Title: Data tables, dimension witnesses, and QKD

Date: May 13, 2011 02:50 PM

URL: http://pirsa.org/11050045

Abstract: We address the problem of testing the dimensionality of classical and quantum systems in a Ã¢ÂÂ€ÂÂ˜black-boxÃ¢ÂÂ€ÂÂ™ scenario. Imagine two uncharacterized devices. The first one allows an experimentalist to prepare a physical system in various ways. The second one allows the experimentalist to perform some measurement on the system. After collecting enough statistics, the experimentalist obtains a Ã¢ÂÂ€ÂÂ˜data tableÃ¢ÂÂ€ÂÂ™, featuring the probability distribution of the measurement outcomes for each choice of preparation (of the system) and of measurement. Here, we develop a general formalism to assess the minimal dimensionality of classical and quantum systems necessary to reproduce a given data table. To illustrate these ideas, we provide simple examples of classical and quantum Ã¢ÂÂ€ÂÂ˜dimension witnessesÃ¢ÂÂ€ÂÂ™. In general quantum systems are more economical than classical ones in terms of dimensionality, in the sense that there exist data tables obtainable from quantum systems of dimension d which can only be generated from classical systems of dimension strictly greater than d. By drawing connections to communication complexity one can find data tables for which this classical/quantum separation is dramatic. Finally, these ideas can also be used to demonstrate security of one-way QKD in a semi-device-independent scenario, in which devices are uncharacterized, but only assumed to produce quantum systems of a given dimension.

Data tables, dimension witnesses and QKD

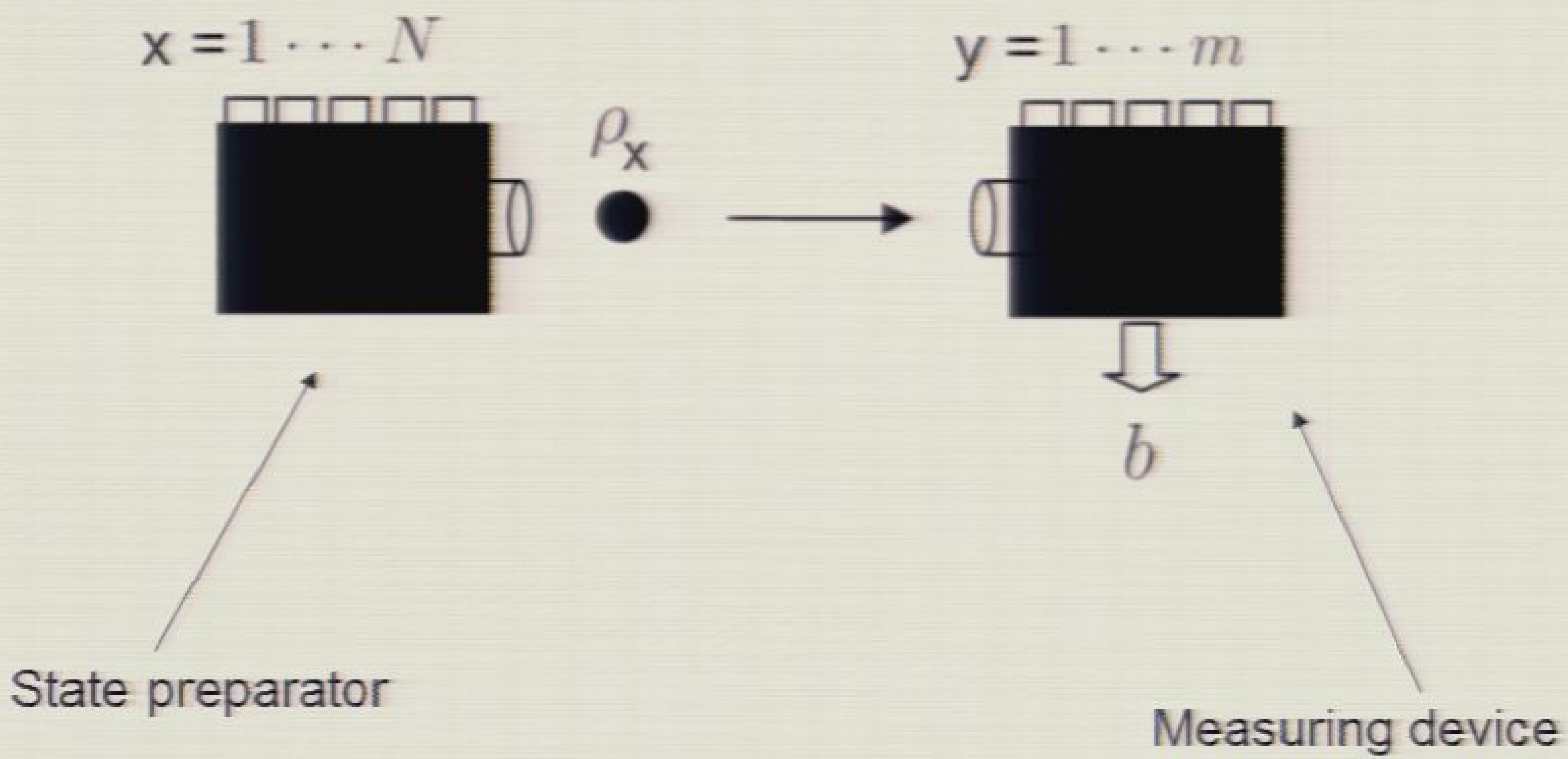
Nicolas Brunner

Joint work with: Rodrigo Gallego, Chris Hadley, Antonio Acin
Jonathan Barrett, Christian Gogolin
Marcin Pawlowski

University of BRISTOL

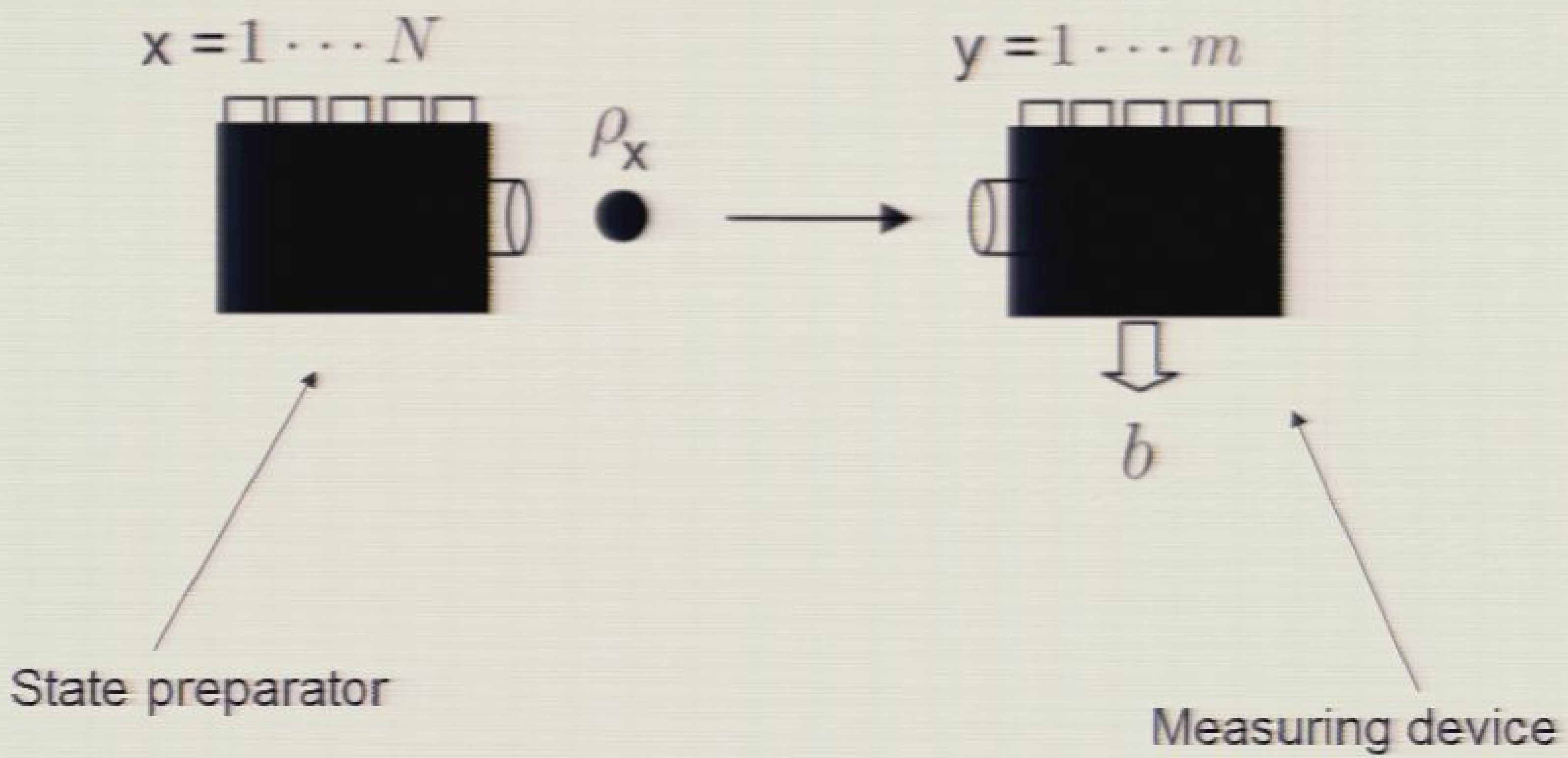
EPSRC
Engineering and Physical Sciences

Setup



x = $1 \cdots N$
ρ_x
y = $1 \cdots m$
b
State preparator
Measuring device

Setup



$\Rightarrow$ P(b|x,y)

Can we make a device-independent (DI) statement about the dimensionality of ρx?

Data Table

	m1		m2		
	+1	-1	+1	-1	...
P1	P(+1¦1,1)	P(-1¦1,1)	P(+1¦1,2)	P(-1¦1,2)	
P2	P(+1¦2,1)	P(-1¦2,1)	P(+1¦2,2)	P(-1¦2,2)	
...					

Given a data table, can we find useful bounds on the classical and quantum dimensions?

Separation between classical and quantum systems for a given dimension

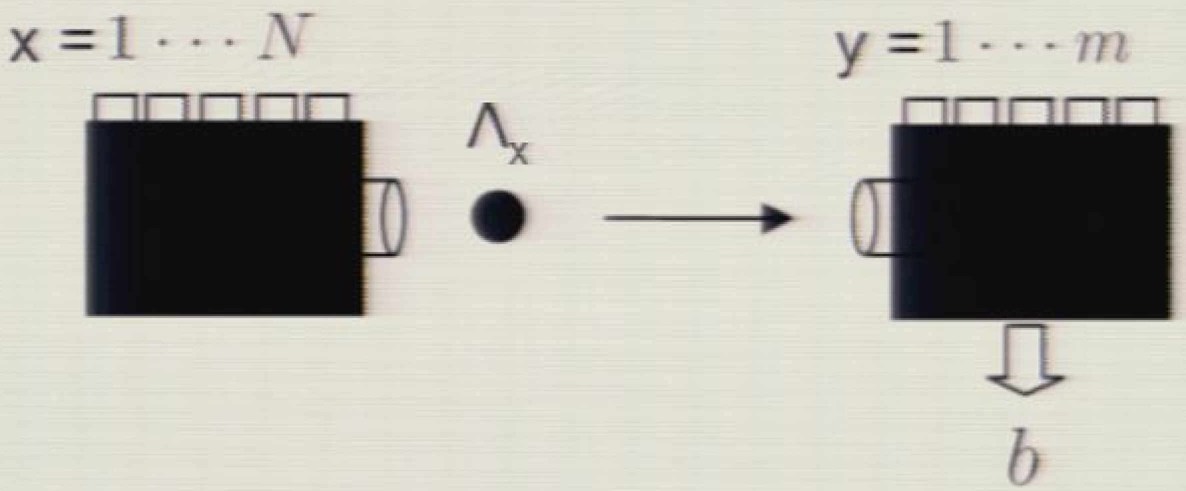
Is this quantum advantage interesting/useful?

N. Harrigan, T. Rudolph, and S. Aaronson, arXiv:0709.1149

Here...

- Present simple formalism to handle data tables
  Method for DI tests of classical and quantum dimension
- Foundational interest, e.g. ontological models (cf talk of Jon Barrett)
- Application in QKD

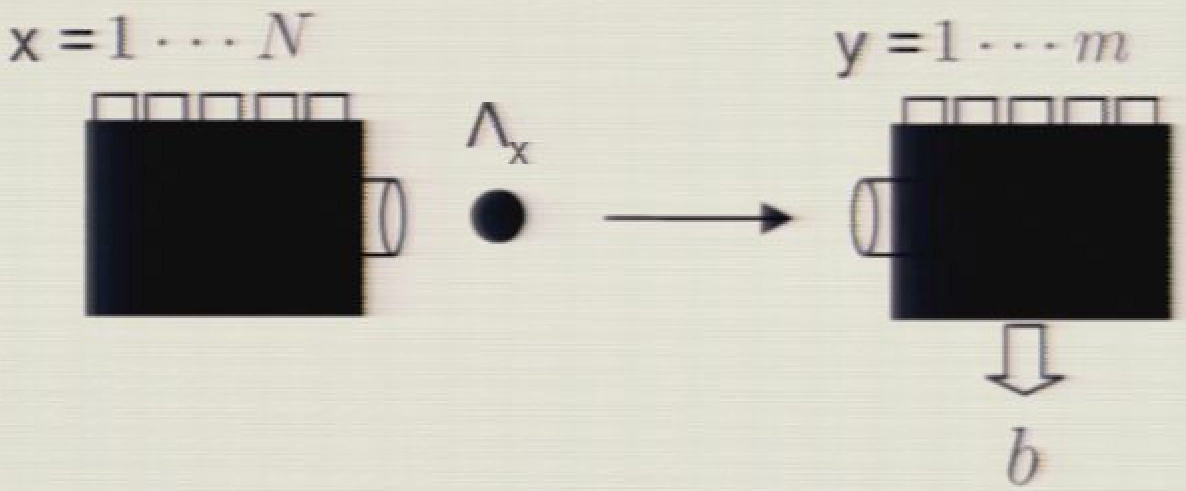
Testing classical systems



Λ_x is a classical state of dimension d, ie a probability distribution over dits

Experiment = se $\vec{E}$ of correlator: $E_{xy} = P(b=+1|x,y) - P(b=-1|x,y)$

Testing classical systems



Λ_x is a classical state of dimension d, ie a probability distribution over dits

Experiment = se $\vec{E}$ of correlator: $E_{xy} = P(b=+1|x,y) - P(b=-1|x,y)$

Dimension witness $\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq C_d$

(~Bell inequality for data tables)

R. Gallego, NB, S. Hadley, A. Acin, PRL 2010

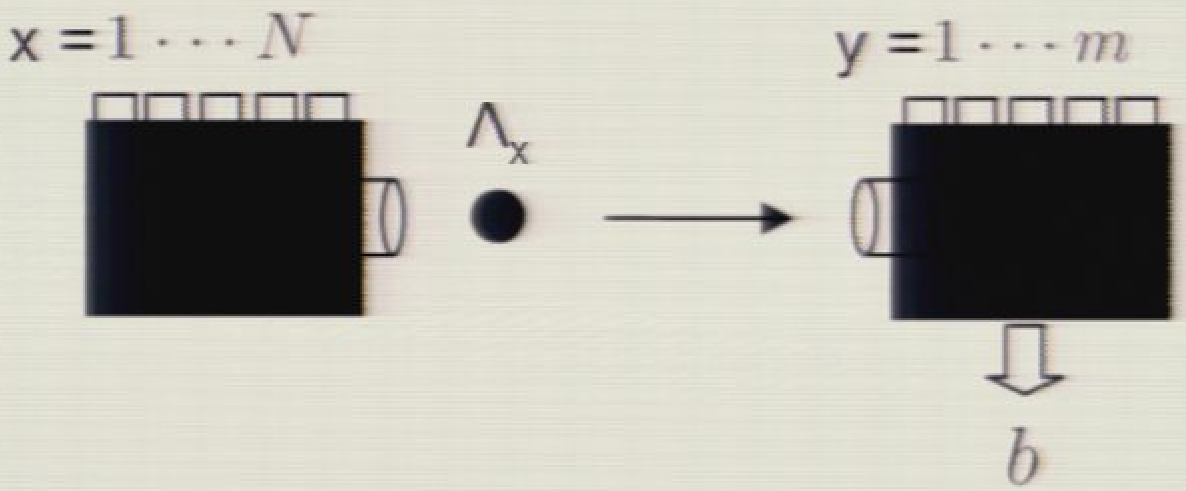
Geometry

Each exp $\vec{E}$ nent can be viewed as vector in R^{Nm}

Simple observation: if $N \le d$ then all experiments can be reproduced classically

$N > d$ (more preparations than tested

Testing classical systems



Λ_x is a classical state of dimension d, ie a probability distribution over dits

Experiment = se $\vec{E}$ of correlators $E_{xy} = P(b=+1|x,y) - P(b=-1|x,y)$

Dimension witness $\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq C_d$

(~Bell inequality for data tables)

Geometry

Each exp $\vec{E}$ nent can be viewed as vector in R^{Nm}

Simple observation: if N<=d then all experiments can be reproduced classically

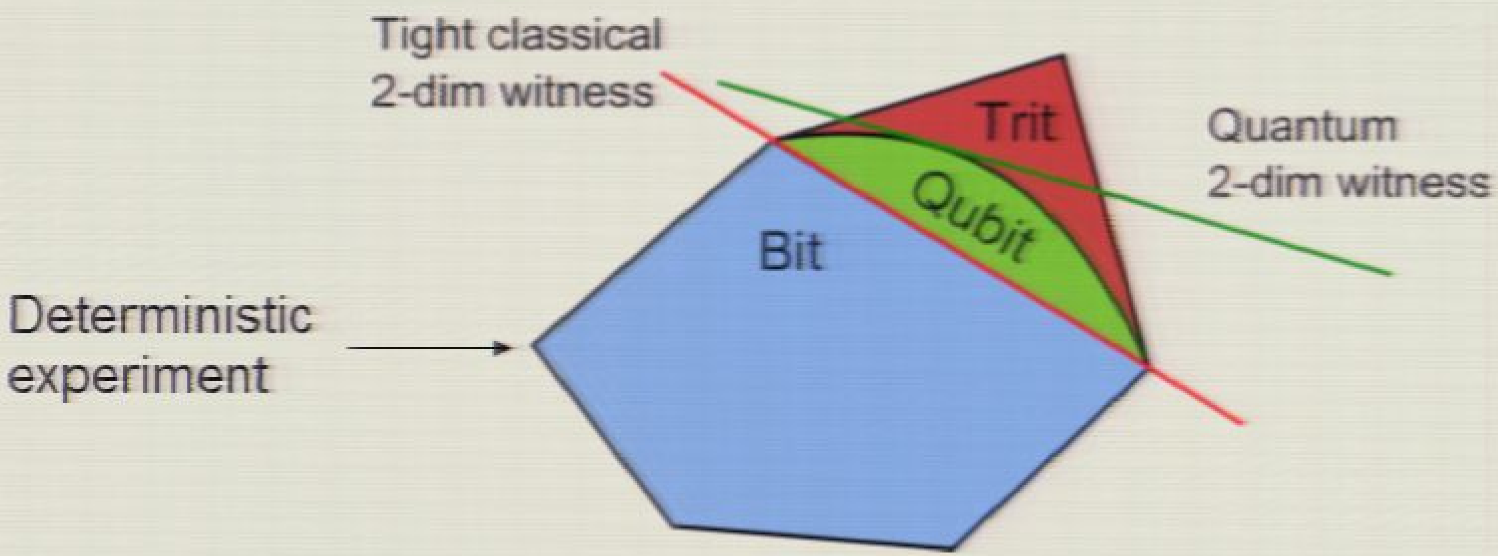
$N > d$ (more preparations than tested

Geometry

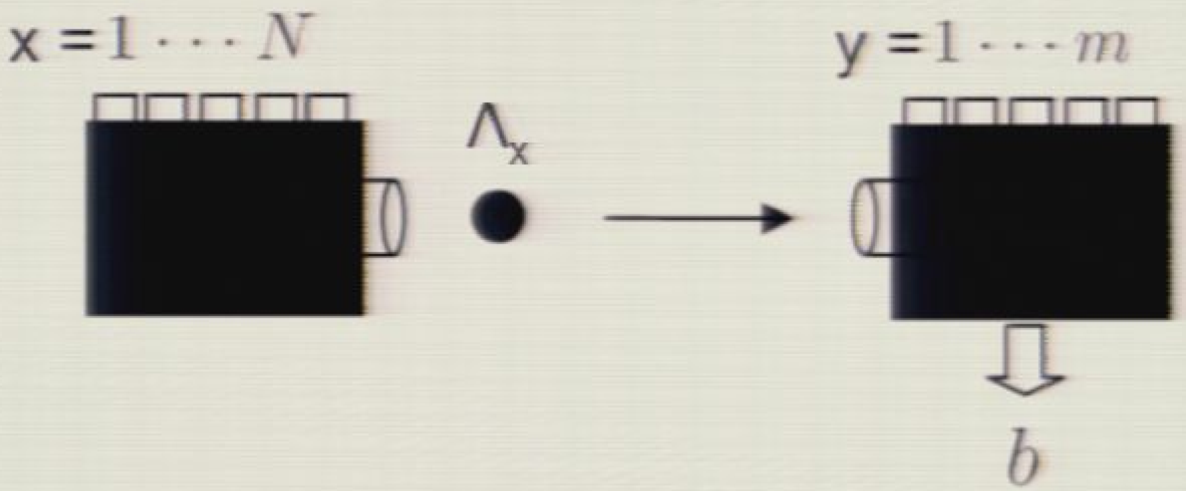
Each exp $\vec{E}$ nent can be viewed as vector in R^{Nm}

Simple observation: if N<=d then all experiments can be reproduced classically

⇒ N > d (more preparations than tested



Testing classical systems



Λ_x is a classical state of dimension d, ie a probability distribution over dits

Experiment = se $\vec{E}$ of correlator: $E_{xy} = P(b = +1|x, y) - P(b = -1|x, y)$

Dimension witness $\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq C_d$

(~Bell inequality for data tables)

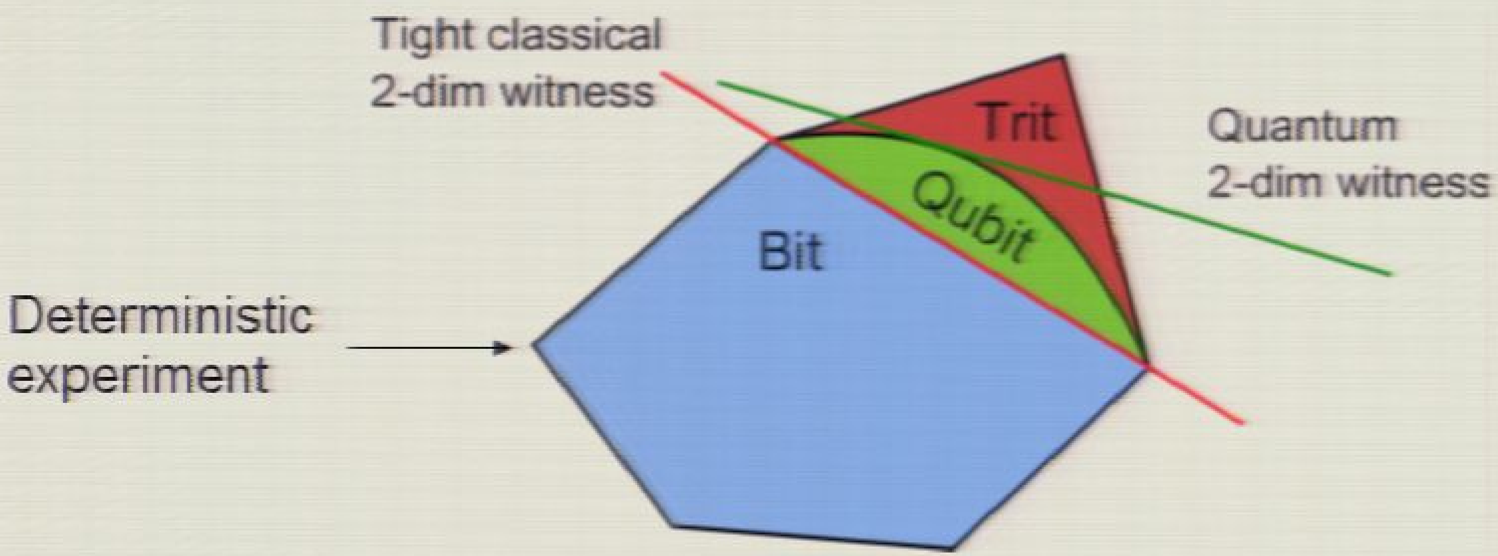
R. Gallego, NB, S. Hadley, A. Acin, PRL 2010

Geometry

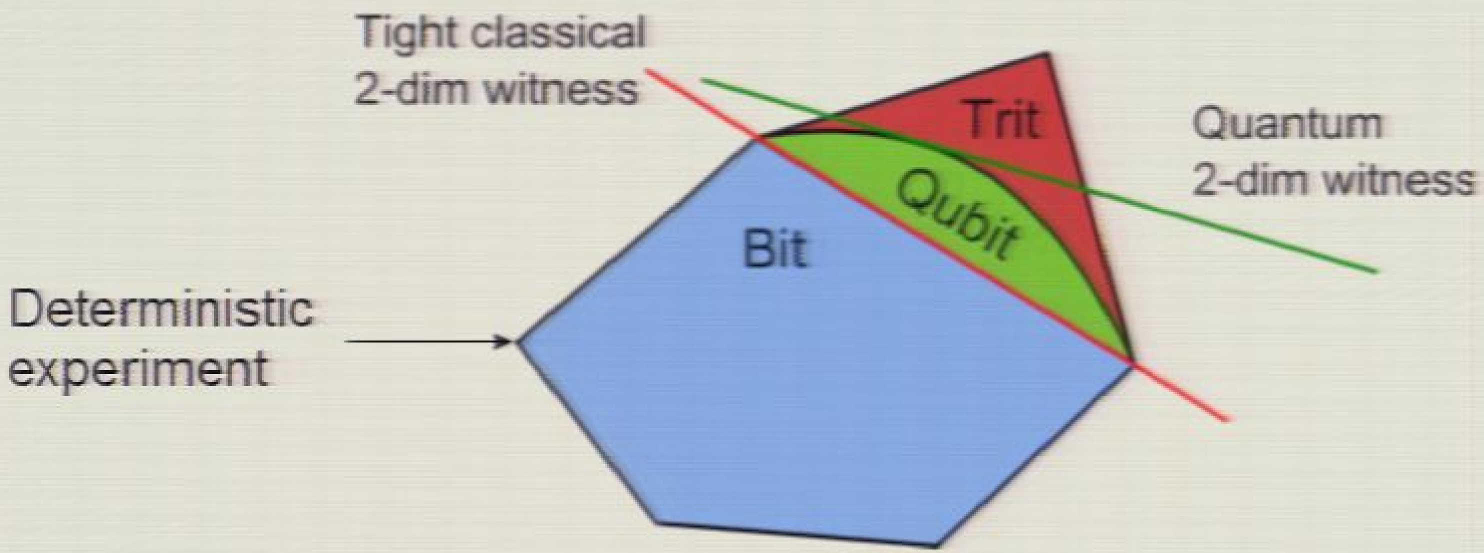
Each exp $\vec{E}$ ment can be viewed as vector in R^{Nm}

Simple observation: if N<=d then all experiments can be reproduced classically

⇒ N > d (more preparations than tested



Geometry



Set of experiments possible with classical systems of dim d is a polytope

→ Facets = Tight classical dim-witness

$$\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq C_d$$

$$\leq Q_d$$

Quantum dimension witness

Example

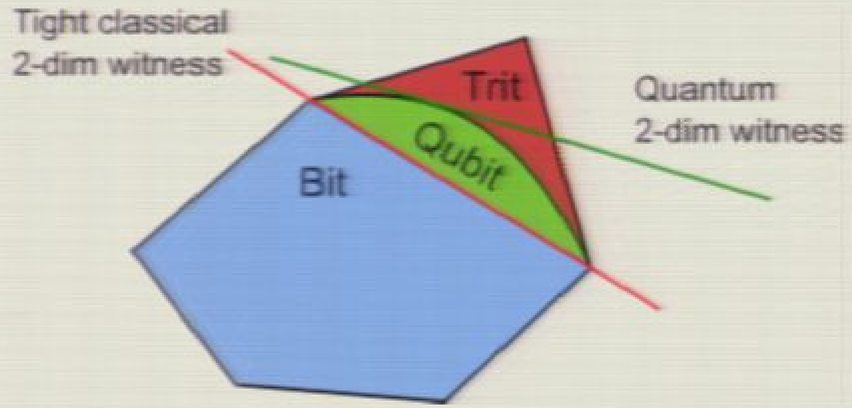
Simplest case: 3 preparations and 2 measurements

$$I_3 \equiv |E_{11} + E_{12} + E_{21} - E_{22} - E_{31}| \leq 3.$$

	M1	M2
P1	+	+
P2	+	-
P3	-	

$\leq$ 3 (bit)

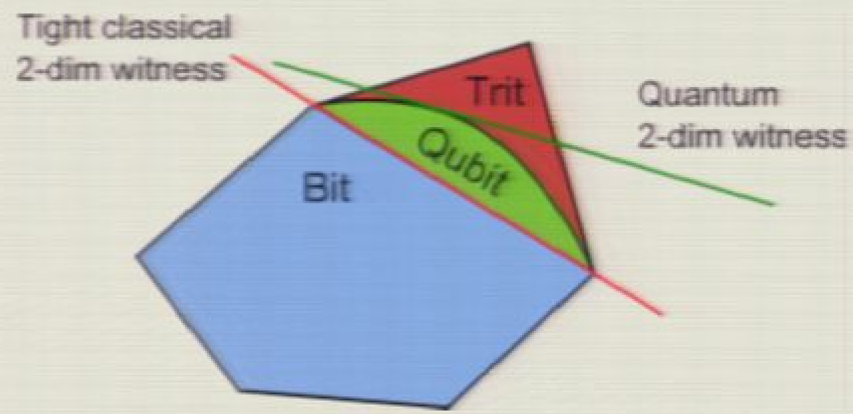
$\leq$ 5 (trit)



Example

Simplest case: 3 preparations and 2 measurements

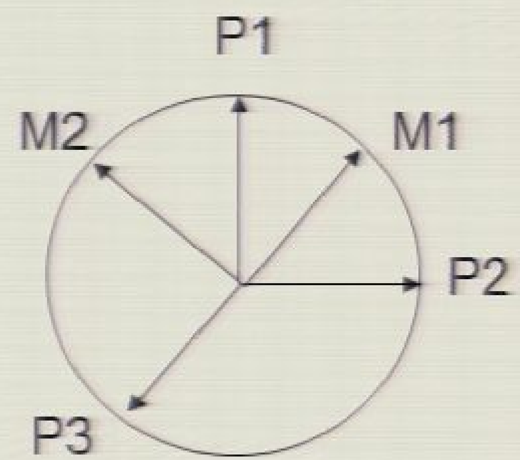
$$I_3 \equiv |E_{11} + E_{12} + E_{21} - E_{22} - E_{31}| \leq 3.$$



	M1	M2
P1	+	+
P2	+	-
P3	-	

$\leq$ 3 (bit)

$\leq$ 5 (trit)



With qubits: $I_3 \leq 1 + 2\sqrt{2} \approx 3.8284$

Importance of 3rd preparation: CHSH is not a witness (Leggett-Garg not DI)

Quantum advantage

What can we do with this quantum advantage?

- Exponential separation (communication complexity)
- Security proof for 1-way QKD

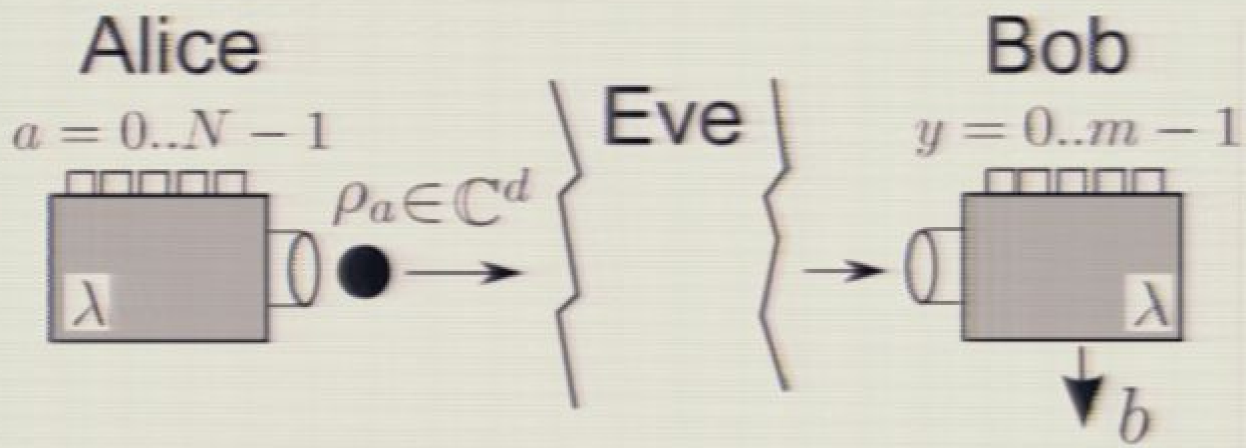
Exponential separation

Family of data tables leading to exponential separation
i.e. feasible with quantum systems of dim d
Unfeasible (even with small errors) with classical systems of dim less than 2^d

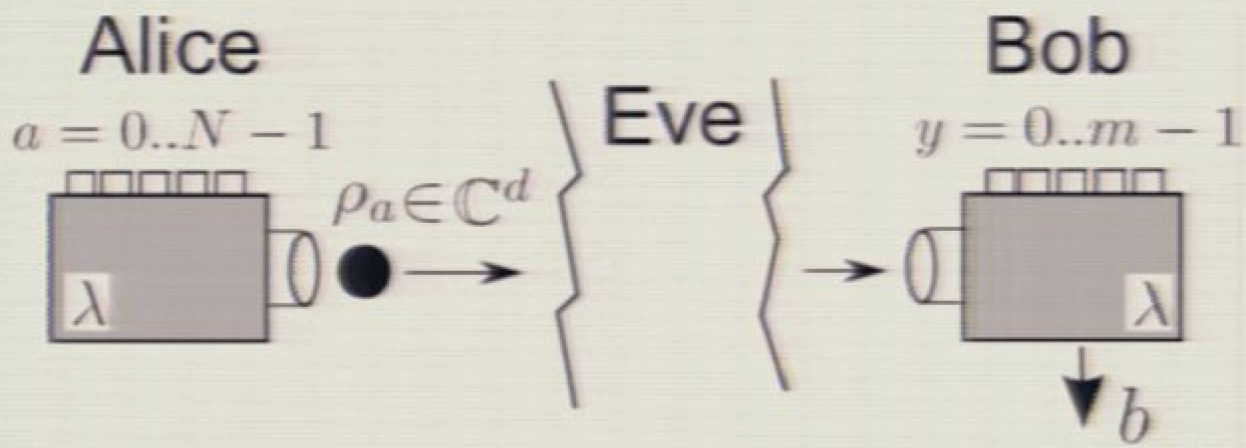
Communication complexity (e.g. Klartag & Regev 2010)

No-go theorem for ontological models (cf talk of Jon Barrett)

QKD



QKD



Semi-DI scenario Non-characterized devices, but systems of bound

Security proof against individual attacks

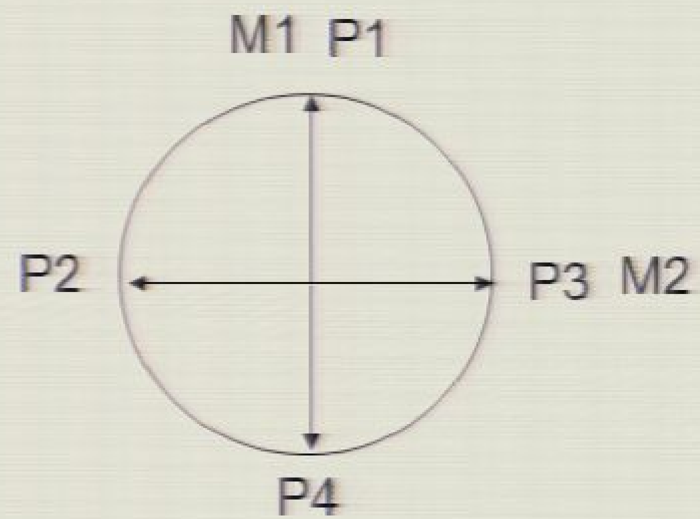
Based on the violation of a dimension witness

Not based on entanglement or nonlocality
(First proof that applies to the one-way case)

BB84

4 qubit preparations ($|+z\rangle$, $|-z\rangle$, $|+x\rangle$, $|-x\rangle$) and 2 measurements (Z,X)

	M1	M2
P1	+1	0
P2	0	-1
P3	0	+1
P4	-1	0



Does not violate any 2-dim classical witness!

Can be reproduced by sending a classical bit

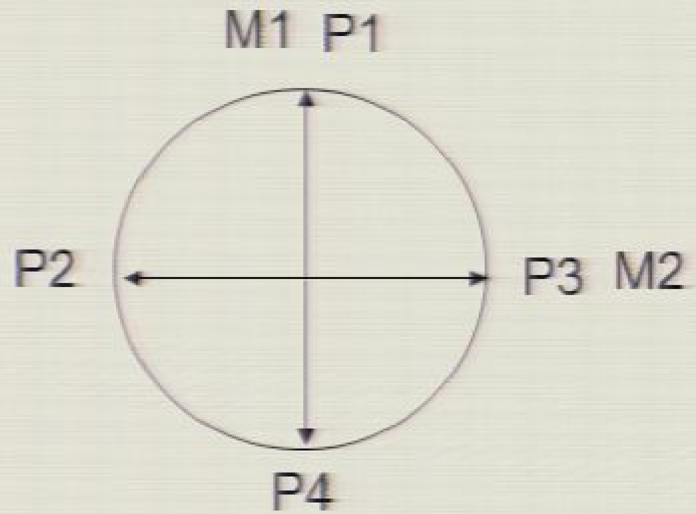
→ **No security in a semi-DI scenario**

BB84

4 qubit preparations (¦+z>, ¦-z>, ¦+x>, ¦-x>) and 2 measurements (Z,X)

asis → a0, outcome → a1

a0	a1		M1	M2
0	0	P1	+1	0
1	0	P2	0	-1
1	1	P3	0	+1
0	1	P4	-1	0



Does not violate any 2-dim classical witness!

Can be reproduced by sending a classical bit

No security in a semi-DI scenario

Strategy $\lambda=0$: Alice sends $m=a0+a1$, Bob outputs $b=m+y$

If $y=a0$, then $b=a1$ else $b=a1+1$

$\lambda=1$: Alice sends $m=a1$, Bob outputs $b=m=a1$

Dimension witness and random access codes

	M1	M2
P1	+	+
P2	+	-
P3	-	+
P4	-	-

<=4 (for classical bits)

Dimension witness and random access codes

a0	a1		M1	M2
0	0	P1	+	+
0	1	P2	+	-
1	0	P3	-	+
1	1	P4	-	-

<=4 (for classical bits)

This witness corresponds exactly to a 1-out-of-2 random access code (RAC)

$\Rightarrow$ P_guess = (I + 8) / 16

I <= 4 corresponds to P_guess <= ¾
(classical limit for RAC)

Dimension witness and random access codes

a0	a1		M1	M2
0	0	P1	+	+
0	1	P2	+	-
1	0	P3	-	+
1	1	P4	-	-

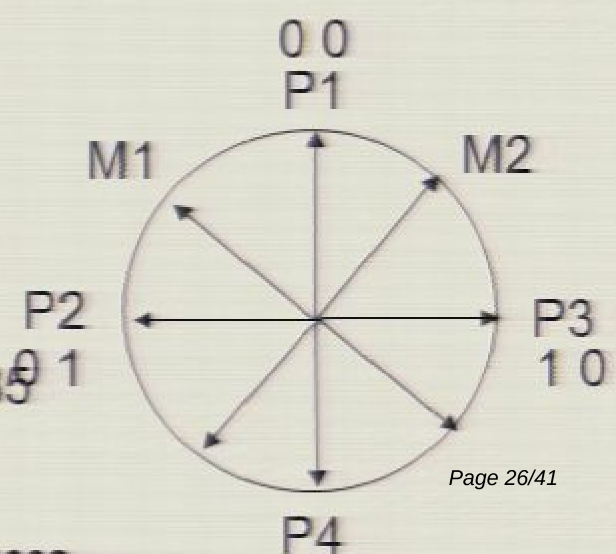
<=4 (for classical bits)

This witness corresponds exactly to a 1-out-of-2 random access code (RAC)

→ P_guess = (I+8)/16

I <= 4 corresponds to P_guess <= ¾
(classical limit for RAC)

For qubits, P_guess <= $\cos^2(\pi/8) \sim 0.85$



Security proof

Individual attacks: Csiszar & Korner (197 $I(A:B) > I(A:E)$

$P_B > P_E$ ⟹ Positive key rate

Proof based on a result by R. König (PhD thesis)

F_n : set of balanced boolean functions on n-bit strings

Alice receives a (uniformly chosen) n-bit string; Bob receives a function in F_n
Alice sends s qubits to Bob. Bob's probability of guessing is bounded by

$$P_n \leq \frac{1}{2}\left(1 + \sqrt{\frac{2^s - 1}{2^n - 1}}\right)$$

Security proof

We have n=2, s=1 $$P_B(a_0) + P_B(a_1) + P_B(a_0 \oplus a_1) \le \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

Assume Bob and Eve collaborate

$$P_{BE}(a_0) + P_{BE}(a_1) + P_{BE}(a_0 \oplus a_1) \ge 2P_B(a_0) + 2P_E(a_1) - 1$$

$$\begin{aligned} P_{BE}(a_0 \oplus a_1) &\ge P_{BE}(a_0, a_1) \\ &\ge P_{BE}(a_0) + P_{BE}(a_1) - 1 \end{aligned}$$

$$P_{BE}(a_i) \ge P_B(a_i)$$

⇒ $$P_B(a_0) + P_E(a_1) \le \frac{5+\sqrt{3}}{4}$$ ⇒ $$P_B + P_E \le \frac{5+\sqrt{3}}{4}$$

⇒ $P_B > P_E$ when $P_B > \frac{5+\sqrt{3}}{8} \approx 0.8415$

Security proof

We have n=2, s=1 $$P_B(a_0) + P_B(a_1) + P_B(a_0 \oplus a_1) \leq \frac{3}{2}\left(1 + \frac{1}{\sqrt{3}}\right)$$

Assume Bob and Eve collaborate

$$P_{BE}(a_0) + P_{BE}(a_1) + P_{BE}(a_0 \oplus a_1) \geq 2P_B(a_0) + 2P_E(a_1) - 1$$

$$\begin{aligned} P_{BE}(a_0 \oplus a_1) &\geq P_{BE}(a_0, a_1) \\ &\geq P_{BE}(a_0) + P_{BE}(a_1) - 1 \end{aligned}$$

$$P_{BE}(a_i) \geq P_B(a_i)$$

$\Rightarrow$ $P_B(a_0) + P_E(a_1) \leq \frac{5+\sqrt{3}}{4}$ $\Rightarrow$ $P_B + P_E \leq \frac{5+\sqrt{3}}{4}$

$\Rightarrow$ $P_B > P_E$ when $P_B > \frac{5+\sqrt{3}}{8} \approx 0.8415$

Qubits can reach $P_B = \cos^2(\pi/8)) \approx 0.8536$

Security

Dimension witness and random access codes

a0	a1		M1	M2
0	0	P1	+	+
0	1	P2	+	-
1	0	P3	-	+
1	1	P4	-	-

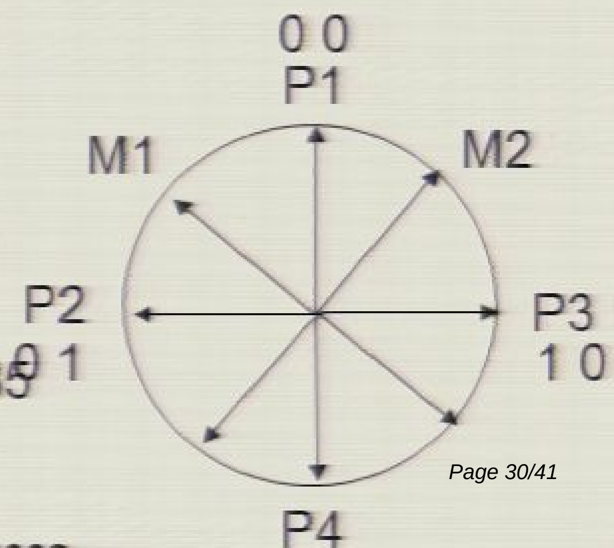
<=4 (for classical bits)

This witness corresponds exactly to a 1-out-of-2 random access code (RAC)

→ P_guess = (I+8)/16

I <= 4 corresponds to P_guess <= ¾ (classical limit for RAC)

For qubits, P_guess <= $\cos^2(\pi/8) \sim 0.85$



Security proof

We have n=2, s=1 $P_B(a_0)+P_B(a_1)+P_B(a_0\oplus a_1)\leq \frac{3}{2}\left(1+\frac{1}{\sqrt{3}}\right)$

Assume Bob and Eve collaborate

$$P_{BE}(a_0)+P_{BE}(a_1)+P_{BE}(a_0\oplus a_1)\geq 2P_B(a_0)+2P_E(a_1)-1$$

$$\begin{aligned} P_{BE}(a_0\oplus a_1) &\geq P_{BE}(a_0,a_1) \\ &\geq P_{BE}(a_0)+P_{BE}(a_1)-1 \end{aligned}$$

$$P_{BE}(a_i)\geq P_B(a_i)$$

$\Rightarrow$ $P_B(a_0)+P_E(a_1)\leq \frac{5+\sqrt{3}}{4}$ $\Rightarrow$ $P_B+P_E\leq \frac{5+\sqrt{3}}{4}$

$\Rightarrow$ $P_B > P_E$ when $P_B > \frac{5+\sqrt{3}}{8}\approx 0.8415$

Qubits can reach $P_B=\cos^2(\pi/8))\approx 0.8536$

Security

Is this semi-DI approach relevant?

Alice is Semi-DI (preparations are of given dimension but non-characterized)
Bob is fully DI
Relaxation compared to usual security proofs

Works for 1-way configuration

Security only against a specific type of attacks (what about more general ones?)

Conclusion

- Data tables
- DI tests of classical and quantum dimension
- Ontological models; exponential separation
- Semi-DI security of 1-way QKD

Conclusion

- Data tables
- DI tests of classical and quantum dimension
- Ontological models; exponential separation
- Semi-DI security of 1-way QKD

Open Questions

- Connection to contextuality (preparation contextuality)
- Generalized models
- Connection to nonlocality (RAC, Information Causality)

Conclusion

- Data tables
- DI tests of classical and quantum dimension
- Ontological models; exponential separation
- Semi-DI security of 1-way QKD

Dimension witness and random access codes

a0	a1		M1	M2
0	0	P1	+	+
0	1	P2	+	-
1	0	P3	-	+
1	1	P4	-	-

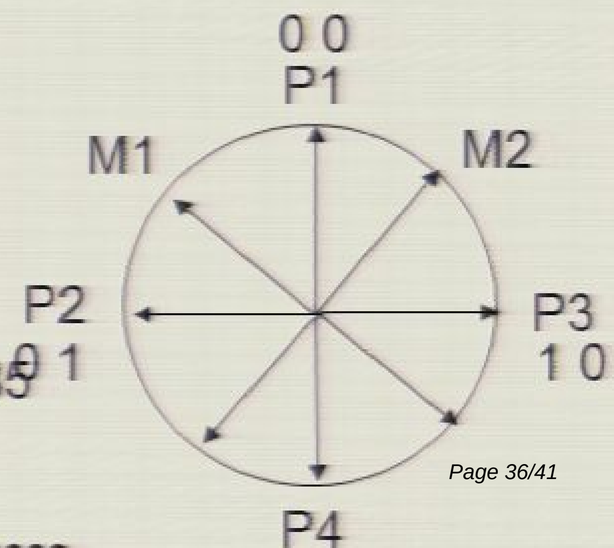
<=4 (for classical bits)

This witness corresponds exactly to a 1-out-of-2 random access code (RAC)

⇒ P_guess = (I+8)/16

I <= 4 corresponds to P_guess <= ¾
(classical limit for RAC)

For qubits, P_guess <= $\cos^2(\pi/8) \sim 0.85$



Conclusion

- Data tables
- DI tests of classical and quantum dimension
- Ontological models; exponential separation
- Semi-DI security of 1-way QKD

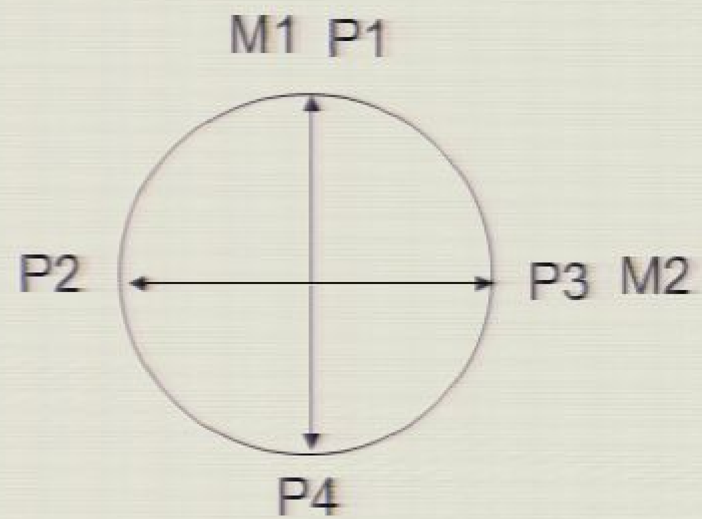
Open Questions

- Connection to contextuality (preparation contextuality)
- Generalized models
- Connection to nonlocality (RAC, Information Causality)

BB84

4 qubit preparations (|+z>, |-z>, |+x>, |-x>) and 2 measurements (Z,X)

	M1	M2
P1	+1	0
P2	0	-1
P3	0	+1
P4	-1	0

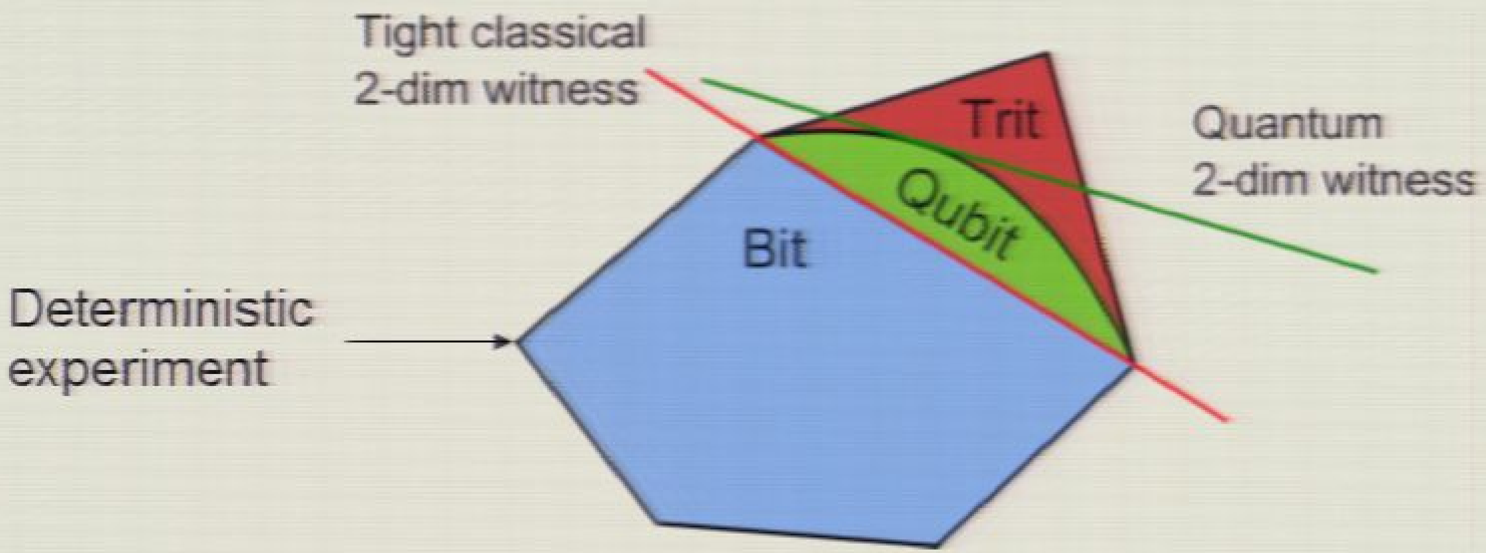


Does not violate any 2-dim classical witness!

Can be reproduced by sending a classical bit

→ **No security in a semi-DI scenario**

Geometry



Set of experiments possible with classical systems of dim d is a polytope

→ Facets = Tight classical dim-witness

$$\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq C_d$$

$$\leq Q_d$$

Quantum dimension witness