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

De Pedalternorotandomovens centroculatus articulosus ontstond,(generatio spontanea!) uit onbevredigdheid over het in de natuur ontbreken van wielvormige, levende schepselen met het vermogen zich rollend voort te bewegen. Het hierbij afgebeelde diertje, in de volksmond genaamd „wentelteefje" of „rolpens", tracht dus in een diepgevoelde behoefte te voorzien. Biologische bijzonderheden zijn nog schaars: is het een zoogdier, een reptiel of een insekt? Het heeft een langgerekt, uit verhoornde geledingen gevormd lichaam en drie paren poten, waarvan de uiteinden gelijkenis vertonen met de menselijke voet. In het midden van de dikke, ronde kop, die voorzien is van een sterk gebogen papagaaiensnavel, bevinden zich de bolvormige ogen, die, op stelen geplaatst, ter weerszijden van de kop ver uitsteken. In gestrekte positie kan het dier zich, traag en bedachtzaam, door middel van zijn zes poten, voort bewegen over een willekeurig substraat (het kan eventueel steile trappen opklimmen of afdalen, door struikgewas heendringen of over rotsblokken klauteren). Zodra het echter een lange weg moet afleggen en daartoe een betrekkelijk vlakke baan tot zijn beschikking heeft, drukt het zijn kop op de grond en rolt zich bliksemsnel op, waarbij het zich afduwt met zijn poten, voor zoveel deze dan nog de grond raken. In opgerolde toestand vertoont het de gedaante van een discus-schijf, waarvan de centrale as gevormd wordt door de ogen-op-stelen. Door zich beurtelings af te zetten met één van zijn drie paren poten, kan het een grote snelheid bereiken. Ook trekt het naar believen tijdens het rollen (bv. bij het afdalen van een helling, of om zijn vaart uit te lopen) de poten in en gaat „freewheelende" verder. Wanneer het er aanleiding toe heeft, kan het op twee wijzen weer in wandel-positie overgaan: ten eerste abrupt, door zijn lichaam plotseling te strekken, maar dan ligt het op zijn rug, met zijn poten in de lucht en ten tweede door geleidelijke snelheidsvermindering (remming met de poten) en langzame achterwaartse ontrolling in stilstaande toestand.

XI-'51

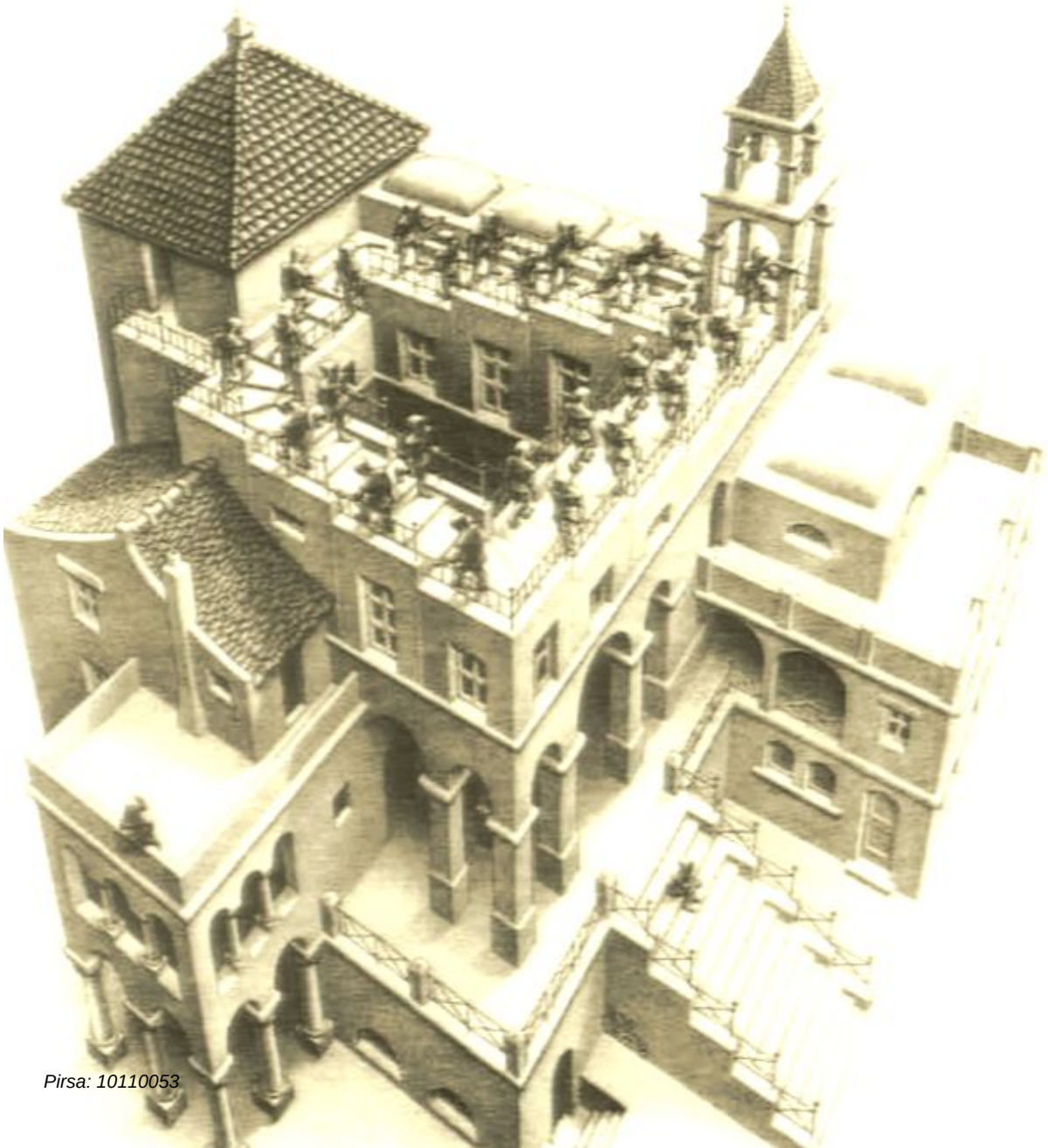
Why?

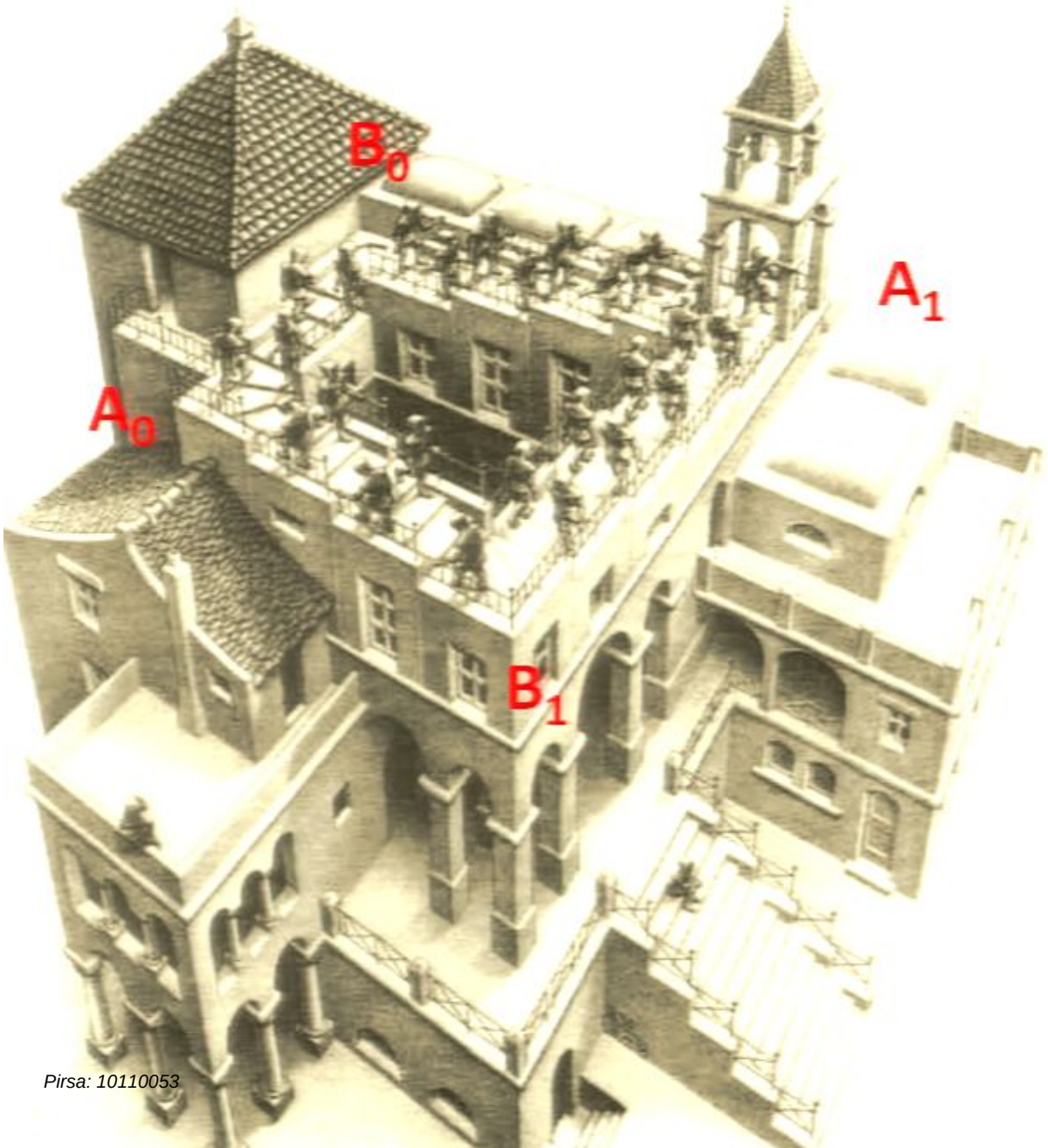
What?

How?

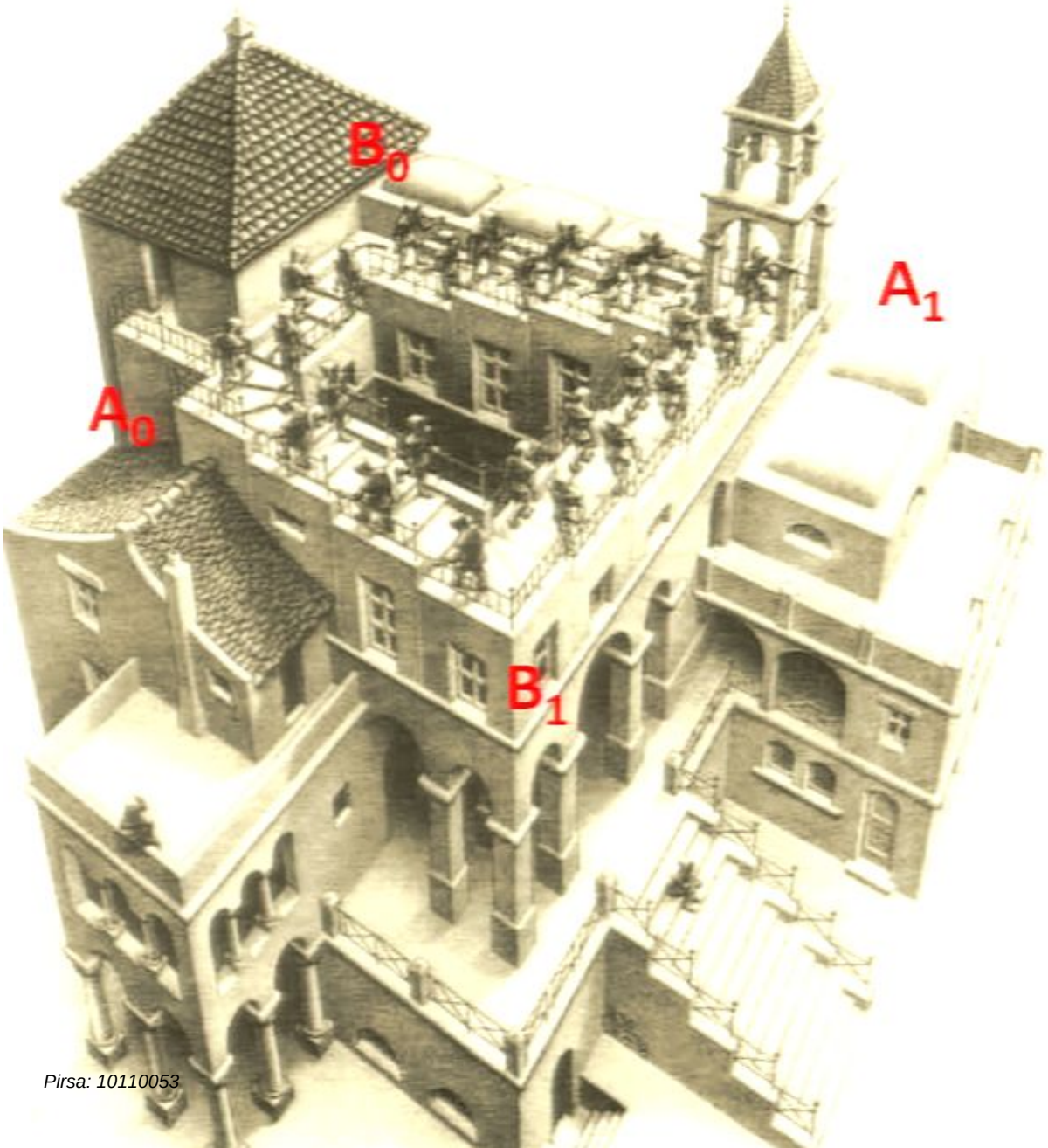
Results

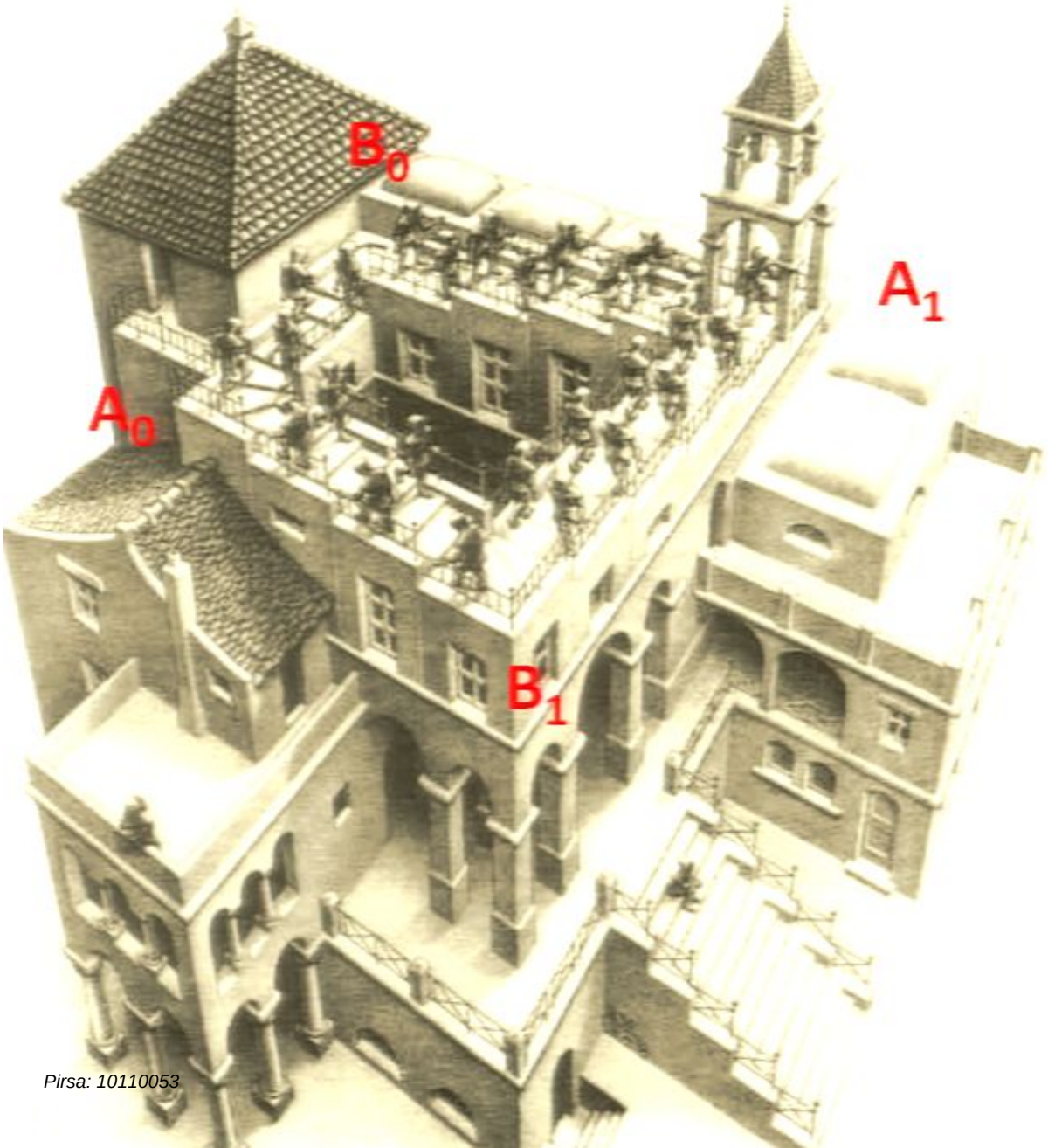
Why?




B_0
A_1
A_0
B_1

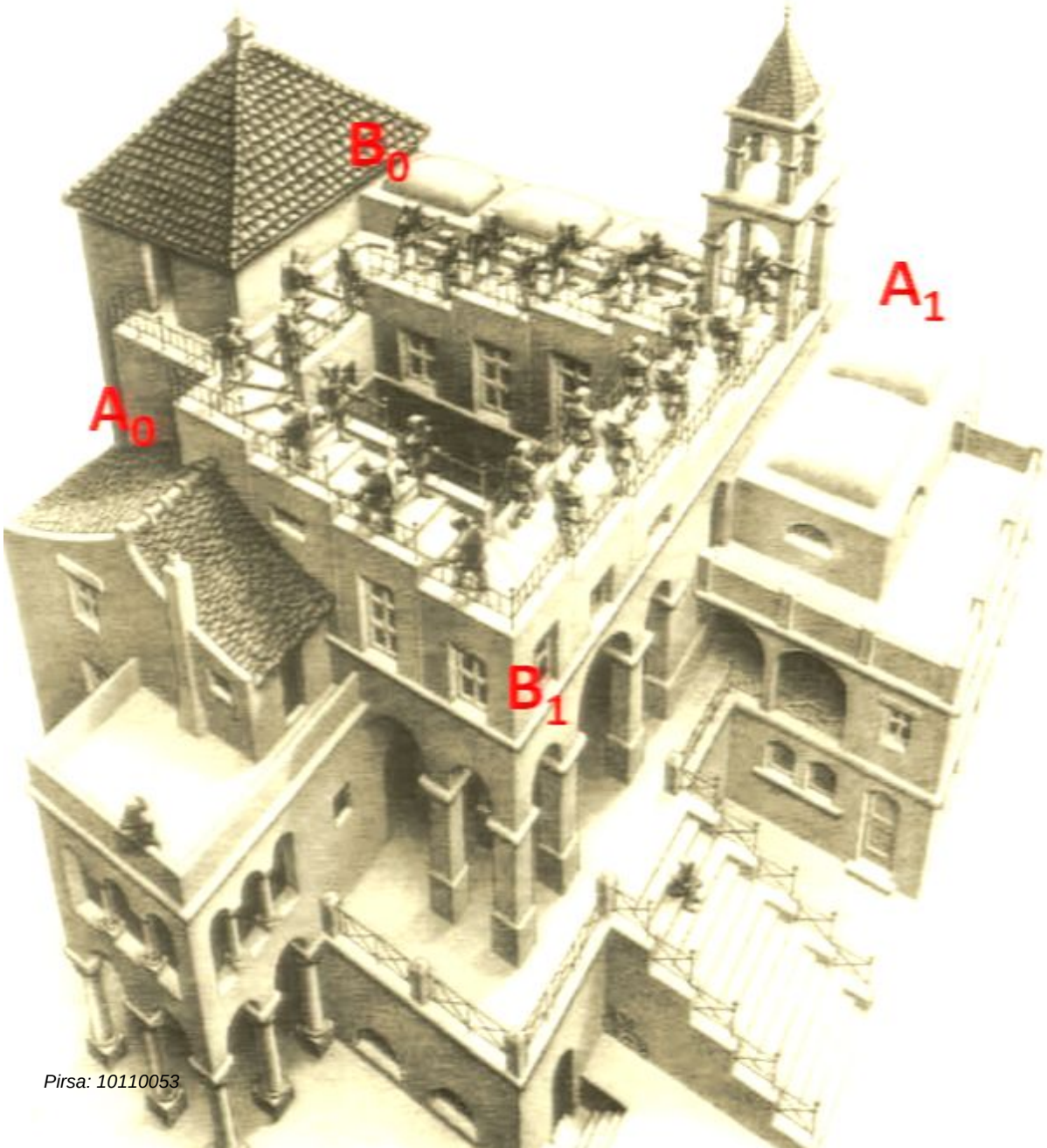
$A_0 > B_0 > A_1 > B_1 \geq A_0$





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

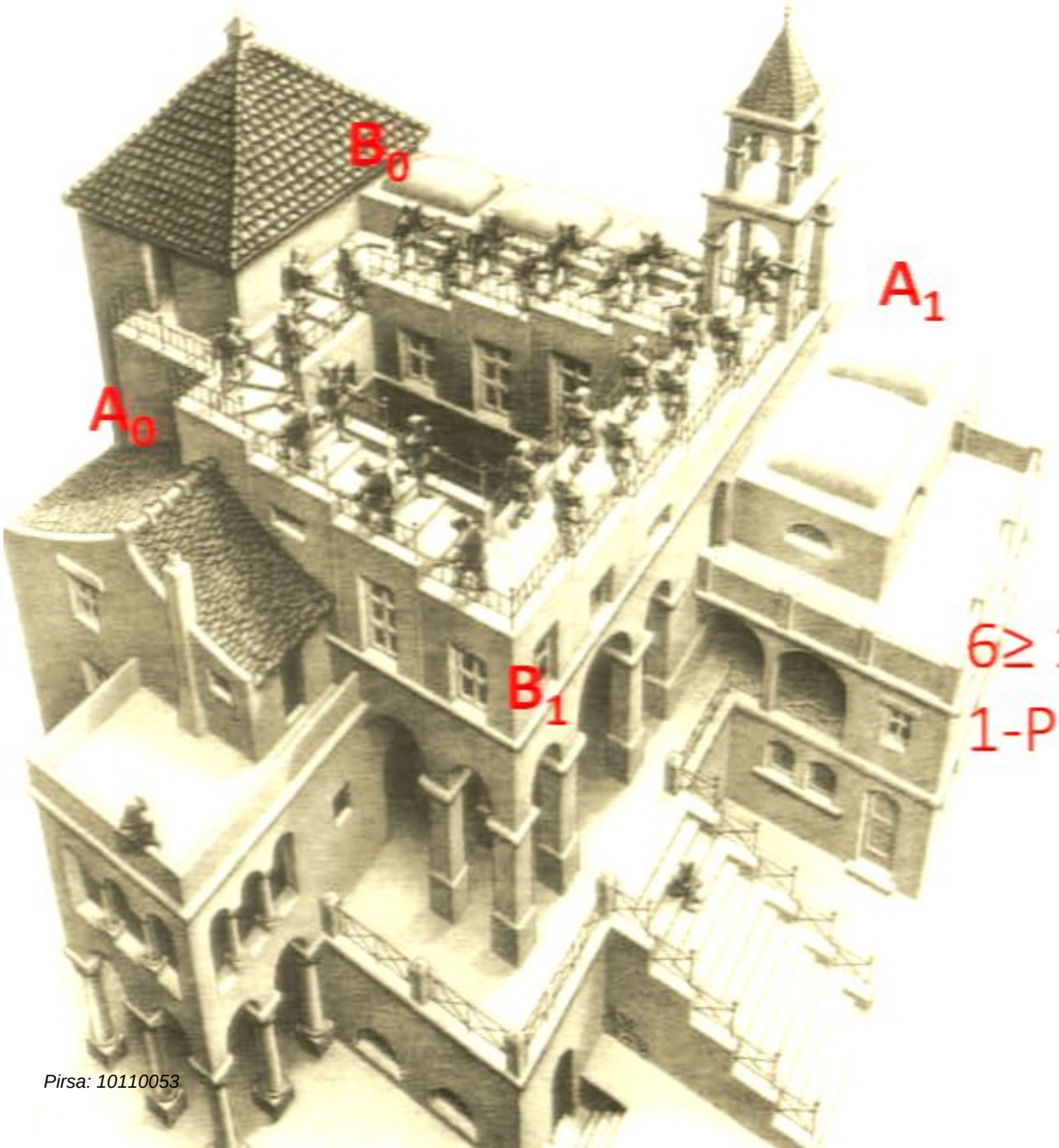
$$3 \geq P(A_0 > B_0) + P(B_0 > A_1) + P(A_1 > B_1) + P(B_1 \geq A_0) \geq 1$$



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

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

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

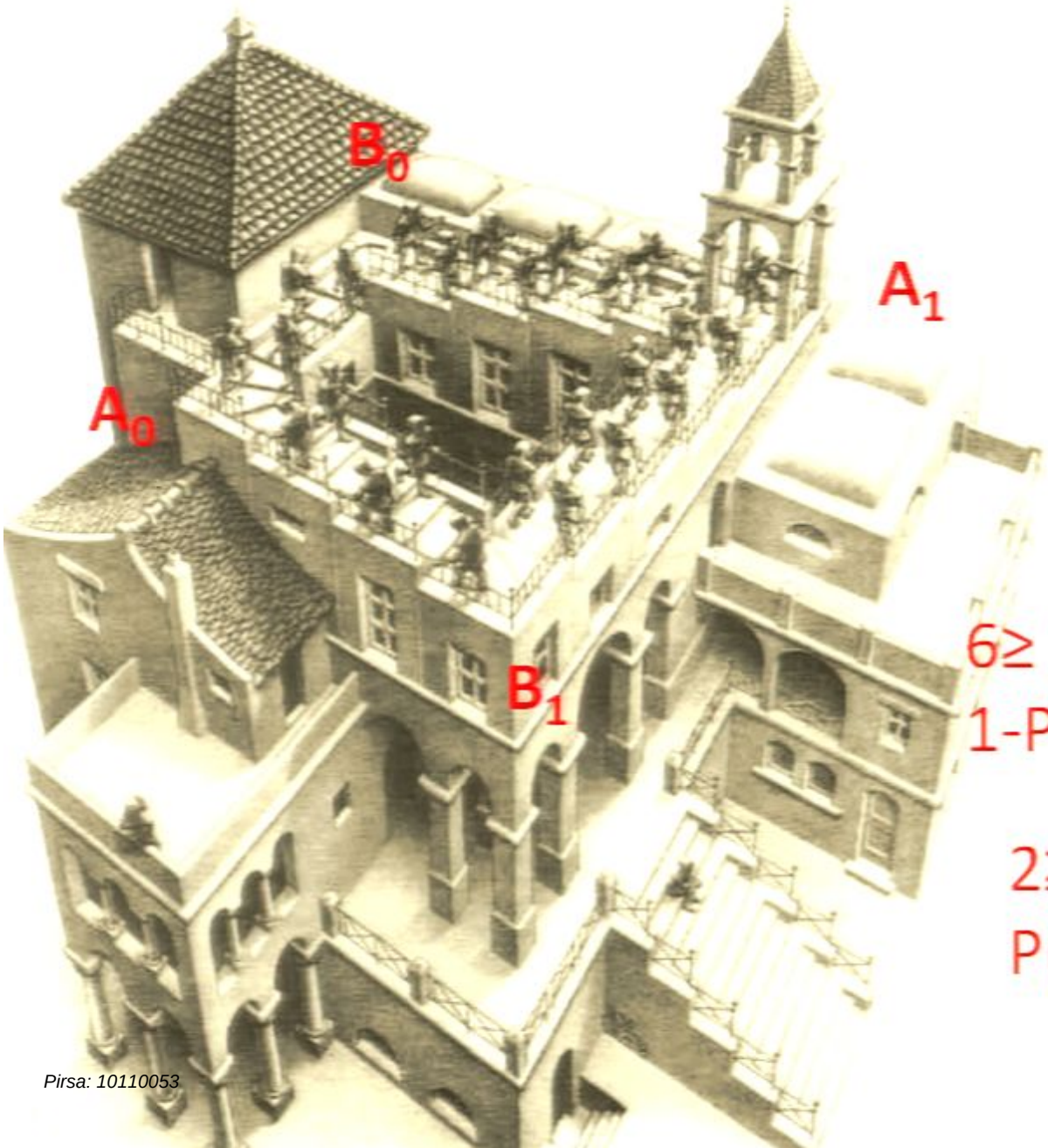


$$A_0 > B_0 > A_1 > B_1 \geq A_0$$

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

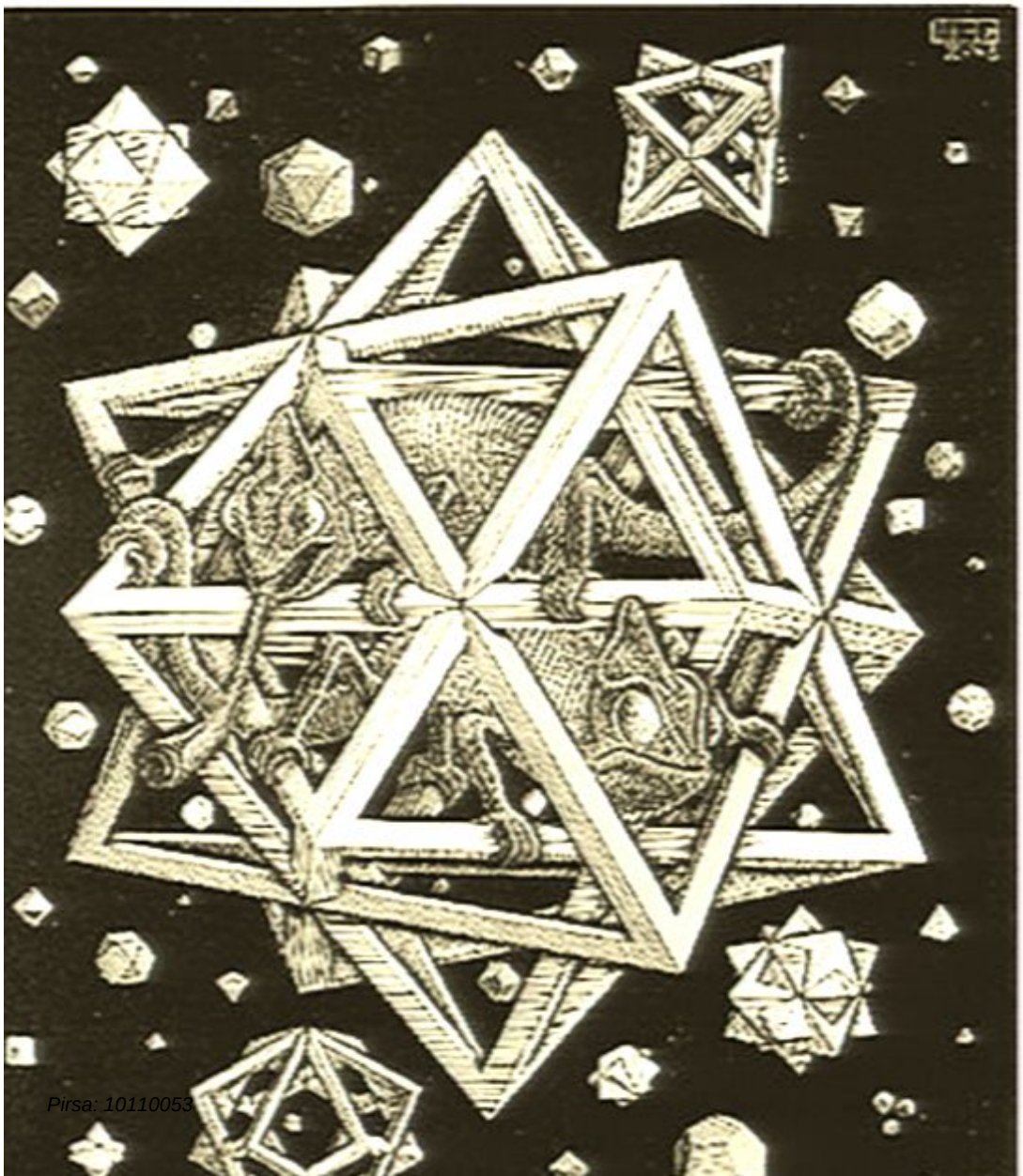
$$P(A_0=B_0)+ P(B_0=A_1)+ P(A_1=B_1) +P(B_1 \neq A_0) \leq 3$$

$$A.B.a.b \in 0.1$$

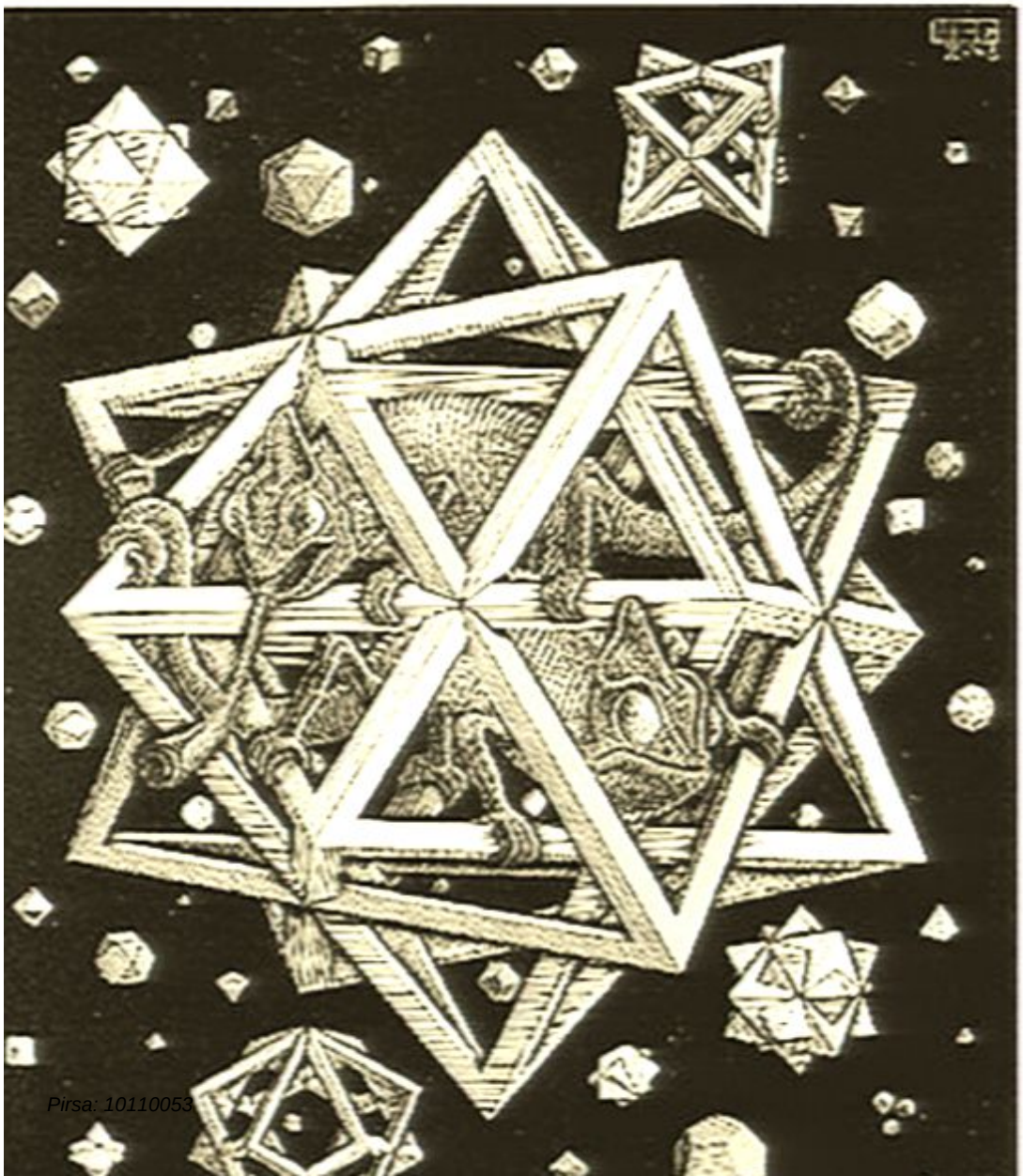
$$\beta = \frac{1}{4}\sum_{a.b} P(A \oplus B = ab|a.b) \leq \frac{3}{4}$$

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

How?

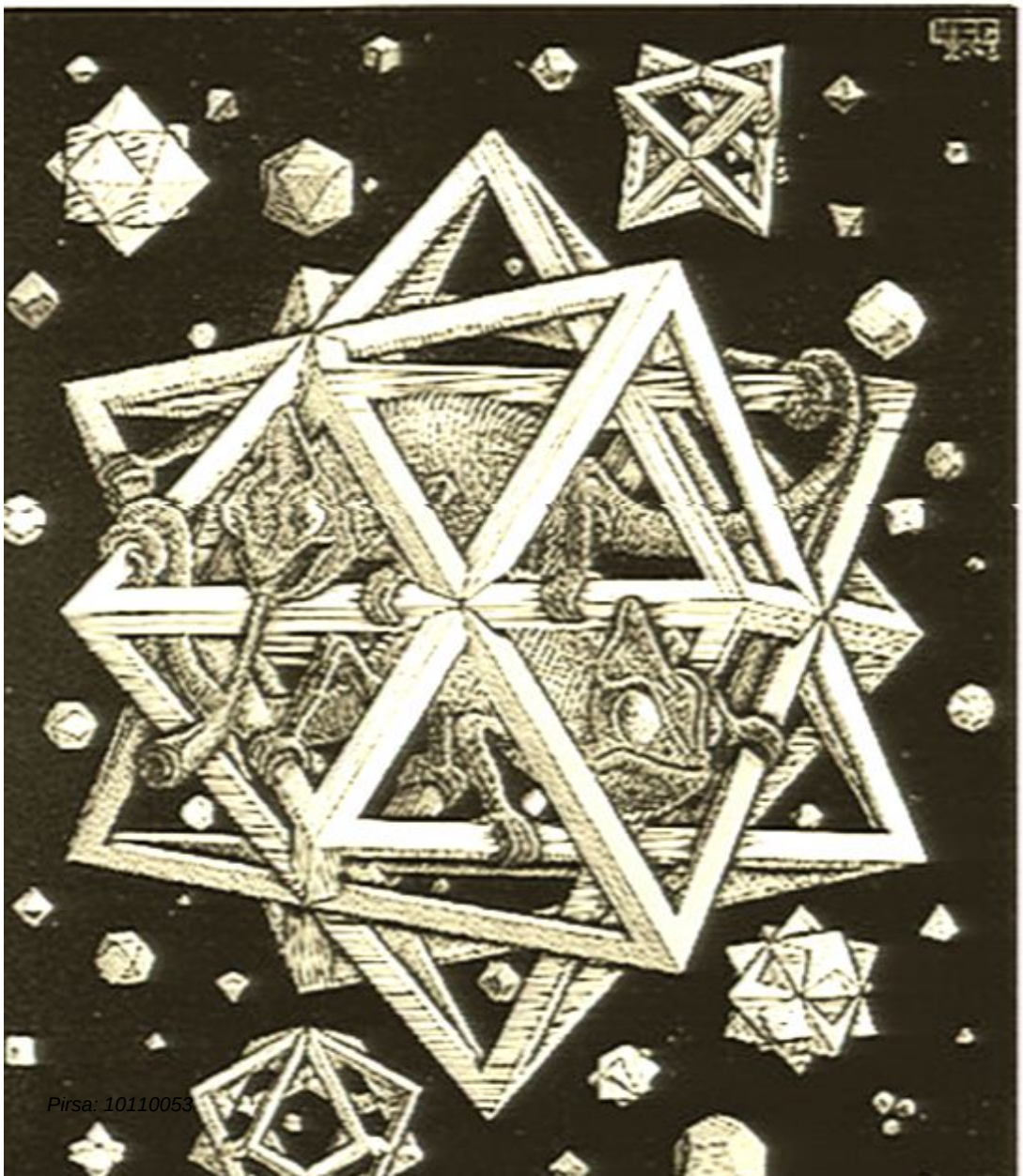


How?



No signalling

How?



No signalling

Communication complexity

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

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

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

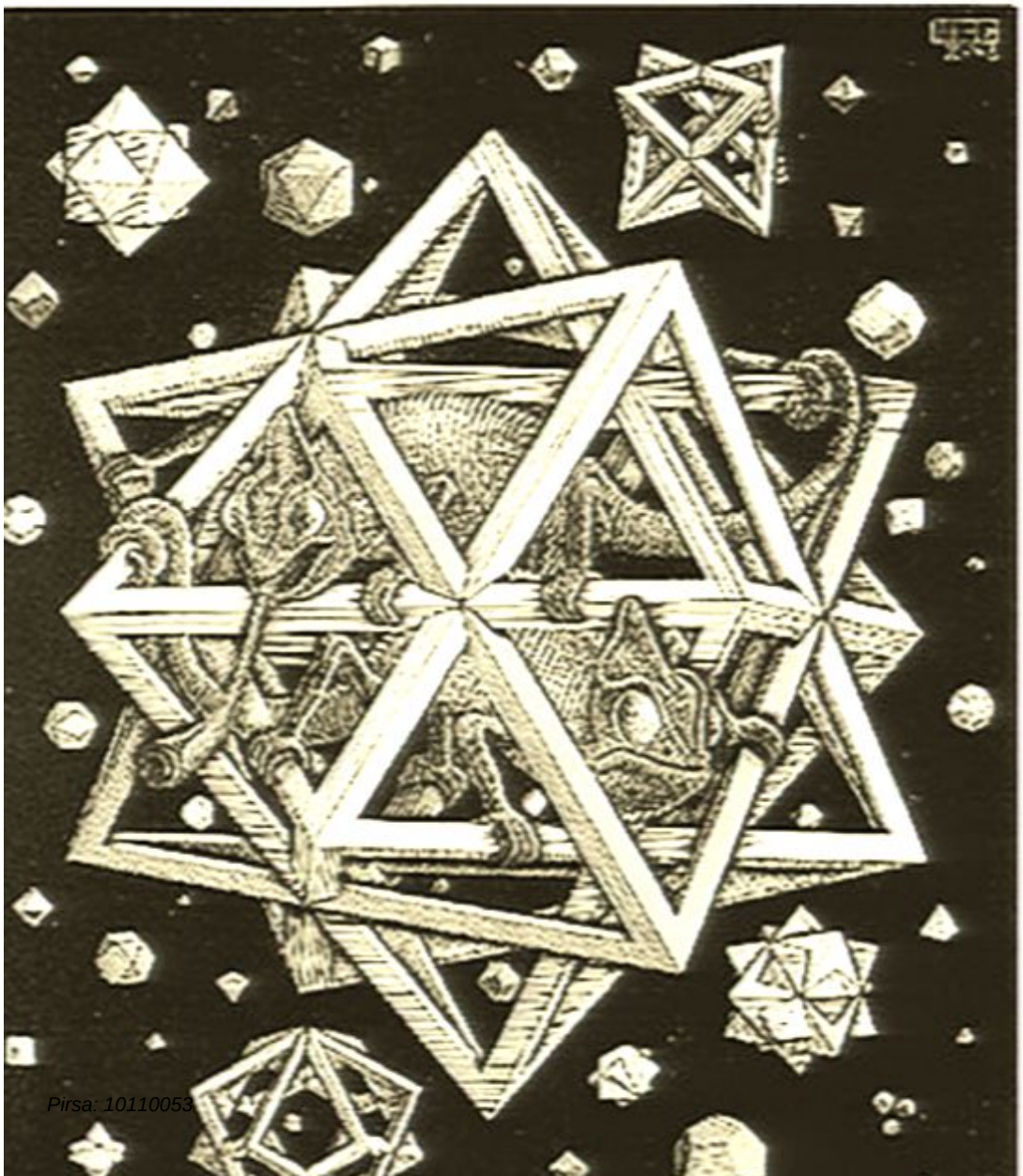
$$A, B, a, b \in 0, 1$$

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

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

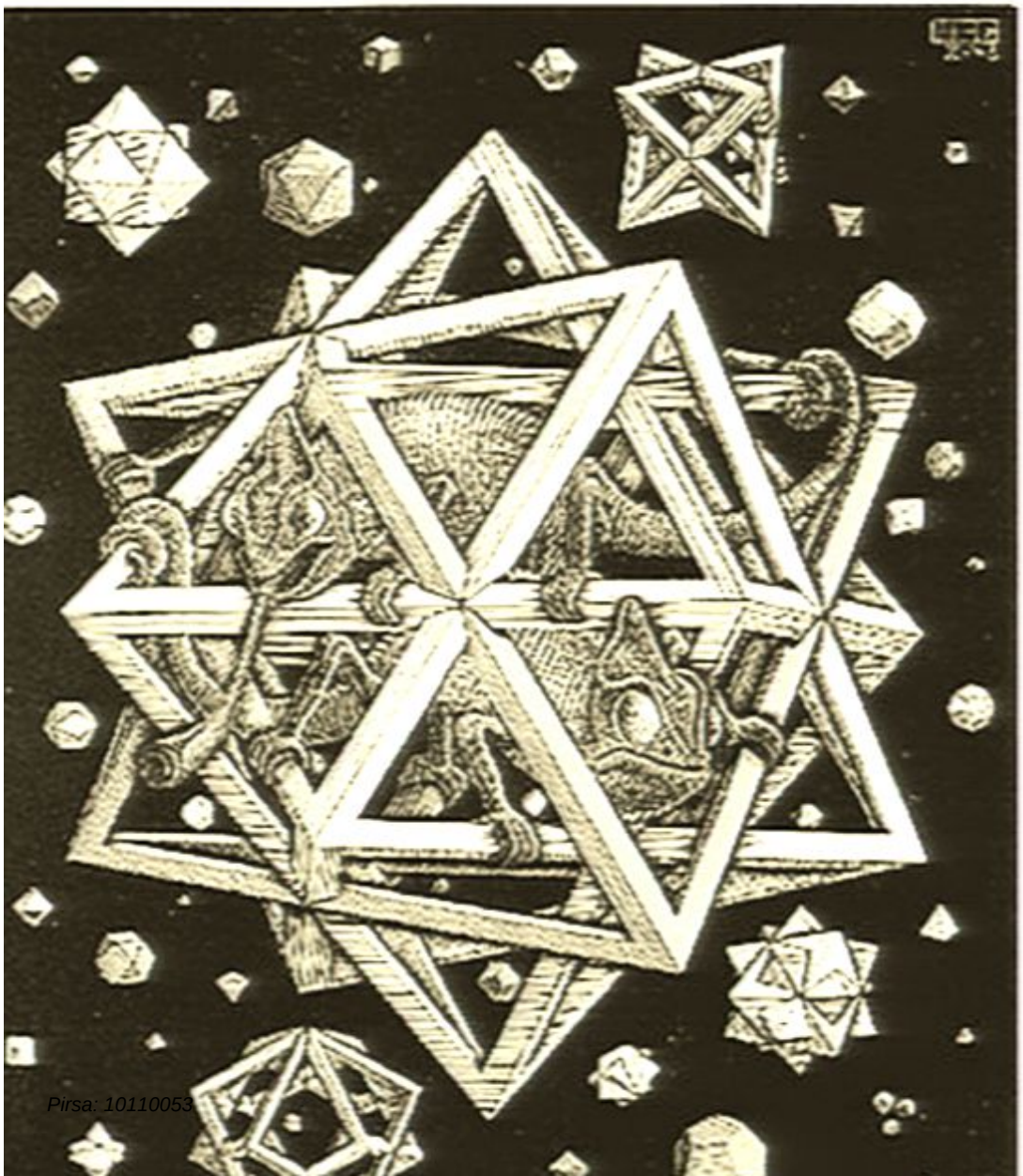
$$\beta_{NS} = 1$$

How?



No signalling

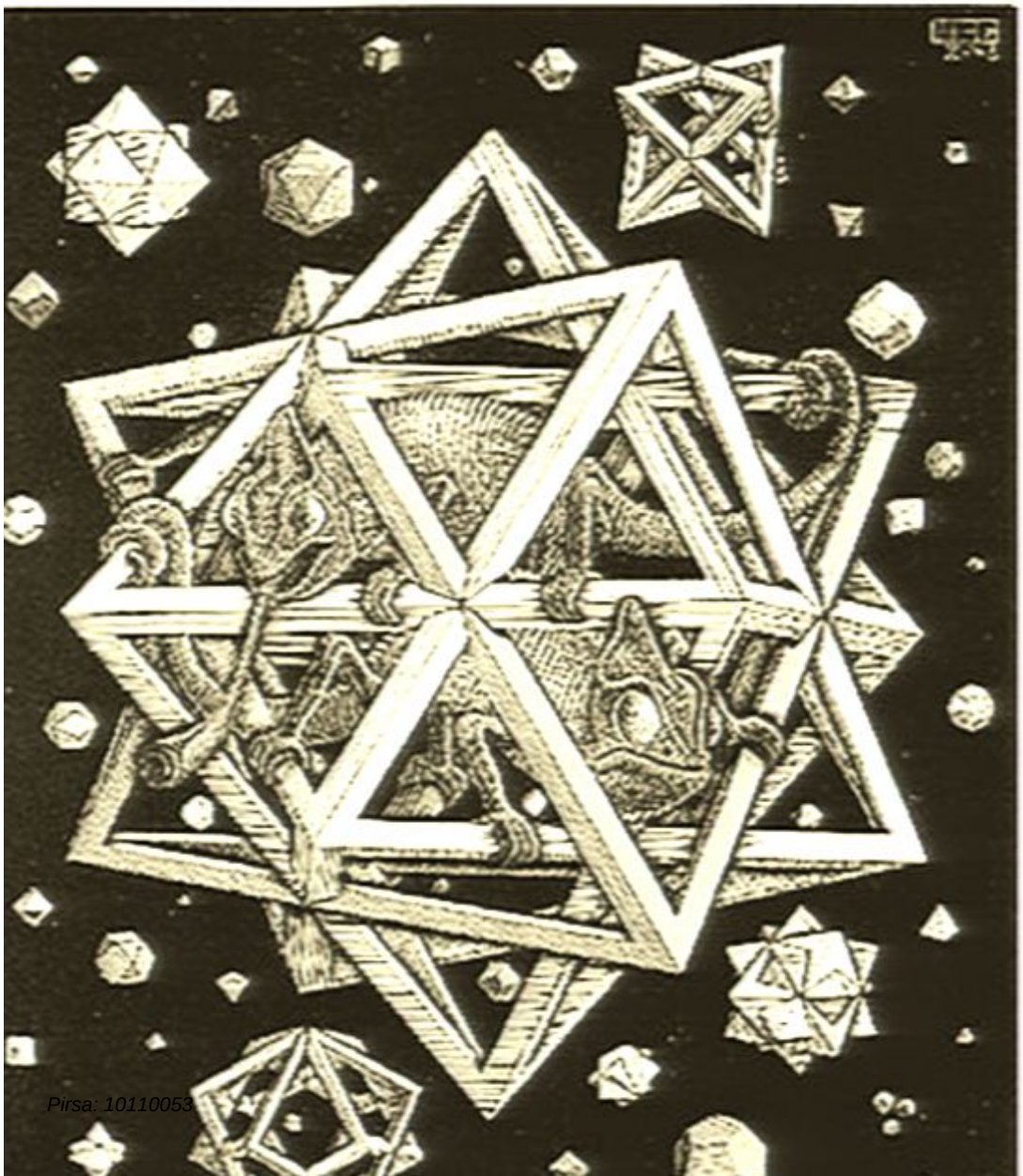
How?



No signalling

Communication complexity

How?



No signalling

Communication complexity

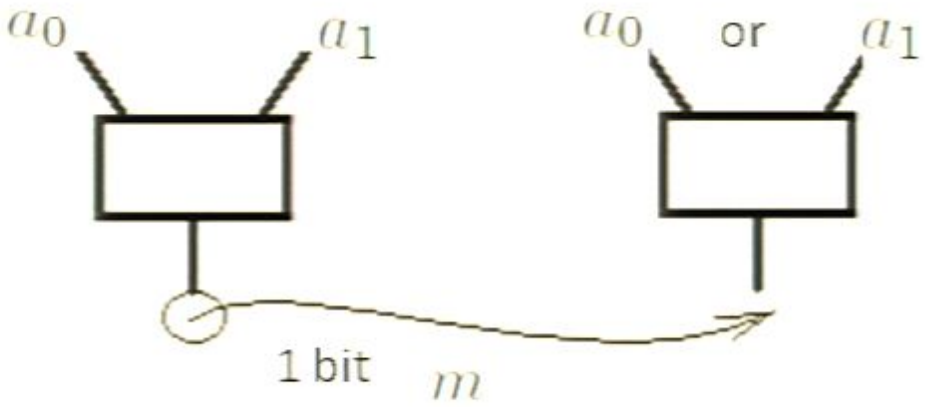
Information causality

Random access codes

$A \oplus B = ab$ with probability 3

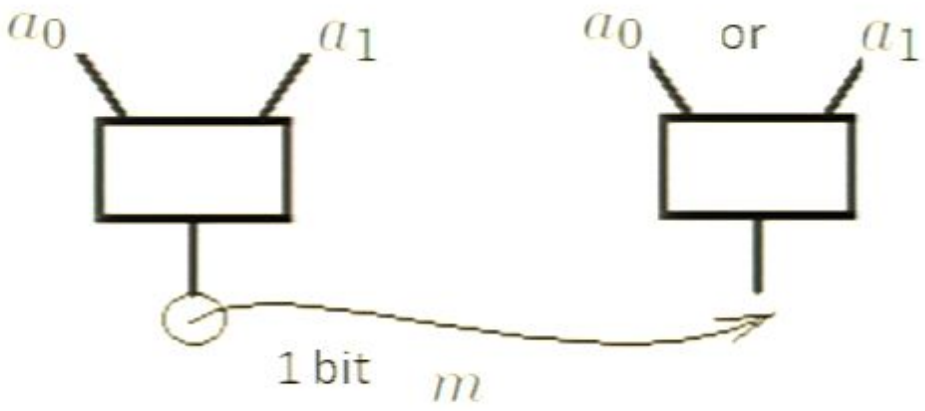
Random access codes

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



Random access codes

$A \oplus B = ab$ with probability β

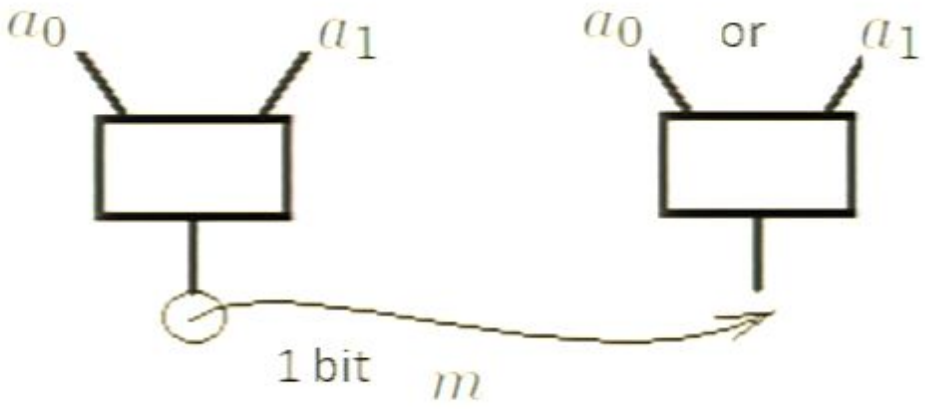


$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

Random access codes

$A \oplus B = ab$ with probability β



$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

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

(N -> m) Random access code

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

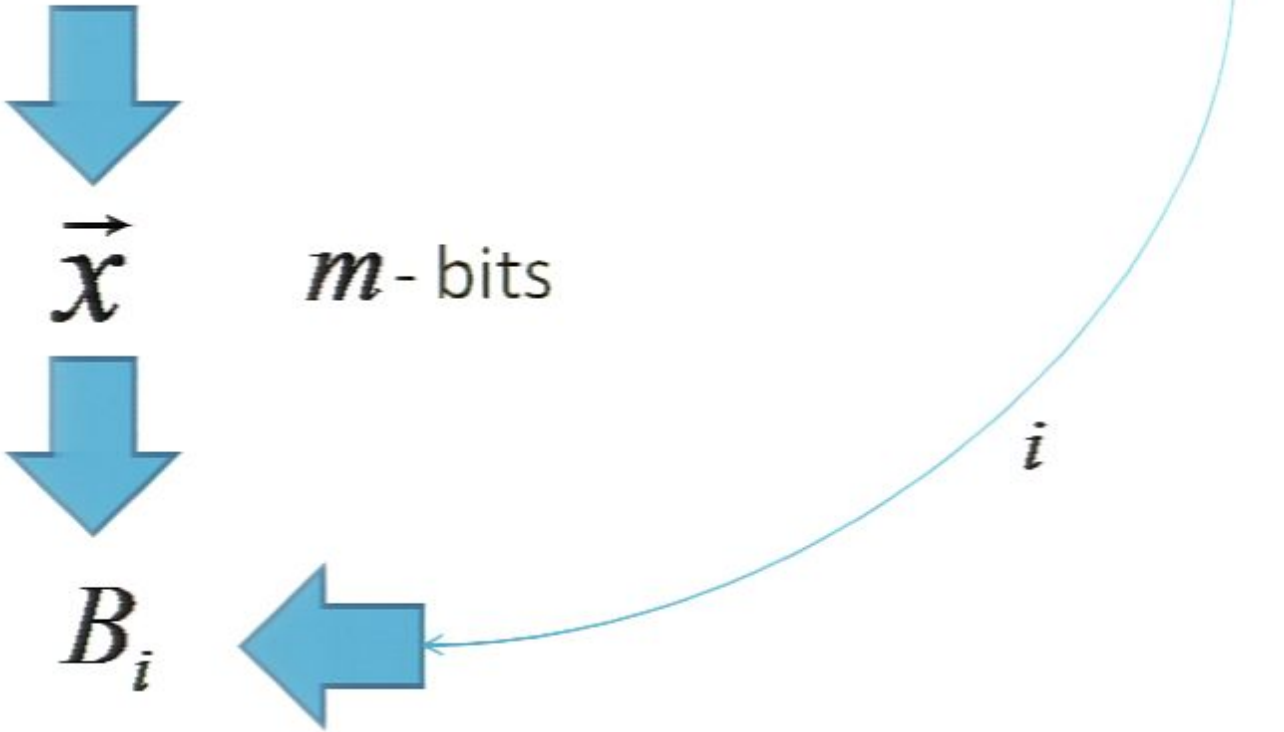
(N -> m) Random access code

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

$\vec{x}$ m - bits

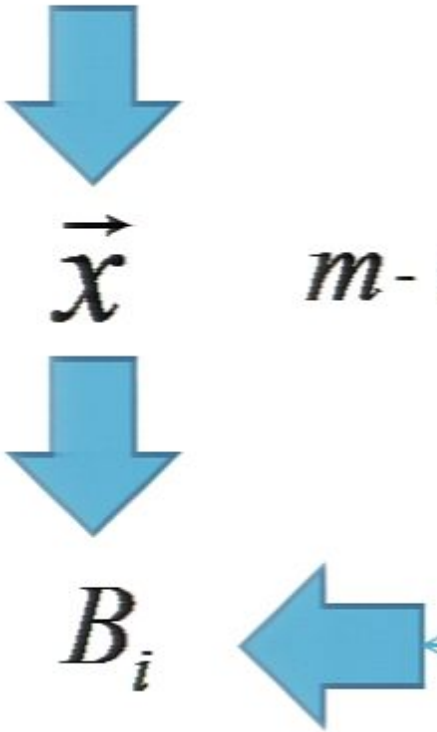
(N -> m) Random access code

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



(N -> m) Random access code

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



$\vec{x}$ m - bits

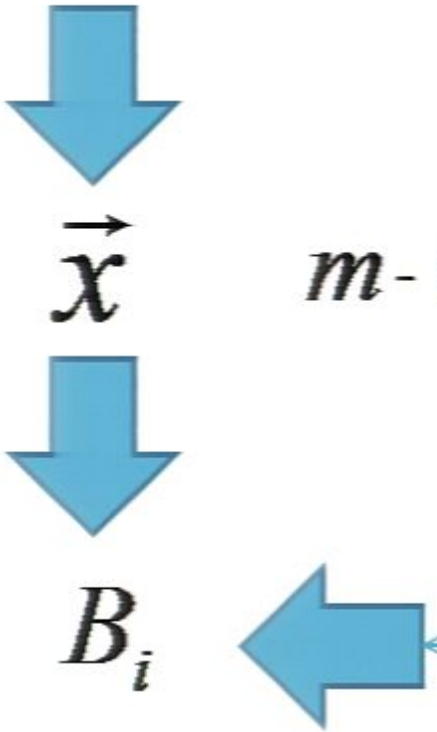
i

B_i

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

(N -> m) Random access code

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



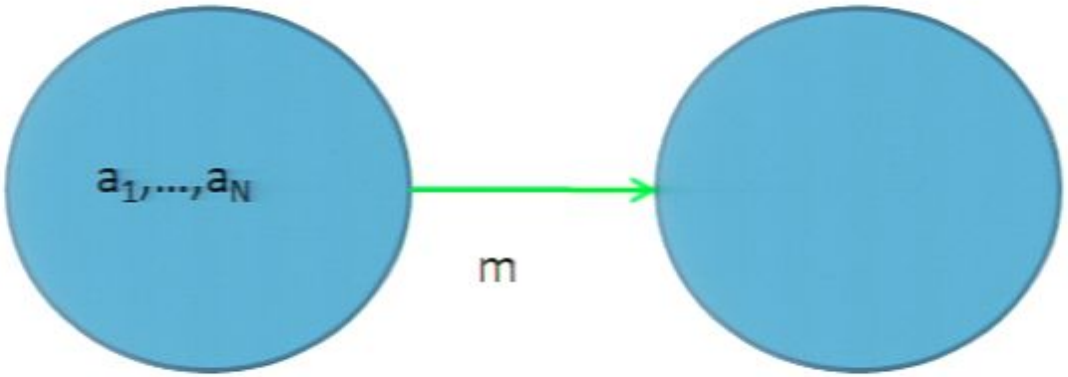
$\vec{x}$ m - bits

i

B_i

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

It is the sender who decides what the message is about



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

More comments on reasonability

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

More comments on reasonability

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

a_i indpendently distributed $\Longrightarrow$ $$I(\vec{a}:\vec{x},B)\geq \sum_{i=0}^{N-1} I(a_i:\vec{x},B)$$

More comments on reasonability

$$I(\vec{a}:B)=0 \Longrightarrow I(\vec{a}:\vec{x},B)\le m$$

a_i indpendently distributed $\Longrightarrow$ $$I(\vec{a}:\vec{x},B)\ge\sum_{i=0}^{N-1}I(a_i:\vec{x},B)$$

Local processing $\Longrightarrow$ $$I(a_i:\vec{x},B)\ge I(a_i:B_i)$$

More comments on reasonability

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

a_i indpendently distributed $\Rightarrow$ $$I(\vec{a}:\vec{x},B)\ge\sum_{i=0}^{N-1}I(a_i:\vec{x},B)$$

Local processing $\Rightarrow$ $$I(a_i:\vec{x},B)\ge I(a_i:B_i)$$

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


0.854
1
3

More comments on reasonability

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

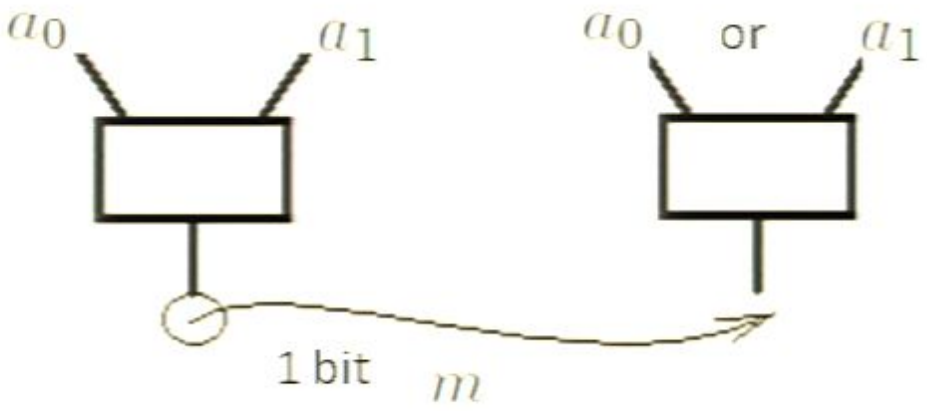
a_i indpendently distributed $\Rightarrow$ $$I(\vec{a}:\vec{x},B)\ge\sum_{i=0}^{N-1}I(a_i:\vec{x},B)$$

Local processing $\Rightarrow$ $$I(a_i:\vec{x},B)\ge I(a_i:B_i)$$

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

Random access codes

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

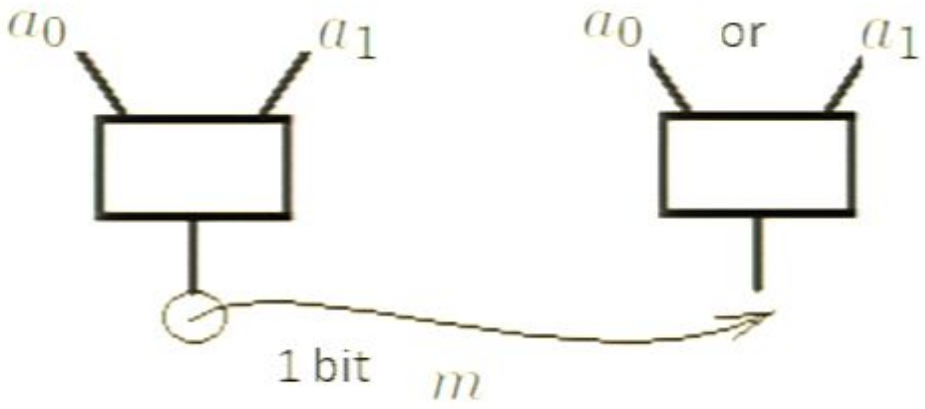


$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

Random access codes

$A \oplus B = ab$ with probability β



$$a = a_0 \oplus a_1$$

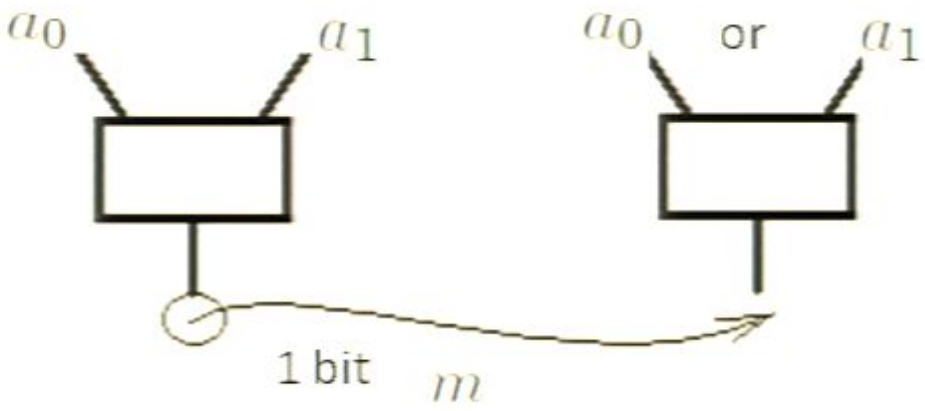
$$m = A \oplus a_0$$

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


0.854
1
3

Random access codes

$A \oplus B = ab$ with probability β

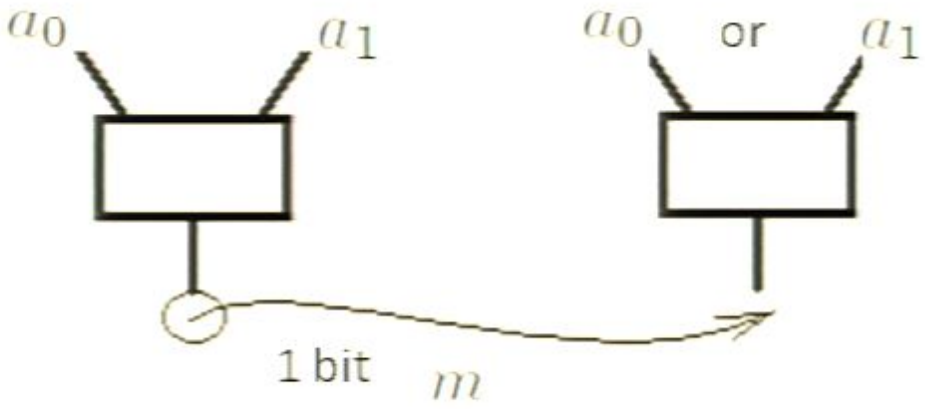


$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

Random access codes

$A \oplus B = ab$ with probability β



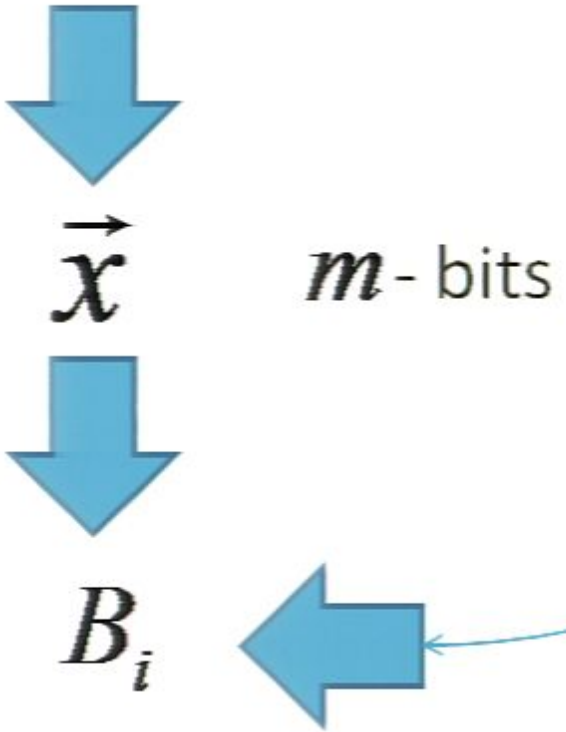
$$a = a_0 \oplus a_1$$

$$m = A \oplus a_0$$

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

(N -> m) Random access code

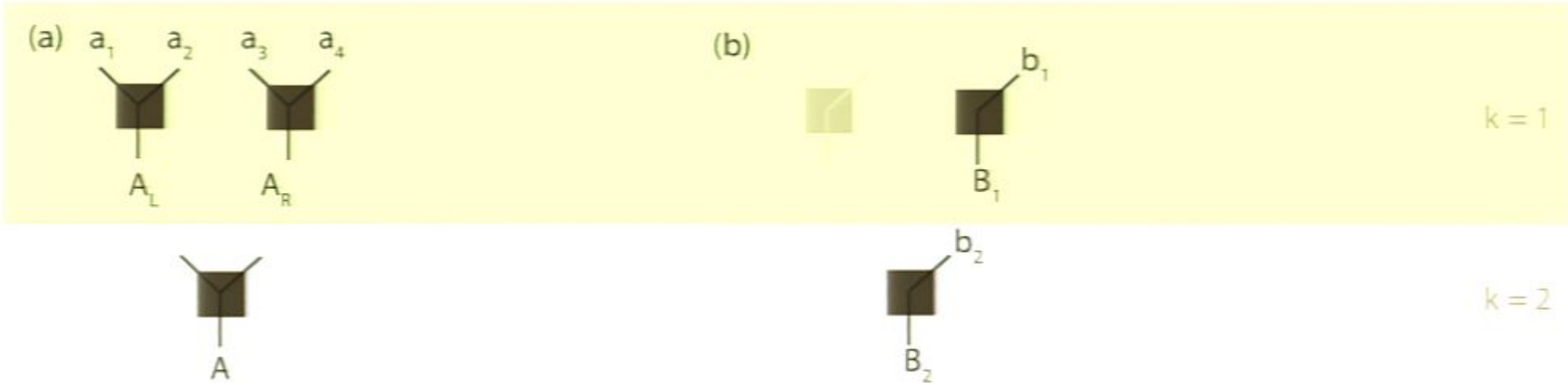
$\vec{a} = (a_0, a_1, \ldots, a_{N-1})$ independent of B



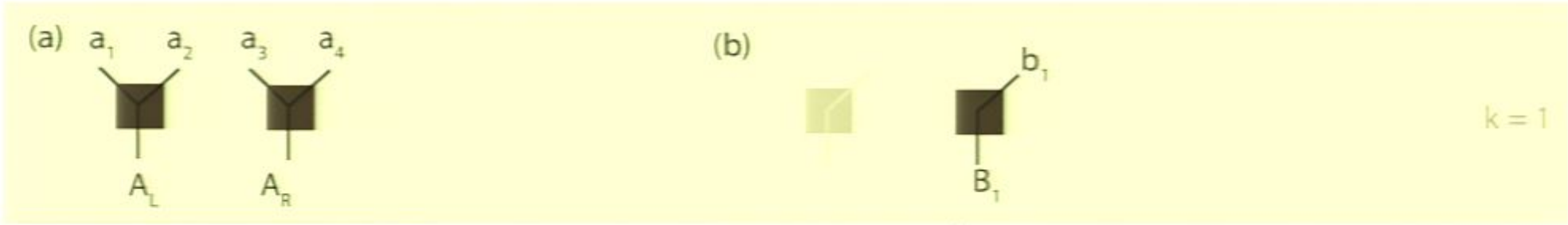
$$\sum_{i=0}^{N-1} I(a_i : B_i) \leq m$$


0.854
1
3


3
0.854
1


(a)
a1
a2
a3
a4
AL
AR
A
(b)
b1
B1
b2
B2
k = 1
k = 2


3
0.854
1


(a)
a1
a2
a3
a4
AL
AR
(b)
b1
B1
k = 1
b2
B2
k = 2
A


3
0.854
1

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"

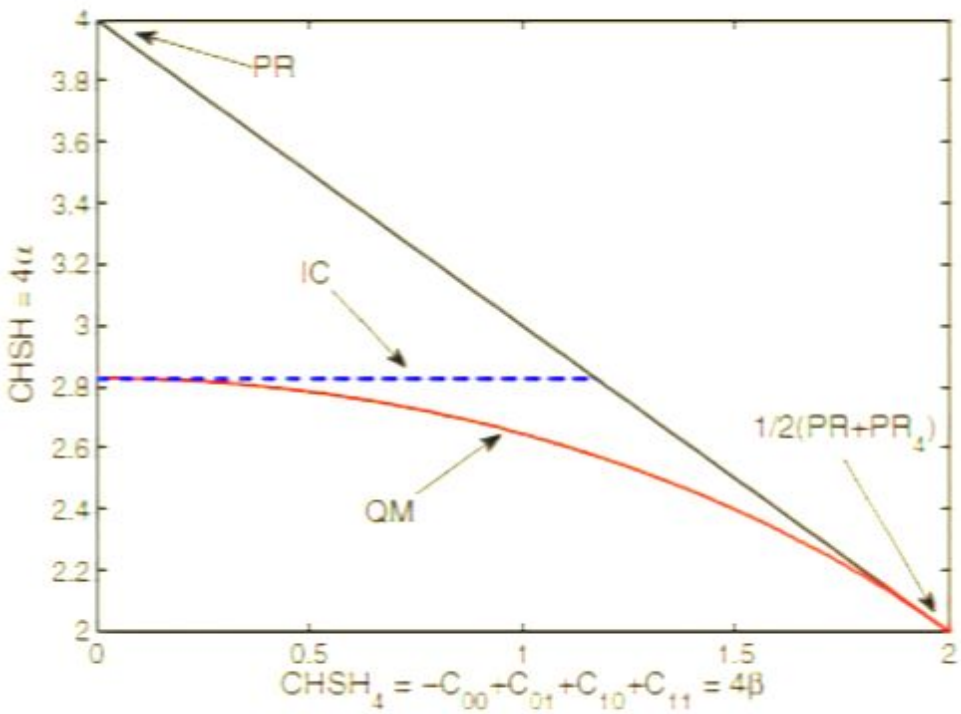
$$I(A:B)$$

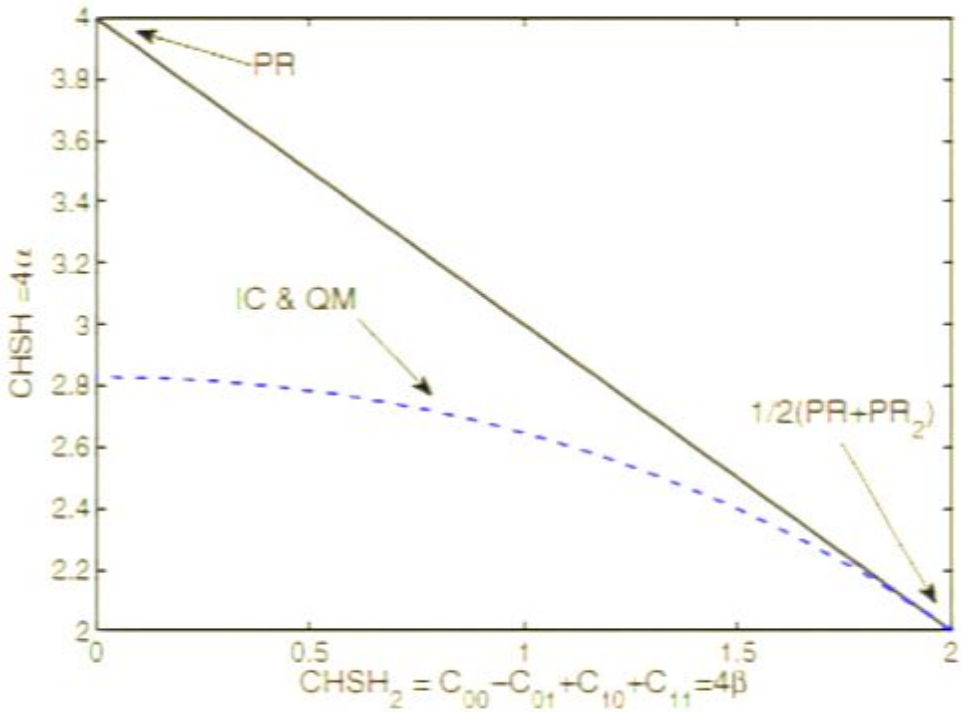
1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object
4. Chain rule

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

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

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"

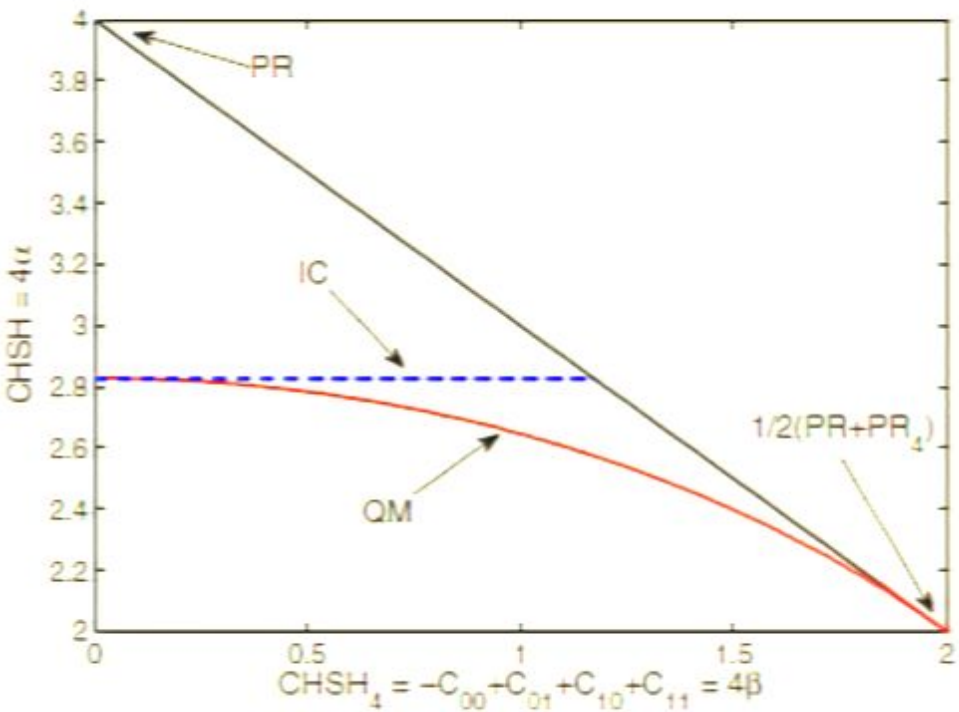
$$I(A:B)$$

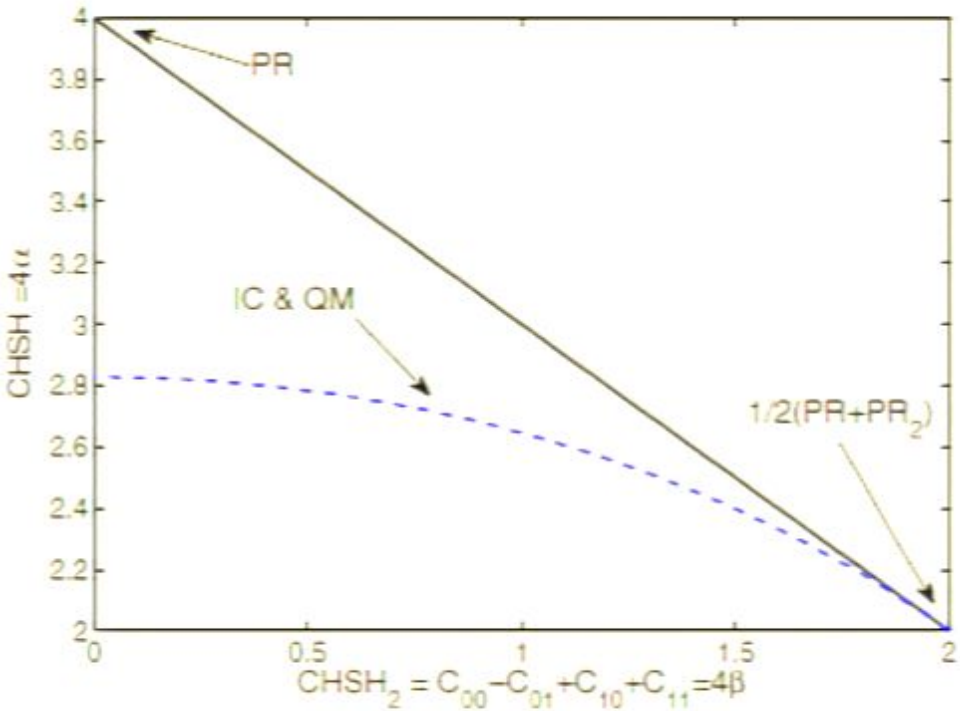
1. No-signaling
2. Data processing inequality
3. Bounded by m for classical object
4. Chain rule

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

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

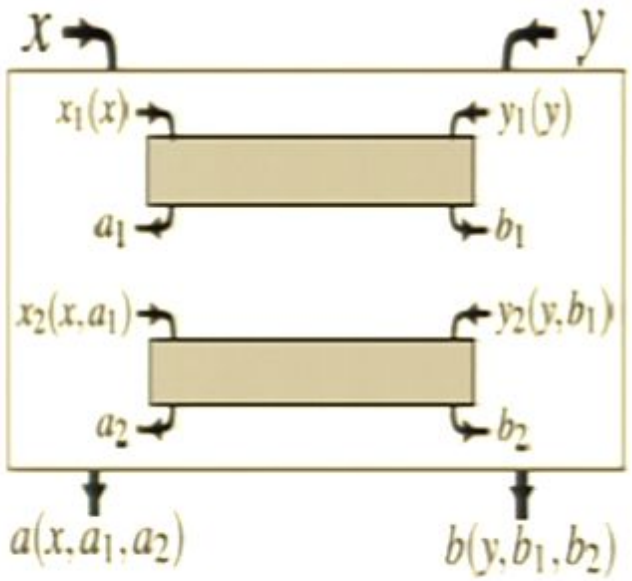
Unballanced boxes

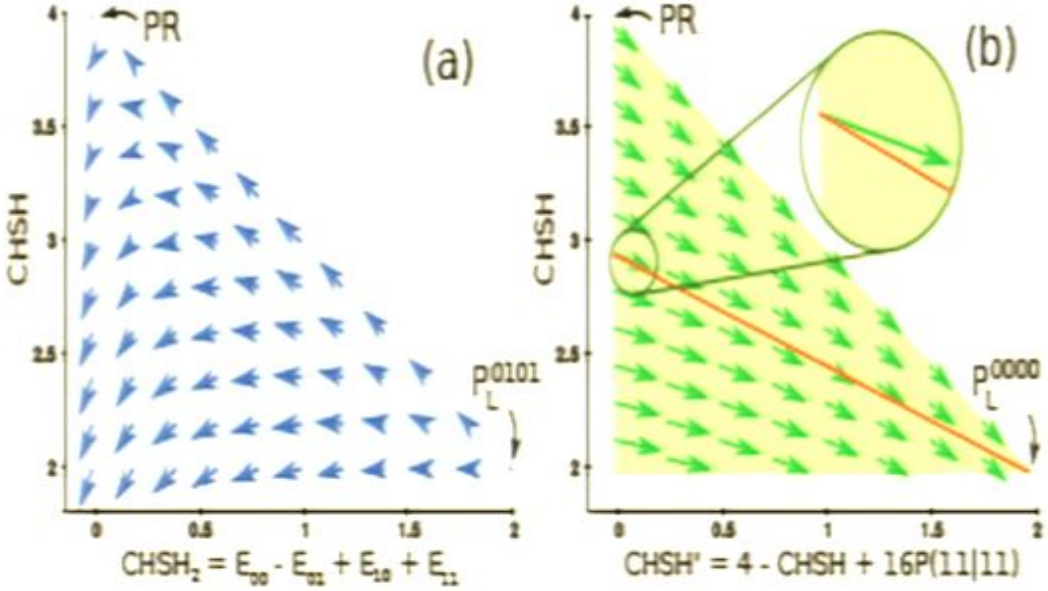


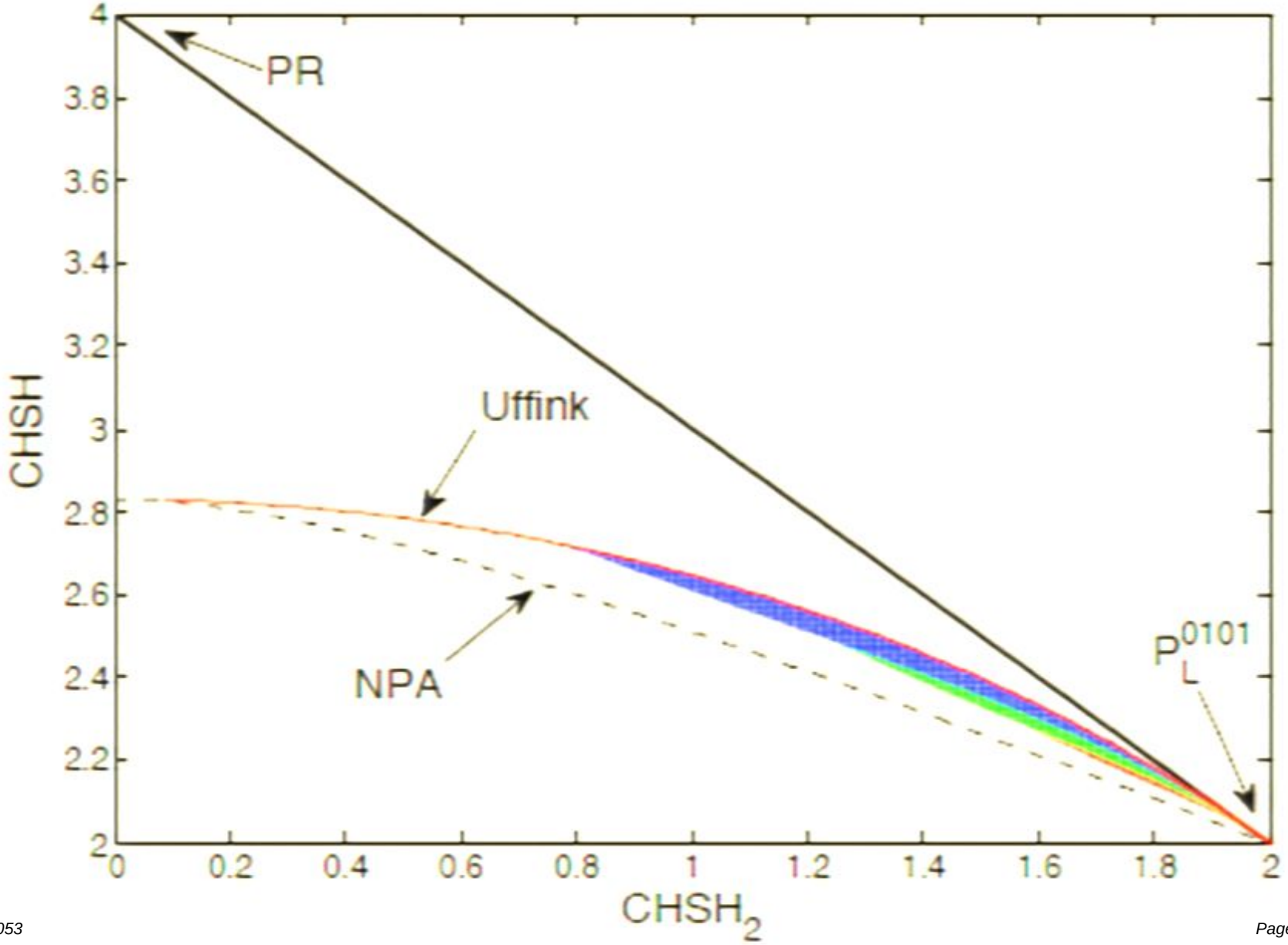


$$\beta = \frac{1}{4}\sum_{a,b} P(A \oplus B = ab|a,b)$$

Distillation

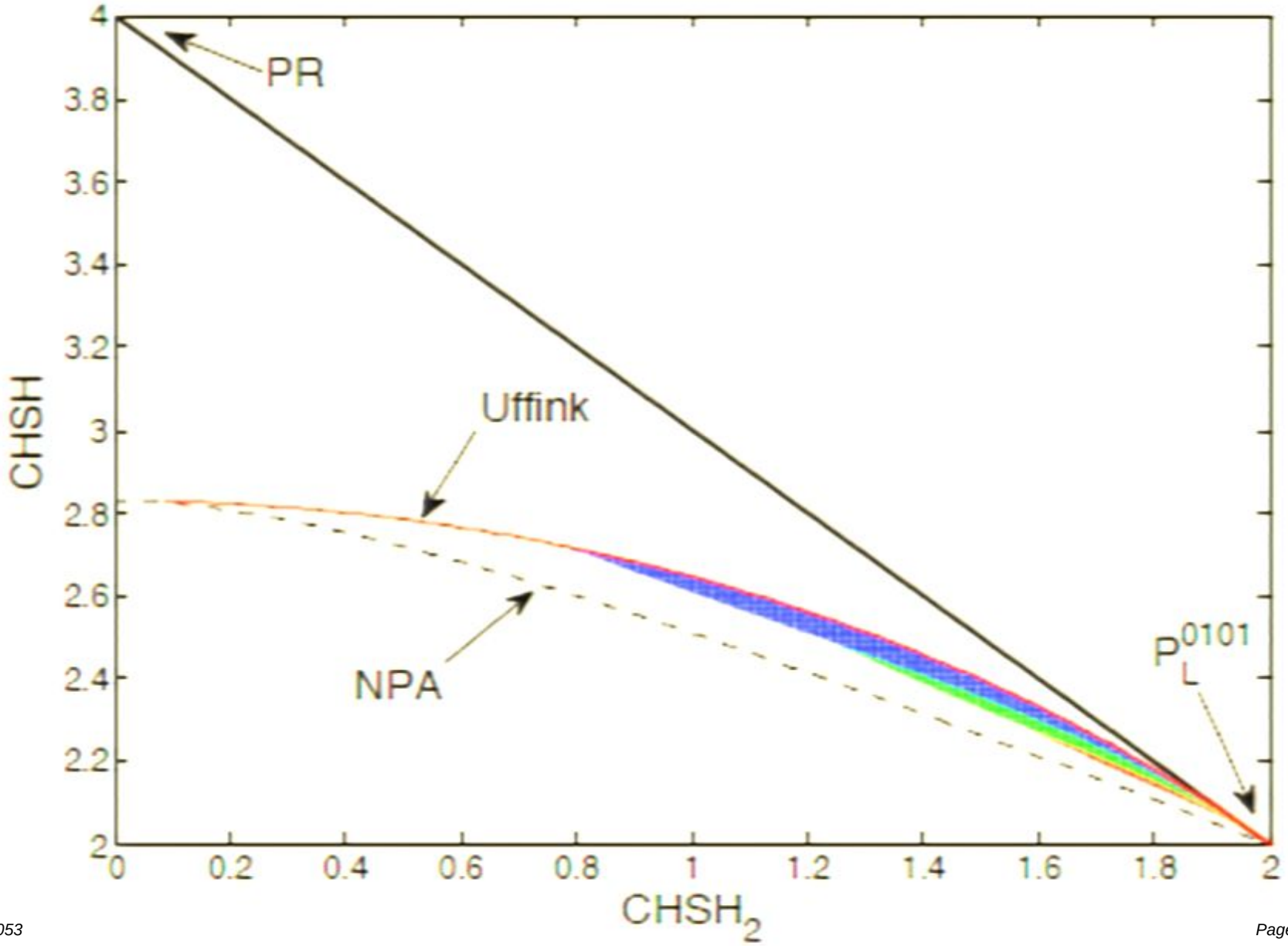





PR
Uffink
NPA
P_L^{0101}
CHSH
$CHSH_2$
4
3.8
3.6
3.4
3.2
3
2.8
2.6
2.4
2.2
2
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2

More complicated boxes

Other stuff


PR
Uffink
NPA
P_L^{0101}
CHSH
$CHSH_2$
4
3.8
3.6
3.4
3.2
3
2.8
2.6
2.4
2.2
2
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2

More complicated boxes

Other stuff

More complicated boxes

- Every (n->1)RAC

Other stuff

More complicated boxes

- Every (n->1)RAC
- Multipartite boxes

Other stuff

More complicated boxes

- Every (n->1)RAC
- Multipartite boxes
- 2 inputs more outputs

Other stuff

More complicated boxes

- Every (n->1)RAC
- Multipartite boxes
- 2 inputs more outputs

Other stuff

- Uncertainty relations

More complicated boxes

- Every (n->1)RAC
- Multipartite boxes
- 2 inputs more outputs

Other stuff

- Uncertainty relations
- Application in crypto

More complicated boxes

- Every (n->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

$$I(A:B)=0$$