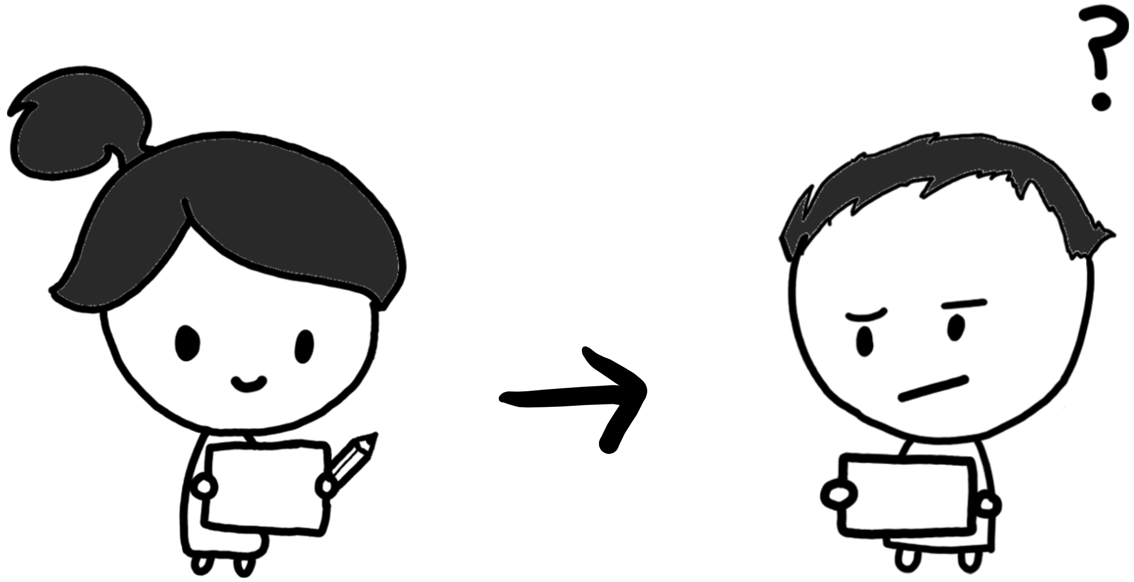
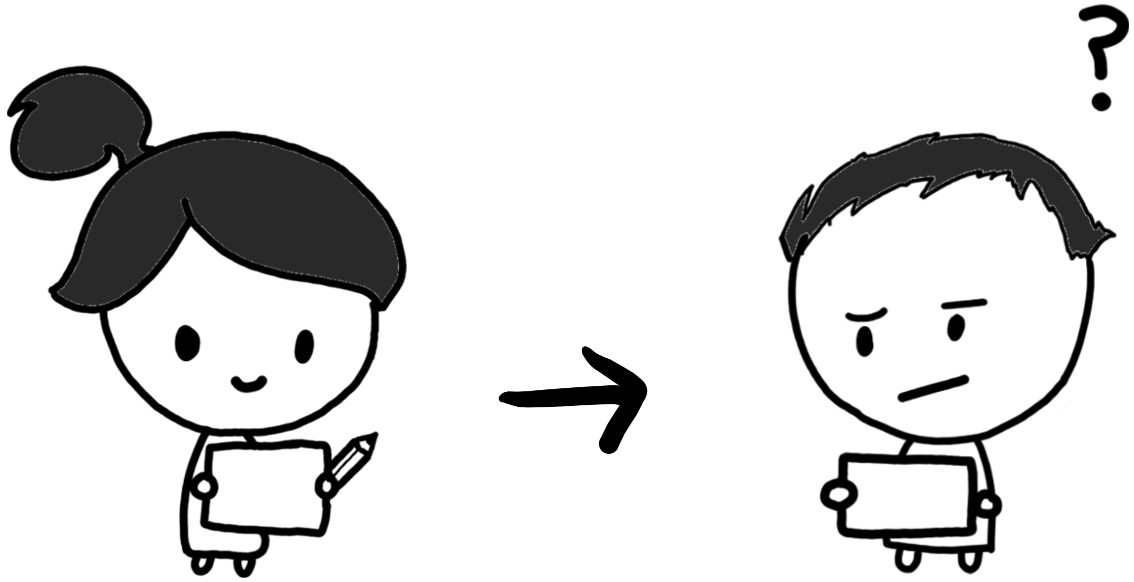
Implications of Information Causality and its Generalisations

Prabhav Jain[1], Nikolai Miklin[2], Mariami Gachechiladze[1]

[1] Technische Universität Darmstadt, [2] Technische Universität Hamburg

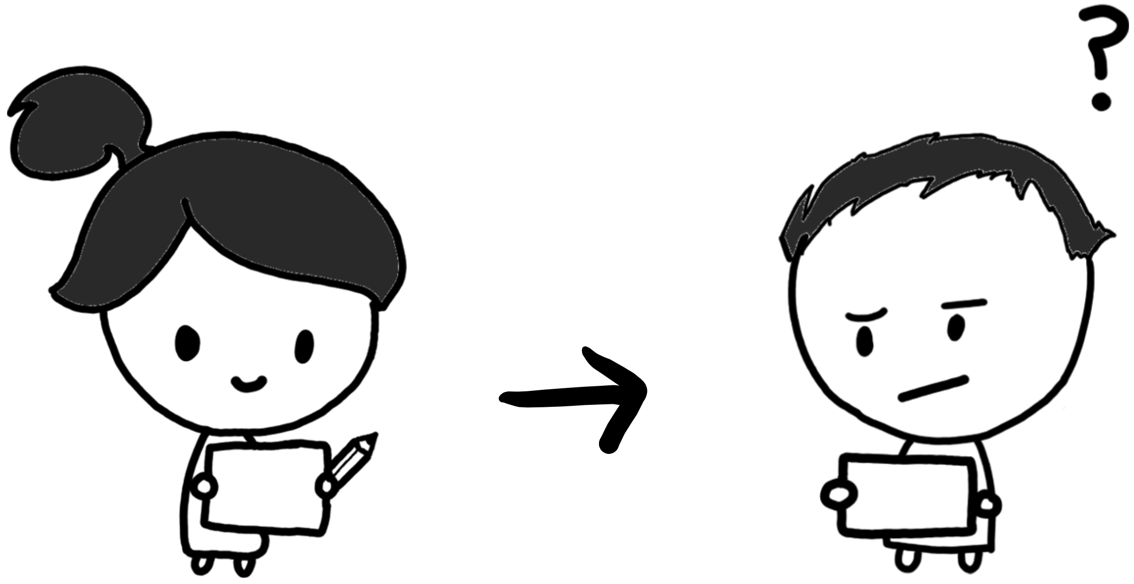


MOTIVATION



Pawłowski M., Paterek T., Kaszlikowski D., Scarani V., Winter A. and Żukowski M. (2009). Information causality as a physical principle. Nature, 461(7267):1101–1104

MOTIVATION

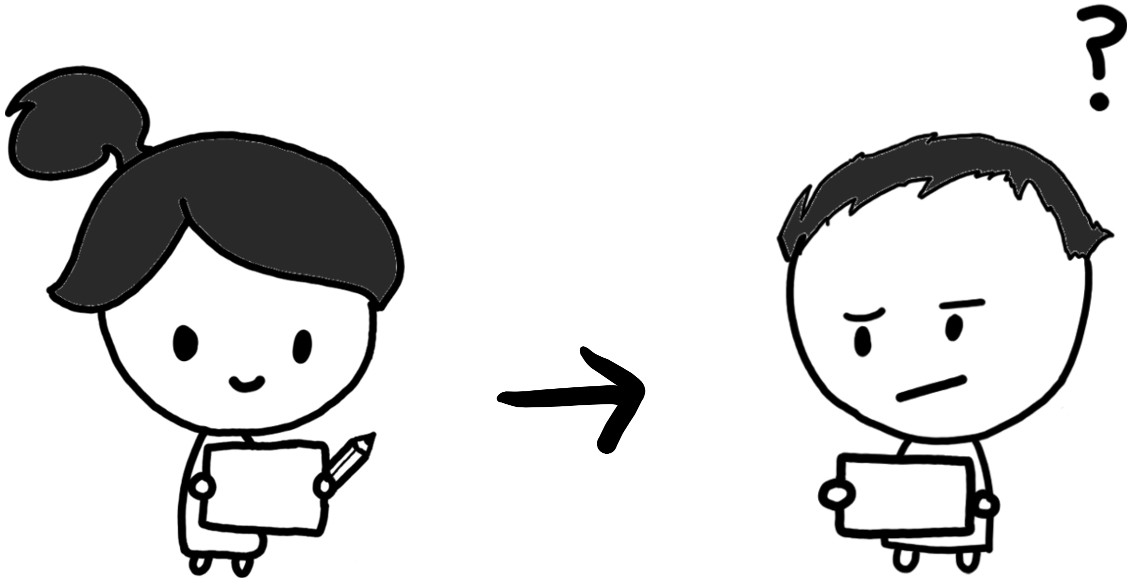


information sent by Alice $\geq$ information available to Bob

Pawłowski M., Paterek T., Kaszlikowski D., Scarani V., Winter A. and Żukowski M. (2009). Information causality as a physical principle. Nature, 461(7267):1101–1104

MOTIVATION

For such scenarios, one can show: $I(A;B) \leq \mathcal{C}$



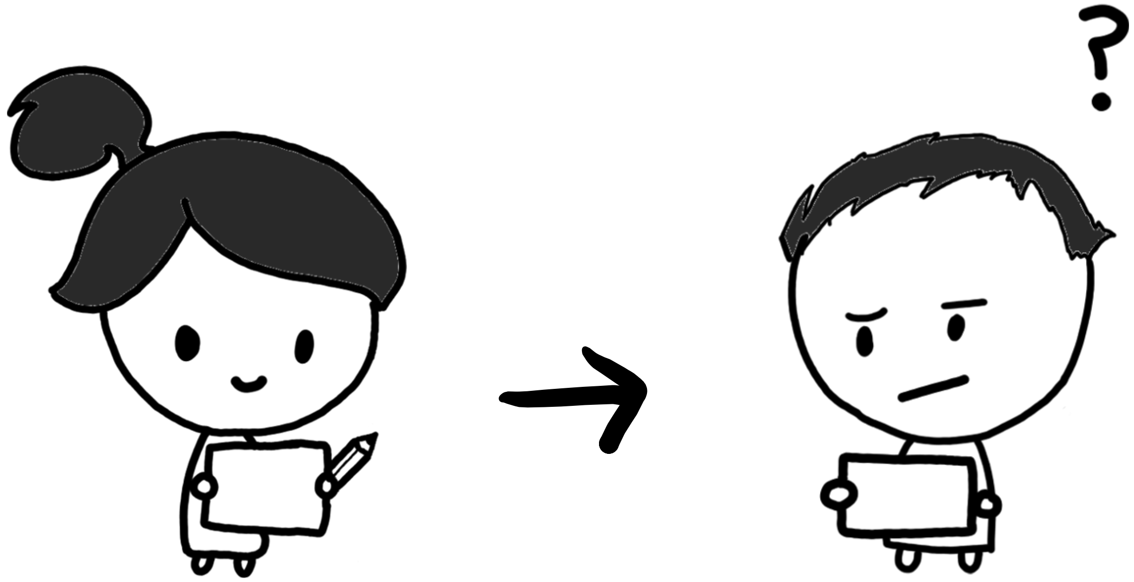
information sent by Alice $\geq$ information available to Bob

Pawłowski M., Paterek T., Kaszlikowski D., Scarani V., Winter A. and Żukowski M. (2009). Information causality as a physical principle. Nature, 461(7267):1101–1104

MOTIVATION

For such scenarios, one can show:

$$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

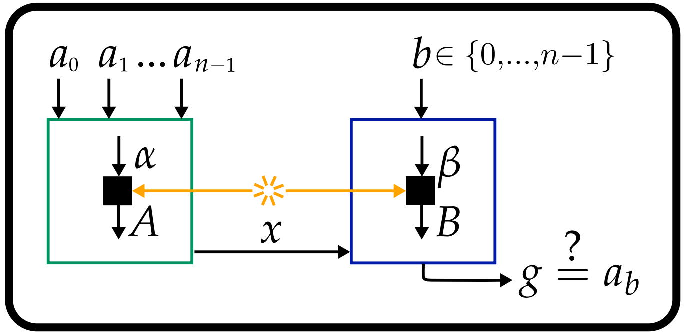


information sent by Alice ≥ information available to Bob

Pawłowski M., Paterek T., Kaszlikowski D., Scarani V., Winter A. and Żukowski M. (2009). Information causality as a physical principle. Nature, 461(7267):1101–1104

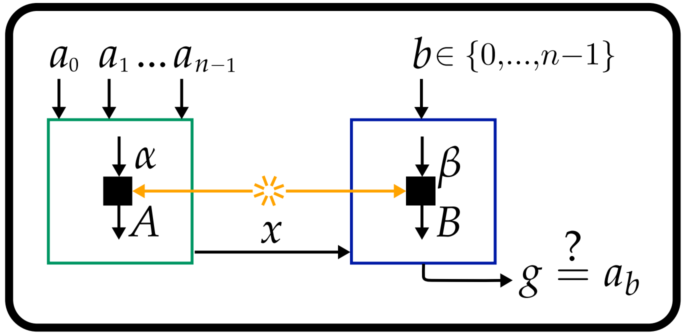
OUTLINE

OUTLINE

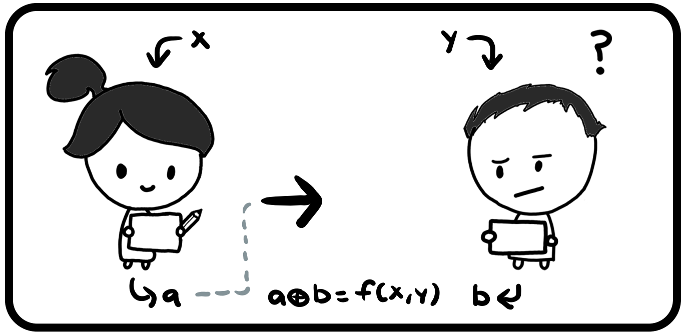


THE ALGORITHM

OUTLINE

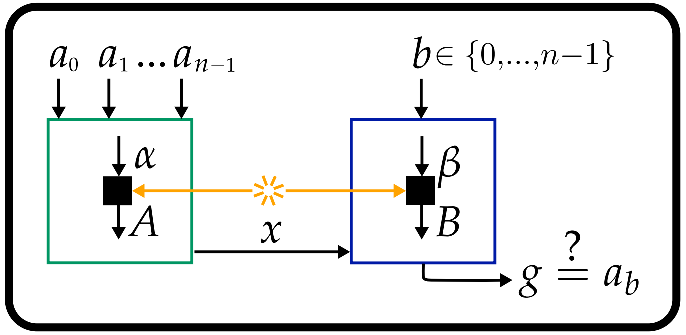


THE ALGORITHM

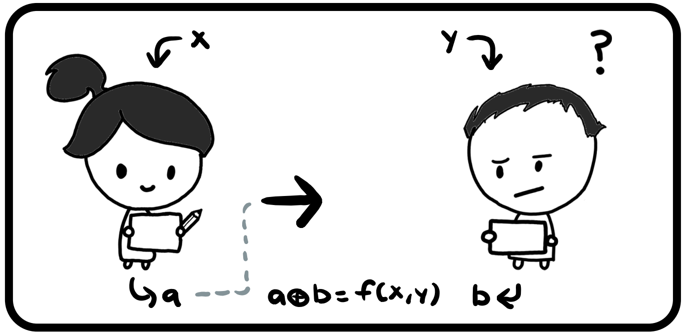


EXTENDED IC

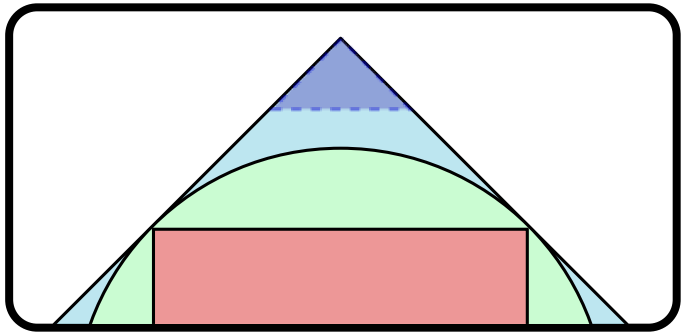
OUTLINE



THE ALGORITHM



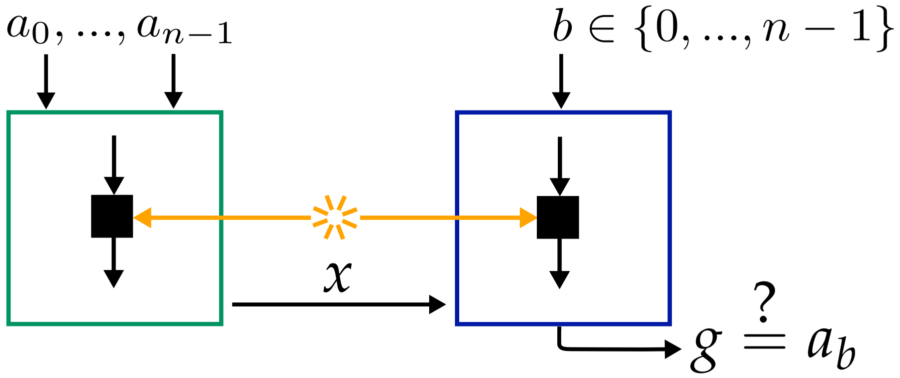
EXTENDED IC



IC VS. NTCC

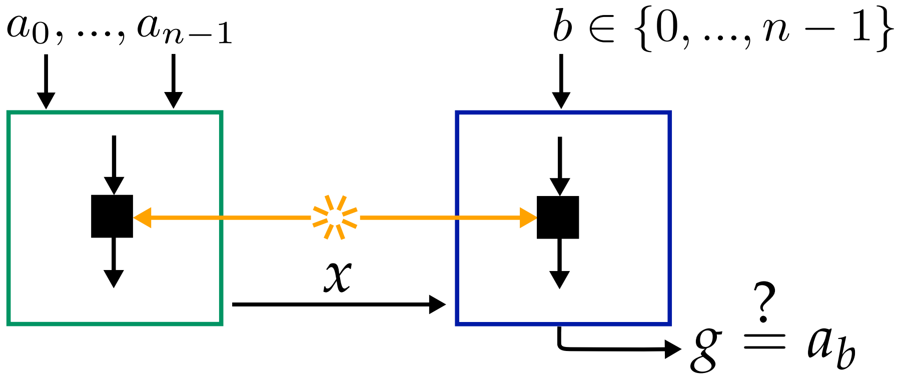
THE ALGORITHM

QRAC



P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

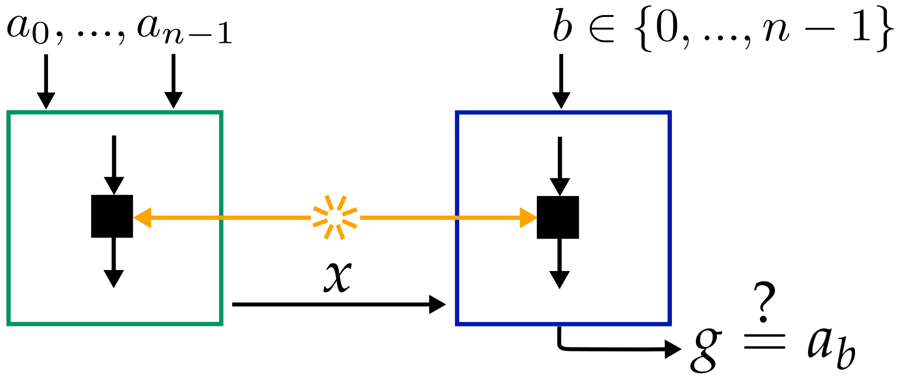
QRAC



Consider the "unbiased error" case

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC

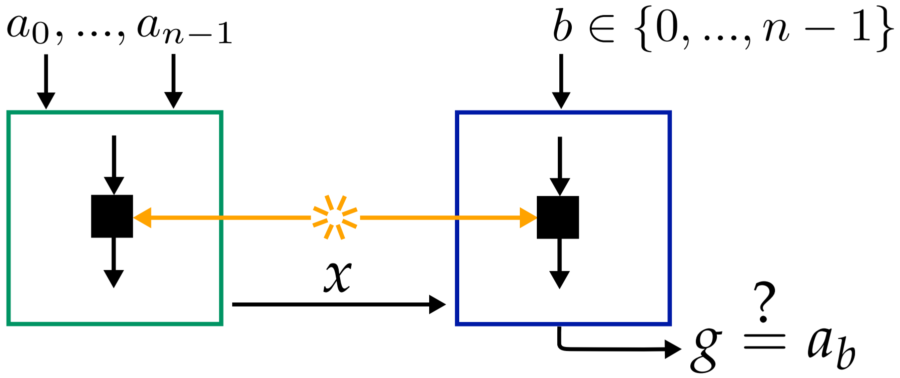


Consider the “unbiased error” case

$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



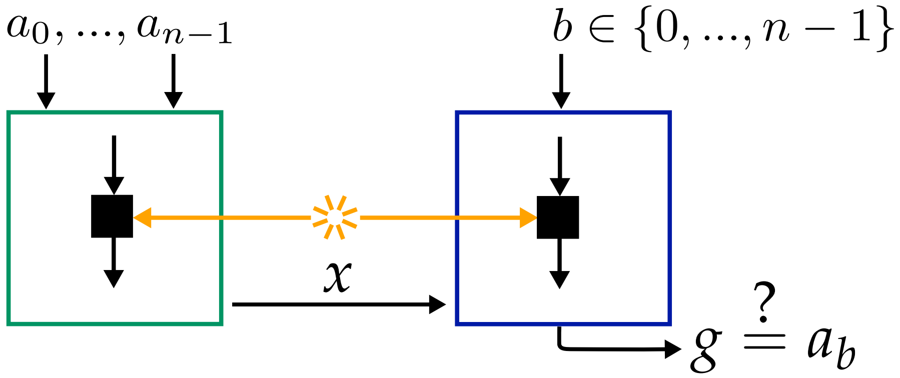
Consider the “unbiased error” case

$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

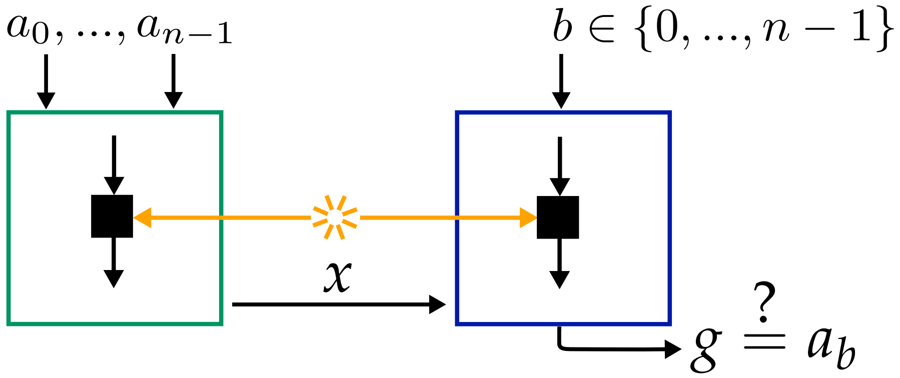
$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

(two rights) **(two wrongs)**

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

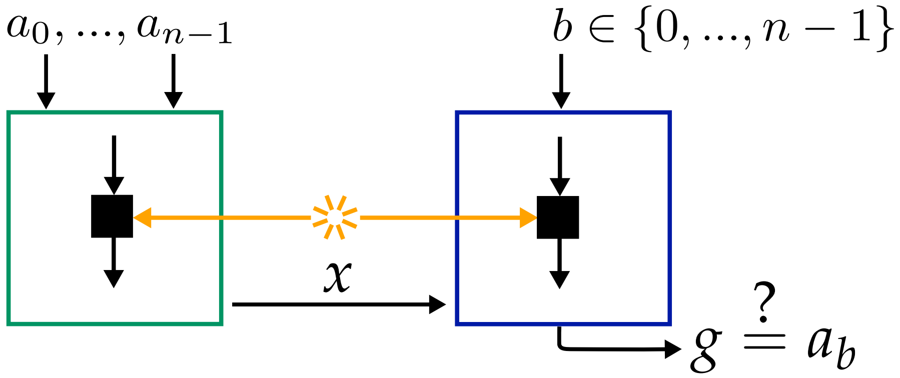
$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

Fano's Inequality: $1 - h(p(x=y)) \leq I(x;y)$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

$$p_{\text{win}} = \text{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

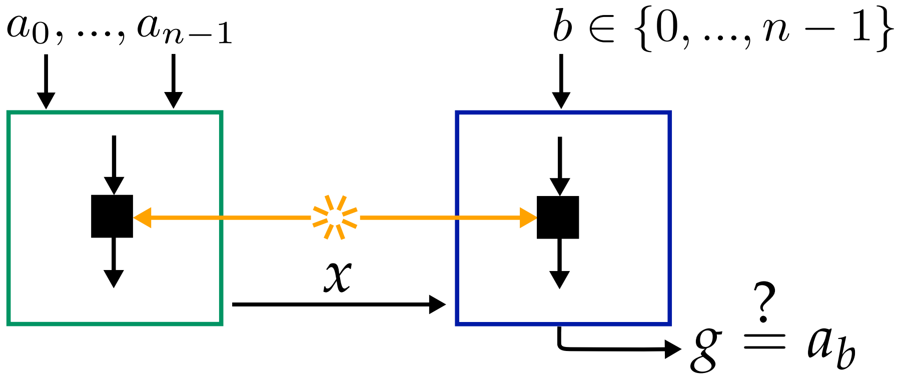
Fano's Inequality: $1 - h(p(x=y)) \leq I(x;y)$

From IC we have,

$$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

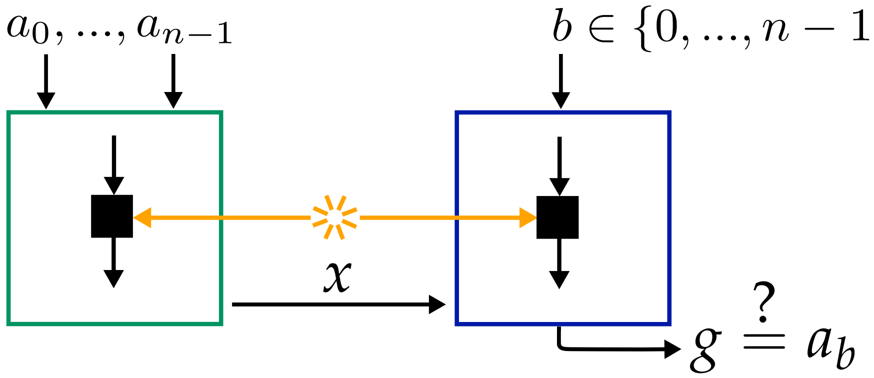
Fano's Inequality: $1 - h(p(x=y)) \leq I(x;y)$

From IC we have,

$$n\,(1 - h(p)) \leq \sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C} = 1 - h(p_c)$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

Fano's Inequality: $1 - h(p(x=y)) \leq I(x;y)$

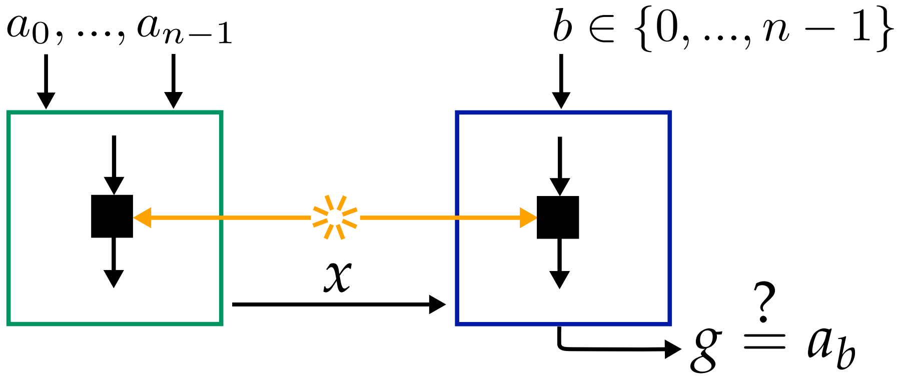
From IC we have,

$$n\,(1 - h(p)) \leq \sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C} = 1 - h(p_c)$$

$$n\,(1 - h(p)) \leq 1 - h(p_c)$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

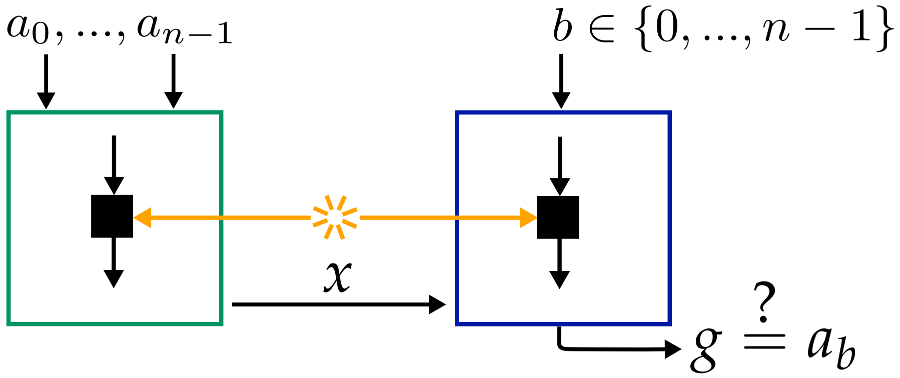
$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

$$n\,(1-h(p)) \leq 1 - h(p_c) \quad \equiv \quad n\left(1 - h\left(\frac{1+e_c e}{2}\right)\right) \leq 1 - h\left(\frac{1+e_c}{2}\right)$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

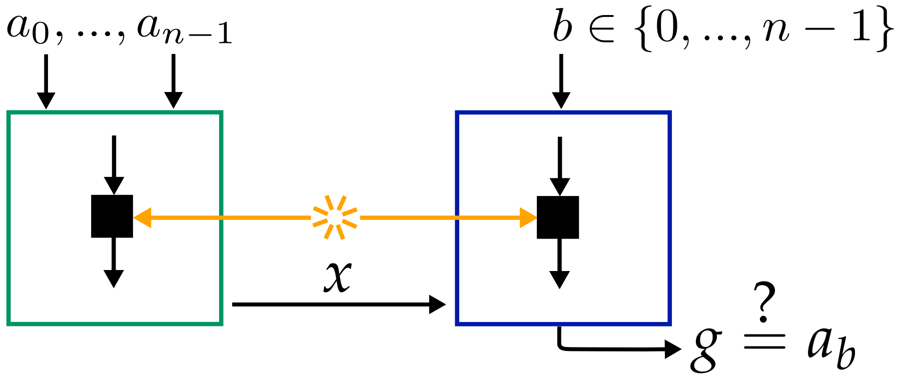
$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

$$n\left(1 - h(p)\right) \leq 1 - h(p_c) \quad \equiv \quad n\left(1 - h\left(\frac{1+e_c e}{2}\right)\right) \leq 1 - h\left(\frac{1+e_c}{2}\right)$$

vanishes when $e_c \to 0$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

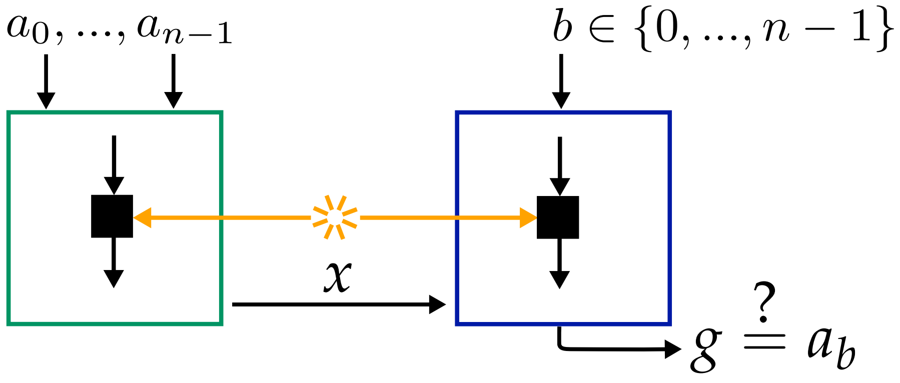
$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

$$n\,(1-h(p)) \leq 1-h(p_c) \quad \equiv \quad n\left(1-h\left(\frac{1+e_c e}{2}\right)\right) \leq 1-h\left(\frac{1+e_c}{2}\right)$$

vanishes when $e_c \rightarrow 0$ | also vanishes when $e_c \rightarrow 0$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

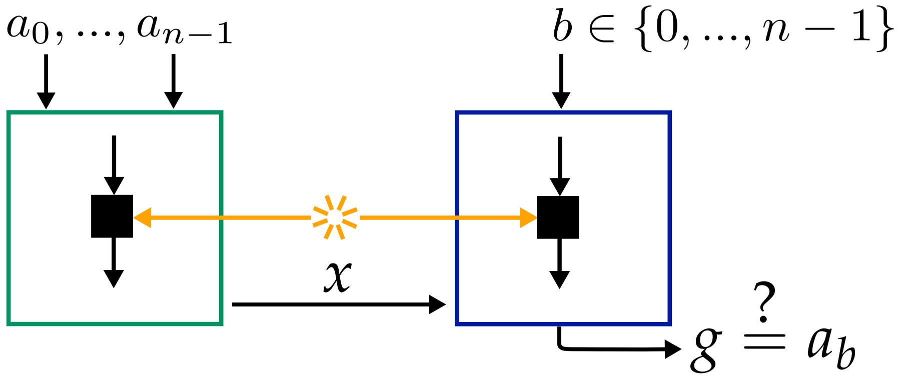
$$n\left(1 - h(p)\right) \leq 1 - h(p_c) \quad \equiv \quad n\left(1 - h\left(\frac{1+e_c e}{2}\right)\right) \leq 1 - h\left(\frac{1+e_c}{2}\right)$$

vanishes when $e_c \rightarrow 0$ **also vanishes when $e_c \rightarrow 0$**

since both LHS and RHS vanish, we can use L'Hôpital's rule and differentiate twice to get rid of the logarithms

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

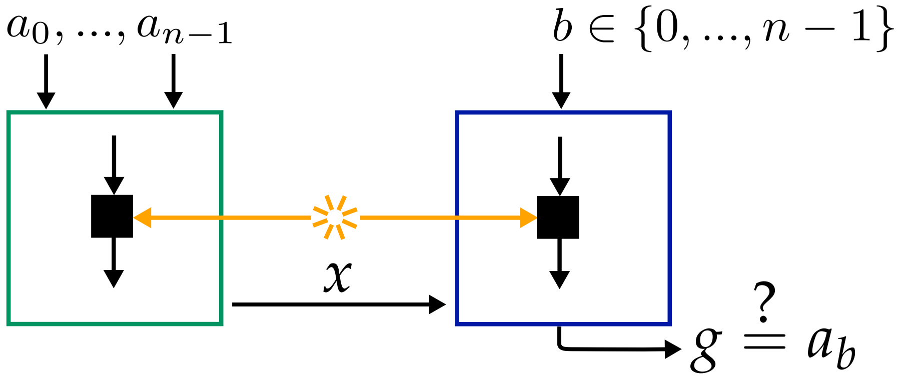
$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

$$n\,(1 - h(p)) \leq 1 - h(p_c) \quad \Longrightarrow \quad e^2 \leq \frac{1}{n}$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

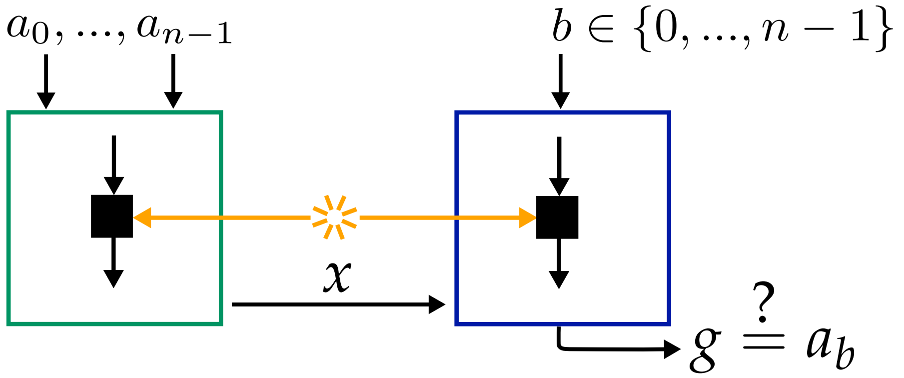
$$p_{\text{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

$$n\left(1 - h(p)\right) \leq 1 - h(p_c) \implies e^2 \leq \frac{1}{n} \quad \equiv \quad p \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{n}}\right)$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

QRAC



Consider the "unbiased error" case

$$p_{\mathrm{win}} = \mathrm{P}(g = a_i | b = i) = \frac{1+e}{2} \quad \forall i$$

$$p = \frac{1+e}{2}\frac{1+e_c}{2} + \frac{1-e}{2}\frac{1-e_c}{2} = \frac{1+e_c e}{2}$$

$$n\left(1 - h(p)\right) \leq 1 - h(p_c) \implies e^2 \leq \frac{1}{n} \quad \equiv \quad p \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{n}}\right)$$

can be easily generalised to higher dimensions

$$p \leq \frac{1}{d}\left(1 + \frac{d-1}{\sqrt{n}}\right)$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

$$p(g = a_i | b = i) = \frac{1 + e_c(e_{0i} + (-1)^i e_{1i})}{2}$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

$$p(g = a_i | b = i) = \frac{1 + e_c(e_{0i} + (-1)^i e_{1i})}{2}$$

$$(e_{00} + e_{10})^2 + (e_{01} - e_{11})^2 \leq 4$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

$$p(g = a_i | b = i) = \frac{1 + e_c(e_{0i} + (-1)^i e_{1i})}{2}$$

$$p(g = a_i | b = i) = \frac{1 + b_{kl}}{d^2} \sum_{m=0}^{d-1} \frac{1 + (d-1)e_{c_m}}{d} \frac{1 + (d-1)e_{\overline{k} \oplus i}^{j \oplus \overline{k} \oplus \overline{m}}}{d}$$

$$(e_{00} + e_{10})^2 + (e_{01} - e_{11})^2 \leq 4$$

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

$$p(g = a_i | b = i) = \frac{1 + e_c(e_{0i} + (-1)^i e_{1i})}{2}$$

$$(e_{00} + e_{10})^2 + (e_{01} - e_{11})^2 \leq 4$$

$$p(g = a_i | b = i) = \frac{1 + b_{kl}}{d^2} \sum_{m=0}^{d-1} \frac{1 + (d-1)e_{c_m}}{d} \frac{1 + (d-1)e^{j \oplus \overline{k} \oplus \overline{m}}_{\overline{k} \oplus i}}{d}$$

YOU DO NOT WANT TO SEE

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

$$p(g = a_i | b = i) = \frac{1 + e_c(e_{0i} + (-1)^i e_{1i})}{2}$$

$$(e_{00} + e_{10})^2 + (e_{01} - e_{11})^2 \leq 4$$

$$p(g = a_i | b = i) = \frac{1 + b_{kl}}{d^2} \sum_{m=0}^{d-1} \frac{1 + (d-1)e_{c_m}}{d} \frac{1 + (d-1)e^{j \oplus \overline{k} \oplus \overline{m}}_{\overline{k} \oplus i}}{d}$$

YOU DO NOT WANT TO SEE

Algorithm:

Protocol agnostic and works for any input/outcome setting

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

$$p(g = a_i | b = i) = \frac{1 + e_c(e_{0i} + (-1)^i e_{1i})}{2}$$

$$(e_{00} + e_{10})^2 + (e_{01} - e_{11})^2 \leq 4$$

$$p(g = a_i | b = i) = \frac{1 + b_{kl}}{d^2} \sum_{m=0}^{d-1} \frac{1 + (d-1)e_{c_m}}{d} \frac{1 + (d-1)e_{\overline{k} \oplus i}^{j \oplus \overline{k} \oplus \overline{m}}}{d}$$

YOU DO NOT WANT TO SEE

Algorithm:

Protocol agnostic and works for any input/outcome setting

$$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

turns this

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

Getting Inequalities

If we actually compute p, it works the same but you get inequalities

$$p(g = a_i|b = i) = \frac{1 + e_c(e_{0i} + (-1)^i e_{1i})}{2}$$

$$(e_{00} + e_{10})^2 + (e_{01} - e_{11})^2 \leq 4$$

$$p(g = a_i|b = i) = \frac{1 + b_{kl}}{d^2} \sum_{m=0}^{d-1} \frac{1 + (d-1)e_{c_m}}{d} \frac{1 + (d-1)e_{\overline{k}\oplus i}^{j\oplus\overline{k}\oplus\overline{m}}}{d}$$

YOU DO NOT WANT TO SEE

Algorithm:

Protocol agnostic and works for any input/outcome setting

$$\sum_{i=0}^{n-1} I(g; a_i|b = i) \leq \mathcal{C}$$

turns this

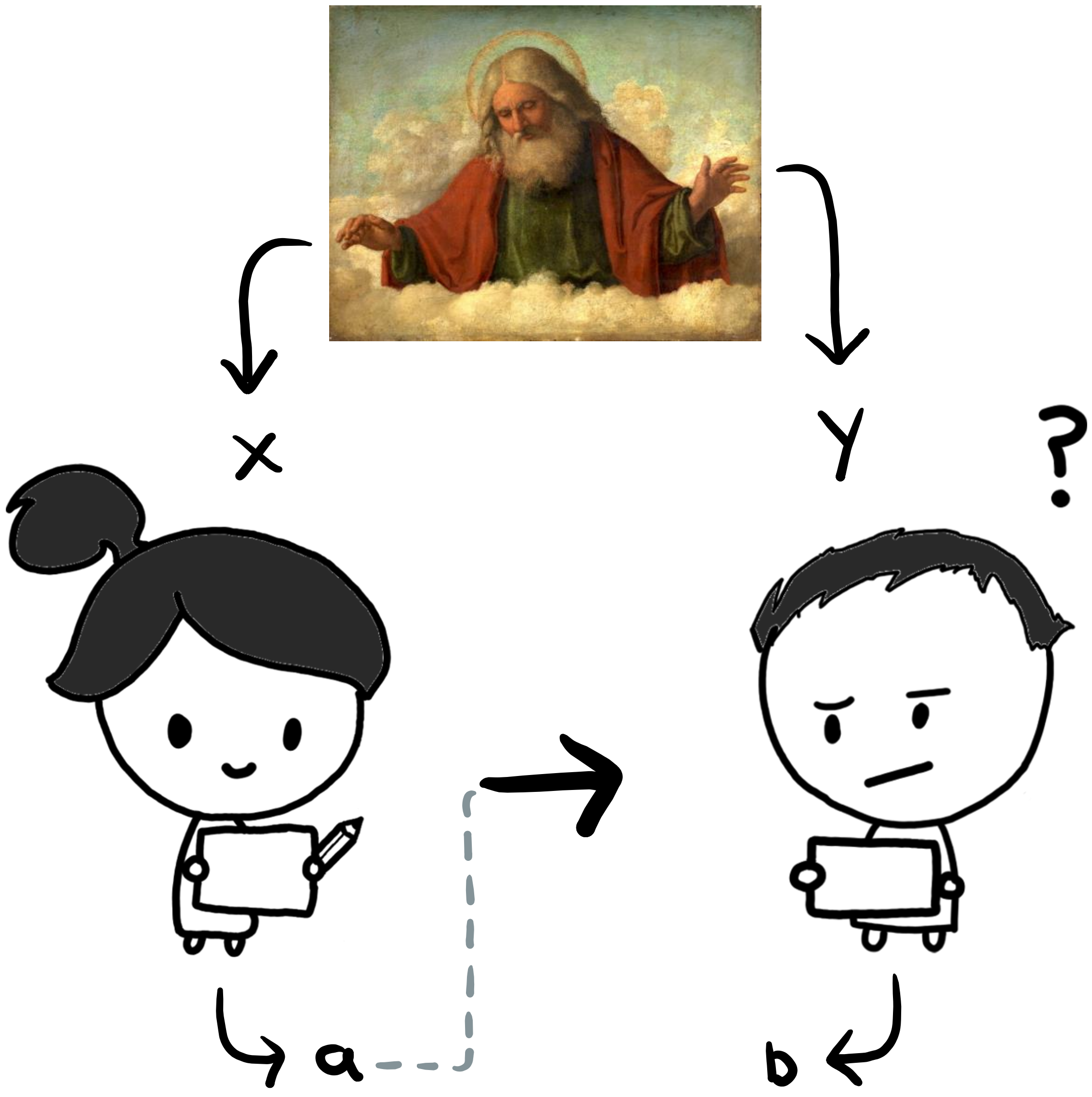
$$(e_{00}+e_{10})^2+(e_{01}-e_{11})^2\leq 4$$

into this

(inequalities bounding the quantum set)

P. Jain, M. Gachechiladze, and N. Miklin, Information causality as a tool for bounding the set of quantum correlations, Phys. Rev. Lett. 133, 160201 (2024)

EXTENDED IC



$$f(x,y) = a \oplus b$$

EIC Warm Up: Index Function

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

(condition over all ‘previous’ values)

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

Consider the INDEX function,

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

Consider the INDEX function,

$$\text{INDEX: } f(x,y) = x_y \qquad x = x_0 \ldots x_{n-1}, \quad y \in 0, \cdots, n-1$$

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

Consider the INDEX function,

$$\text{INDEX: } f(x,y) = x_y \qquad x = x_0 \ldots x_{n-1}, \quad y \in 0, \cdots, n-1$$

$$\{f(x,j)\}_{j<y} = \{x_0, \ldots, x_{y-1}\}$$

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

Consider the INDEX function,

$$\text{INDEX: } f(x,y) = x_y \qquad x = x_0 \ldots x_{n-1}, \quad y \in 0, \cdots, n-1$$

$$\{f(x,j)\}_{j<y} = \{x_0, \ldots, x_{y-1}\}$$

Plugging it in extended IC, we get:

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

Consider the INDEX function,

$$\text{INDEX: } f(x,y) = x_y \qquad x = x_0 \ldots x_{n-1}, \quad y \in 0, \cdots, n-1$$

$$\{f(x,j)\}_{j<y} = \{x_0, \ldots, x_{y-1}\}$$

Plugging it in extended IC, we get:

$$\sum_{i=0}^{n-1} I(g; x_y | y = i, \{x_0, \cdots, x_{y-1}\}) \leq \mathcal{C}$$

EIC Warm Up: Index Function

For such a scenario, one can show:

$$\sum_{i=0}^{|\mathcal{Y}|-1} I(g; f(x,y) | y = i, \{f(x,j)\}_{j<y}) \leq \mathcal{C}$$

Consider the INDEX function,

$$\text{INDEX: } f(x,y) = x_y \qquad x = x_0 \ldots x_{n-1}, \quad y \in 0, \cdots, n-1$$

$$\{f(x,j)\}_{j<y} = \{x_0, \ldots, x_{y-1}\}$$

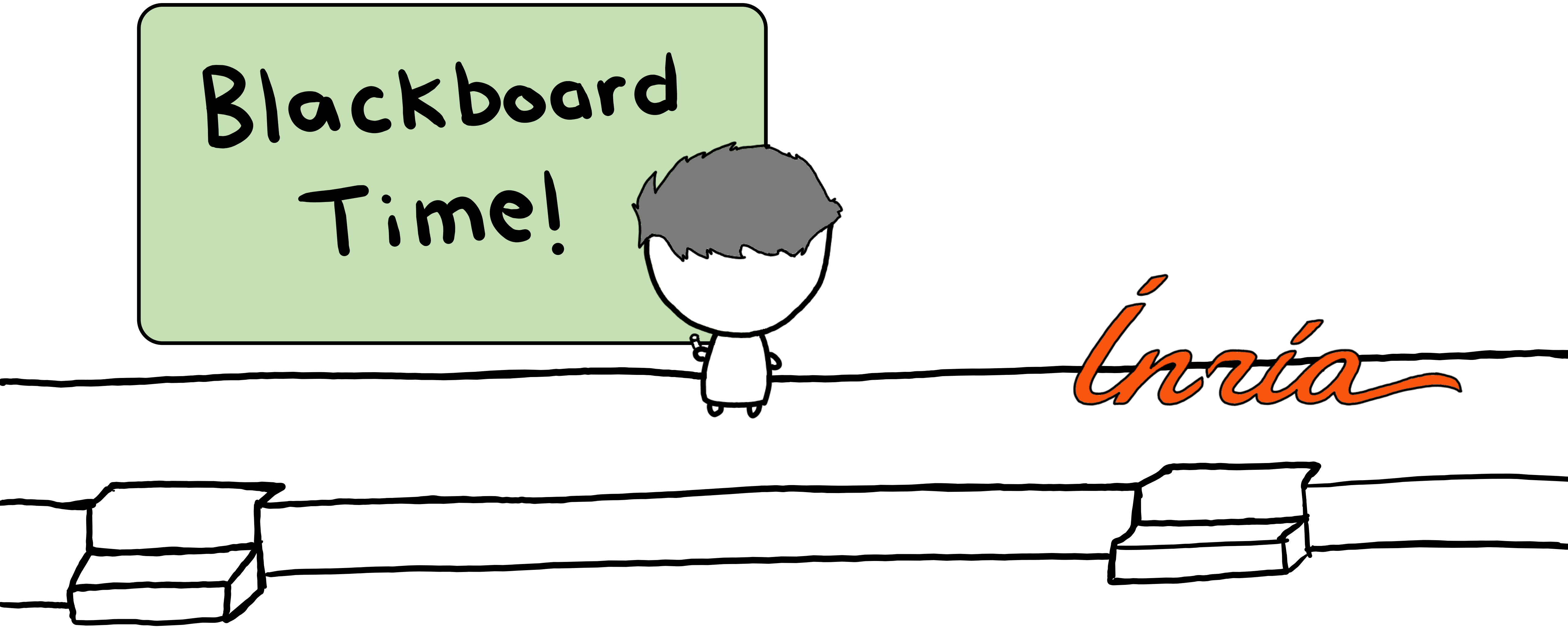
Plugging it in extended IC, we get:

$$\sum_{i=0}^{n-1} I(g; x_y | y = i, \{x_0, \cdots, x_{y-1}\}) \leq \mathcal{C}$$

Reduces to original IC statement!

EIC Main Course: Inner Product Function

EIC Main Course: Inner Product Function



EIC Main Course: Inner Product Function

$$\mathrm{IP}_2 : f(x,y) = x \cdot y \mod 2 \equiv x_0 \cdot y_0 \oplus x_1 \cdot y_1$$

$$\begin{aligned} & I(g; f(x,00)|y=00) \\ +& I(g; f(x,01)|y=01, f(x,00)) \\ +& I(g; f(x,10)|y=10, f(x,00), f(x,01)) \\ +& I(g; f(x,11)|y=11, f(x,00), f(x,01), f(x,10)) \leq \mathcal{C} \end{aligned}$$

$$\begin{aligned} & I(g; 0|y=00) \\ +& I(g; x_1|y=01, 0) \\ +& I(g; x_0|y=10, 0, x_1) \\ +& I(g; x_0 \oplus x_1)|y=11, 0, x_1, x_0) \leq \mathcal{C} \end{aligned}$$

$$I(g;0|y=00) + I(g;x_1|y=01,0) + I(g;x_0|y=10,0,x_1) + I(g;x_0 \oplus x_1)|y=11,0,x_1,x_0) \leq \mathcal{C}$$

$$I(g;x_1|y=01) + I(g;x_0|y=10,x_1) \leq \mathcal{C} \qquad I(g;a_0|b=0) + I(g;a_1|b=1,a_0) \leq \mathcal{C}$$

IT IS EQUIVALENT TO INDEX!

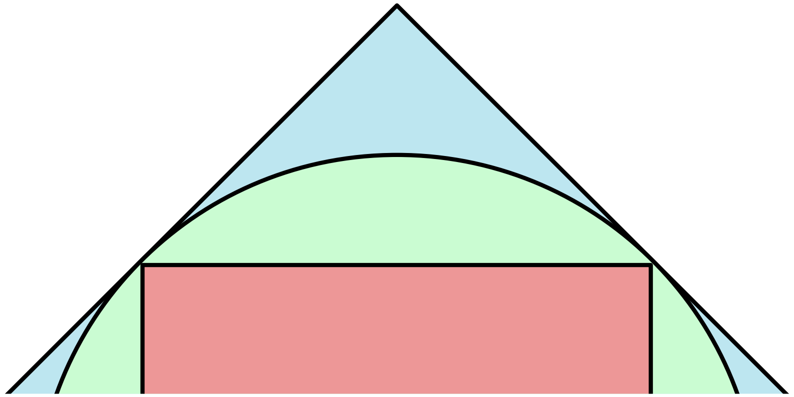
this holds true for any n, and surprisingly a similar reduction follows for $\mathrm{DISJOINT}(x,y)$

IC vs NTCC

What is NTCC?

Non-Trivial Communication Complexity (NTCC)

In a communication scenario, there are functions which are 'hard' to compute i.e. their communication cost/complexity increases with the input size.



What is NTCC?

Non-Trivial Communication Complexity (NTCC)

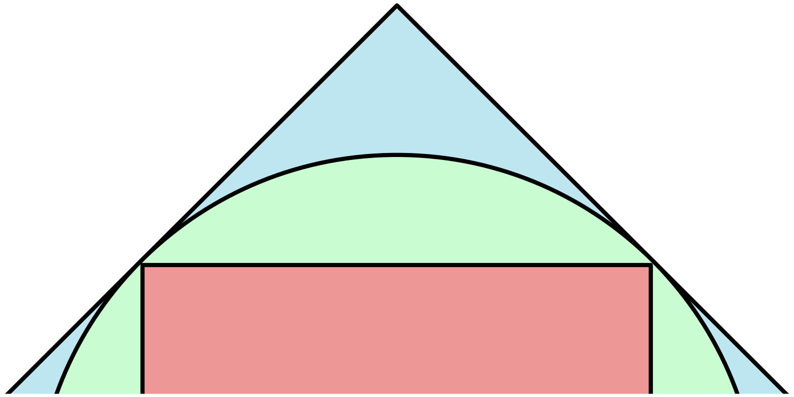
In a communication scenario, there are functions which are 'hard' to compute i.e. their communication cost/complexity increases with the input size.

Trivial Functions

$\mathrm{PARITY}(x \oplus y)$

$f(x, y) = g(x), h(y)$

(can be decided in 1 bit)



What is NTCC?

Non-Trivial Communication Complexity (NTCC)

In a communication scenario, there are functions which are 'hard' to compute i.e. their communication cost/complexity increases with the input size.

Trivial Functions

$\text{PARITY}(x \oplus y)$

$f(x, y) = g(x), h(y)$

(can be decided in 1 bit)

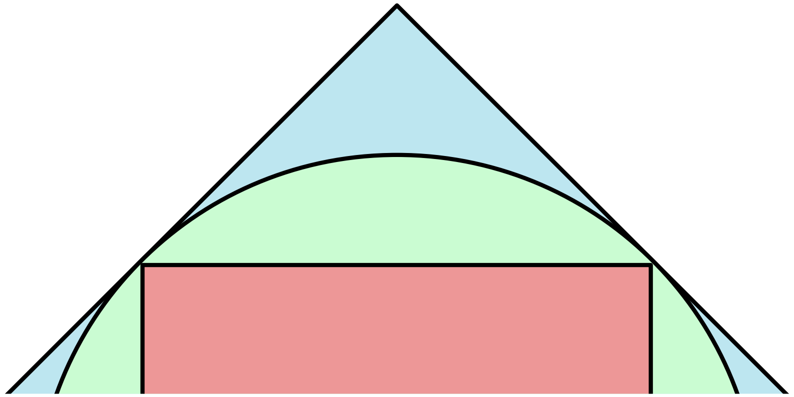
Non-Trivial Functions

$\text{IP}(x, y)$

$\text{INDEX}(x, y)$

$\text{EQUALITY}(x, y)$

(cannot be decided in 1 bit)



What is NTCC?

Non-Trivial Communication Complexity (NTCC)

In a communication scenario, there are functions which are ‘hard’ to compute i.e. their communication cost/complexity increases with the input size.

Trivial Functions

$\mathrm{PARITY}(x \oplus y)$

$f(x, y) = g(x), h(y)$

(can be decided in 1 bit)

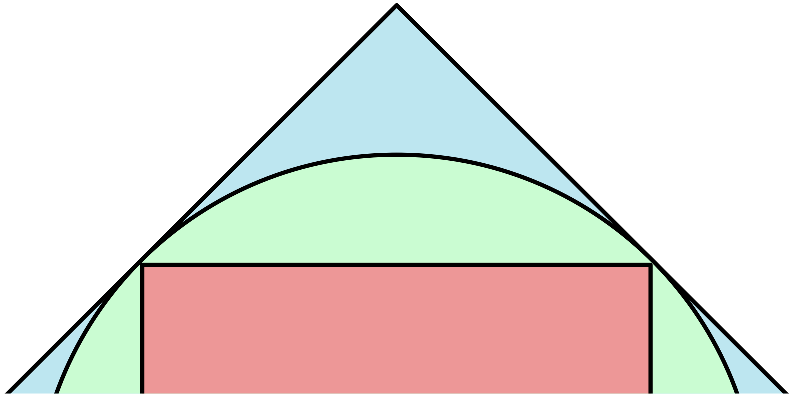
Non-Trivial Functions

$\mathrm{IP}(x, y)$

$\mathrm{INDEX}(x, y)$

$\mathrm{EQUALITY}(x, y)$

(cannot be decided in 1 bit)



In the randomised version we ask:
for a given protocol, the winning probability should be strictly greater that 1/2

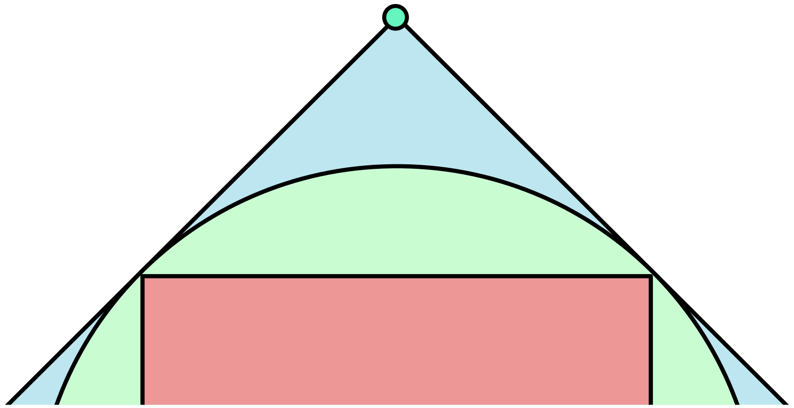
What is NTCC?

Non-Trivial Communication Complexity (NTCC)

In a communication scenario, there are functions which are ‘hard’ to compute i.e. their communication cost/complexity increases with the input size.

PR Boxes ‘collapse’ communication complexity

With enough PR boxes, ANY function can be decided using a single bit



Wim van Dam. Implausible consequences of superstrong nonlocality. Natural Computing, 12(1): 9–12, (2013).

What is NTCC?

Non-Trivial Communication Complexity (NTCC)

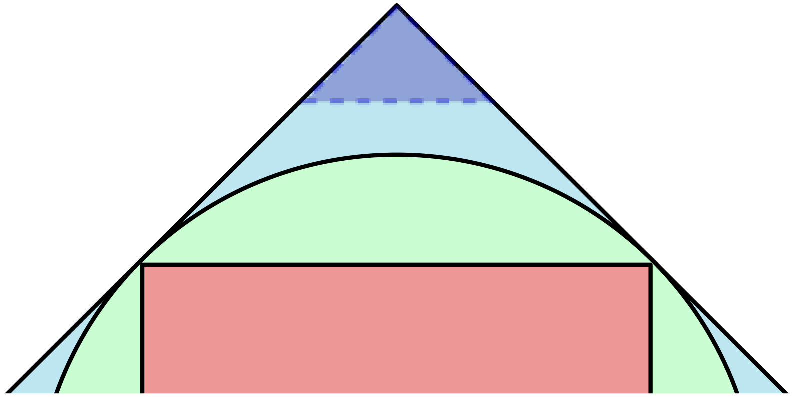
In a communication scenario, there are functions which are ‘hard’ to compute i.e. their communication cost/complexity increases with the input size.

PR Boxes ‘collapse’ communication complexity

With enough PR boxes, ANY function can be decided using a single bit

Noisy PR Boxes collapse randomised complexity

Boxes winning CHSH game with $p \geq \frac{3+\sqrt{6}}{6}$ collapse CC



Wim van Dam. Implausible consequences of superstrong nonlocality. Natural Computing, 12(1): 9–12, (2013).
G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, Limit on nonlocality in any world in which communication complexity is not trivial, Phys. Rev. Lett. 96, 250401 (2006).

IC implies NTCC: An intuitive proof

IC implies NTCC: An intuitive proof

Consider the statement: $$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

IC implies NTCC: An intuitive proof

Consider the statement: $$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

$$I(g; a_0 | b = 0) + I(g; a_1 | b = 1) + \cdots + I(g; a_{n-1} | b = n-1) \leq \mathcal{C}$$

IC implies NTCC: An intuitive proof

Consider the statement: $$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

$$I(g; a_0 | b = 0) + I(g; a_1 | b = 1) + \cdots + I(g; a_{n-1} | b = n-1) \leq \mathcal{C}$$

$p > \frac{1}{2}$ $\quad$ $p > \frac{1}{2}$ $\quad$ $p > \frac{1}{2}$

IC implies NTCC: An intuitive proof

Consider the statement: $$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

$$I(g; a_0 | b = 0) \; + \; I(g; a_1 | b = 1) + \quad \cdots \quad + I(g; a_{n-1} | b = n-1) \leq \mathcal{C}$$

$p > \frac{1}{2}$ $\quad$ $p > \frac{1}{2}$ $\quad$ $p > \frac{1}{2}$

≈ 1 $\quad$ ≈ 1 $\quad$ ≈ 1

IC implies NTCC: An intuitive proof

Consider the statement:

$$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

$$I(g; a_0 | b = 0) + I(g; a_1 | b = 1) + \quad \cdots \quad + I(g; a_{n-1} | b = n-1) \leq \mathcal{C}$$

$p > \frac{1}{2}$ $\quad$ $p > \frac{1}{2}$ $\quad$ $p > \frac{1}{2}$

≈ 1 $\quad$ ≈ 1 $\quad$ ≈ 1

What does that tell us?

IC implies NTCC: An intuitive proof

Consider the statement: $$\sum_{i=0}^{n-1} I(g; a_i | b = i) \leq \mathcal{C}$$

$$I(g; a_0 | b = 0) + I(g; a_1 | b = 1) + \cdots + I(g; a_{n-1} | b = n-1) \leq \mathcal{C}$$

$p > \frac{1}{2}$ $\qquad$ $p > \frac{1}{2}$ $\qquad$ $p > \frac{1}{2}$

≈ 1 $\qquad$ ≈ 1 $\qquad$ ≈ 1

What does that tell us? **The capacity must be growing!**

IC implies NTCC: More rigorously

IC implies NTCC: More rigorously

Define the average winning probability: $p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$

IC implies NTCC: More rigorously

Define the average winning probability: $p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$

Using Fano's inequality again:

IC implies NTCC: More rigorously

Define the average winning probability: $p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$

Using Fano's inequality again:

$$\sum_{i=0}^{n-1} 1 - h(p_i) \leq \sum_{i=0}^{n-1} I(g, x_i | y = i) \leq m$$

$$\Rightarrow n - \sum_{i=0}^{n-1} h(p_i) \leq m$$

$$\Rightarrow n(1 - h(p)) \leq m$$

IC implies NTCC: More rigorously

Define the average winning probability: $p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$

Using Fano's inequality again:

$$\sum_{i=0}^{n-1} 1 - h(p_i) \leq \sum_{i=0}^{n-1} I(g, x_i | y = i) \leq m$$

$$\Rightarrow n - \sum_{i=0}^{n-1} h(p_i) \leq m$$

$$\Rightarrow n(1 - h(p)) \leq m$$

if p>1/2 then 1-h(p) ≠ 0 and m scales with n

IC implies NTCC: More rigorously

Define the average winning probability: $p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$

Using Fano's inequality again:

$$\sum_{i=0}^{n-1} 1 - h(p_i) \leq \sum_{i=0}^{n-1} I(g, x_i | y = i) \leq m$$

$$\Rightarrow n - \sum_{i=0}^{n-1} h(p_i) \leq m$$

$$\Rightarrow n(1 - h(p)) \leq m$$

if p>1/2 then 1-h(p) ≠ 0 and m scales with n , and thus:

$\mathrm{P}(ab|xy)$ satsifies IC $\Longrightarrow$ $\mathrm{P}(ab|xy)$ satsifies NTCC

But wait, there’s more

But wait, there's more

$$p = \frac{1}{n} \sum_{i=0}^{n-1} p_i$$

$$n(1 - h(p)) \leq m$$

But wait, there's more

$$p = \frac{1}{n} \sum_{i=0}^{n-1} p_i$$

if we ask that $p_i = 1$ for all i, then p=1

$$n(1 - h(p)) \leq m$$

But wait, there's more

$$p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$$

if we ask that $p_i = 1$ for all i, then p=1

(so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

But wait, there's more

$$p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$$

if we ask that $p_i = 1$ for all i, then p=1

(so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$

But wait, there's more

$$p = \frac{1}{n} \sum_{i=0}^{n-1} p_i$$

if we ask that p_i = 1 for all i, then p=1

(so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$

or

$$CC_0(\mathrm{INDEX}_n) = \Omega(n)$$

But wait, there's more

$$p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$$

if we ask that p_i = 1 for all i, then p=1 (so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$ **or** $CC_0(\text{INDEX}_n) = \Omega(n)$

We also remember,

But wait, there's more

$$p = \frac{1}{n} \sum_{i=0}^{n-1} p_i$$

if we ask that p_i = 1 for all i, then p=1

(so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$ **or** $$CC_0(\text{INDEX}_n) = \Omega(n)$$

We also remember,

IC for INDEX$_n$

But wait, there's more

$$p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$$

if we ask that p_i = 1 for all i, then p=1 (so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$

or $CC_0(\text{INDEX}_n) = \Omega(n)$

We also remember,

IC for INDEX_n

IC for IP_n

But wait, there's more

$$p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$$

if we ask that $p_i = 1$ for all i, then p=1

(so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$

or

$$CC_0(\text{INDEX}_n) = \Omega(n)$$

We also remember,

IC for INDEX$_n$

IC for IP$_n$

IC for DISJOINT$_n$

But wait, there's more

$$p = \frac{1}{n} \sum_{i=0}^{n-1} p_i$$

if we ask that p_i = 1 for all i, then p=1 (so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$ **or** $$CC_0(\text{INDEX}_n) = \Omega(n)$$

We also remember,

IC for INDEX_n = IC for IP_n = IC for DISJOINT_n

But wait, there's more

$$p = \frac{1}{n} \sum_{i=0}^{n-1} p_i$$

if we ask that p_i = 1 for all i, then p=1 (so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$ **or** $CC_0(\text{INDEX}_n) = \Omega(n)$

We also remember,

IC for INDEX_n = **IC for IP_n** = **IC for DISJOINT_n**

$$CC_0(\text{INDEX}_n) = CC_0(\text{IP}_n) = CC_0(\text{DISJOINT}_n) = \Omega(n)$$

But wait, there's more

$$p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$$

if we ask that $p_i = 1$ for all i, then p=1

(so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$

or $CC_0(\text{INDEX}_n) = \Omega(n)$

We also remember,

IC for INDEX_n = **IC for IP_n** = **IC for DISJOINT_n**

$CC_0(\text{INDEX}_n)$ = $CC_0(\text{IP}_n)$ = $CC_0(\text{DISJOINT}_n) = \Omega(n)$

get deterministic complexity bounds for free!

But wait, there's more

$$p = \frac{1}{n}\sum_{i=0}^{n-1} p_i$$

if we ask that p_i = 1 for all i, then p=1 (so average case and worst case complexity coincide)

$$n(1 - h(p)) \leq m$$

$$\Rightarrow n \leq m \equiv m = \Omega(n)$$ **or** $CC_0(\text{INDEX}_n) = \Omega(n)$

We also remember,

IC for INDEX_n = **IC for IP_n** = **IC for DISJOINT_n**

$$CC_0(\text{INDEX}_n) = CC_0(\text{IP}_n) = CC_0(\text{DISJOINT}_n) = \Omega(n)$$

get deterministic complexity bounds for free!

in a theory independent manner!

CONCLUSION

CONCLUSION

An algorithm to derive quantum Bell inequalities

which is protocol agnostic and works for arbitrary number of measurements and outcomes

CONCLUSION

An algorithm to derive quantum Bell inequalities

which is protocol agnostic and works for arbitrary number of measurements and outcomes

Extending the IC principle to any distributed computation scenario

Proved the extended IC statement, showed its reduction to original IC.
The reduction scheme implies an equivalence class structure on the space of all functions.

CONCLUSION

An algorithm to derive quantum Bell inequalities

which is protocol agnostic and works for arbitrary number of measurements and outcomes

Extending the IC principle to any distributed computation scenario

Proved the extended IC statement, showed its reduction to original IC.
The reduction scheme implies an equivalence class structure on the space of all functions.

INDEX
IP
DISJ

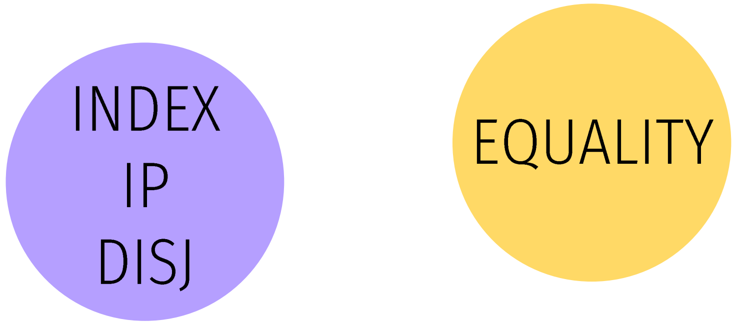
CONCLUSION

An algorithm to derive quantum Bell inequalities

which is protocol agnostic and works for arbitrary number of measurements and outcomes

Extending the IC principle to any distributed computation scenario

Proved the extended IC statement, showed its reduction to original IC.
The reduction scheme implies an equivalence class structure on the space of all functions.



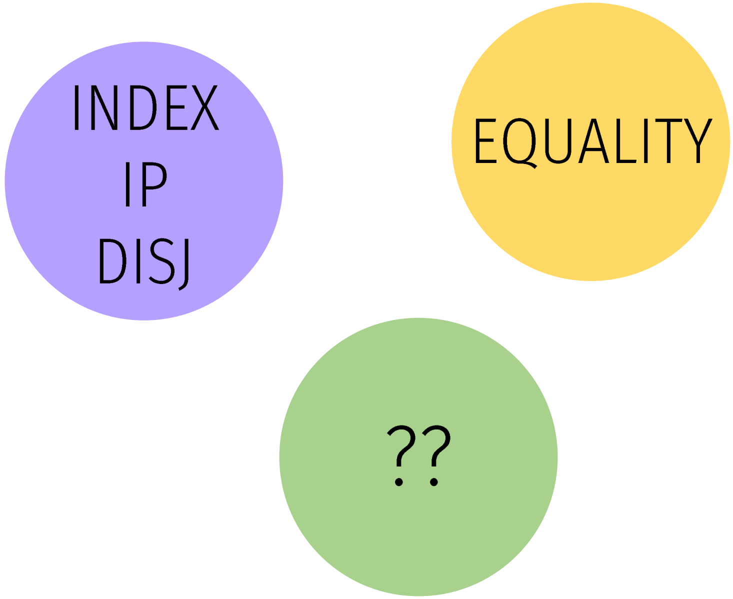
CONCLUSION

An algorithm to derive quantum Bell inequalities

which is protocol agnostic and works for arbitrary number of measurements and outcomes

Extending the IC principle to any distributed computation scenario

Proved the extended IC statement, showed its reduction to original IC.
The reduction scheme implies an equivalence class structure on the space of all functions.



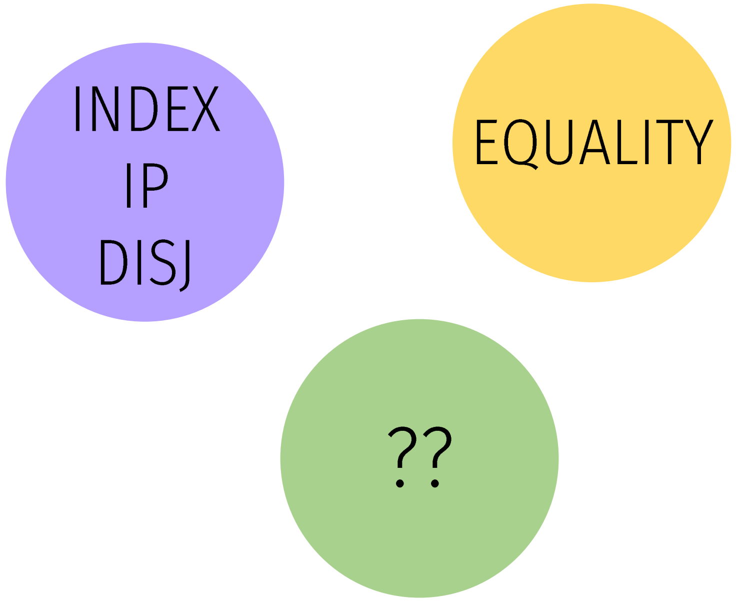
CONCLUSION

An algorithm to derive quantum Bell inequalities

which is protocol agnostic and works for arbitrary number of measurements and outcomes

Extending the IC principle to any distributed computation scenario

Proved the extended IC statement, showed its reduction to original IC.
The reduction scheme implies an equivalence class structure on the space of all functions.



Showed IC to be strictly stronger than NTCC and derived communication complexity bounds

Demonstrated that IC supersedes NTCC and used the principle to prove deterministic complexity bounds in a theory-independent manner.

CONCLUSION

An algorithm to derive quantum Bell inequalities

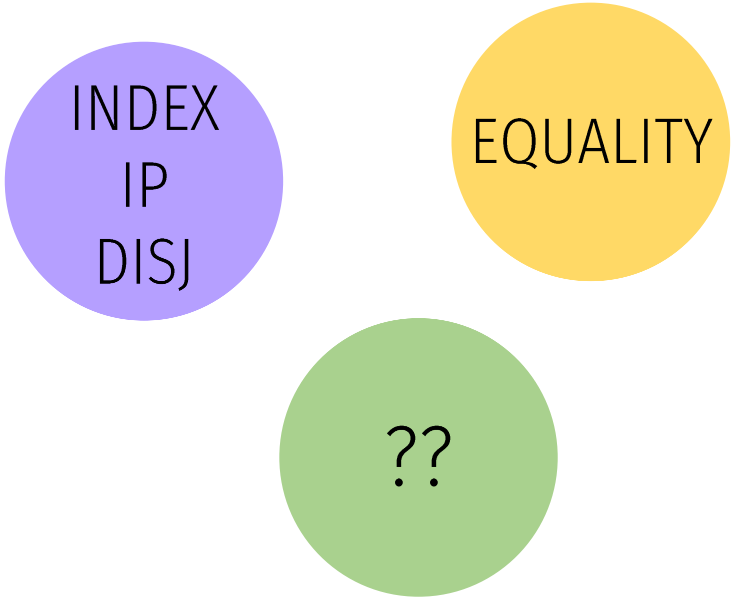
which is protocol agnostic and works for arbitrary number of measurements and outcomes

Extending the IC principle to any distributed computation scenario

Proved the extended IC statement, showed its reduction to original IC.
The reduction scheme implies an equivalence class structure on the space of all functions.

Showed IC to be strictly stronger than NTCC and derived communication complexity bounds

Demonstrated that IC supersedes NTCC and used the principle to prove deterministic complexity bounds in a theory-independent manner.



THANK YOU!

Appendix: for the nosy ones

- If two function have identical IC statements, the one which requires less number of PR boxes to decide has more bounding power. Why?

$$P(g = i|x = j, y = k) = \frac{1 + e_c(\,)\ldots(\,)}{d}$$

In the convolution, each bias being smaller than 1 causes the probability and hence the mutual information to be smaller in magnitude since the effective bias is smaller.

- The argument for bounding does not work for the randomised case because if p is probabilistic, it is some complicated function of n, as we see below

$$n(1 - h(p_n)) \leq m(n), \quad p_n = \frac{1}{2} + \sum_i q_i(n)$$

Hence, extracting the dependence of the message size on n by eliminating p_n is not straightforward and you have to consider the protocol in detail to invert the relation, optimise over the best ones and then get a bound.