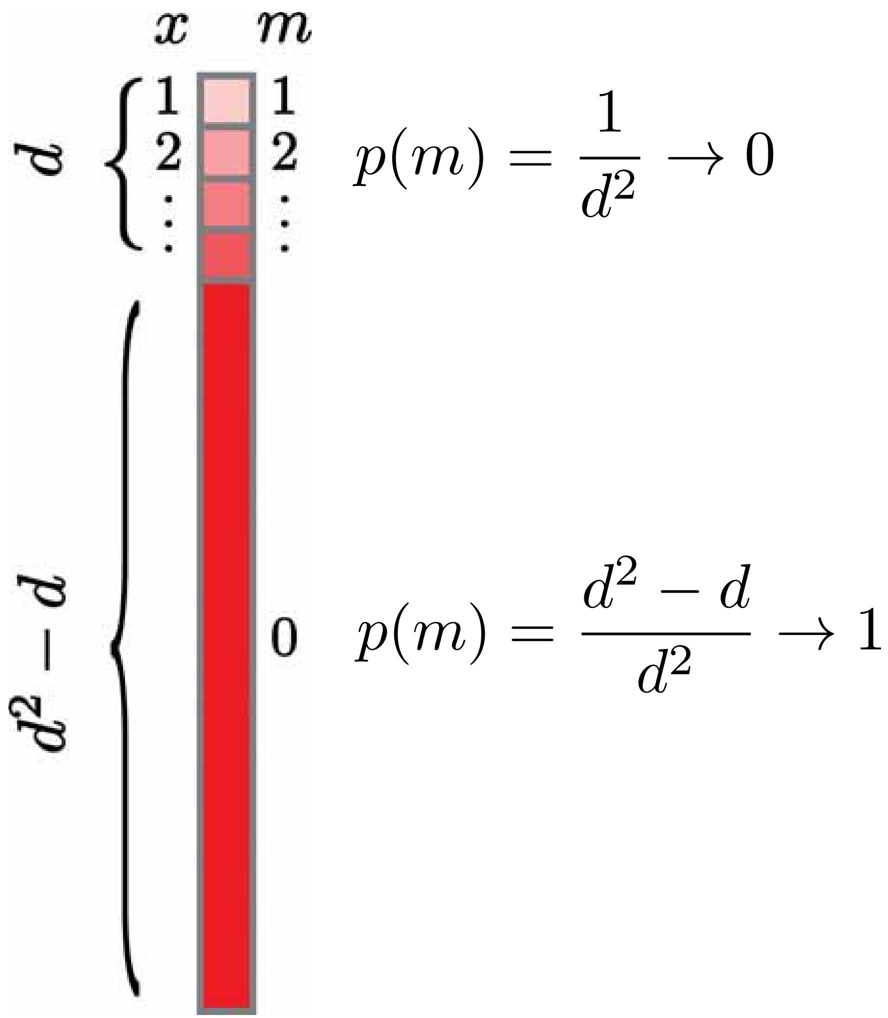
Entropy and dimension are different quantities

Classical strategy for d^2 preparations
and d^2-1 measurements, binary output.

The entropy is

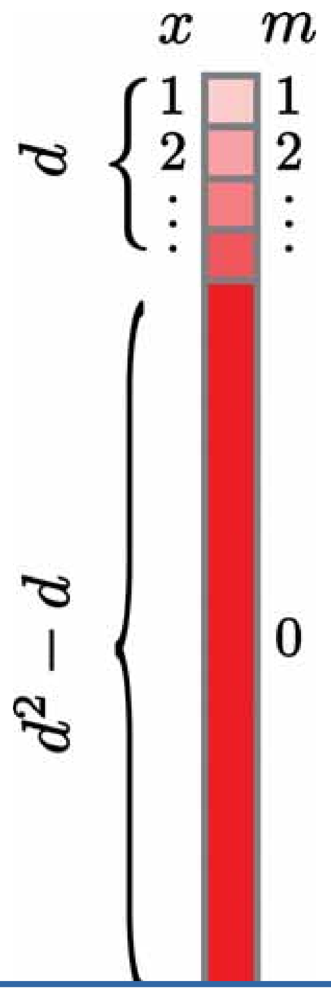
$$S(\rho) = -\sum_m \log(p(m))$$

Dimension witness of Gallego *et al.* (PRL'10)
→ Requires message dimension at least d+1



Entropy and dimension are different quantities

Classical strategy for d^2 preparations
and d^2-1 measurements, binary output.



$$p(m) = \frac{1}{d^2} \to 0$$

$$p(m) = \frac{d^2 - d}{d^2} \to 1$$

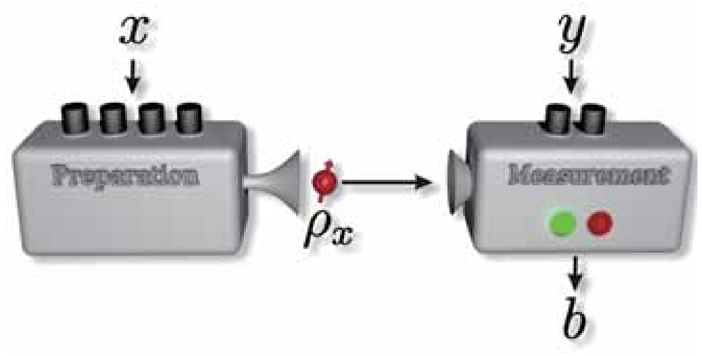
The entropy is

$$S(\rho) = -\sum_m \log(p(m))$$

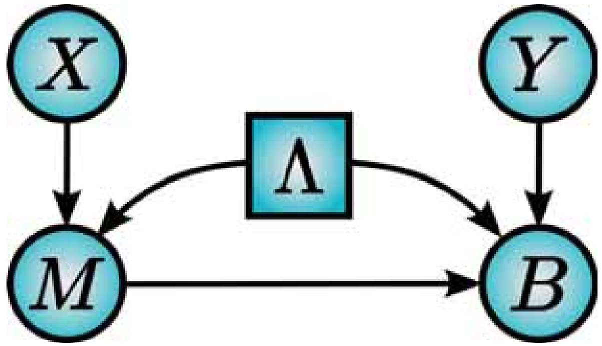
Dimension witness of Gallego *et al.* (PRL'10)
→ Requires message dimension at least *d*+1

Dimension diverges Entropy vanishes	*worst case communication* vs. *average* communication

Causal inference method



Associate DAG



Causal relationships captured by linear equations in the entropies

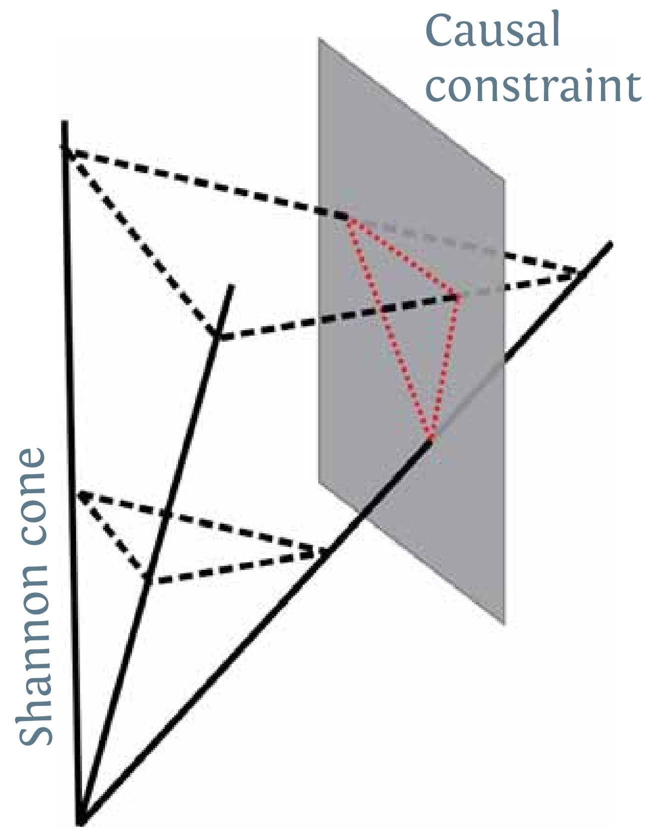
$$
\begin{aligned}
H(X,Y,\Lambda) &= H(X) + H(Y) + H(\Lambda) \\
H(M|X,\Lambda) &= 0 \\
H(B|Y,M,\Lambda) &= 0
\end{aligned}
$$

Form vectors of all joint entropies. E.g. for *n* variables:

$$[H(\emptyset), H(X_1), \ldots, H(X_1, X_2), \ldots, H(X_1, \ldots, X_n)] \in \mathbb{R}^{2^n}$$

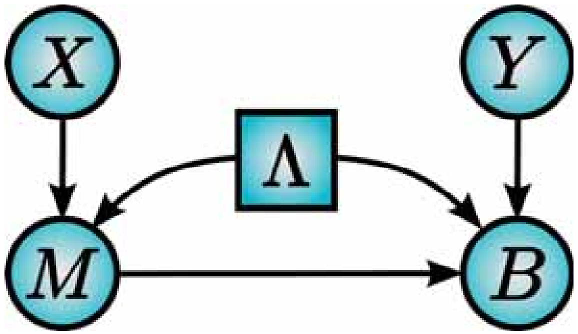
Entropy vectors are restricted by the causal constraints and by Shannon-type inequalities.

- Monotonicity (uncertainty of larger set is larger)
- Strong subadditivity (positivity of cond. info.)
- Positivity, normalisation.



Deriving inequalities

1) List Shannon-type inequalities.
2) List causal constraints.
3) Marginalise to observable variables.



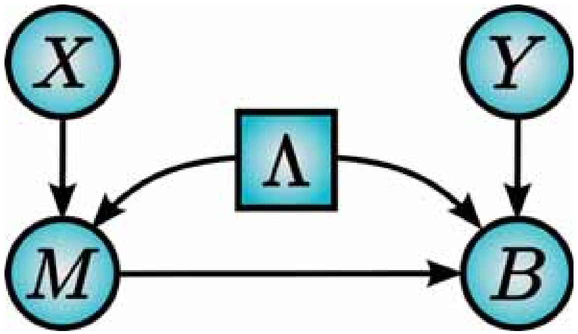
Quantum: some joint entropies not physical.

$$\cancel{S(\rho, B)}$$

→ Replace constraints by data processing.
(Chaves, Majenz, Gross, Nat. Comm.'15).

Deriving inequalities

1) List Shannon-type inequalities.
2) List causal constraints.
3) Marginalise to observable variables.



Quantum: some joint entropies not physical.

$$\cancel{S(\rho, B)}$$

→ Replace constraints by data processing. (Chaves, Majenz, Gross, Nat. Comm.'15).

$$H(X, Y, \Lambda) = H(X) + H(Y) + H(\Lambda)$$

$$H(M|X, \Lambda) = 0$$

$$H(B|Y, M, \Lambda) = 0$$

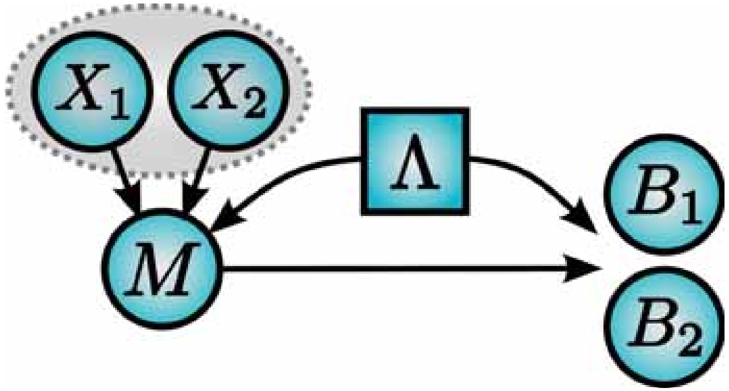
Only non-trivial inequality

$$S(\rho) \geq I(X : Y, B)$$

Also follows directly from the Holevo bound.

Fine-graining a bit more

We can fine-grain by adapting the graph to a fixed number of measurements



Get the nontrivial inequality

$$S(\rho) \geq I(X_1 : B_1) + I(X_2 : B_2) + I(X_1 : X_2|B_1) - I(X_1 : X_2)$$

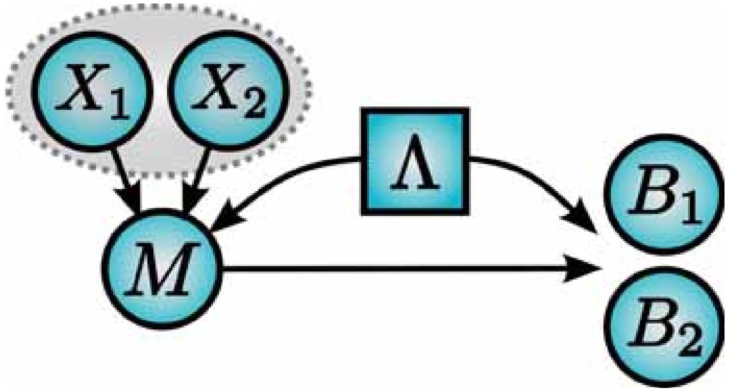
Generalising

$$S(\rho) \geq \sum_{i=1}^{l} I(X_i : B_i) + \sum_{i=2}^{l} I(X_1 : X_i|B_i) - \sum_{i=1}^{l} H(X_1) + H(X_1, \ldots, X_l)$$

Reminiscent of Information Causality, but here: classical corr. / quantum comm.
IC: quantum corr. / classical comm.

Fine-graining a bit more

We can fine-grain by adapting the graph to a fixed number of measurements



Get the nontrivial inequality

$$S(\rho) \geq I(X_1 : B_1) + I(X_2 : B_2) + I(X_1 : X_2|B_1) - I(X_1 : X_2)$$

Valid for arbitrary number of inputs/outputs
but does not distinguish quantum from classical.

Generalising

$$S(\rho) \geq \sum_{i=1}^{l} I(X_i : B_i) + \sum_{i=2} I(X_1 : X_i|B_i) - \sum_{i=1} H(X_1) + H(X_1, \ldots, X_l)$$

Reminiscent of Information Causality, but here: classical corr. / quantum comm.
IC: quantum corr. / classical comm.


classical
I AM NOT A DOG

Convex optimisation method

Decompose observed data over deterministic strategies

$$m = g_\lambda(x)$$
$$b = f_\lambda(y, m)$$

$$p(b|xy) = \sum_{\lambda,m} q_\lambda \delta_{b,f_\lambda(y,m)} \delta_{m,g_\lambda(x)}$$

Enough to consider message dimension = number of preparations → finite no. of strategies

Convex optimisation method

Decompose observed data over deterministic strategies

$$m = g_\lambda(x) \qquad b = f_\lambda(y,m)$$

$$p(b|xy) = \sum_{\lambda,m} q_\lambda \delta_{b,f_\lambda(y,m)} \delta_{m,g_\lambda(x)}$$

Enough to consider message dimension = number of preparations → finite no. of strategies

$$\boxed{\min_{\mathbf{q}} H(M) \text{ subject to } \mathbf{A}\mathbf{q} = \mathbf{p},\ q_\lambda \geq 0,\ \sum_\lambda q_\lambda = 1}$$

$$\left.\begin{array}{r} H(M) \text{ concave in } \mathbf{q} \\ \mathbf{q} \text{ lives in polytope} \end{array}\right\}$$ Enough to check extremal points

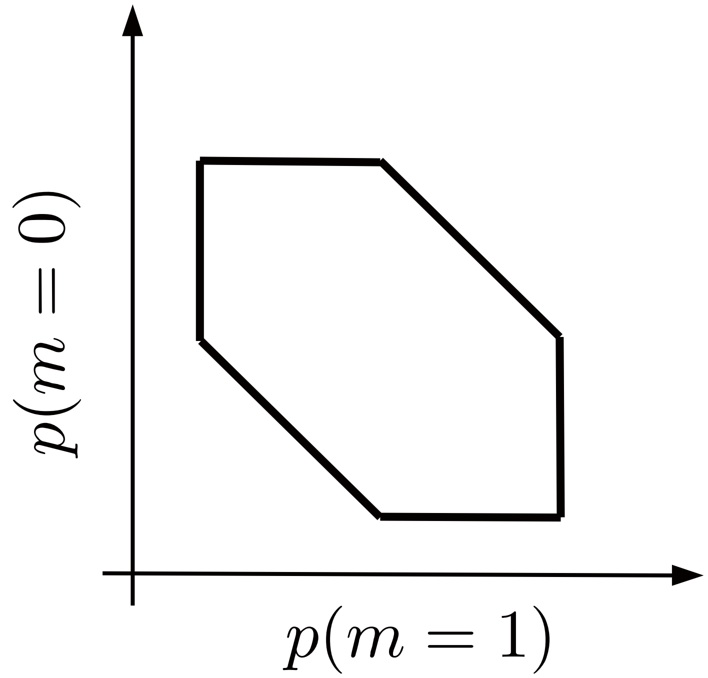
To reduce complexity

Size of polytope is intractable
→ Note: to evaluate the entropy we only need the distribution

$$p(m) = \sum_{\lambda,x} p(m|x,\lambda)p(x)q_\lambda = \frac{1}{n}\sum_{\lambda,x} p(m|x,\lambda)q_\lambda$$

Observed data implies linear constraints on this.
Find polytope by a sequence of linear programs.

→ significantly reduces complexity.



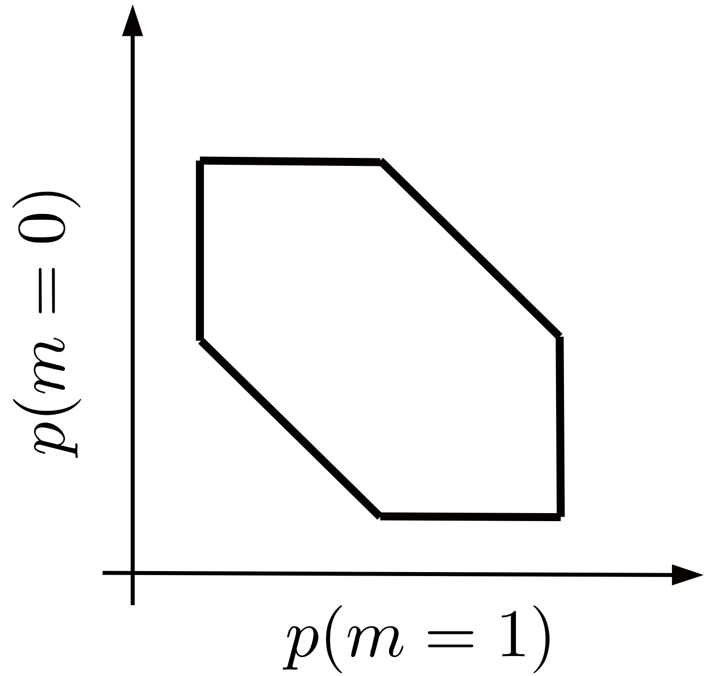
To reduce complexity

Size of polytope is intractable
→ Note: to evaluate the entropy we only need the distribution

$$p(m) = \sum_{\lambda,x} p(m|x,\lambda)p(x)q_\lambda = \frac{1}{n}\sum_{\lambda,x} p(m|x,\lambda)q_\lambda$$

Observed data implies linear constraints on this.
Find polytope by a sequence of linear programs.

→ significantly reduces complexity.



In addition, consider only linear functions of data : dimension witnesses.

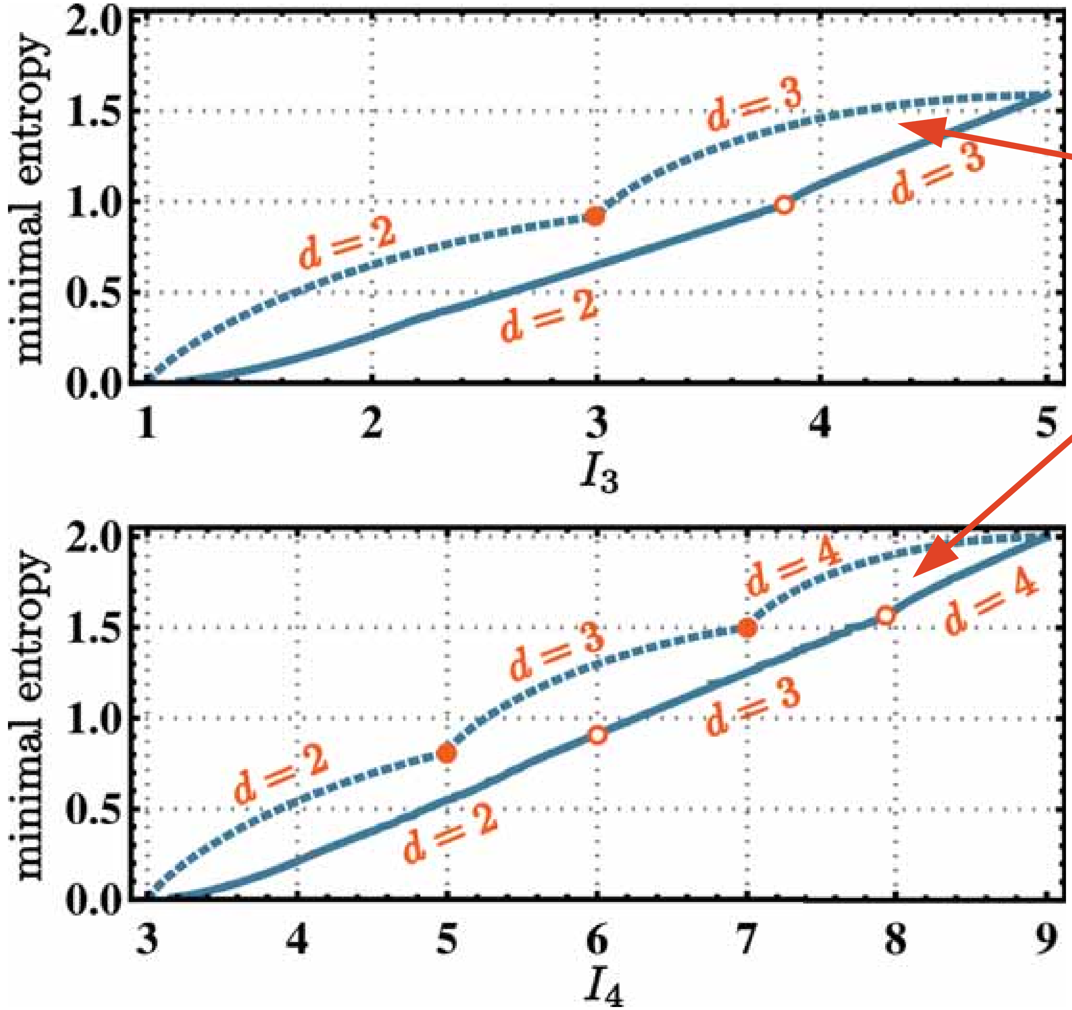
$$\mathbf{p} = \mathbf{A}\mathbf{q} \to \mathbf{I}\mathbf{p} = \mathbf{I}\mathbf{A}\mathbf{q}$$

Use witness of Gallego *et al.*, PRL'10, for *n* preparations, *n-1* measurements, binary ouputs.

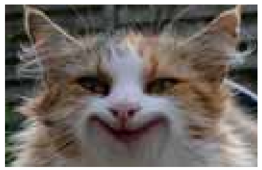
Convex optimisation result

Compare bound for classical messages with numerical optimisation for quantum messages.

The classical bound is tight.



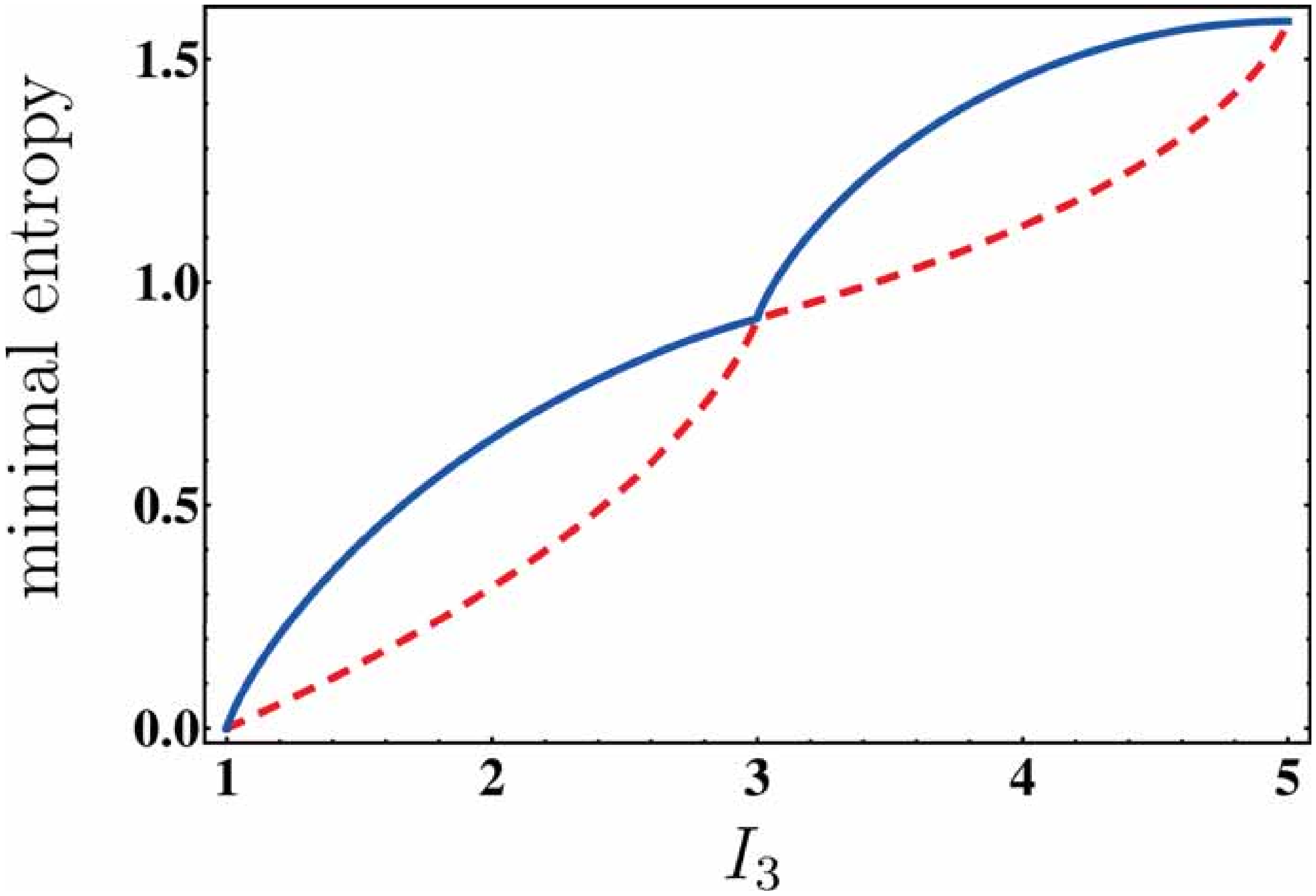
Quantum advantage!



Notice: No advantage by increasing quantum message dimension.

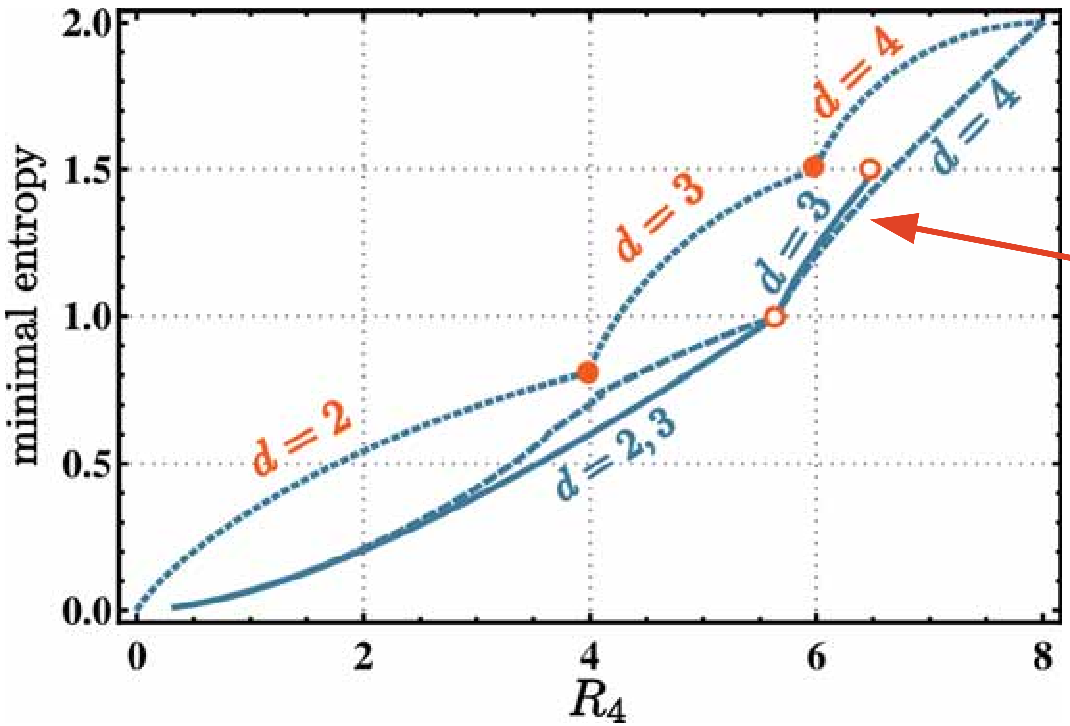
Compare the entropic and convex optimisation approaches

Comparison for a <u>specific</u> observed distribution (saturating the convex opt. bound).
→ the entropic approach is clearly not tight.



Possible advantage of higher dimensions

Random Access Code for 4 preparation and 2 measurements, binary output

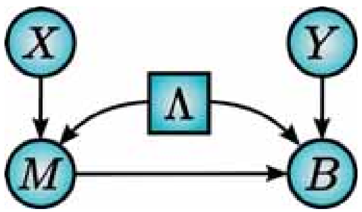


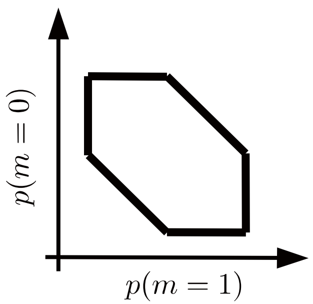
Possible advantage of dim. 4 over dim. 3.

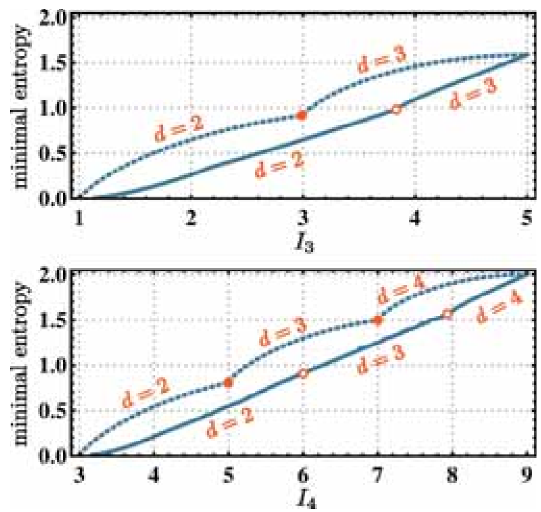
$$R_4 = E_{11} + E_{12} + E_{21} - E_{22} - E_{31} + E_{32} - E_{41} - E_{42}$$

Summary

- Device-independent tests of entropy in prepare & measure scenario.
- Two approaches: entropic based on causal inference / convex optimisation.
- Entropic approach : general but non-tight.
- Convex optimisation approach : fixed numbers of inputs, output, but tight.
- Quantum strategies show advantage over classical:
  achieve same dimension witness value with less entropy.







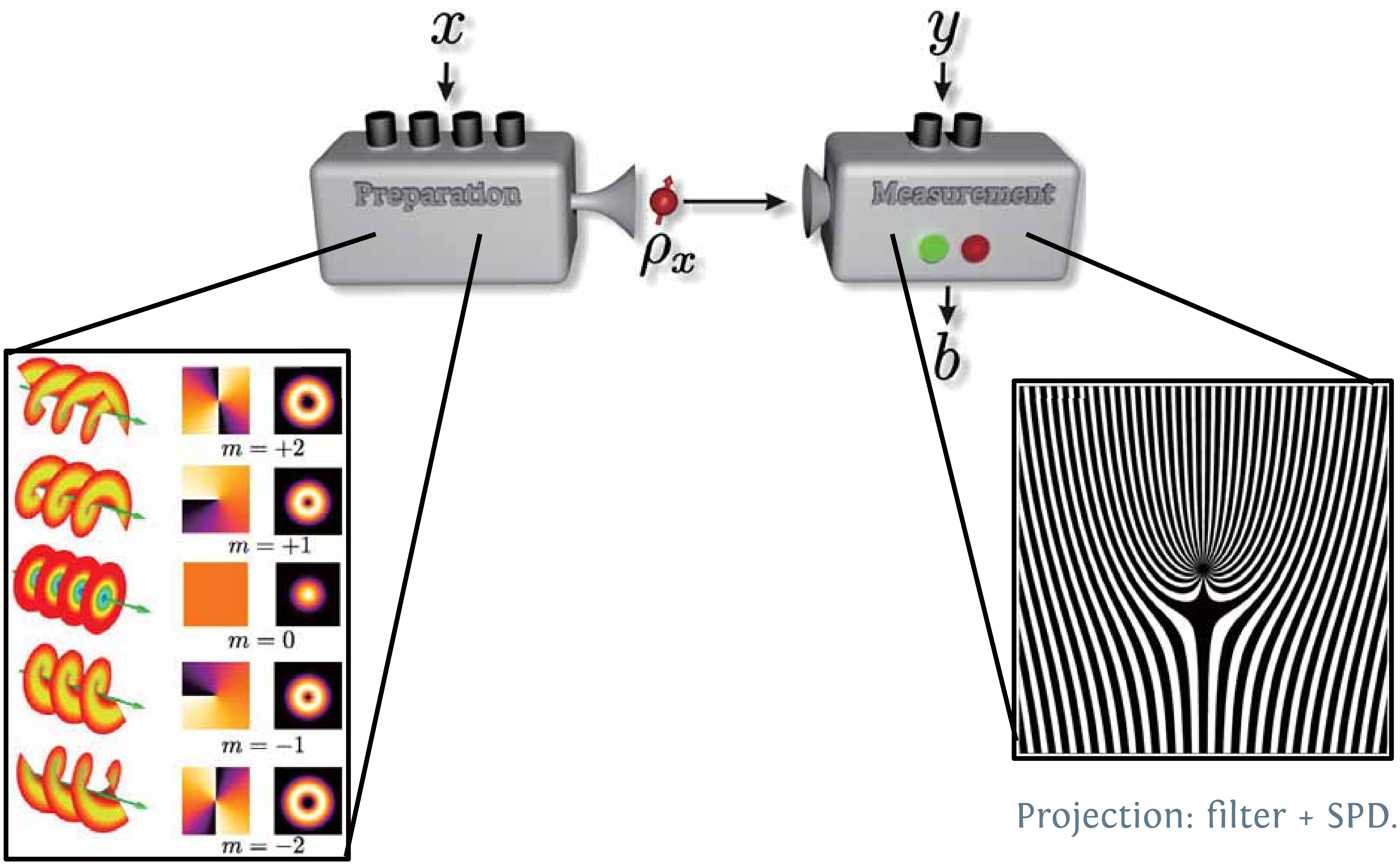
Is there a killer app?

Secure communication?

Randomness generation?

Experiment under way...

Stephen Walborn group, Rio de Janeiro, Brazil.
Optical implementation with single photons.



Orbital angular momentum

Projection: filter + SPD.

Thanks for your attention!

Strategy saturating the convex optimisation bound for witness I_n:

$$\text{for } x \leq d-2 \text{ send } m = x$$

$$\text{for } x = d-1 \text{ send } m = \begin{cases} 0 \text{ with prob. } p \\ x \text{ with prob. } 1-p \end{cases}$$

$$\text{otherwise send } m = 0$$

$$\text{where } p = \frac{1}{2}(L_d - I_n)$$

L_d : classical bound for dimension d

I_n : witness value