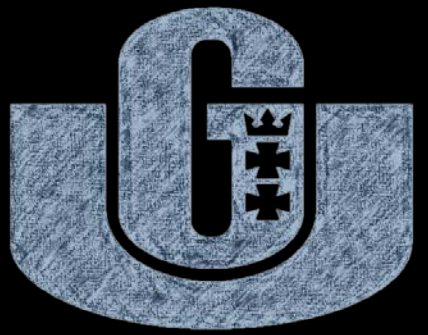


UNIWERSYTET GDAŃSKI

MUTUALLY UNBIASED BASES RANDOM ACCESS CODES SEMI-DEFINITE PROGRAMMING

Marcin Pawłowski

Vienna, 18.9.18

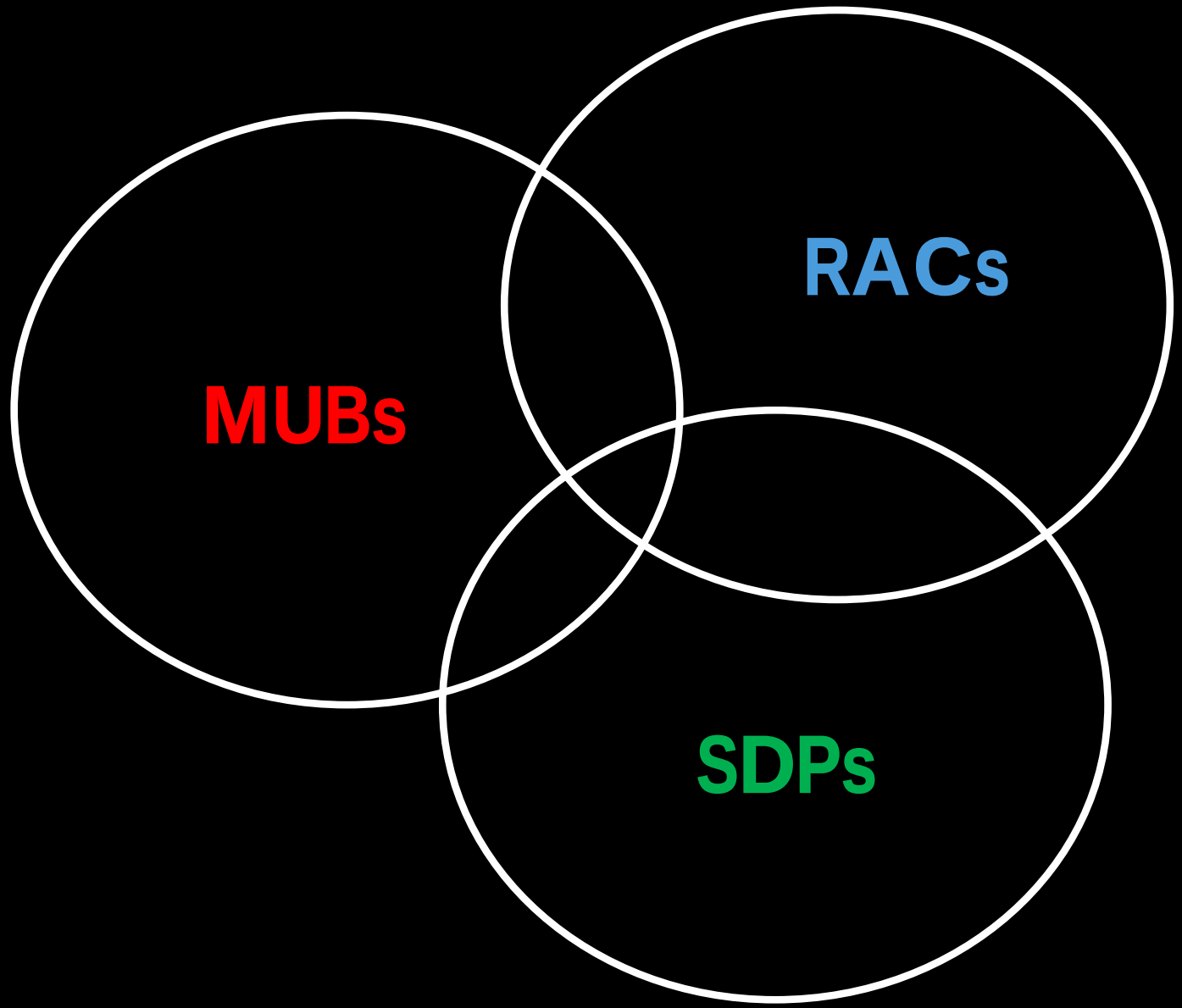
FNP Fundacja na rzec. Nauki Polskiej

NARODOWE CENTRUM NAUKI

CONNECTIONS BETWEEN MUTUALLY UNBIASED BASES AND QUANTUM RANDOM ACCESS CODES

Edgar A. Aguilar, Jakub J. Borkała, Piotr Mironowicz, and Marcin Pawłowski

Phys. Rev. Lett. **121**, 050501



OUTLINE

Bases are **red**,

The codes are **blue**,

Programs are **green**,

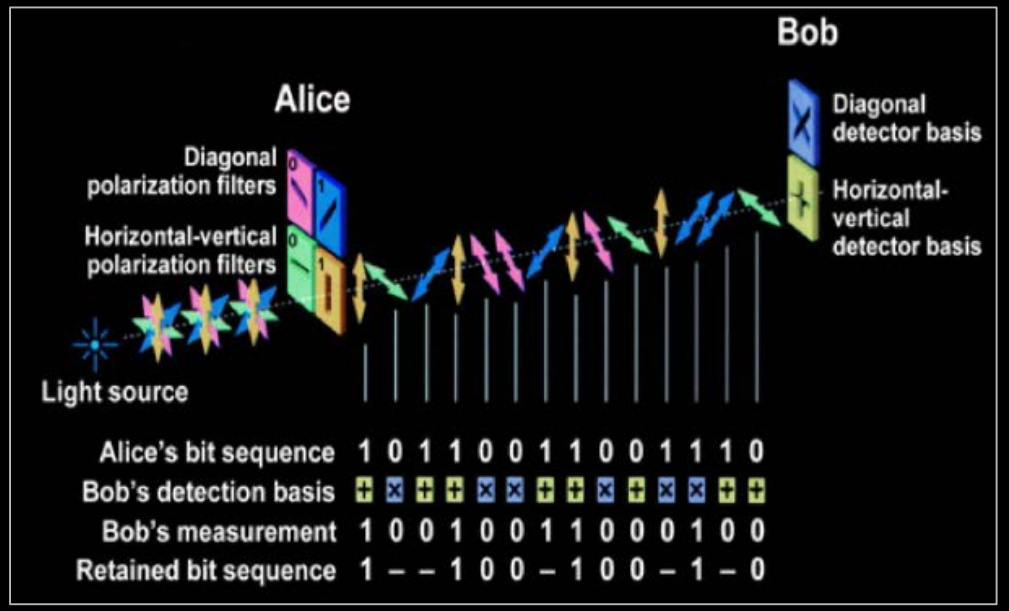
The results are **true.**

MUTUALLY UNBIASED BASES **(MUBs)**

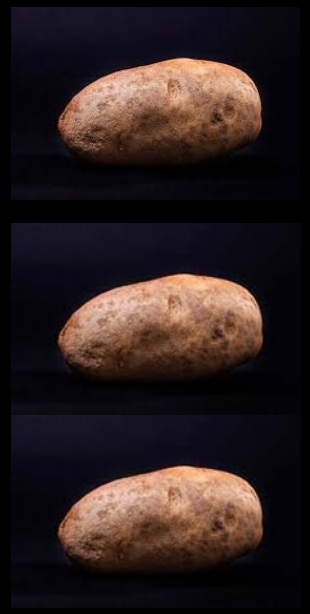
- Definition
  Two orthonormal **bases** $\{|\psi_i^1\rangle\}_i$, and $\{|\psi_j^2\rangle\}_j$ of $\mathbb{C}^d$ are mutually unbiased if:

$$\left|\langle\psi_i^1|\psi_j^2\rangle\right|^2 = \frac{1}{d} \quad \forall\, i,j \in \{1,\dots,d\}$$

- Applications
  - Quantum State Tomography
  - Quantum Key Distribution
  - Quantum Teleportation
  - Dense Coding



INFORMATION THEORETIC APPROACH



Different subspaces – different pieces of information that **<u>can</u>** be accessed independently

Different **bases** – different pieces of information that **<u>cannot</u>** be accessed independently

MUTUALLY UNBIASED BASES (MUBs)

- Known Constructions

$d = p$

$$\left(|\psi_k^0\rangle\right)_l = \delta_{kl}$$
$$\left(|\psi_k^r\rangle\right)_l = \frac{1}{\sqrt{N}} \mathrm{Exp}\left[\frac{2\pi i}{p}(rl^2 + kl)\right] \quad r = 1,2,\dots,p$$

$d = p^n$

$$\left(|\psi_k^0\rangle\right)_l = \delta_{kl}$$
$$\left(|\psi_k^r\rangle\right)_l = \frac{1}{\sqrt{N}} \mathrm{Exp}\left[\frac{2\pi i}{p}\mathrm{Tr}(rl^2 + kl)\right] \quad r,k,l \in \boldsymbol{F}_{p^n},\ r \neq 0$$

- Open Problem
  How many mutually bases exist in composite dimensions? $d = pq$
  - Zauner's Conjecture
    No more than 4 MUBs exist in dimension 6

Ivonovic, *Geometrical description of quantal state determination*, J Phys A 14, 3241 (1981)
Wooters and Fields, *Optimal state determination by mutually unbiased measurements*, Ann Phys 191, 363 (1989)
Zauner, *Quantum Designs: Foundations of a noncommutative design theory*, Int J. Quant Info 09, 445 (2011)

QUANTUM RANDOM ACCESS **CODES**
$2^d \rightarrow 1$ **QRACs**

- Input for Alice

$$\boldsymbol{x} = x_1 x_2 \qquad x_i \in \{1, \dots, d\}$$

- Input for Bob

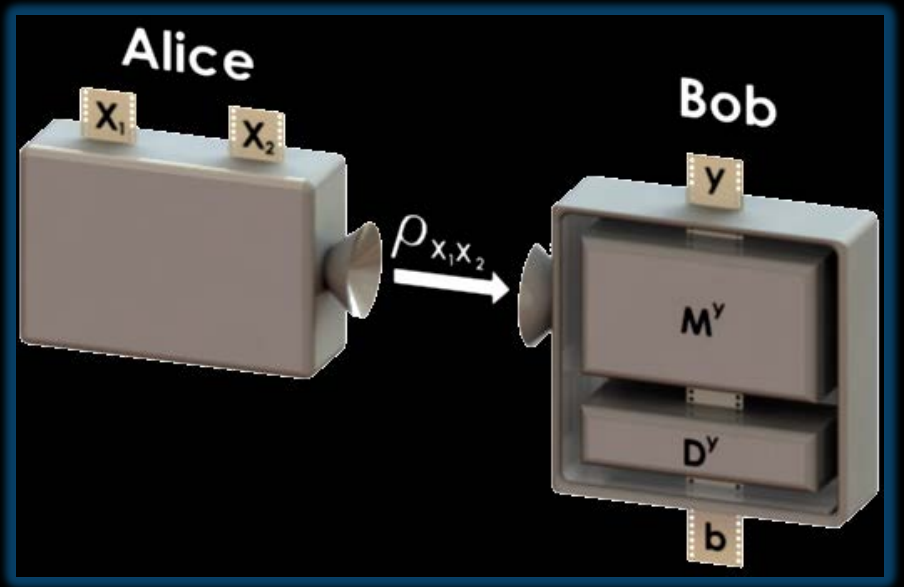
$$y \in \{1,2\}$$

- Rules (Prepare & Measure)
  Alice prepares and sends a d-dimensional state to Bob.
  Bob measures the state and outputs $b \in \{1, \dots, d\}$.
- Success Condition

$$b = x_y$$

- Figure of Merit
  ***A**verage **S**uccess **P**robability*

$$\bar{p}_d = \frac{1}{2d^2} \sum_{\boldsymbol{x},y} p(b = x_y | \boldsymbol{x}, y) = \frac{1}{2} \sum_{y} p(\text{Correctly guessing } x_y)$$



A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Journal of the ACM 49,1 (2002).

ENTANGLEMENT ASSISTED RANDOM ACCESS **CODES**
$2^d \rightarrow 1$ **EARACs**

- Input for Alice

$$\boldsymbol{x} = x_1 x_2 \qquad x_i \in \{1, \dots, d\}$$

- Input for Bob

$$y \in \{1,2\}, m \in \{1, \dots, d\}$$

- Rules (Nonlocal game)
  Alice measures a part of an entangled state. Then she sends a message $m \in \{1, \dots, d\}$ to Bob.
  Bob measures the state and outputs $b \in \{1, \dots, d\}$ based on measurement result and the message m.
- Success Condition

$$b = x_y$$

- Figure of Merit
  ***A**verage **S**uccess **P**robability*

$$\bar{p}_d = \frac{1}{2d^2} \sum_{\boldsymbol{x},y} p(b = x_y | \boldsymbol{x}, y) = \frac{1}{2} \sum_{y} p(\text{Correctly guessing } x_y)$$

Basically a **Bell inequality** test with additonal communication between the parties

M. Pawłowski, M. Żukowski, *Entanglement assisted random access codes*, Phys. Rev. A 81, 042326 (2010).

APPLICATIONS & EXAMPLE

Applications

- Foundations
  M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Żukowski, *Information Causality as a Physical Principle*, Nature 461, 1101 (2009).
- Quantum Key Distribution
  M. Pawłowski, N. Brunner, *Semi-device-independent security of one-way quantum key distribution*, Phys. Rev. A 84, 010302(R), (2011).
- Randomness Generation
  H-W Li, *et. al.* Phys. Rev. A 84, *Semi-Device Independtent Randomness Generation without Entanglement*, 034301, (2011).
- Dimension Witnessing
  J. Ahrens, P. Badziąg, M. Pawłowski, M. Żukowski, M. Bourennane, *Experimental Tests of Classical and Quantum Dimensions*, Phys. Rev. Lett. 112, 140401 (2014).
- Checking the number of **MUBs**

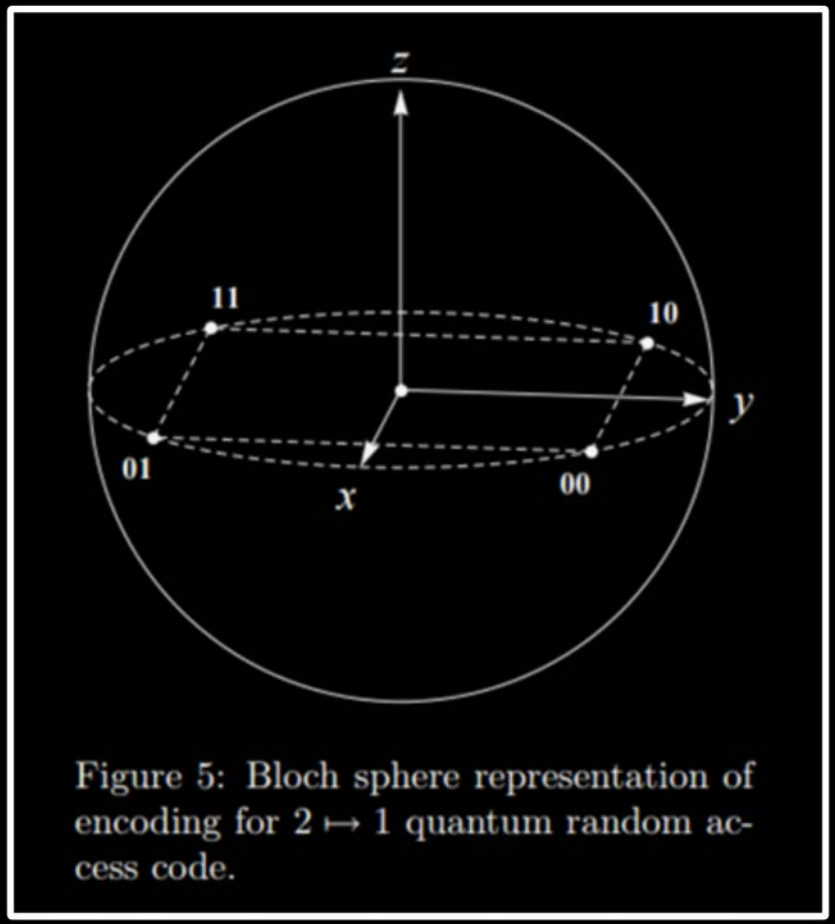


Figure 5: Bloch sphere representation of encoding for $2 \mapsto 1$ quantum random access code.

Example

$2^2 \rightarrow 1$ **QRAC**

if $y = 1$ Bob measures in the ***X*** – basis
if $y = 2$ Bob measures in the ***Y*** – basis

Ambainis et al., *Quantum Random Access Codes with Shared Randomnes*, q-ph: 0810.2937

OPTIMAL QRAC STRATEGY

- Lemma
  For a $2^d \to 1$ **QRAC**, the optimal average success probability
  $$\bar{p}_d = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right)$$
  is obtained if and only if Bob's measurement **bases** are **mutually unbiased**.

- Key Idea
  Design a generalized **code**, whose optimal is achieved iff *n* **MUBs** exist in dimension *d*

PROMISE QRAC

$n^d \to 1$ PQRAC

- Input for Alice

$$\boldsymbol{x} = x_1 x_2 \cdots \mathrm{x_n} \qquad x_i \in \{1, \ldots, d\}$$
$$\boldsymbol{z} = \{z_1, z_2\} \qquad z_1, z_2 \in \{1, \ldots, n\}\ , z_1 < z_2$$

- Input for Bob

$$y \in \{1,2, \ldots, n\}$$

- Promise

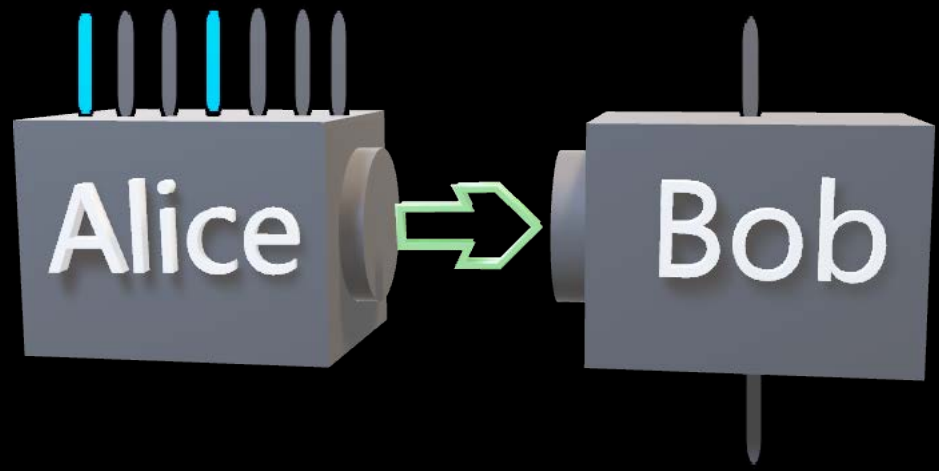
$$y \in \boldsymbol{z}$$

- Success Condition

$$b = x_y$$

- Figure of Merit
  Average Success Probability

$$\tilde{p}_{(n,d)} = \frac{1}{\binom{n}{2} n d^n} \sum_{\boldsymbol{x},y,\boldsymbol{z}} p(b = x_y | \boldsymbol{x}, y, \boldsymbol{z})$$



Lemma

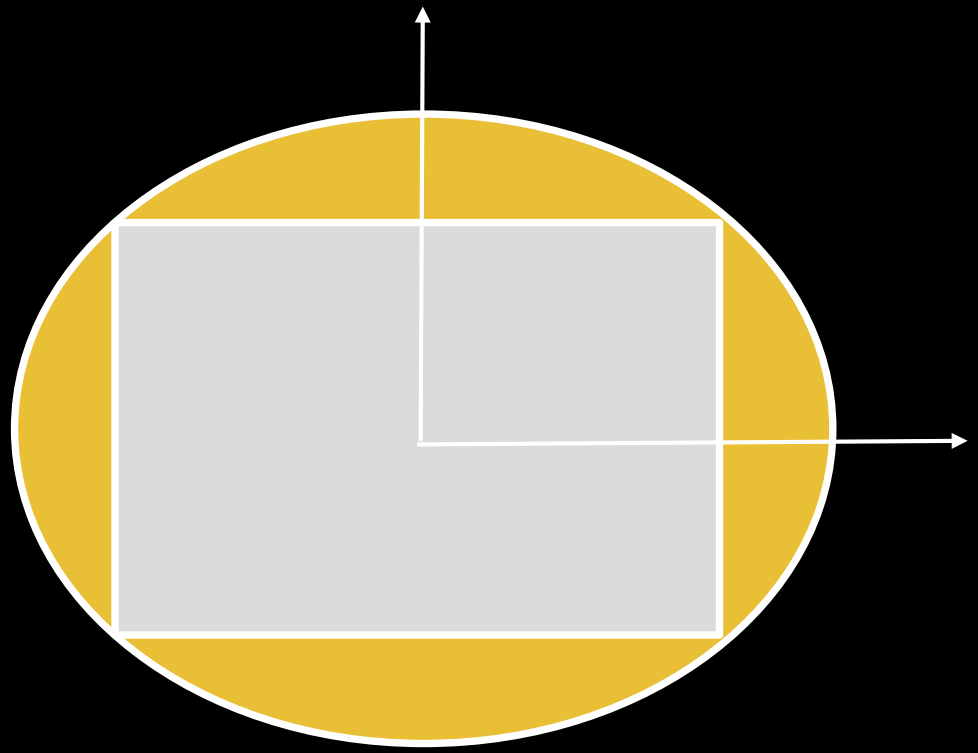
For the optimal quantum strategy:

$$\tilde{p}_{(n,d)} \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right)$$

with equality iff n **MUBs** exist in $\mathbb{C}^d$

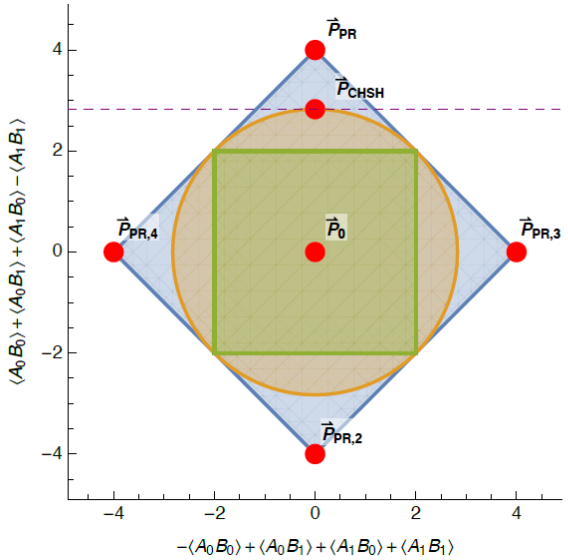
CONDITIONAL PROBABILITY SPACE

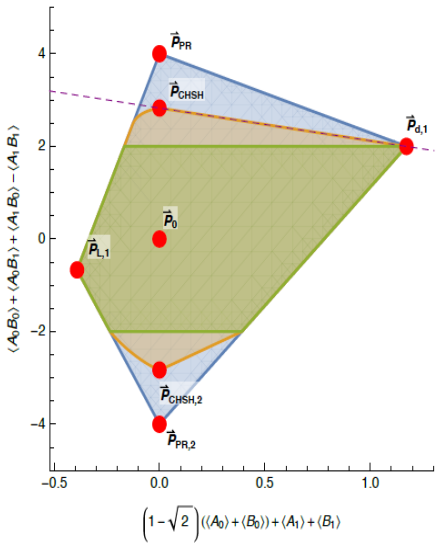
$p(a,b\,|\,x,y)$

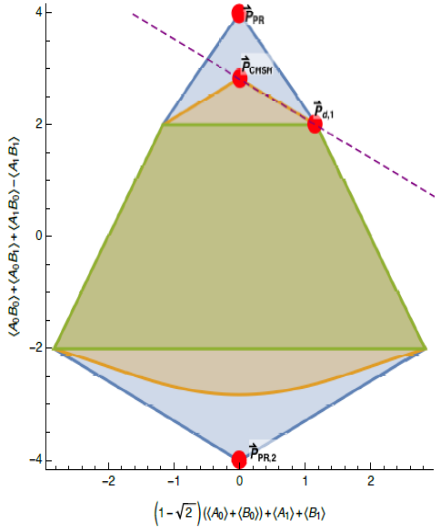


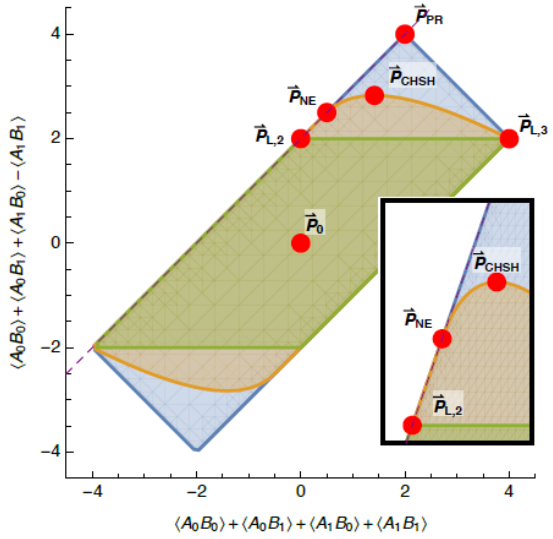
I. Pitowsky, Mathematical Programming 50 395 (1991).

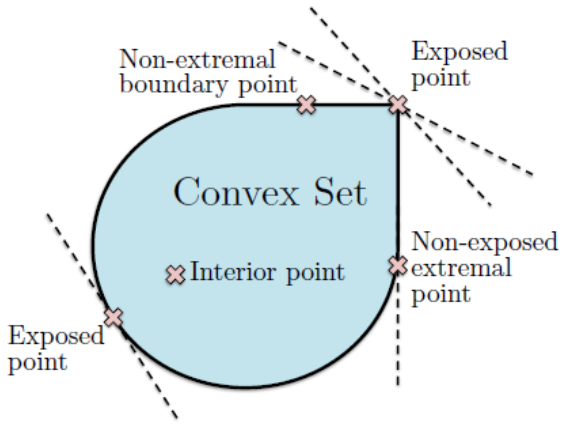
The white slide







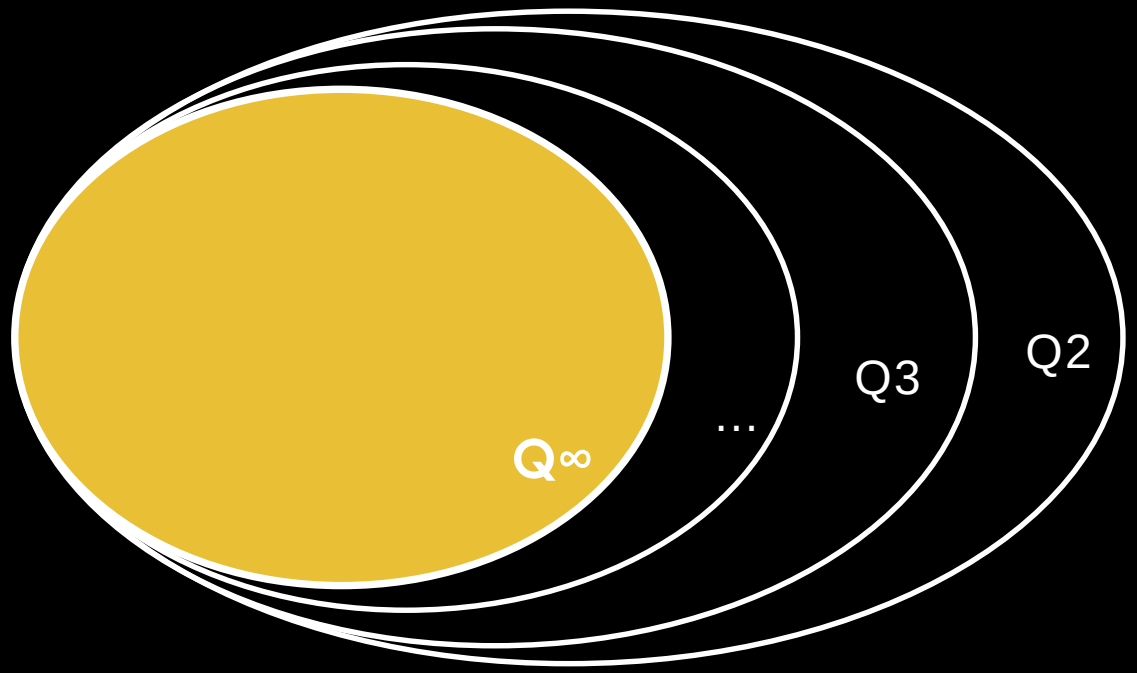




(1) $\beta_{\mathcal{L}} < \beta_{\mathcal{Q}} < \beta_{\mathcal{NS}}$,
(2a) $\beta_{\mathcal{L}} = \beta_{\mathcal{Q}} < \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{L}} \subsetneq \mathcal{F}_{\mathcal{Q}}$,
(2b) $\beta_{\mathcal{L}} = \beta_{\mathcal{Q}} < \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{L}} = \mathcal{F}_{\mathcal{Q}}$,
(3a) $\beta_{\mathcal{L}} < \beta_{\mathcal{Q}} = \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{Q}} \subsetneq \mathcal{F}_{\mathcal{NS}}$,
*(3b) $\beta_{\mathcal{L}} < \beta_{\mathcal{Q}} = \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{Q}} = \mathcal{F}_{\mathcal{NS}}$,
(4a) $\beta_{\mathcal{L}} = \beta_{\mathcal{Q}} = \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{L}} \subsetneq \mathcal{F}_{\mathcal{Q}} \subsetneq \mathcal{F}_{\mathcal{NS}}$,
(4b) $\beta_{\mathcal{L}} = \beta_{\mathcal{Q}} = \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{L}} = \mathcal{F}_{\mathcal{Q}} \subsetneq \mathcal{F}_{\mathcal{NS}}$,
*(4c) $\beta_{\mathcal{L}} = \beta_{\mathcal{Q}} = \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{L}} \subsetneq \mathcal{F}_{\mathcal{Q}} = \mathcal{F}_{\mathcal{NS}}$,
(4d) $\beta_{\mathcal{L}} = \beta_{\mathcal{Q}} = \beta_{\mathcal{NS}}$ and $\mathcal{F}_{\mathcal{L}} = \mathcal{F}_{\mathcal{Q}} = \mathcal{F}_{\mathcal{NS}}$.

K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, V. Scarani, *Geometry of the set of quantum correlations* Phys. Rev. A 97, 022104 (2018)

NAVASCUES-PIRONIO-ACIN HIERARCHY

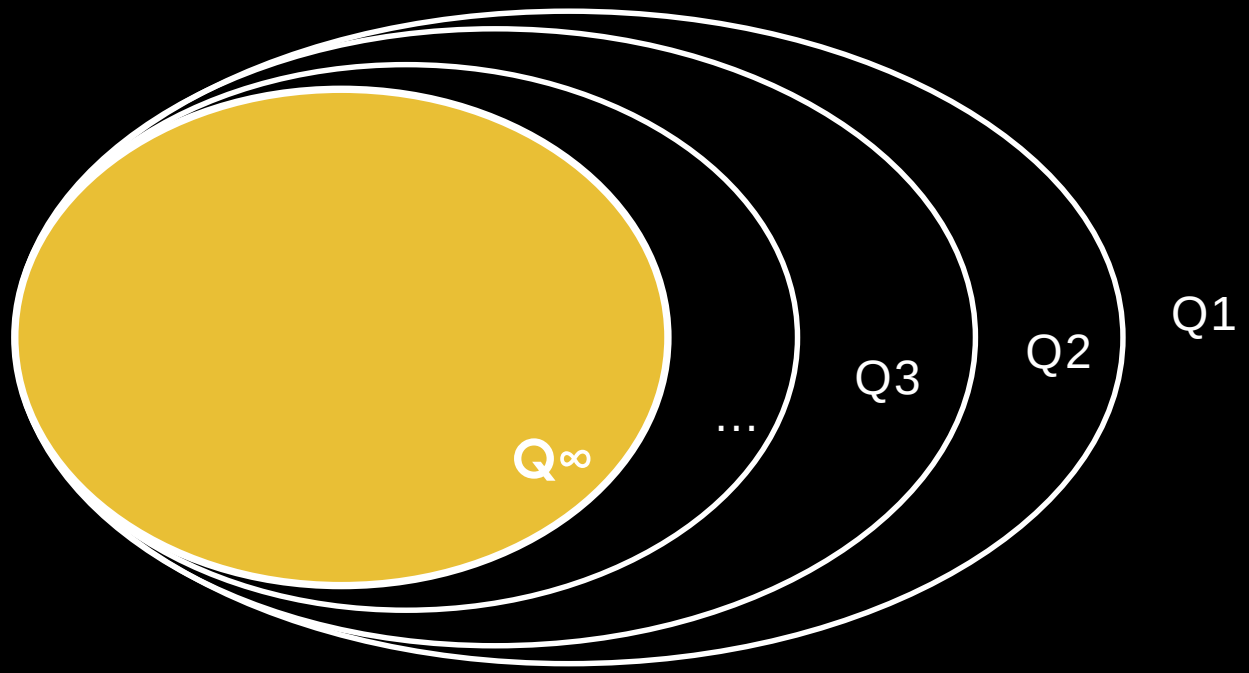


a=0 | x=0	a=1 | x=0	a=0 | x=1	….	b=0 | y=0	…..	
$p^2(a=0 \mid x=0)$	0	$p(a=0 \mid x=0,x=1)$		$p(a=b=0 \mid 00)$		a=0 | x=0
						a=1 | x=0
						a=1 | x=1
						……
						b=0 | y=0
						……

$\Gamma_1 \geq 0$

M. Navascues, S. Pironio, A. Acin, Phys. Rev. Lett. 98, 010401 (2007).

NAVASCUES-PIRONIO-ACIN HIERARCHY



$\Gamma_1 \geq 0$ ⟶ Q1 p(a=0|x=0)

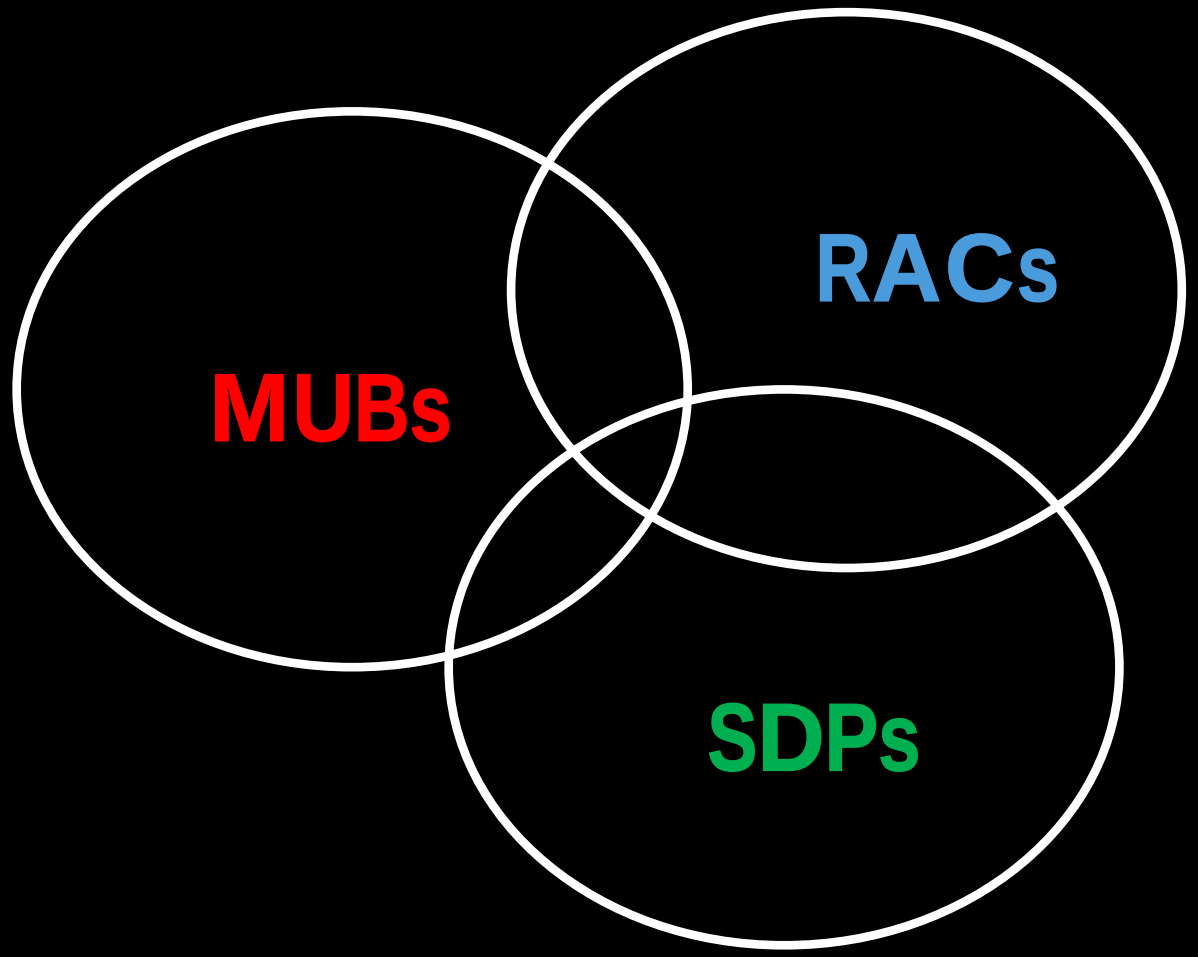
$\Gamma_2 \geq 0$ ⟶ Q2 p(a=0,b=2|x=0,y=1)

$\Gamma_3 \geq 0$ ⟶ Q3 p(a=0,b=2,b=5|x=0,y=1,b=0)

.....

M. Navascues, S. Pironio, A. Acin, Phys. Rev. Lett. 98, 010401 (2007).

TAKE 5 AND REGROUP



MUBs – sets of bases which can store pieces of information in such a way that only one can be read

RACs – codes in which we do lossy comprssion but only one piece of information is important

SDPs – a method of optimizing over all possible quantum states and measurements

There were three guys in **Spain**

Who tried one thing – in **vain**

With finite amount of sets

The quantum one **contain**

SDP - APPLICATIONS

There are efficient algorithms to maximize linear combinations of matrix elements under the constraint that the whole matrix is positive semidefinite.

There are many other hierarchies, intermediate levels and *single* **SDPs**

$\Gamma_3 \geq 0 \longrightarrow$ Q3 $\quad p(a=0,b=2,b=5 \mid x=0,y=1,b=0)$

Applications:

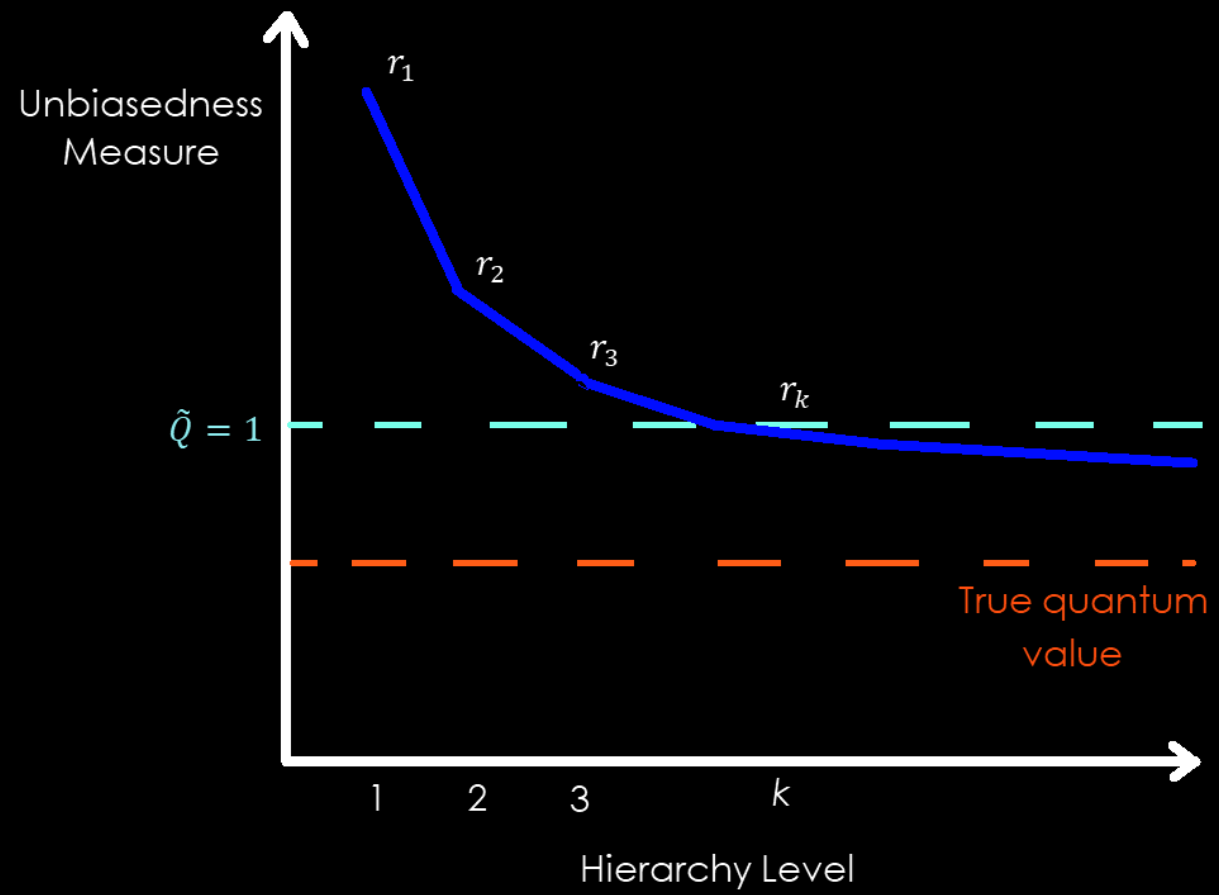
- Tsirelson bounds
- Randomness generation
- Quantum key distribution
- Checking the number of **MUBs**

THE INNER POINT

Algorithm to rule out the existence of n **MUBs** in dimension d

Employ the Navascues-Vertesi method:
- Sequence of **SDP** problems yielding upper bounds $\{r_k\}_k$ to optimization tasks over quantum probability distributions with dimensional constraints.
-Converges to the accurate quantum value.

If at a given level k of the hierarchy $\tilde{Q} < 1$ then $\nexists\, n$ MUBs in $\mathbb{C}^d$



Navascues and Vertesi, *Bounding the set of finite dimensional quantum correlations*, PRL 115, 020501 (2015)

THE RESULTS ARE ….

…..true

…..inconclusive

…..disappointing

…..prelilminary

Even Q3 allows for probability distributions corresponding to 4 **MUBs** in dimension 6.

In fact, Q3 allows also for 4 MUBs in dimension 2. → It's a very complex problem.

Way to go:

- Try Q4
- Try a different way of bounding the average success probability of **PQRAC**.