

Title: What does information causality imply?

Date: Nov 16, 2010 04:00 PM

URL: <http://pirsa.org/10110053>

Abstract: Nonlocality is the most striking feature of quantum mechanics. It might even be considered its defining feature and understanding it may be the most important step towards understanding the whole theory. Yet for a long time it was impossible to pinpoint the reason behind the exact amount of nonlocality allowed by quantum mechanics expressed by Tsirelson bound. Recently information causality has been shown to be the principle from which this bound can be derived. However the whole set of nonlocal correlations and nonlocal information processing protocols that quantum mechanics allows is not specified by the Tsirelson bound. It remains an open question whether this whole zoo of nonlocality can be derived from information causality. In this talk I present the fields where information causality is applied together with most recent results or lack of such.

Information Causality

Marcin Pawłowski







Why?

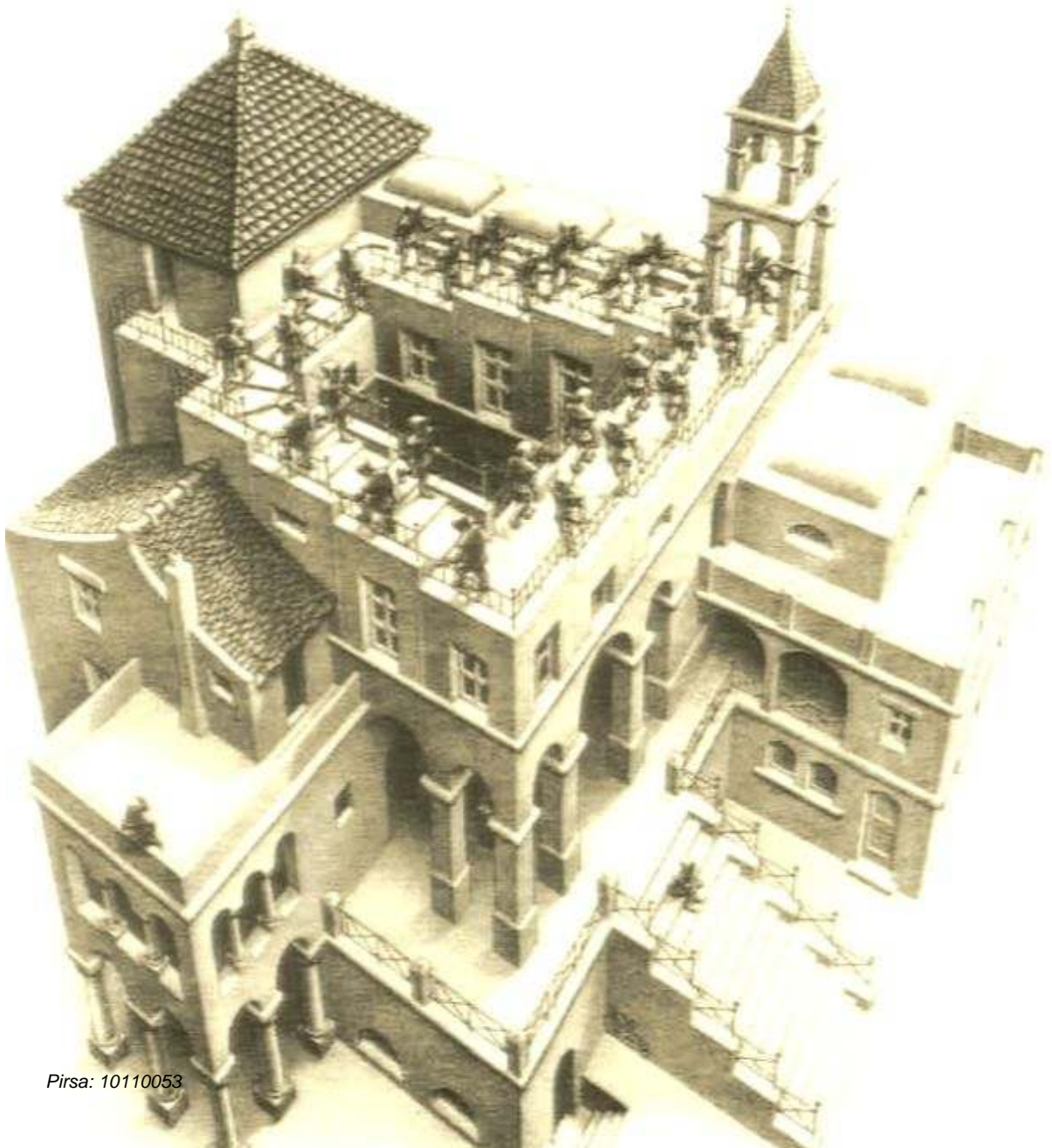
What?

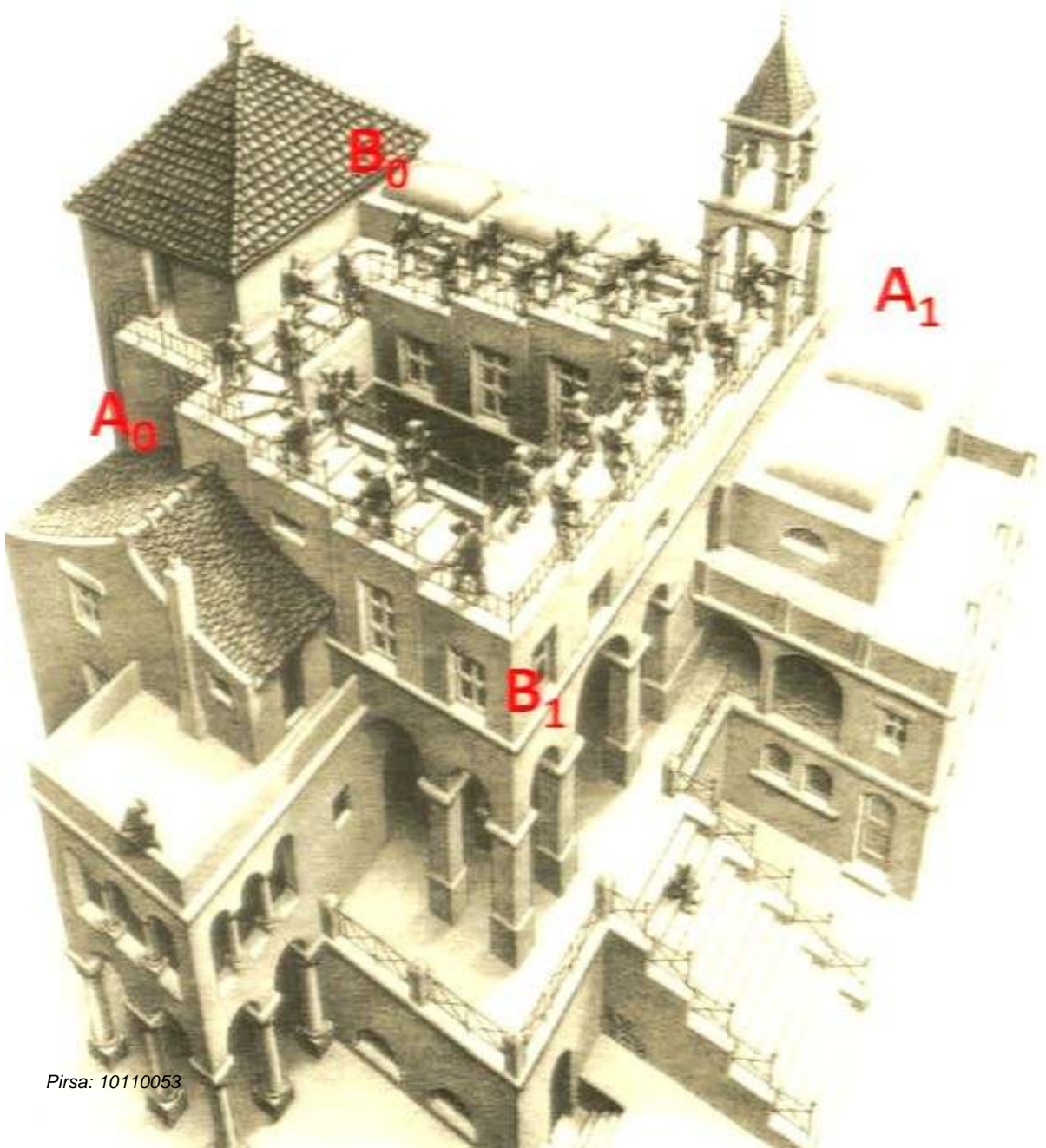
How?

Results

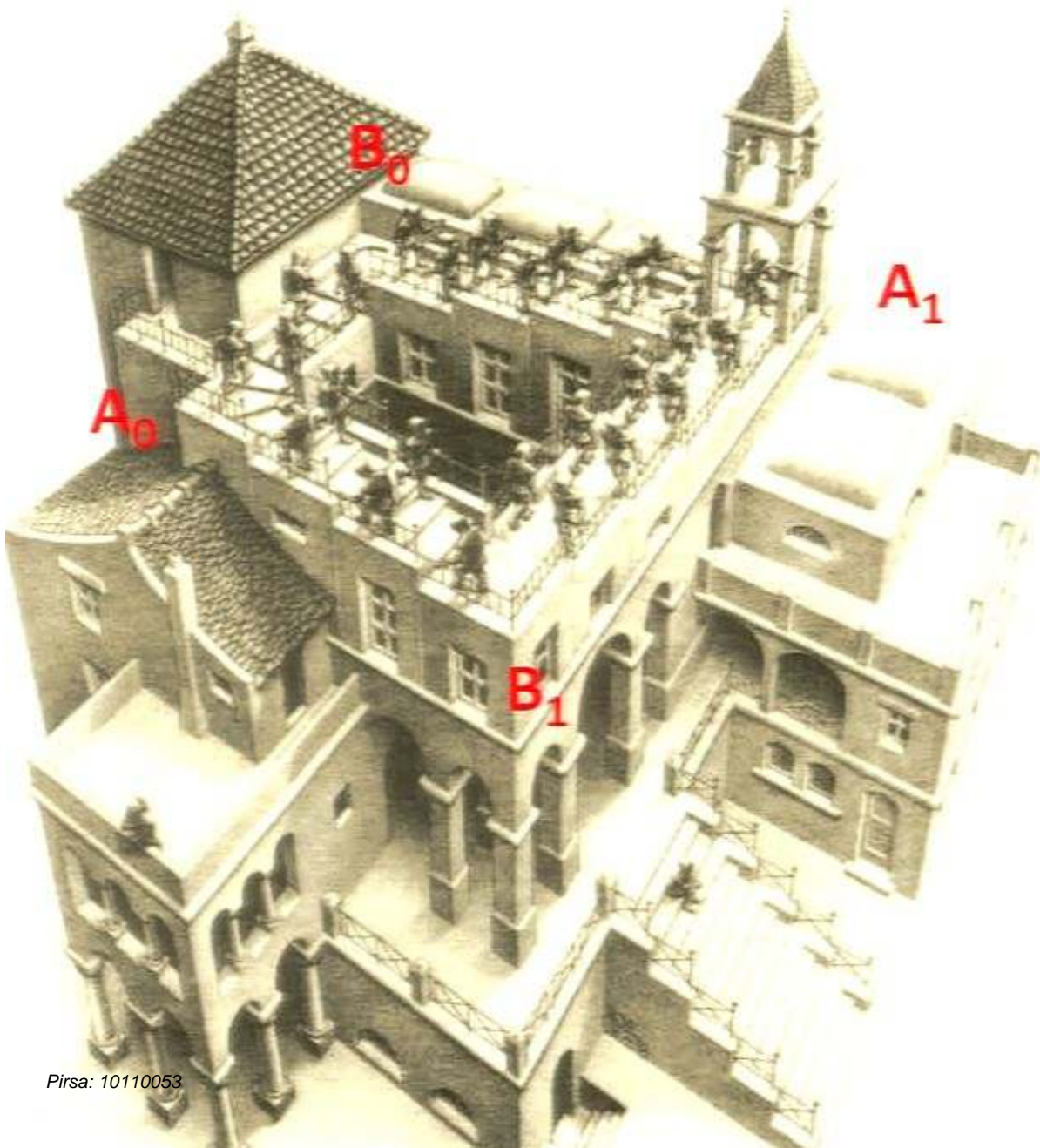
Why?

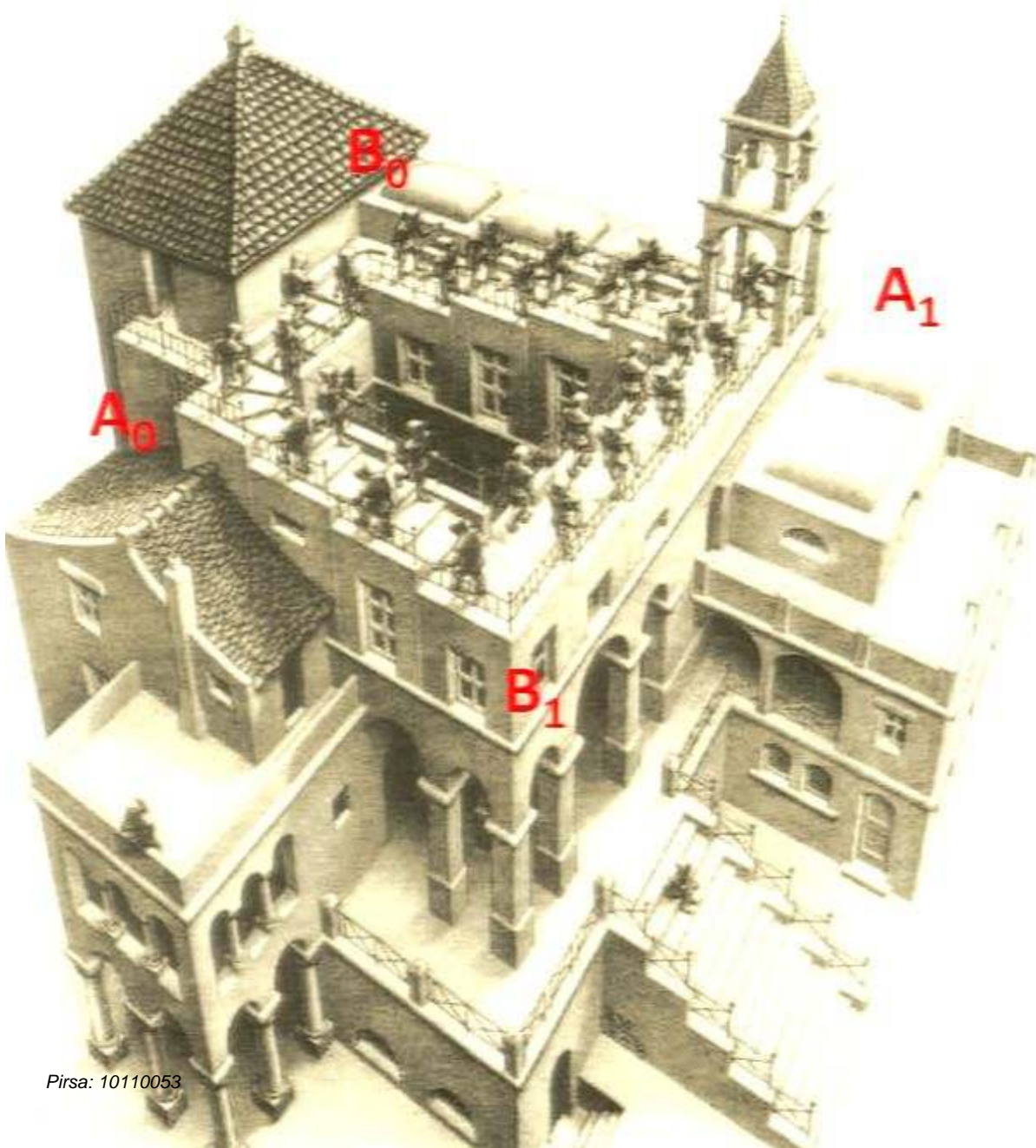






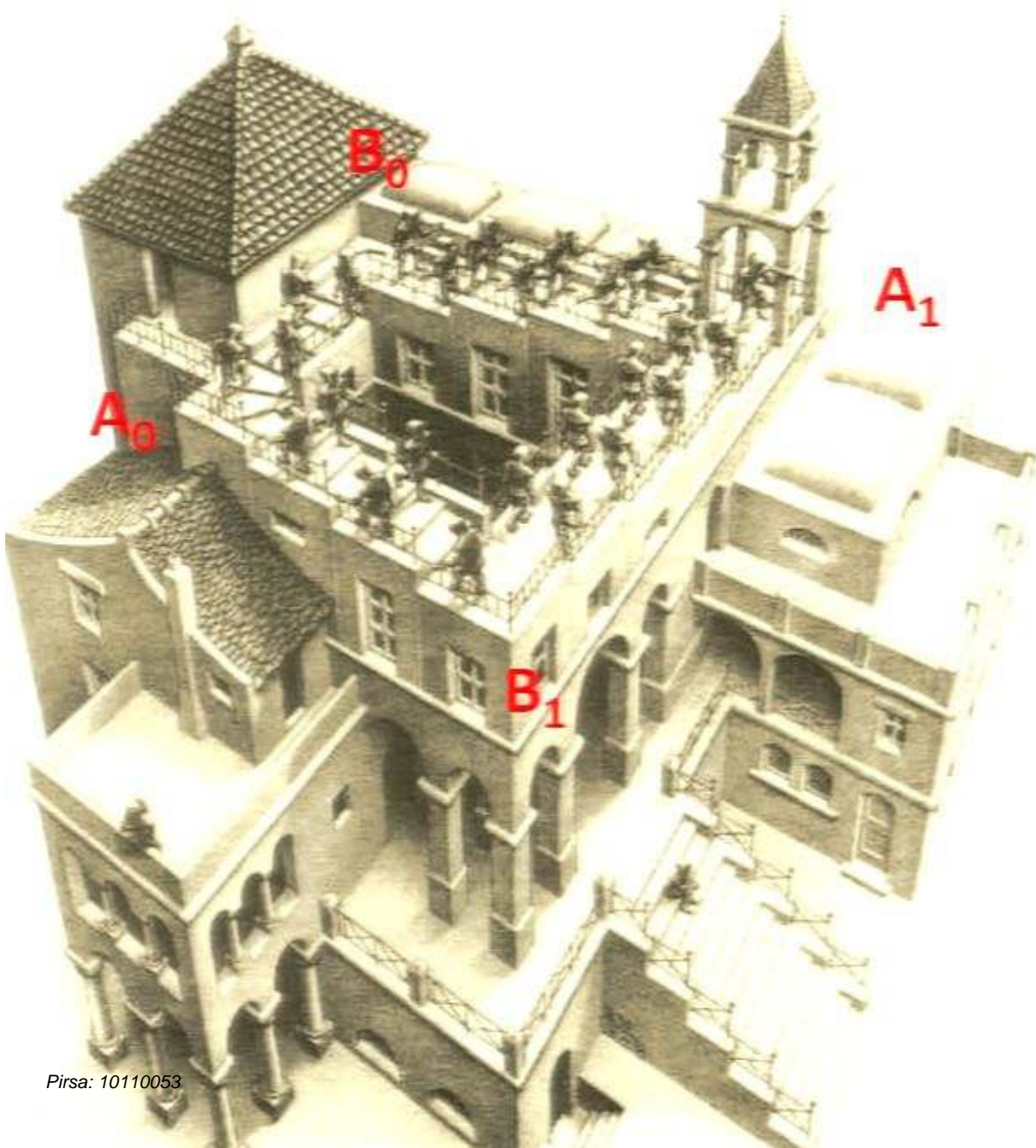
$$A_0 > B_0 > A_1 > B_1 \geq A_0$$





$$A_0 > B_0 > A_1 > B_1 \geq A_0$$

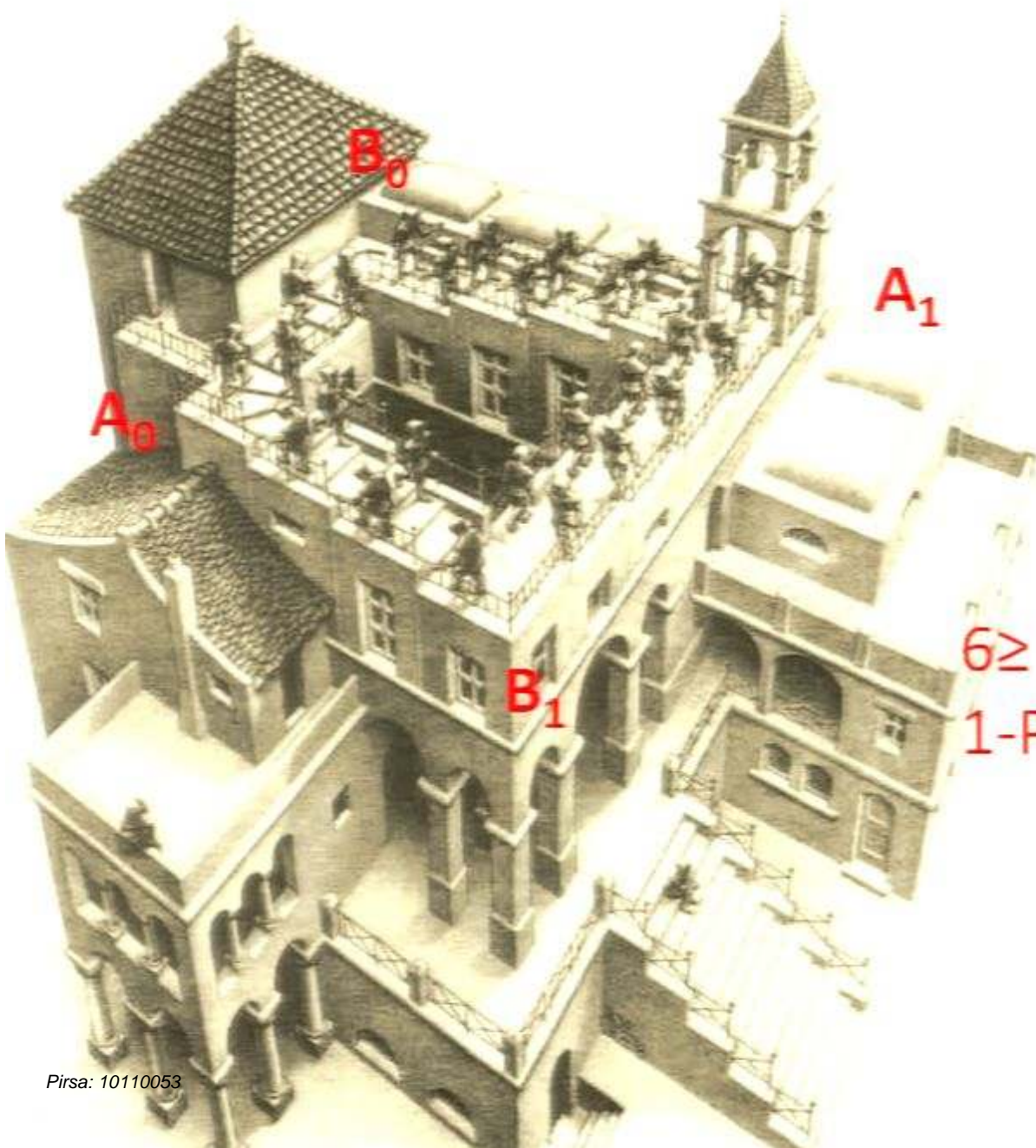
$$3 \geq P(A_0 > B_0) + P(B_0 > A_1) + P(A_1 > B_1) + P(B_1 \geq A_0) \geq 1$$



$$A_0 > B_0 > A_1 > B_1 \geq A_0$$

$$3 \geq P(A_0 > B_0) + P(B_0 > A_1) + P(A_1 > B_1) + P(B_1 \geq A_0) \geq 1$$

$$3 \geq P(A_0 < B_0) + P(B_0 < A_1) + P(A_1 < B_1) + P(B_1 \leq A_0) \geq 1$$

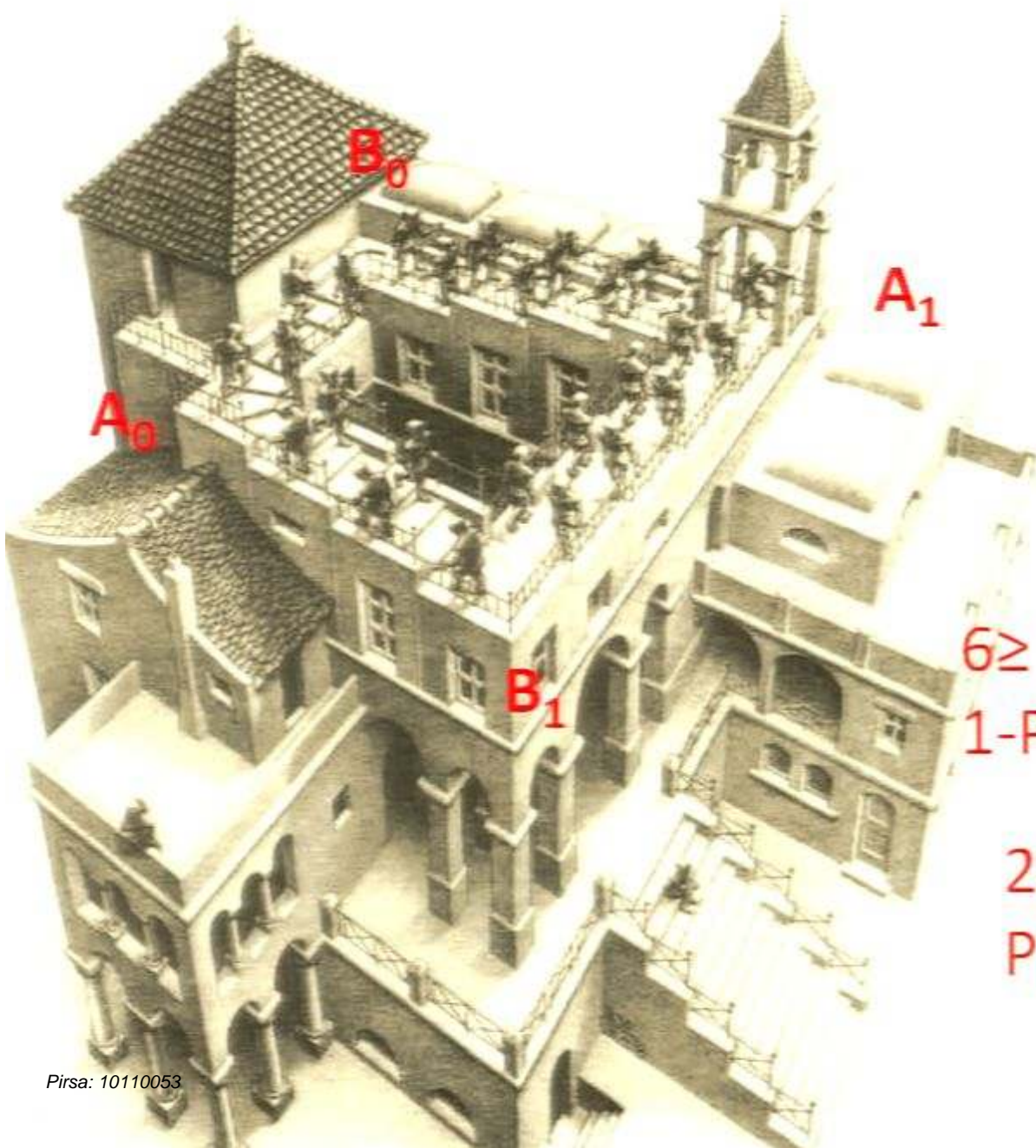


$$A_0 > B_0 > A_1 > B_1 \geq A_0$$

$$3 \geq P(A_0 > B_0) + P(B_0 > A_1) + P(A_1 > B_1) + P(B_1 \geq A_0) \geq 1$$

$$3 \geq P(A_0 < B_0) + P(B_0 < A_1) + P(A_1 < B_1) + P(B_1 \leq A_0) \geq 1$$

$$6 \geq 1 - P(A_0 = B_0) + 1 - P(B_0 = A_1) + 1 - P(A_1 = B_1) + 1 + P(B_1 = A_0) \geq 2$$



$$A_0 > B_0 > A_1 > B_1 \geq A_0$$

$$3 \geq P(A_0 > B_0) + P(B_0 > A_1) + P(A_1 > B_1) + P(B_1 \geq A_0) \geq 1$$

$$3 \geq P(A_0 < B_0) + P(B_0 < A_1) + P(A_1 < B_1) + P(B_1 \leq A_0) \geq 1$$

$$6 \geq 1 - P(A_0 = B_0) + 1 - P(B_0 = A_1) + 1 - P(A_1 = B_1) + 1 + P(B_1 = A_0) \geq 2$$

$$2 \geq P(A_0 = B_0) + P(B_0 = A_1) + P(A_1 = B_1) - P(B_1 = A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - P(B_1=A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - P(B_1=A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - 1 + P(B_1 \neq A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - P(B_1=A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - 1 + P(B_1 \neq A_0) \geq -2$$

$$P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) + P(B_1 \neq A_0) \leq 3$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - P(B_1=A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - 1 + P(B_1 \neq A_0) \geq -2$$

$$P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) + P(B_1 \neq A_0) \leq 3$$

$$A, B, a, b \in 0, 1$$

$$\beta = \frac{1}{4} \sum_{a,b} P(A \oplus B = ab | a, b) \leq \frac{3}{4}$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - P(B_1=A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - 1 + P(B_1 \neq A_0) \geq -2$$

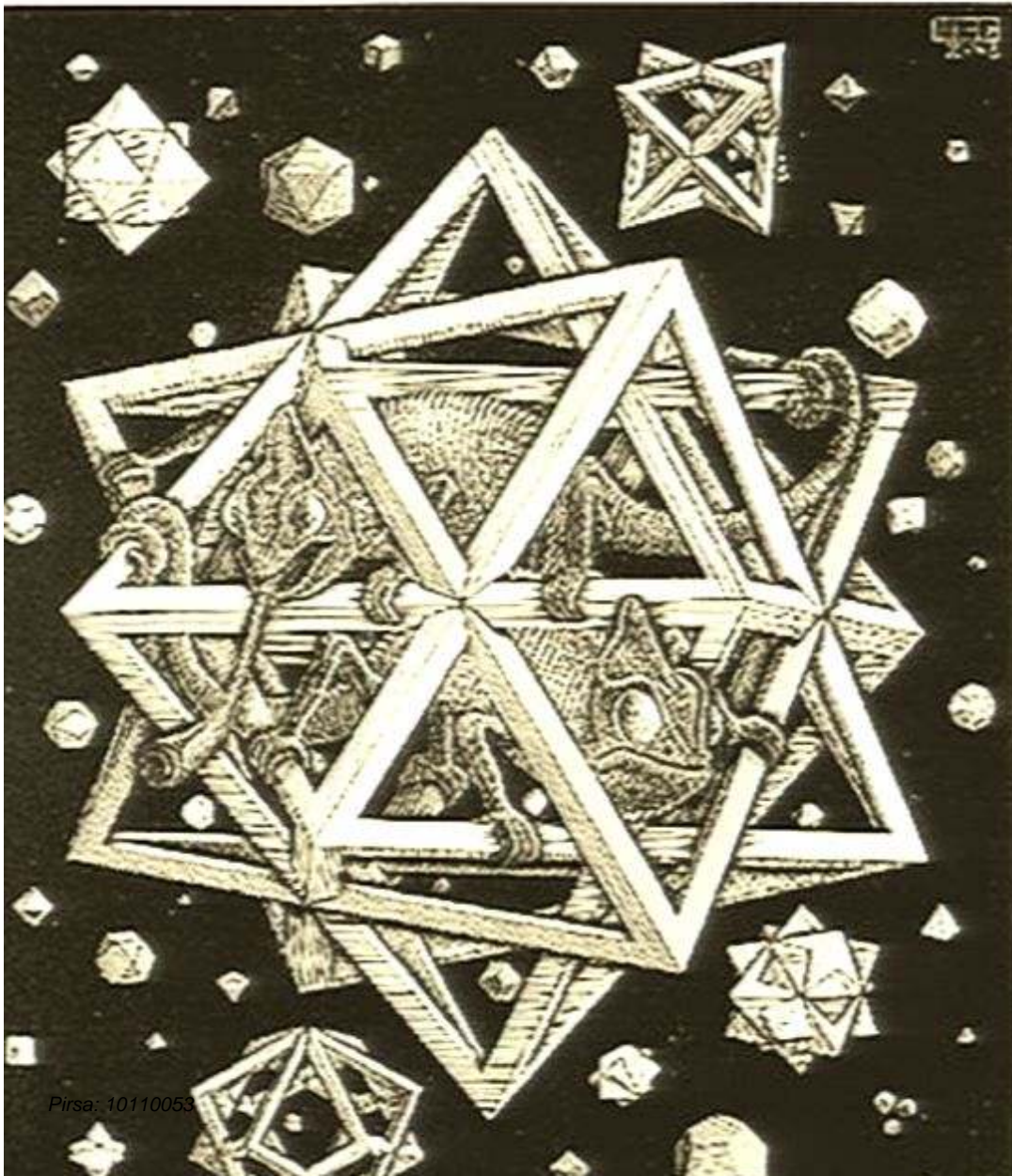
$$P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) + P(B_1 \neq A_0) \leq 3$$

$$A, B, a, b \in 0, 1$$

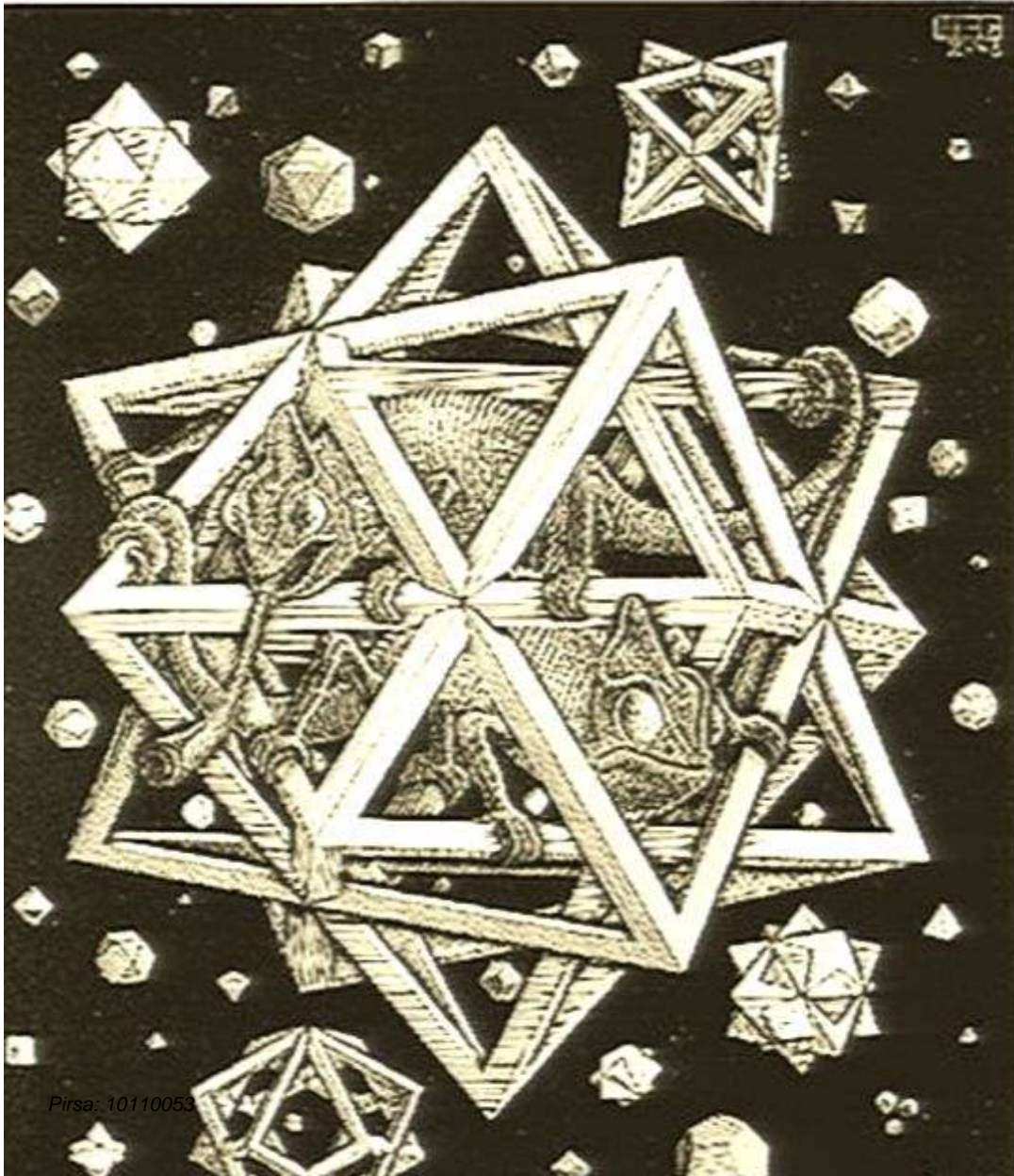
$$\beta = \frac{1}{4} \sum_{a,b} P(A \oplus B = ab | a, b) \leq \frac{3}{4}$$

$$\beta_{QM} = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right) \approx 0.854$$

How?

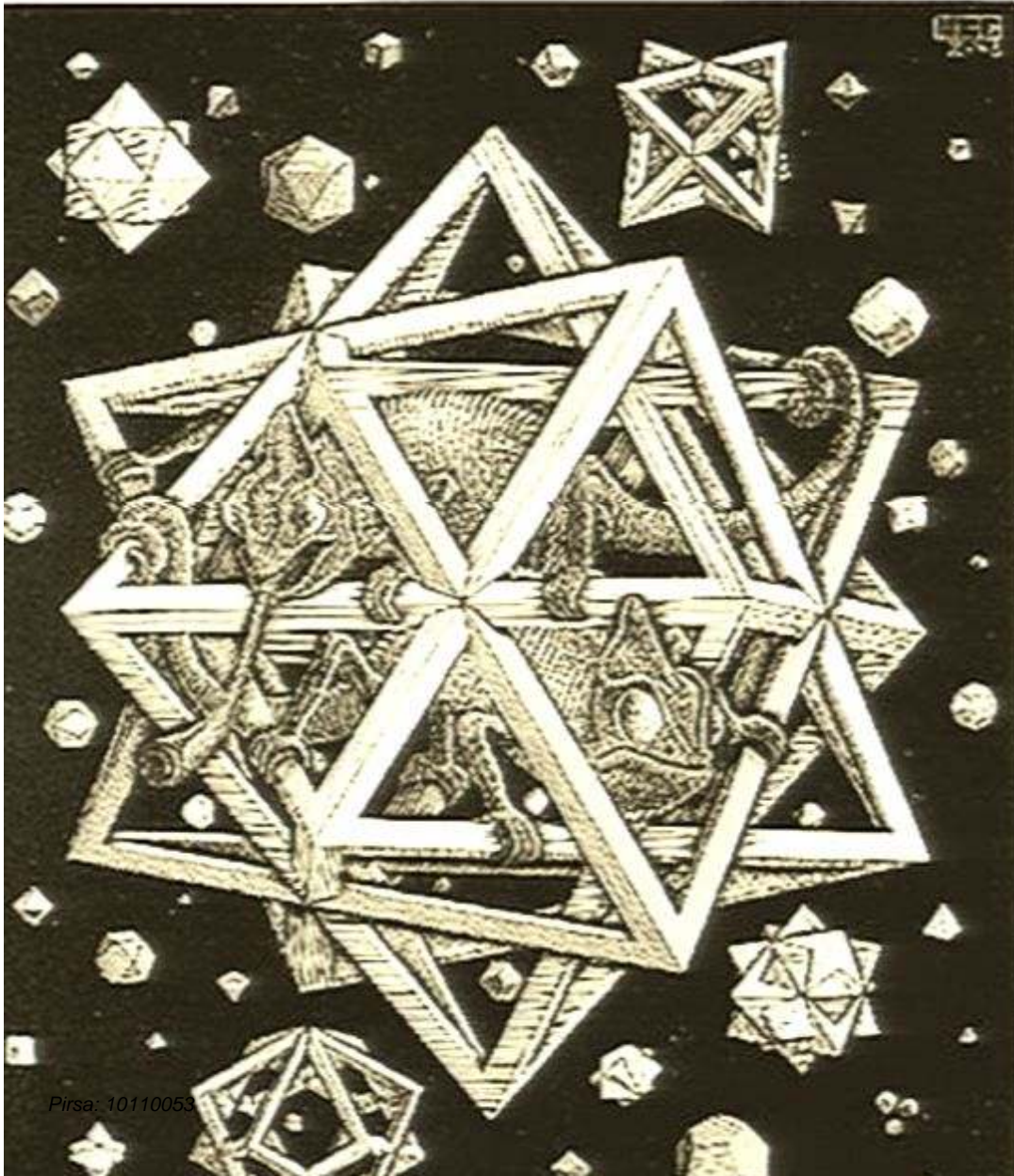


How?



No signalling

How?



No signalling

Communication complexity

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - P(B_1=A_0) \geq -2$$

$$2 \geq P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) - 1 + P(B_1 \neq A_0) \geq -2$$

$$P(A_0=B_0) + P(B_0=A_1) + P(A_1=B_1) + P(B_1 \neq A_0) \leq 3$$

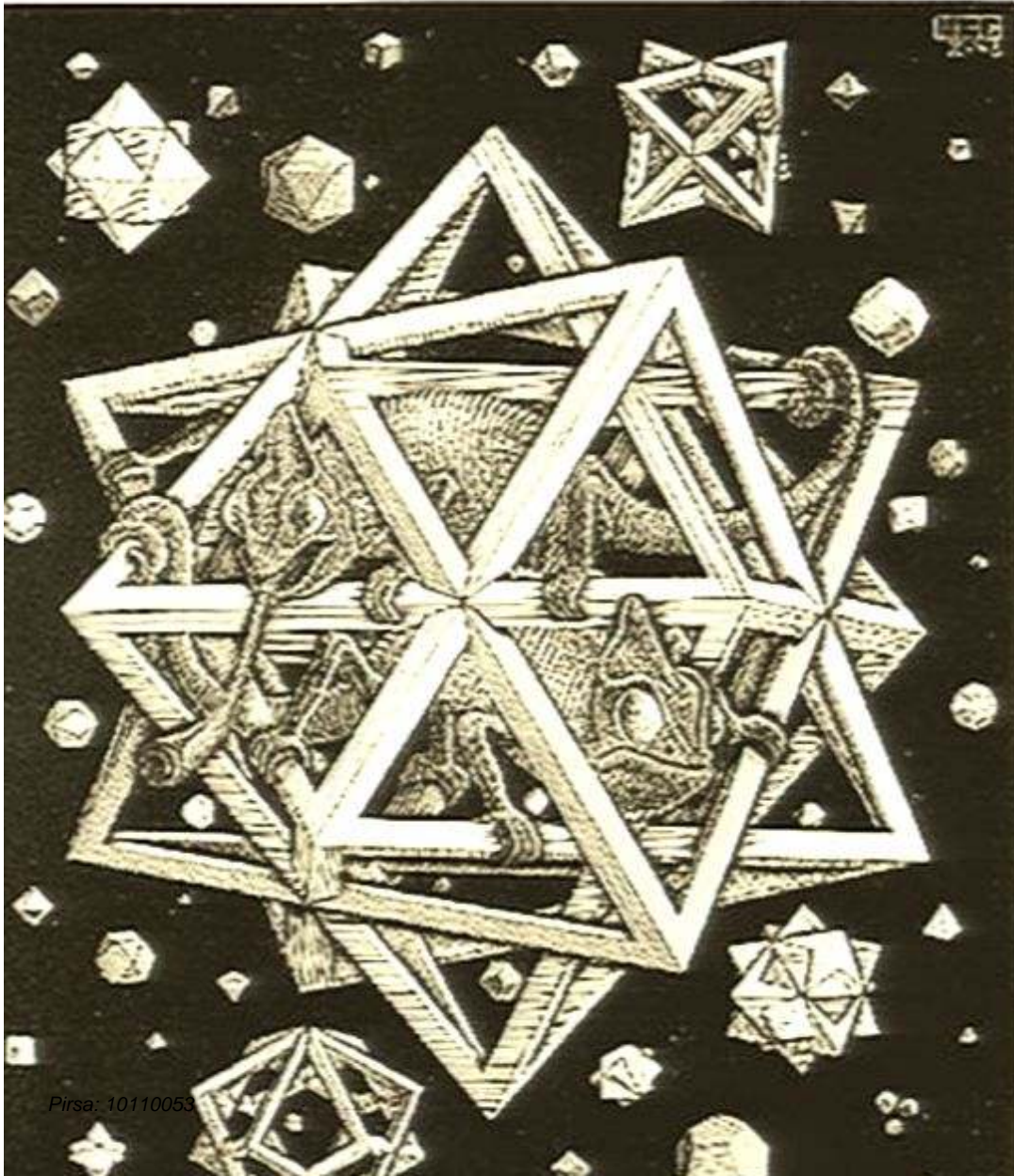
$$A, B, a, b \in 0, 1$$

$$\beta = \frac{1}{4} \sum_{a,b} P(A \oplus B = ab | a, b) \leq \frac{3}{4}$$

$$\beta_{QM} = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right) \approx 0.854$$

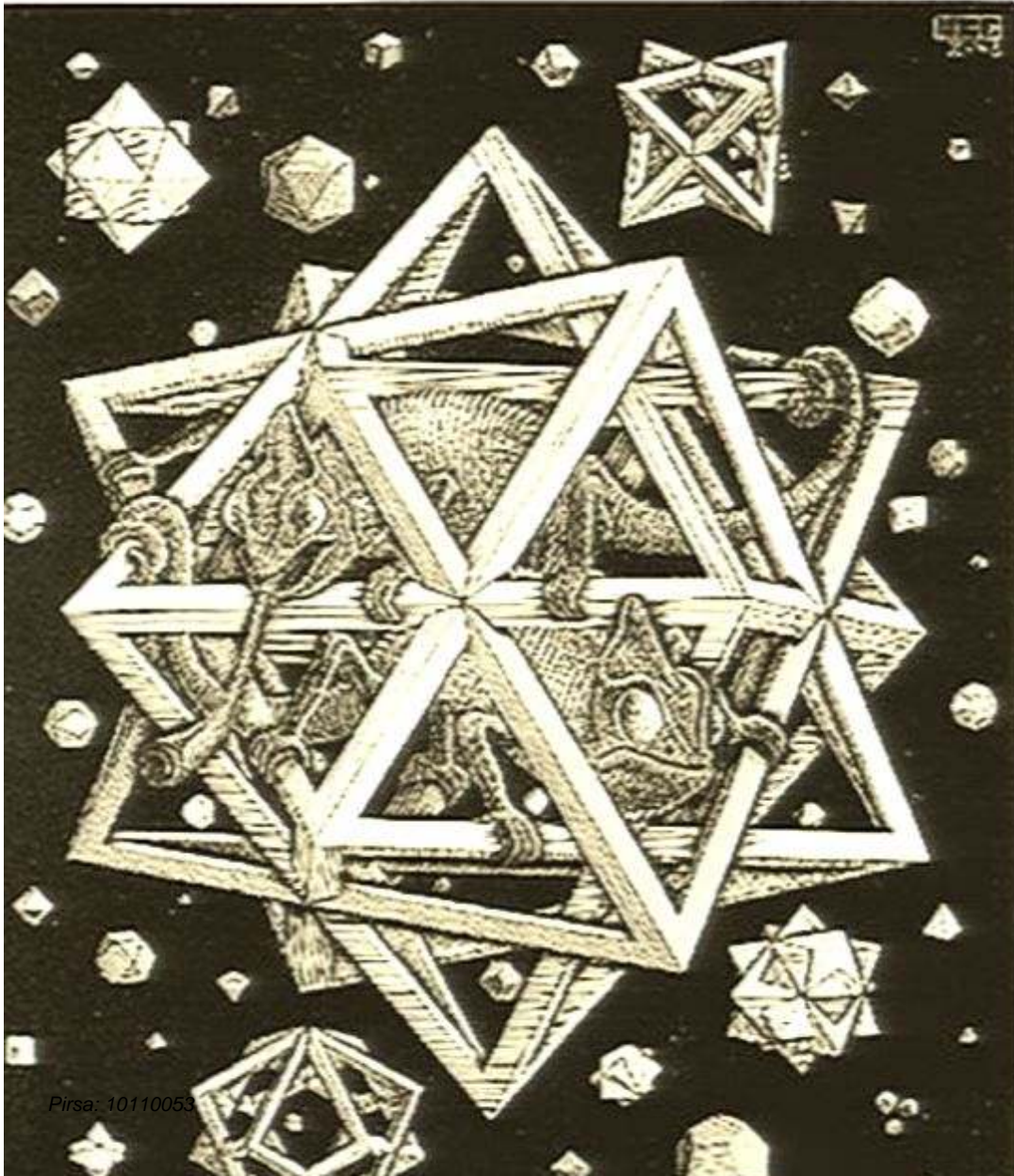
$$\beta_{NS} = 1$$

How?



No signalling

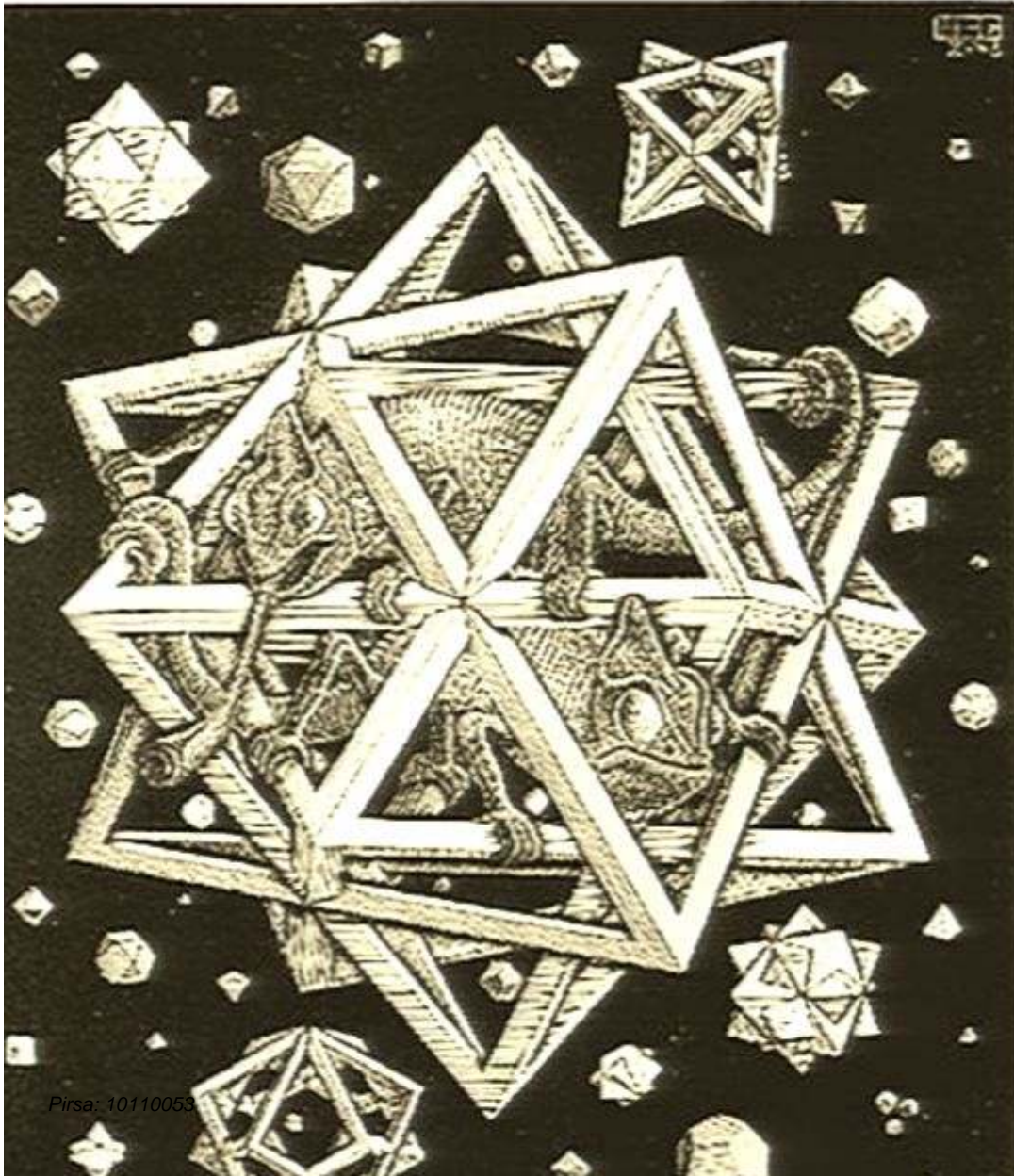
How?



No signalling

Communication complexity

How?



No signalling

Communication complexity

Information causality

Random access codes

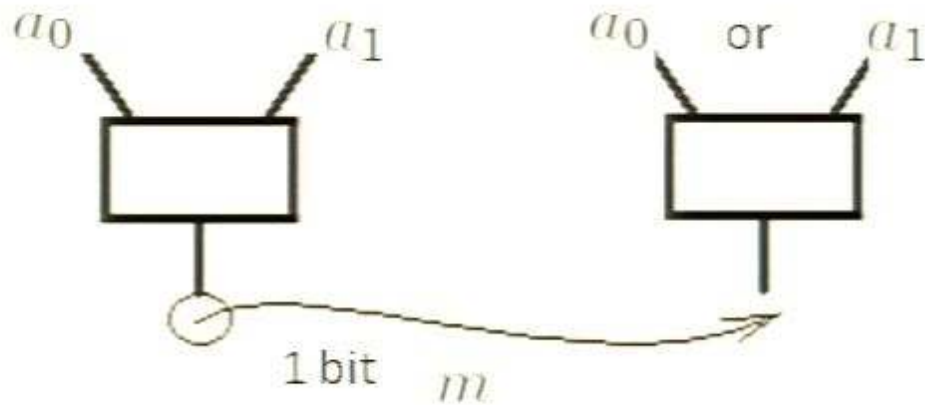


$A \oplus B = ab$ with probability $\frac{3}{4}$

Random access codes



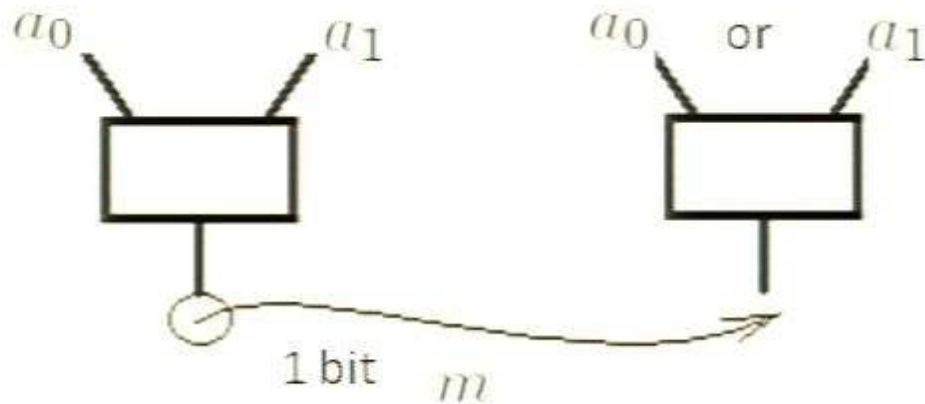
$A \oplus B = ab$ with probability $\frac{3}{4}$



Random access codes



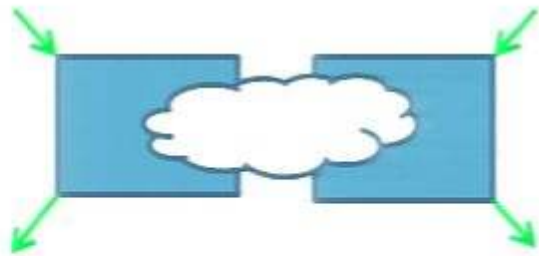
$A \oplus B = ab$ with probability $\frac{1}{3}$



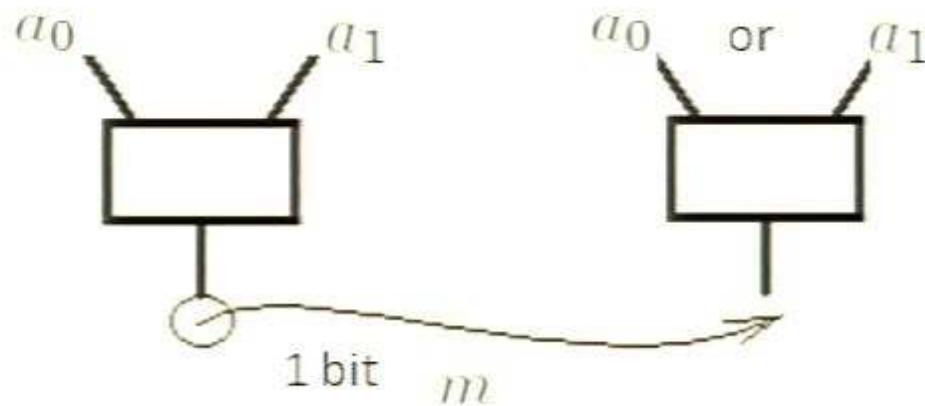
$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

Random access codes



$A \oplus B = ab$ with probability $\frac{1}{3}$



$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

$$B \oplus m = B \oplus A \oplus a_0 = ab \oplus a_0 = (a_0 \oplus a_1)b \oplus a_0 = a_b$$

(N → m) Random access code

$\vec{a} = (a_0, a_1, \dots, a_{N-1})$ independent of B

(N → m) Random access code

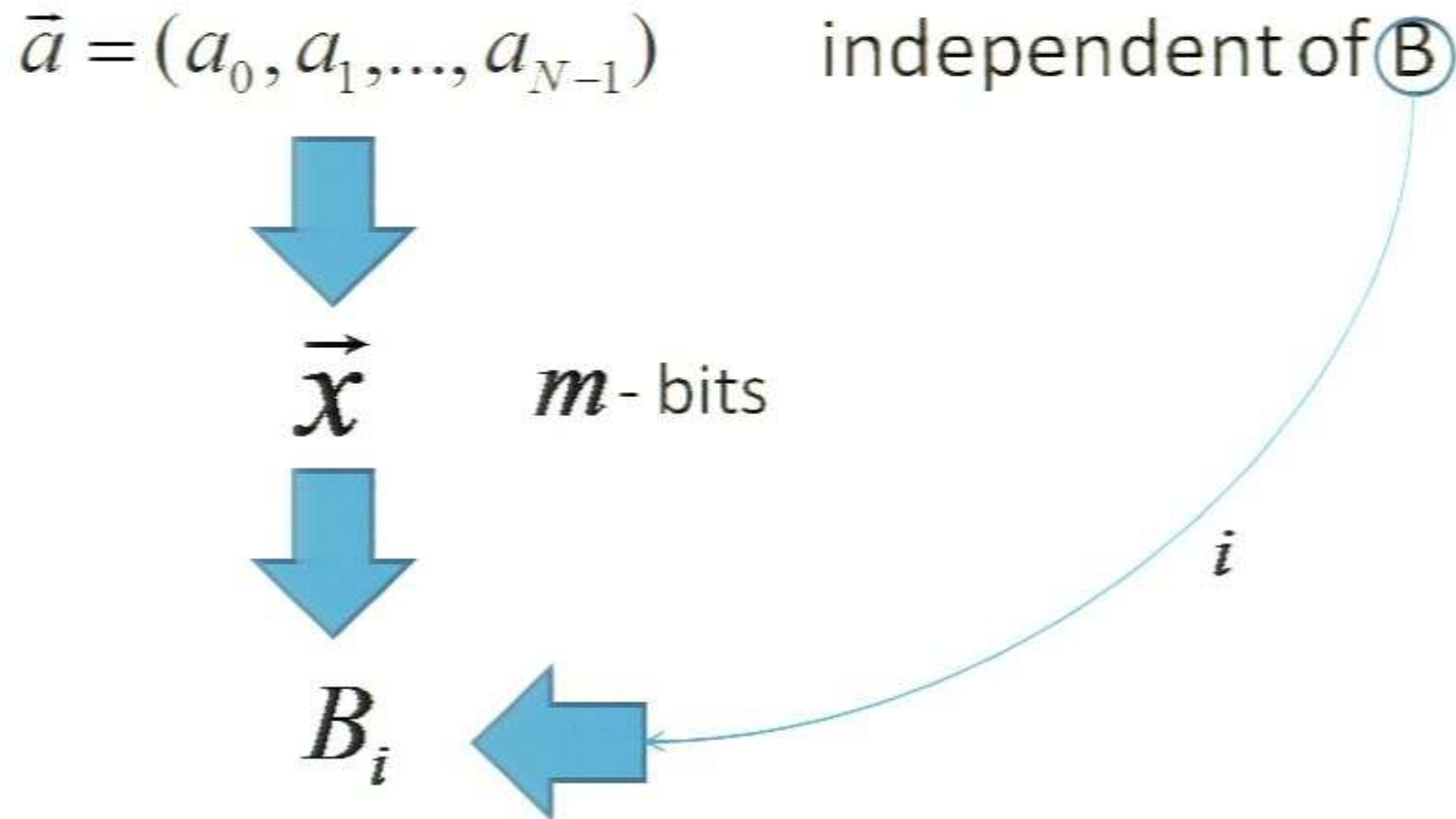
$\vec{a} = (a_0, a_1, \dots, a_{N-1})$ independent of B



\vec{x}

m -bits

(N → m) Random access code



(N → m) Random access code

$\vec{a} = (a_0, a_1, \dots, a_{N-1})$ independent of \mathbb{B}

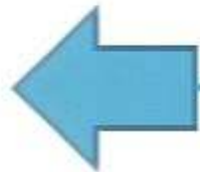


\vec{x}

m -bits



B_i



i

$$\sum_{i=0}^{N-1} I(a_i : B_i) \leq m$$

(N → m) Random access code

$\vec{a} = (a_0, a_1, \dots, a_{N-1})$ independent of \mathbb{B}



\vec{x}

m -bits



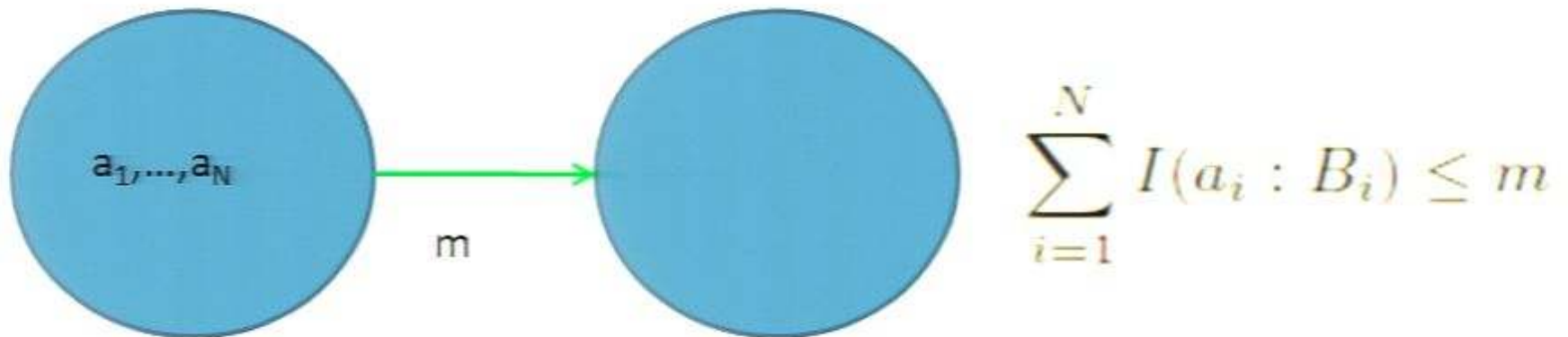
B_i



i

$$\sum_{i=0}^{N-1} I(a_i : B_i) \leq m$$

It is the sender who decides what the message is about



More comments on reasonability

$$I(\vec{a} : B) = 0 \quad \longrightarrow \quad I(\vec{a} : \vec{x}, B) \leq m$$

More comments on reasonability

$$I(\vec{a} : B) = 0 \quad \longrightarrow \quad I(\vec{a} : \vec{x}, B) \leq m$$

$$\mathbf{a}_i \text{ independently distributed} \quad \longrightarrow \quad I(\vec{a} : \vec{x}, B) \geq \sum_{i=0}^{N-1} I(\mathbf{a}_i : \vec{x}, B)$$

More comments on reasonability

$$I(\vec{a} : B) = 0 \quad \Rightarrow \quad I(\vec{a} : \vec{x}, B) \leq m$$

$$\mathbf{a}_i \text{ independently distributed} \quad \Rightarrow \quad I(\vec{a} : \vec{x}, B) \geq \sum_{i=0}^{N-1} I(\mathbf{a}_i : \vec{x}, B)$$

$$\text{Local processing} \quad \Rightarrow \quad I(\mathbf{a}_i : \vec{x}, B) \geq I(\mathbf{a}_i : B_i)$$

More comments on reasonability

$$I(\vec{a} : B) = 0 \quad \Rightarrow \quad I(\vec{a} : \vec{x}, B) \leq m$$

$$\mathbf{a}_i \text{ independently distributed} \quad \Rightarrow \quad I(\vec{a} : \vec{x}, B) \geq \sum_{i=0}^{N-1} I(\mathbf{a}_i : \vec{x}, B)$$

$$\text{Local processing} \quad \Rightarrow \quad I(\mathbf{a}_i : \vec{x}, B) \geq I(\mathbf{a}_i : B_i)$$

$$\sum_{i=0}^{N-1} I(\mathbf{a}_i : B_i) \leq m$$



More comments on reasonability

$$I(\vec{a} : B) = 0 \quad \Rightarrow \quad I(\vec{a} : \vec{x}, B) \leq m$$

$$\mathbf{a}_i \text{ independently distributed} \quad \Rightarrow \quad I(\vec{a} : \vec{x}, B) \geq \sum_{i=0}^{N-1} I(\mathbf{a}_i : \vec{x}, B)$$

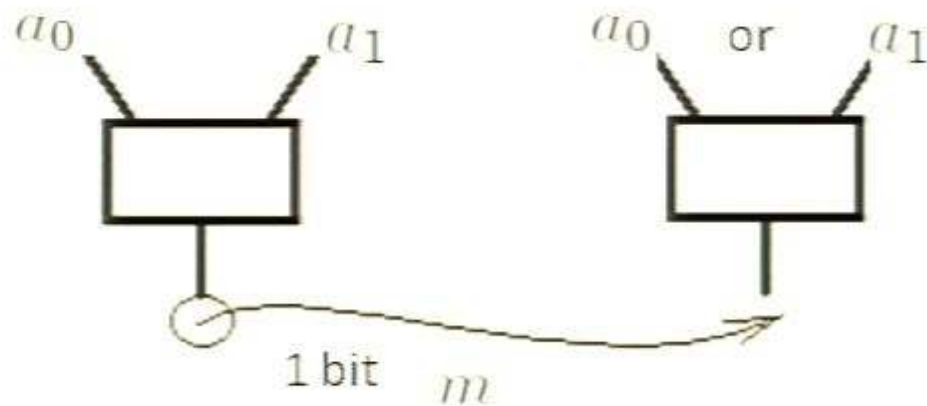
$$\text{Local processing} \quad \Rightarrow \quad I(\mathbf{a}_i : \vec{x}, B) \geq I(\mathbf{a}_i : B_i)$$

$$\sum_{i=0}^{N-1} I(\mathbf{a}_i : B_i) \leq m$$

Random access codes



$A \oplus B = ab$ with probability $\frac{3}{4}$



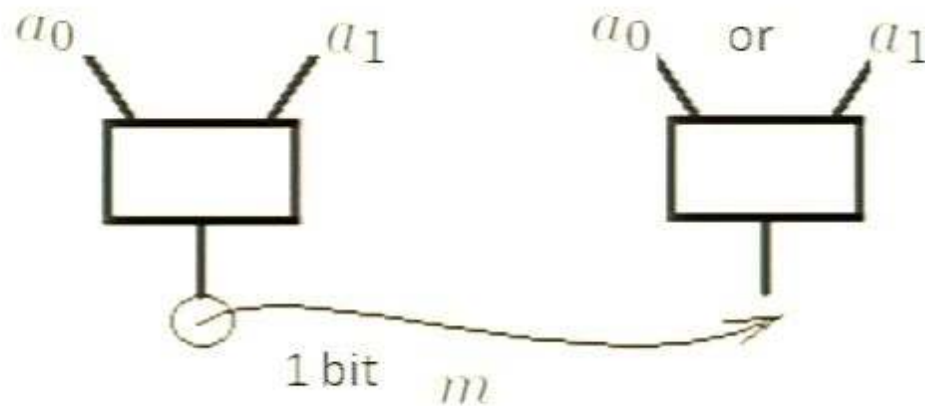
$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

Random access codes



$$A \oplus B = ab \text{ with probability } \frac{1}{3}$$



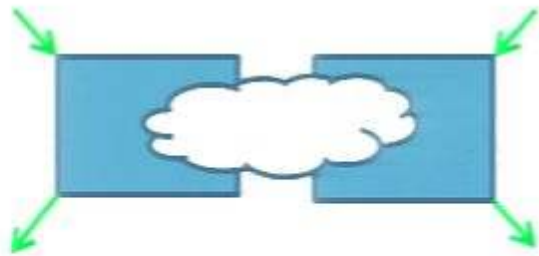
$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

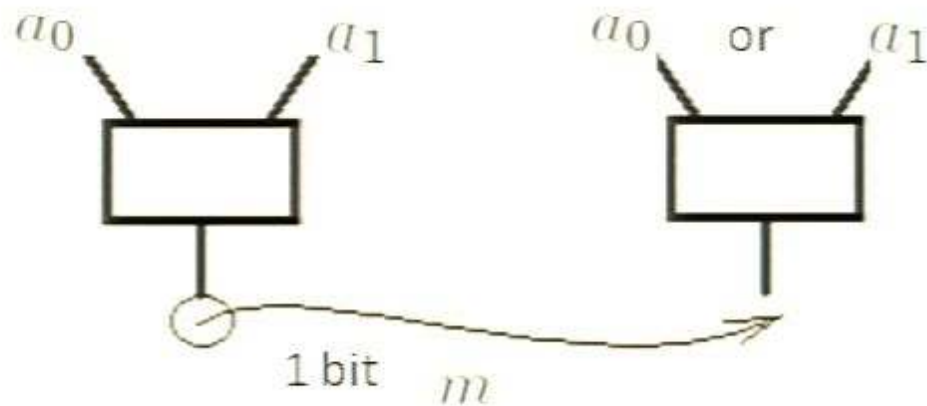
$$B \oplus m = B \oplus A \oplus a_0 = ab \oplus a_0 = (a_0 \oplus a_1)b \oplus a_0 = a_b$$



Random access codes



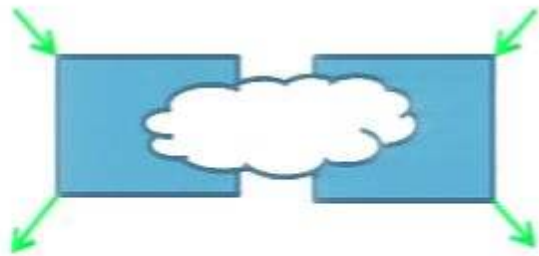
$A \oplus B = ab$ with probability $\frac{3}{4}$



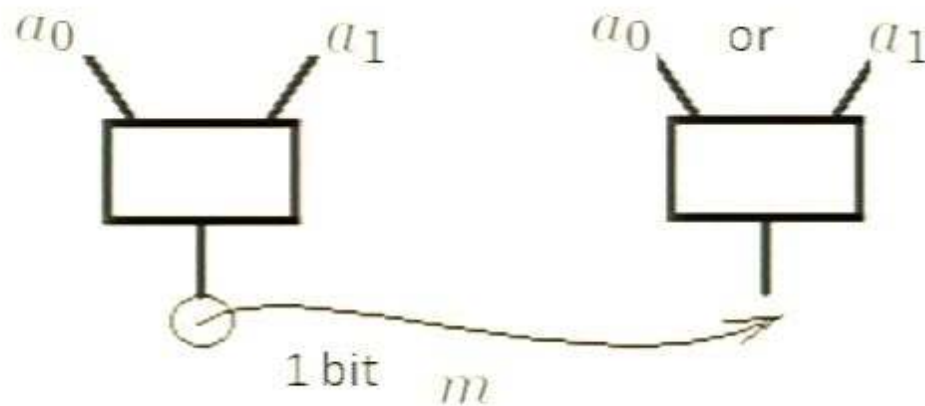
$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

Random access codes



$$A \oplus B = ab \text{ with probability } \frac{1}{3}$$



$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

$$B \oplus m = B \oplus A \oplus a_0 = ab \oplus a_0 = (a_0 \oplus a_1)b \oplus a_0 = a_b$$

(N → m) Random access code

$\vec{a} = (a_0, a_1, \dots, a_{N-1})$ independent of \mathbb{B}



\vec{x}

m -bits



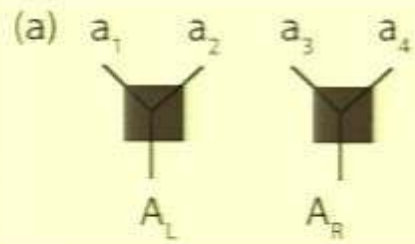
B_i



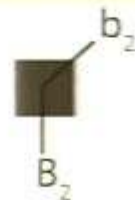
i

$$\sum_{i=0}^{N-1} I(a_i : B_i) \leq m$$

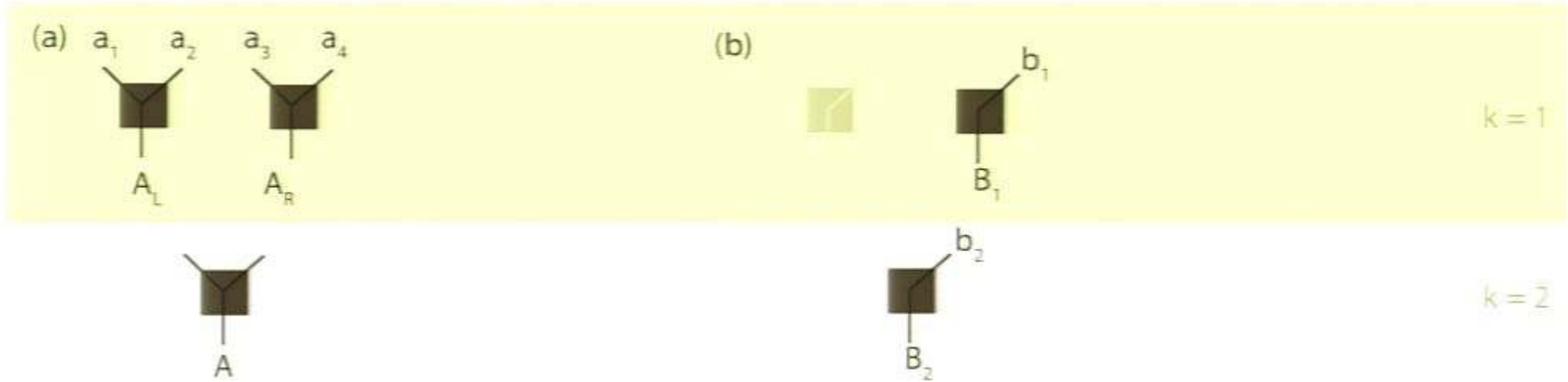




$k=1$



$k=2$



Information causality holds in every theory that allows introduction of „mutual information”

$$I(A:B)$$

1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object
4. Chain rule

Information causality holds in every theory that allows introduction of „mutual information”

$$I(A:B)$$

1. No-signaling
 2. Data processing inequality
 3. Bounded by m for classical object
 4. Chain rule
- $$I(A:B) = 0$$

Information causality holds in every theory that allows introduction of „mutual information”

$$I(A:B)$$

1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object
4. Chain rule

$$A \rightarrow B \rightarrow C$$

$$I(A:B) \geq I(A:C)$$

Information causality holds in every theory that allows introduction of „mutual information”

$$I(A : B)$$

1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object
4. Chain rule

If A has 2^m letter alphabet

$$I(A : A) \leq m$$

Information causality holds in every theory that allows introduction of „mutual information”

$$I(A : B)$$

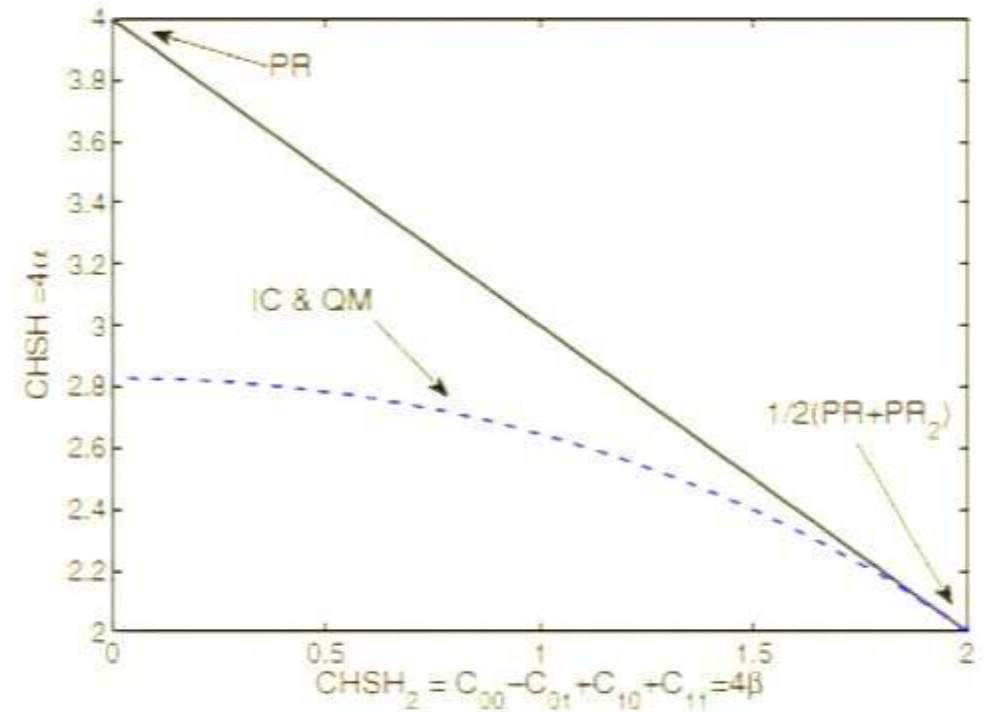
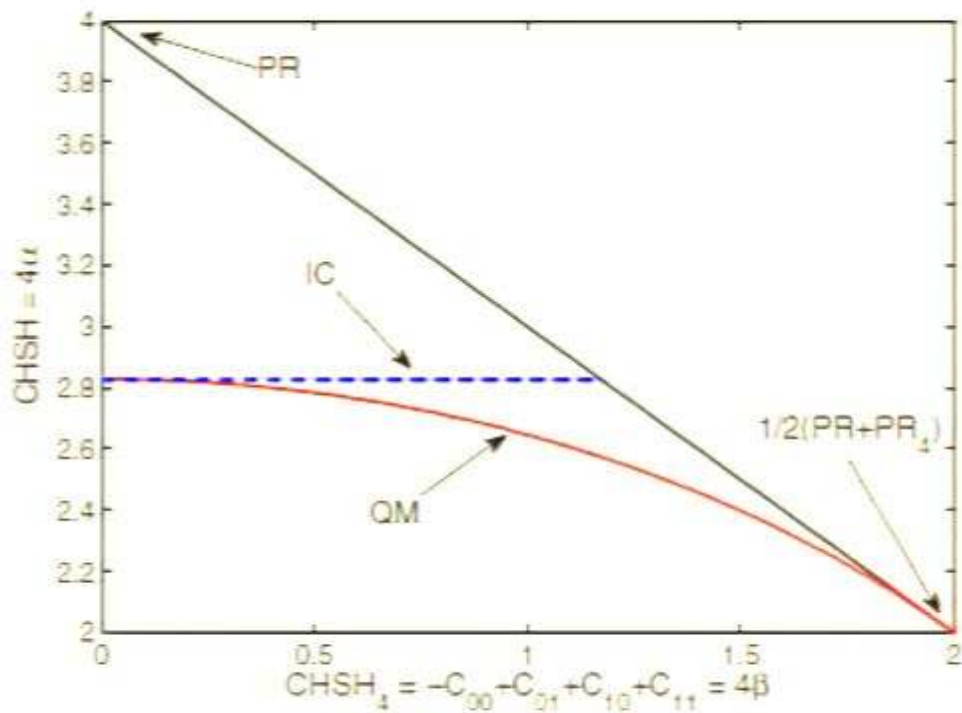
1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object

4. Chain rule

$$I(A : B, C) = I(A : B) + I(A : C | B)$$

$$I(A : B, C) + I(C : B) = I(A : B) + I(C : A, B)$$

Unballanced boxes



$$\beta = \frac{1}{4} \sum_{a,b} P(A \oplus B = ab | a, b)$$

Information causality holds in every theory that allows introduction of „mutual information”

$$I(A : B)$$

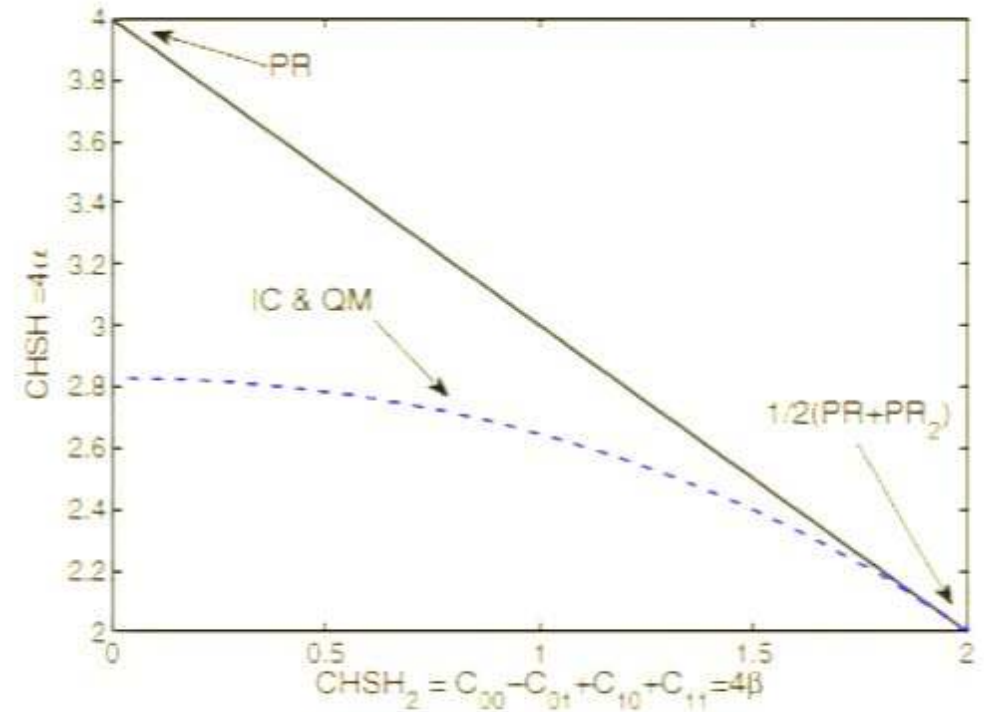
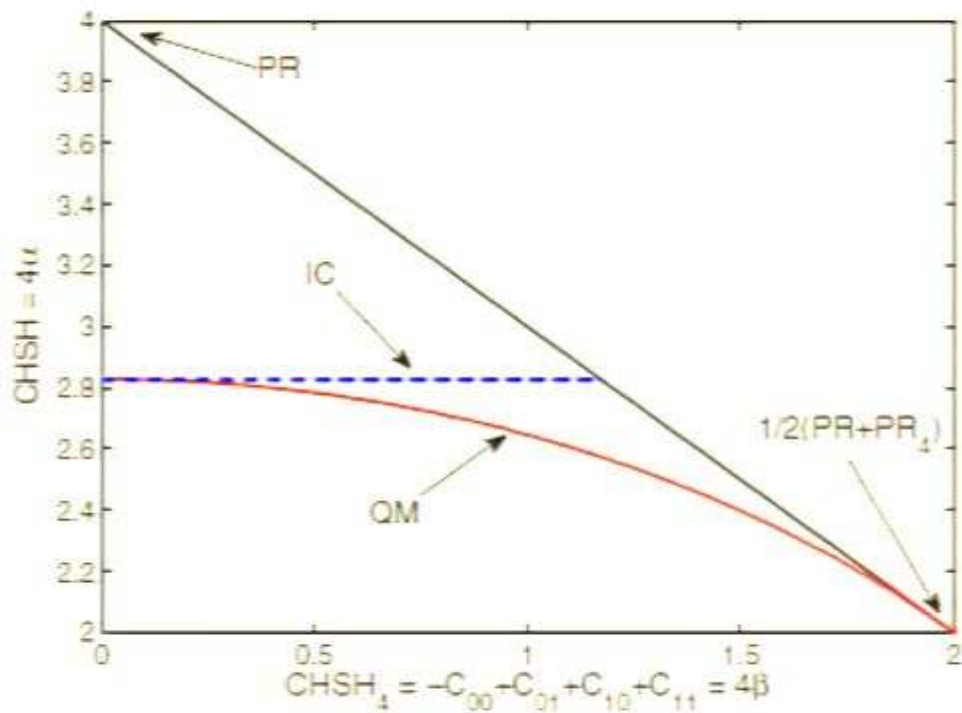
1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object

4. Chain rule

$$I(A : B, C) = I(A : B) + I(A : C | B)$$

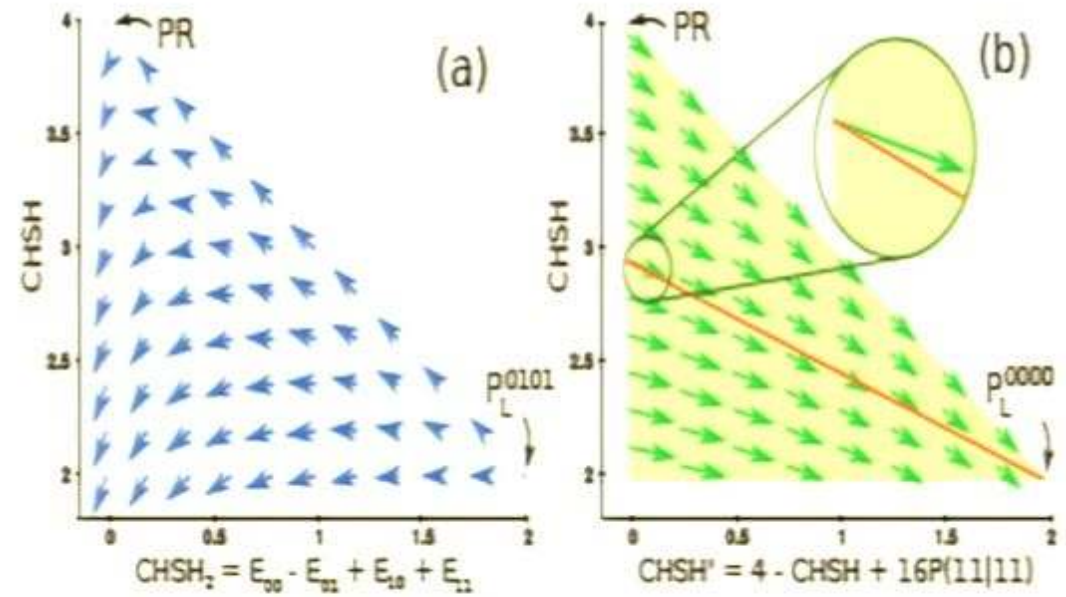
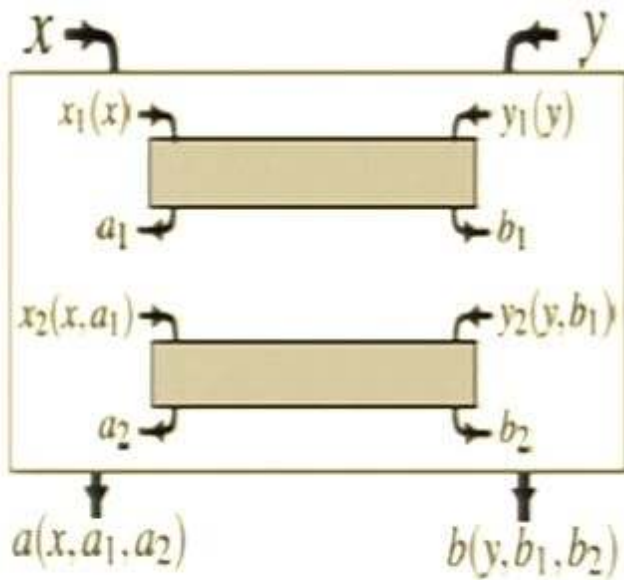
$$I(A : B, C) + I(C : B) = I(A : B) + I(C : A, B)$$

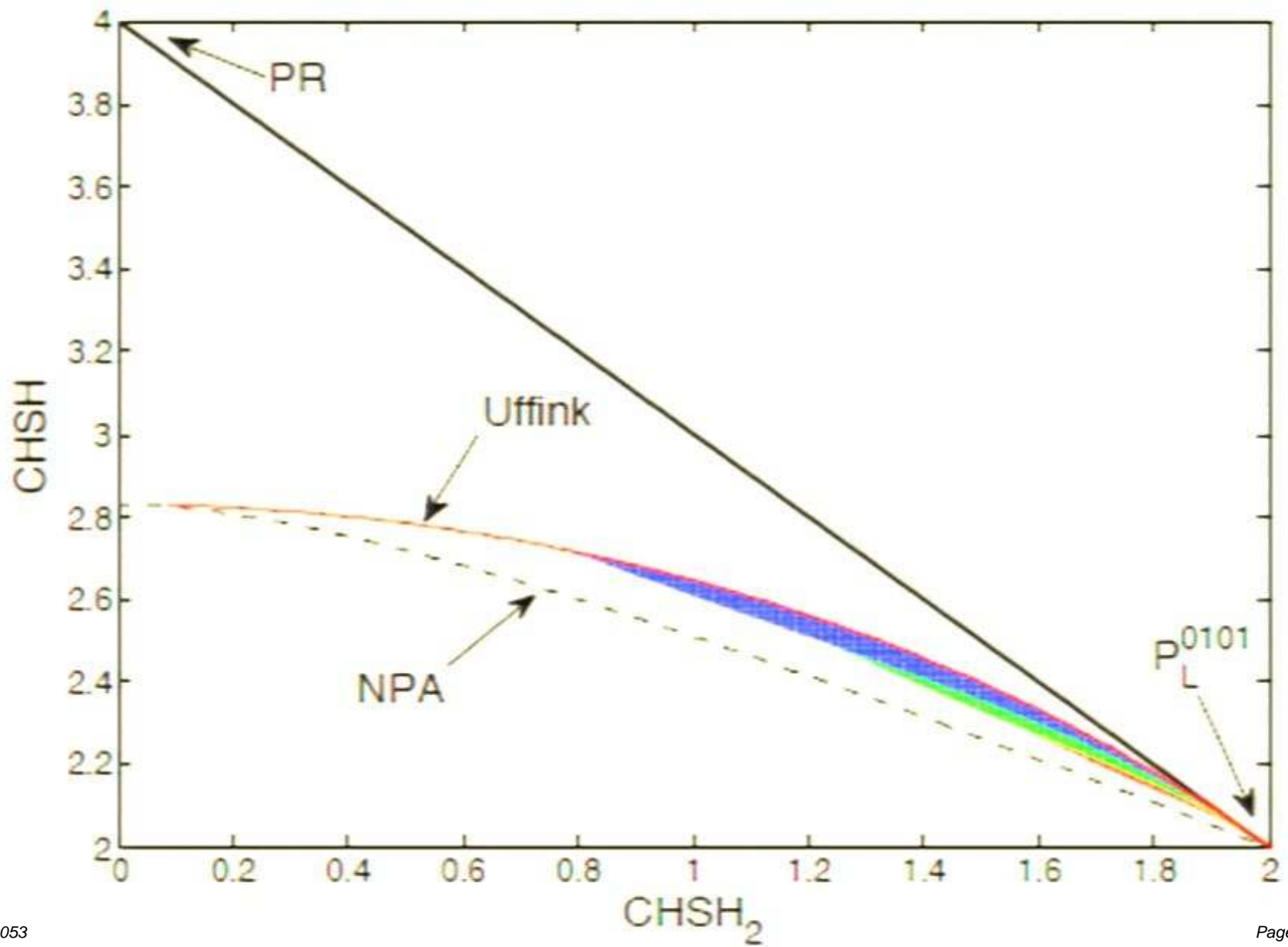
Unballanced boxes



$$\beta = \frac{1}{4} \sum_{a,b} P(A \oplus B = ab | a, b)$$

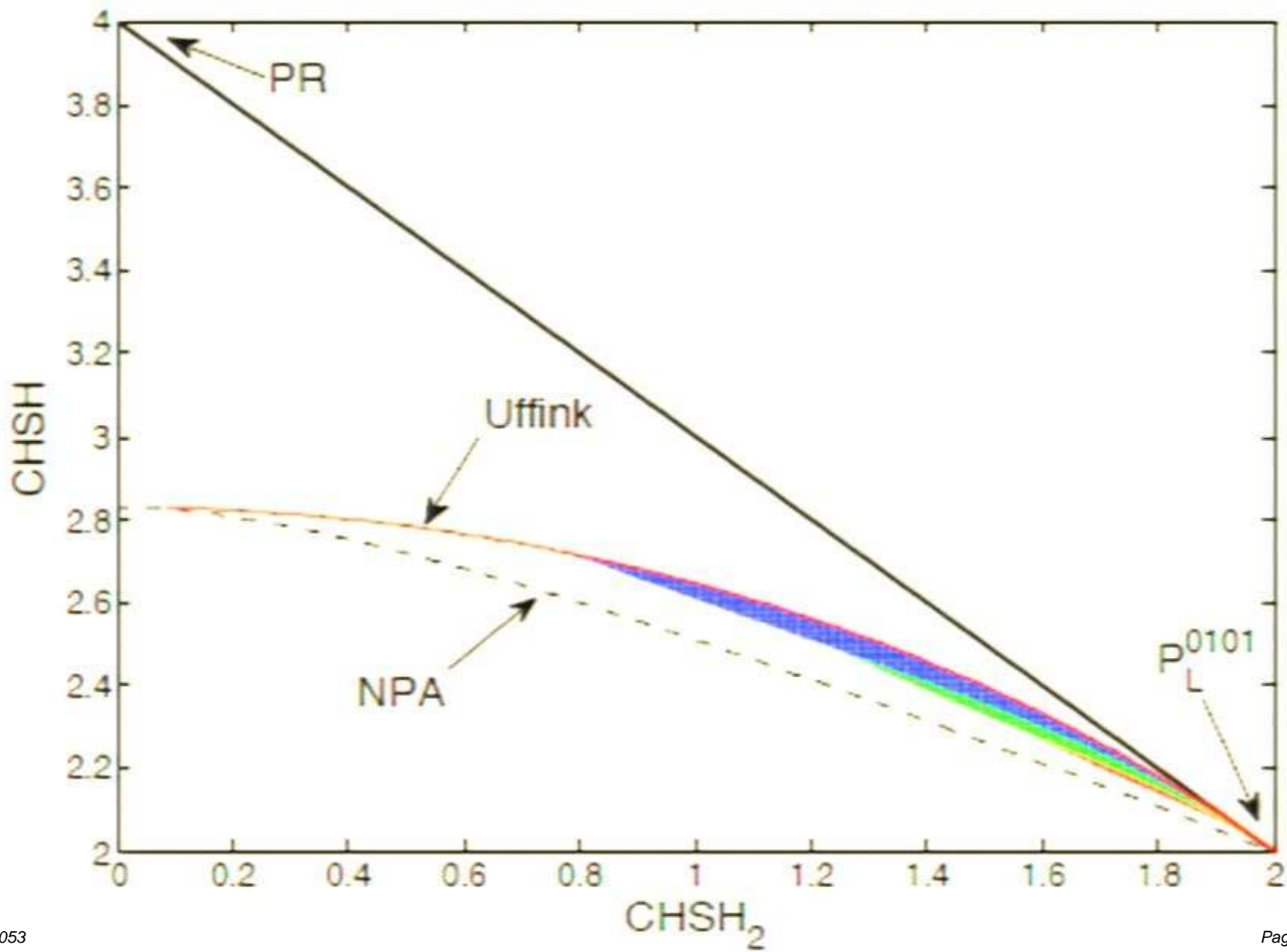
Distillation





More complicated boxes

Other stuff



More complicated boxes

Other stuff

More complicated boxes

- Every $(n \rightarrow 1)$ RAC

Other stuff

More complicated boxes

- Every $(n \rightarrow 1)$ RAC
- Multipartite boxes

Other stuff

More complicated boxes

- Every $(n \rightarrow 1)$ RAC
- Multipartite boxes
- 2 inputs more outputs

Other stuff

More complicated boxes

- Every $(n \rightarrow 1)$ RAC
- Multipartite boxes
- 2 inputs more outputs

Other stuff

- Uncertainty relations

More complicated boxes

- Every $(n \rightarrow 1)$ RAC
- Multipartite boxes
- 2 inputs more outputs

Other stuff

- Uncertainty relations
- Application in crypto

More complicated boxes

- Every $(n \rightarrow 1)$ RAC
- Multipartite boxes
- 2 inputs more outputs

Other stuff

- Uncertainty relations
- Application in crypto
- Information causality and the size of the universe

Information causality holds in every theory that allows introduction of „mutual information”

$$I(A:B)$$

1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object
4. Chain rule

$$A \rightarrow B \rightarrow C$$

$$I(A:B) \geq I(A:C)$$

Information causality holds in every theory that allows introduction of „mutual information”

$$I(A:B)$$

1. No-signaling
 2. Data processing inequality
 3. Bounded by m for classical object
 4. Chain rule
- $$I(A:B) = 0$$