Title: The min-entropy of classical quantum combs and some applications

Speakers: Isaac Smith

Series: Quantum Foundations

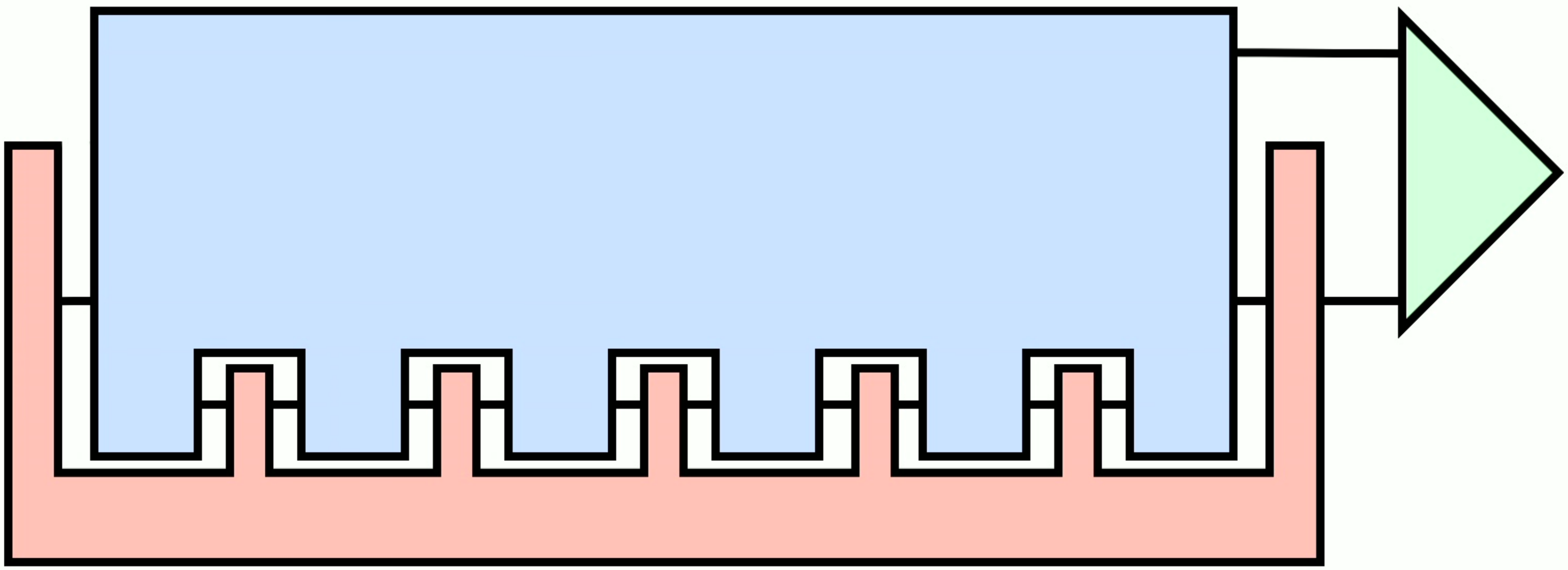
Date: June 08, 2023 - 11:00 AM

URL: https://pirsa.org/23060052

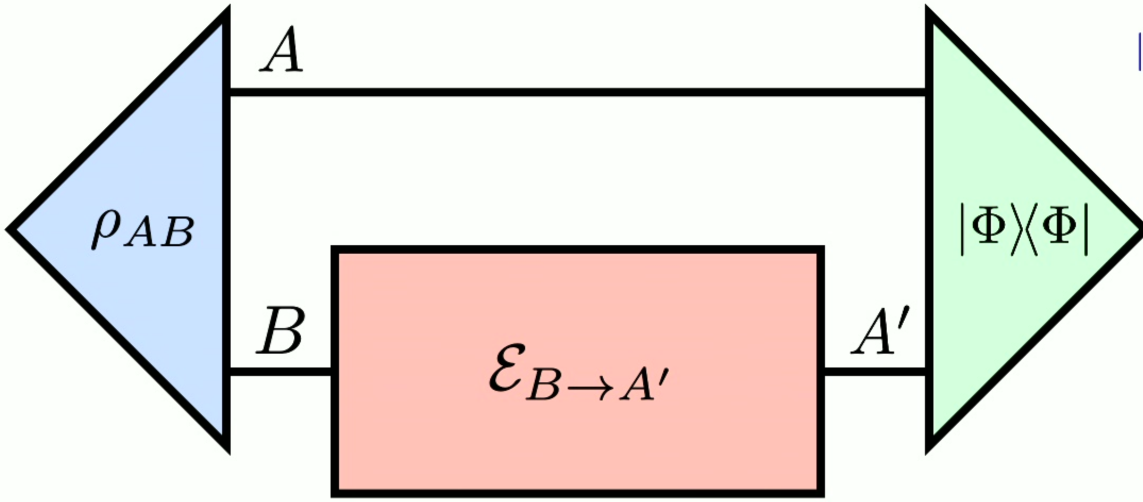
Abstract: It is often the case that interaction with a quantum system does not simply occur between an initial point in time and a final one, but rather over many time steps. In such cases, an interaction at a given time step can have an influence on the dynamics of the system at a much later time. Just as quantum channels model dynamics between two time steps, quantum combs model the more general multi-time dynamics described above, and have accordingly found application in such fields as open quantum systems and quantum cryptography. In this talk, we will consider ensembles of combs indexed by a random variable, dubbed classical-quantum combs, and discuss how much can be learnt about said variable through interacting with the system. We characterise the amount of information gain using the comb min-entropy, an extension of the analogous entropic quantity for quantum states. With combs and the min-entropy in our toolbox, we turn to a number of applications largely inspired by Measurement-Based Quantum Computing (MBQC), including the security analysis of a specific Blind Quantum Computing protocol and some comments regarding learning causal structure.

Zoom Link: https://pitp.zoom.us/j/98315660866?pwd=cWU3RzB6SG9DOGIza1BqV1lqNklvQT09

The min-entropy of classical-quantum combs and some applications



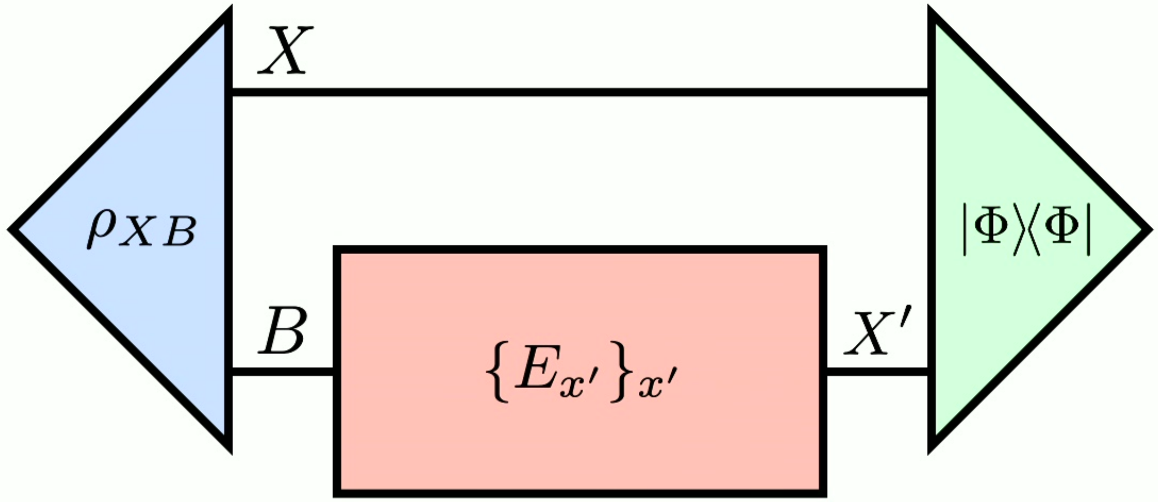
Isaac Smith, 08.06.23, Perimeter Institute



$|\Phi\rangle\langle\Phi|$ unnormalised!

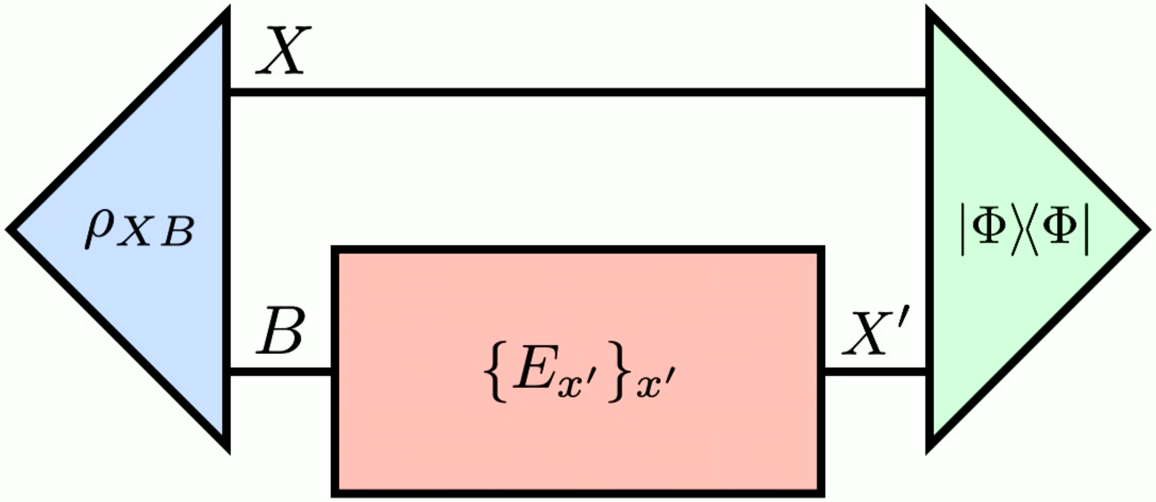
$$H_{\min}(A|B)_{\rho_{AB}} := -\log_2 \max_{\mathcal{E}} \mathrm{Tr}\left[|\Phi\rangle\langle\Phi| \left(I_A \otimes \mathcal{E}\right)\rho_{AB}\right]$$

König, R., et al; *IEEE Transactions on Information theory* 55, no. 9 (2009): 4337-4347.



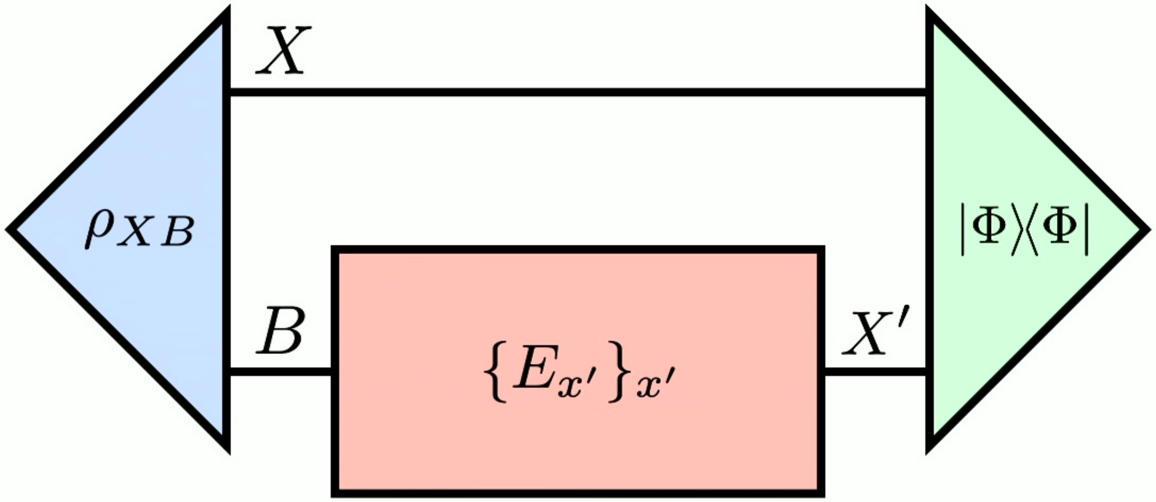
$$\rho_{XB} = \sum_x p_x \, |x\rangle\langle x| \otimes \rho_B^x$$

7



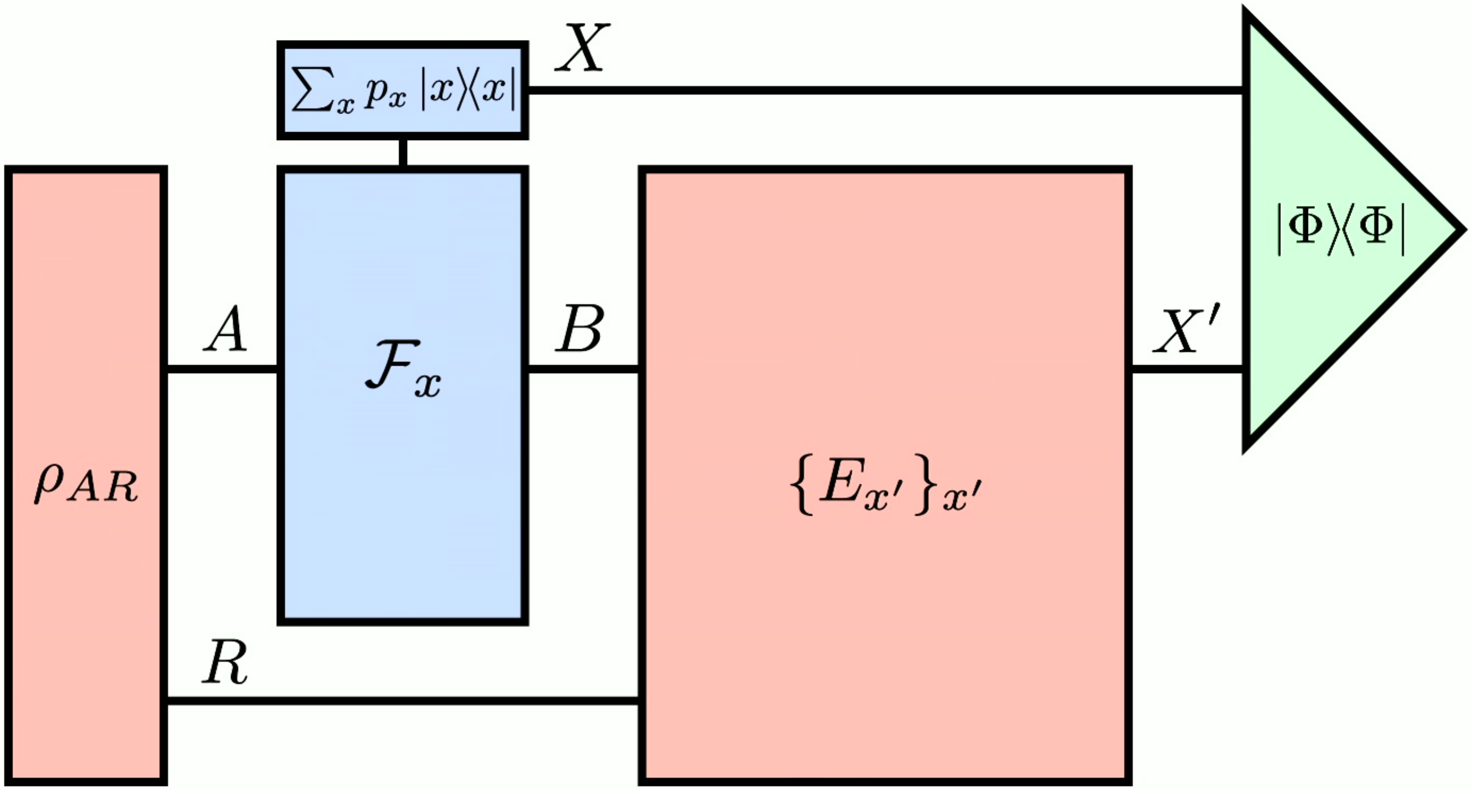
$$\max_{\{E_{x'}\}_{x'}} \sum_{x,x'} p_x \delta_{x,x'} \operatorname{Tr}[E_{x'} \rho_B^x]$$

8



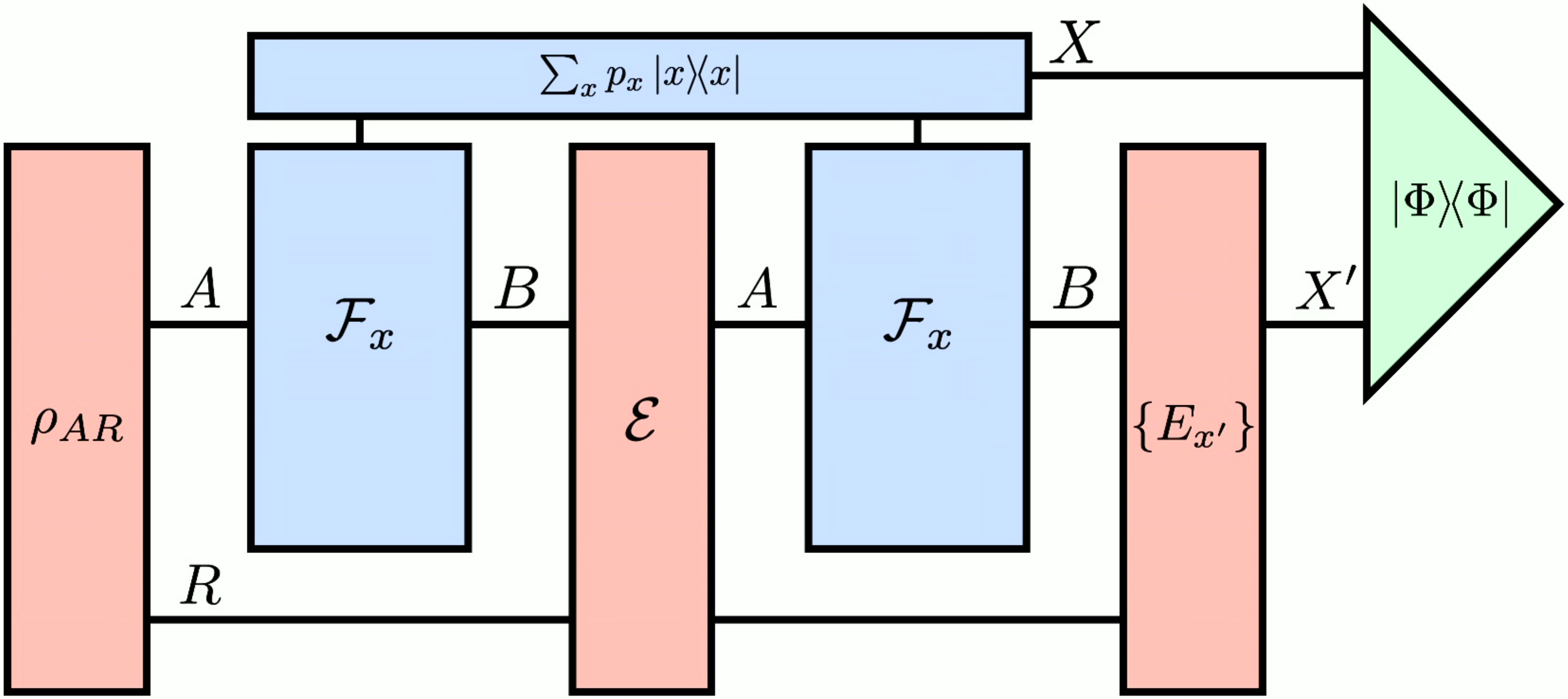
$$\max_{\{E_{x'}\}_{x'}} \sum_{x,x'} p_x \delta_{x,x'} \underbrace{\mathrm{Tr}[E_{x'} \rho_B^x]}_{p_{x'|x}}$$

"How distinguishable are the ρ_B^x"

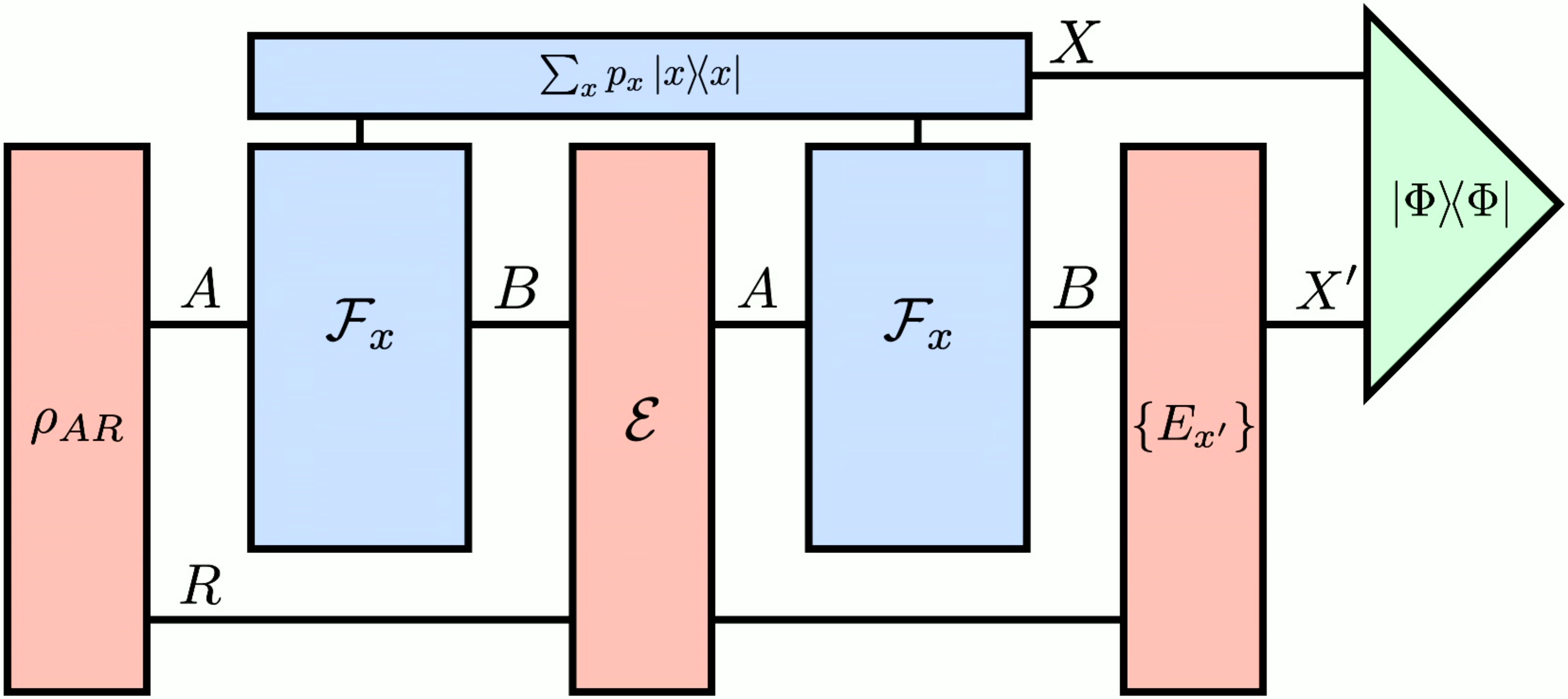


$$\max_{\rho_{AR},\{E_{x'}\}} \sum_x p_x \delta_{x,x'} \,\mathrm{Tr}[E_{x'} \mathcal{F}_x \otimes I_R(\rho_{AR})]$$

11



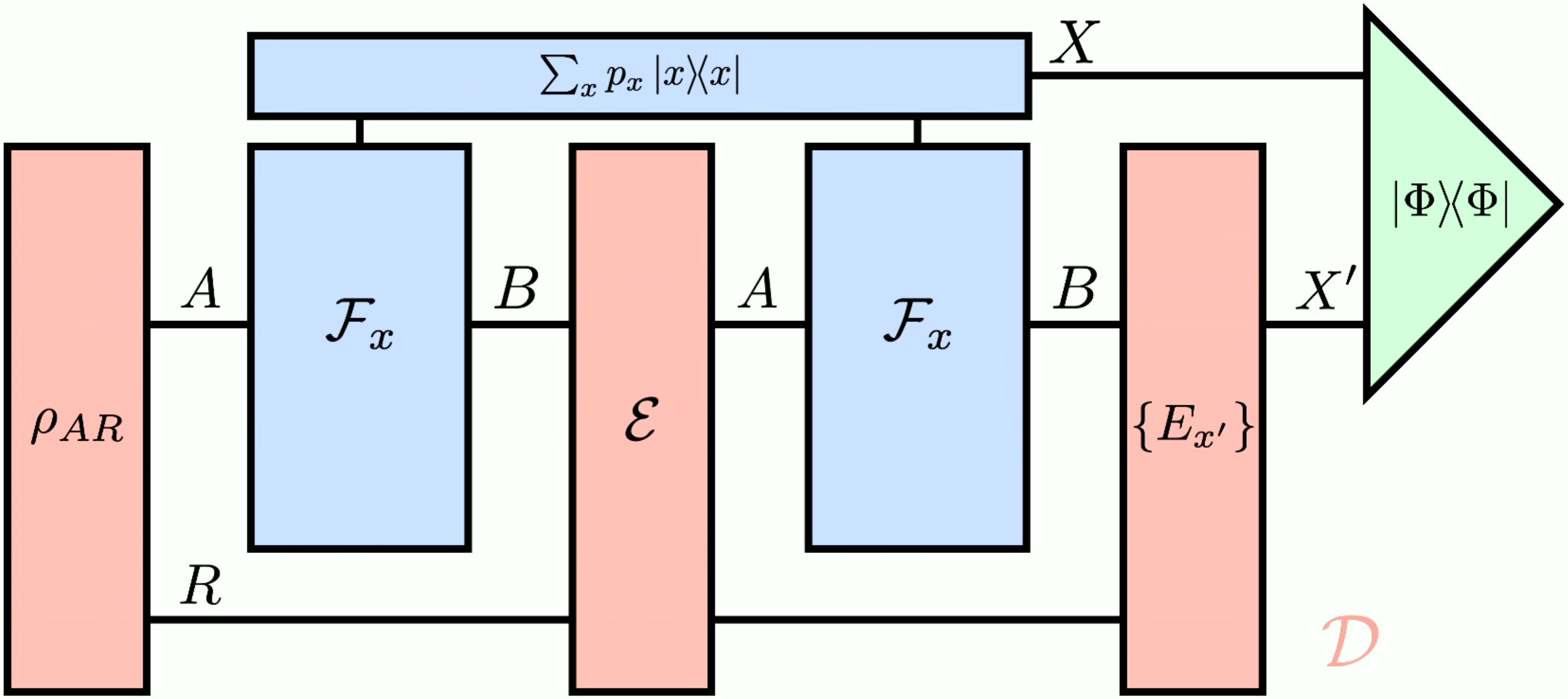
Harrow, AW. et al. *PRA* 81, no. 3 (2010): 032339



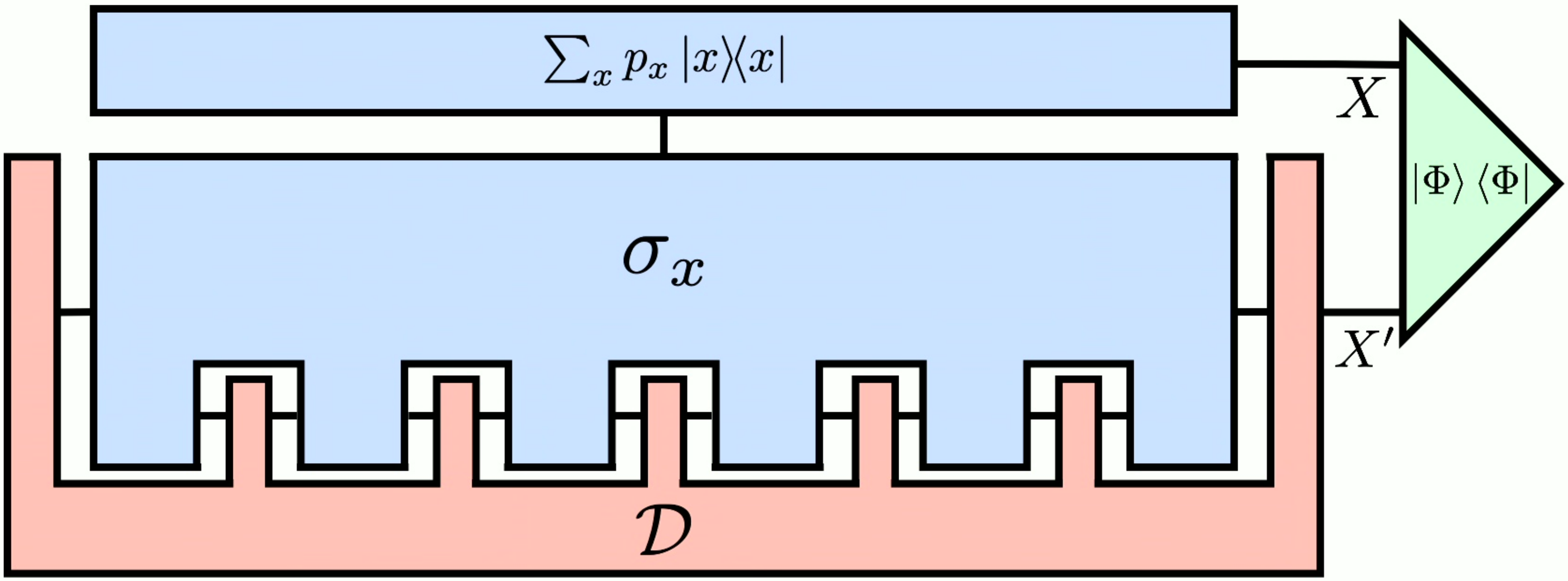
$$\max_{\rho_{AR},\mathcal{E},\{E_{x'}\}} \sum_x p_x \delta_{x,x'} \operatorname{Tr}[E_{x'}(\mathcal{F}_x \otimes R') \circ \mathcal{E} \circ (\mathcal{F}_x \otimes I_R)(\rho_{AR})]$$

Harrow, AW. et al. *PRA* 81, no. 3 (2010): 032339

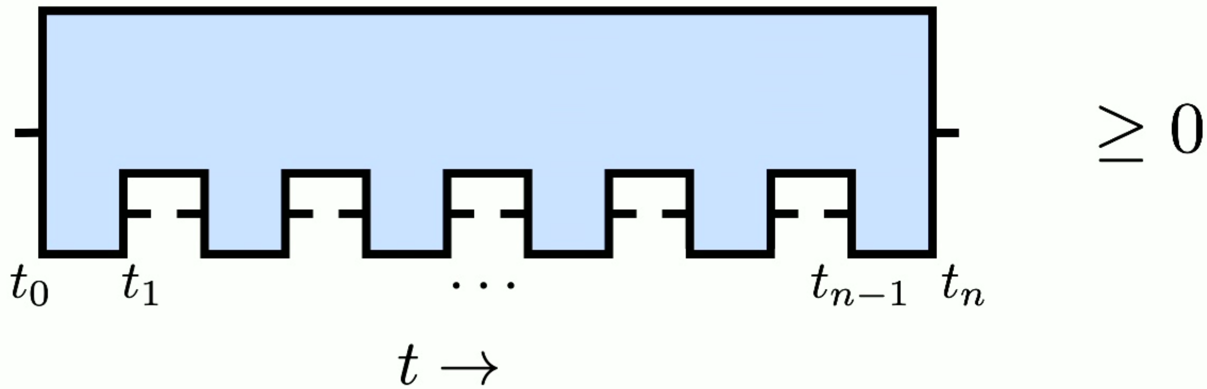
12

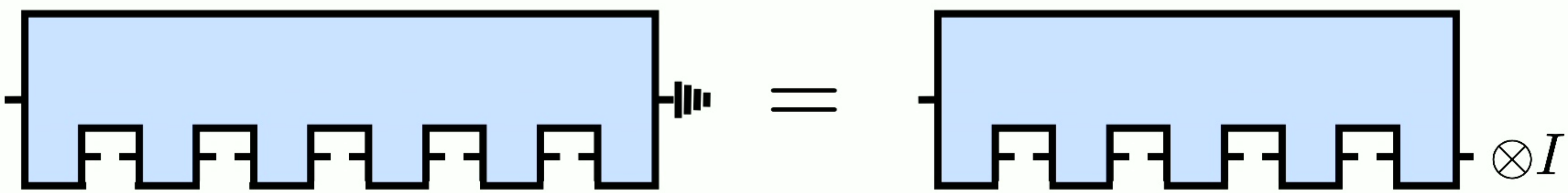


$$\max_{\mathcal{D}} \sum_x p_x |x\rangle\langle x| \otimes \mathcal{F}_x^{\otimes 2} * \mathcal{D}$$



$$\mathcal{C} := \sum_x p_x |x\rangle\langle x| \otimes \sigma_x \qquad \max_{\mathcal{D}} \mathcal{C} * \mathcal{D}$$


≥ 0
t_0 t_1 $\cdots$ t_{n-1} t_n
$t \rightarrow$


$=$
$\otimes I$

$$H_{\min}(t_n, t_{n-1}|t_0, ..., t_{n-2})_{\mathcal{C}} = -\log\left(\underbrace{\max_{\mathcal{D}} \mathcal{C} * \mathcal{D}}_{\text{Semidefinite Program!}}\right)$$

$$\xLeftarrow{\text{Strong Duality}}$$

$$H_{\min}(t_n, t_{n-1}|t_0, ..., t_{n-2})_{\mathcal{C}} = -\log\min_{\Gamma}\min\{\lambda : \mathcal{C} \leq \lambda\Gamma \otimes I_{t_{n-1,n}}\}$$

$$H_{\min}(t_n, t_{n-1}|t_0, ..., t_{n-2})_{\mathcal{C}} = -\log\left(\underbrace{\max_{\mathcal{D}} \mathcal{C} * \mathcal{D}}_{\text{Semidefinite Program!}}\right)$$

Strong Duality $\Longleftarrow$

$$H_{\min}(t_n, t_{n-1}|t_0, ..., t_{n-2})_{\mathcal{C}} = -\log\min_{\Gamma}\min\{\lambda : \mathcal{C} \leq \lambda\Gamma \otimes I_{t_{n-1,n}}\}$$

$$\mathcal{C} := \sum_x p_x\, |x\rangle\langle x| \otimes \sigma_x \qquad\qquad H_{\min}(X|\sigma_x)_{\mathcal{C}}$$

We can hypothesis test structure.

18

MBQC in one slide

MBQC consists of: Entanglement $|G\rangle$

Measurements $|+_\alpha\rangle\langle+_\alpha|$ $|-_\alpha\rangle\langle-_\alpha|$

MBQC in one slide

MBQC consists of:	Entanglement	$\vert G\rangle$	
	Measurements	$\vert +_\alpha\rangle\langle +_\alpha\vert$	$\vert -_\alpha\rangle\langle -_\alpha\vert$
		$\Downarrow$	$\Downarrow$
	Corrections	No	Yes

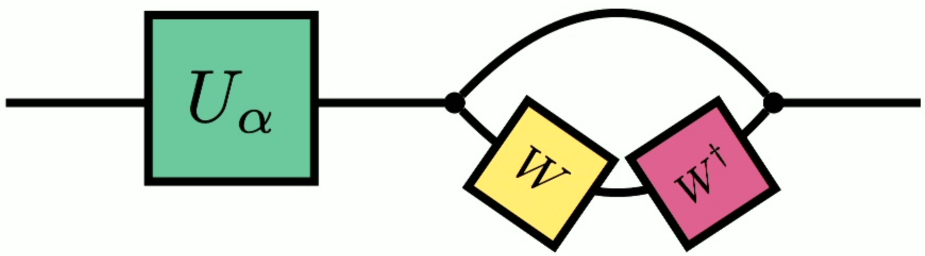
First example and an aside: Routed Circuits

$|+_\alpha\rangle\langle+_\alpha|$

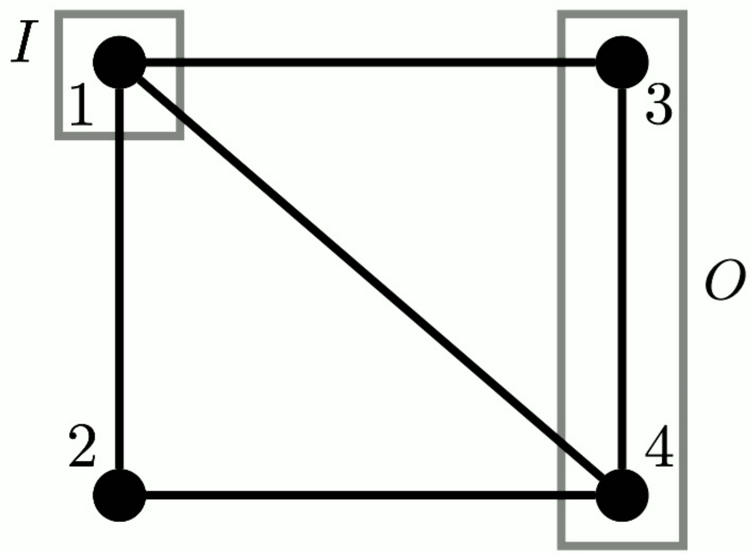
$$|\psi\rangle \mapsto U_\alpha |\psi\rangle$$

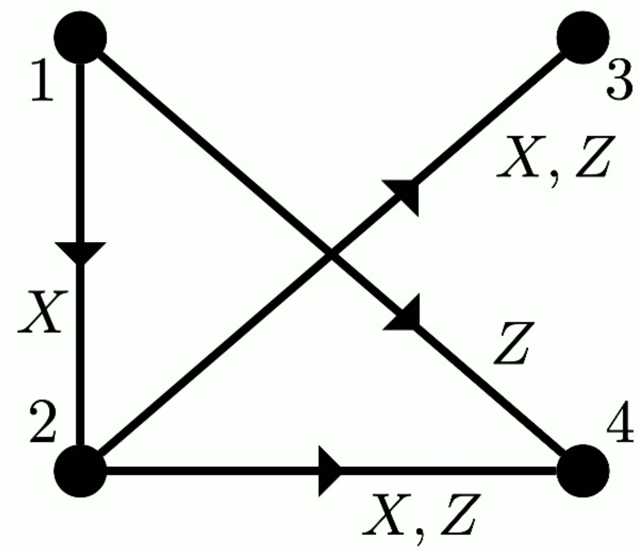
$|-_\alpha\rangle\langle-_\alpha|$

$$|\psi\rangle \mapsto U_{\alpha+\pi} |\psi\rangle = W U_\alpha |\psi\rangle$$



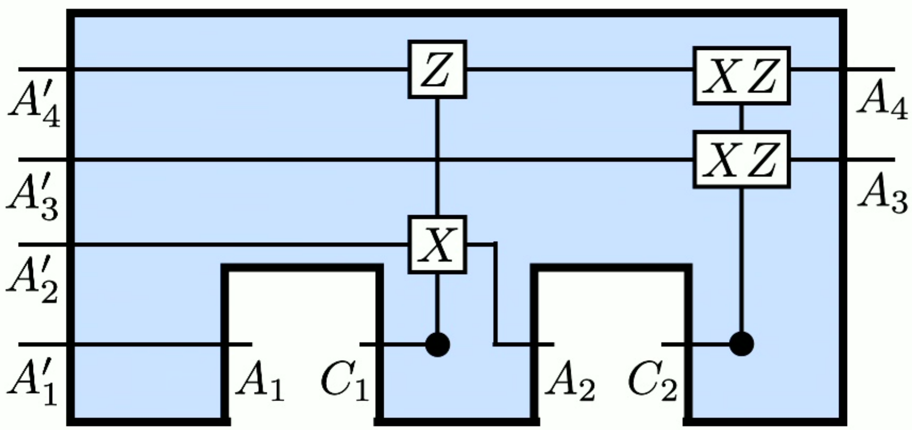
Testing Corrections

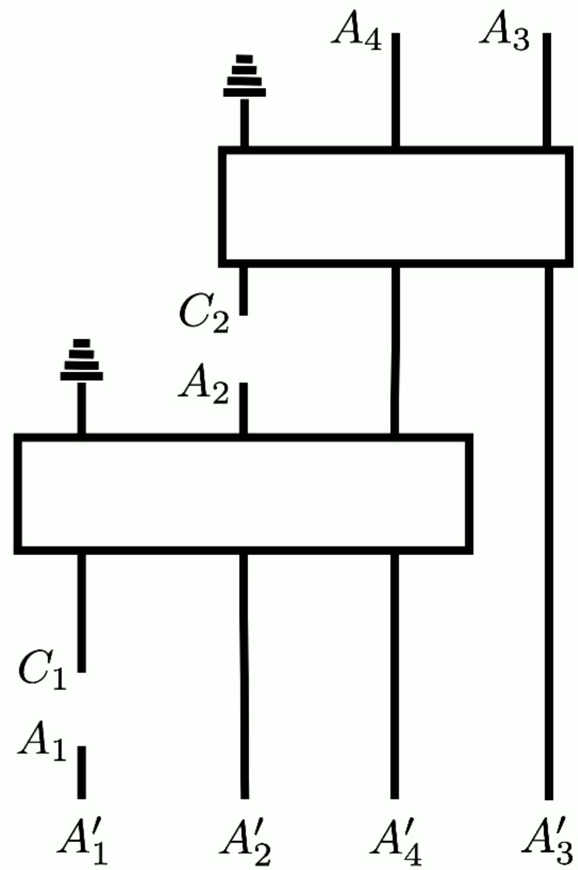




21

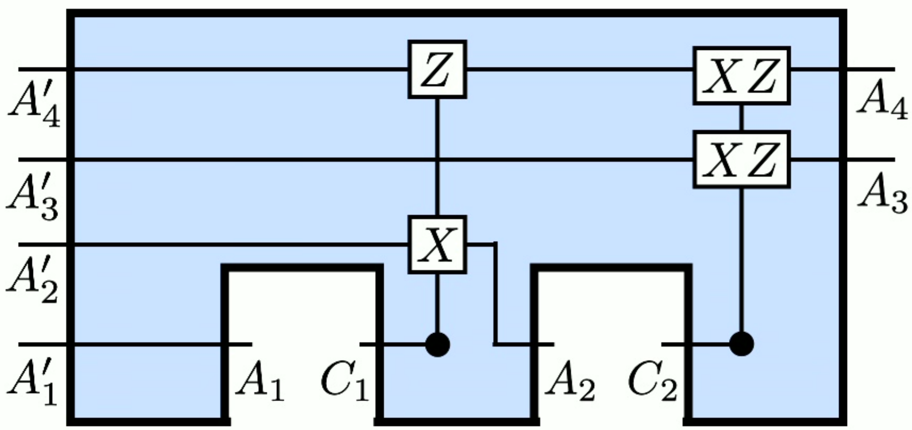
Testing Corrections

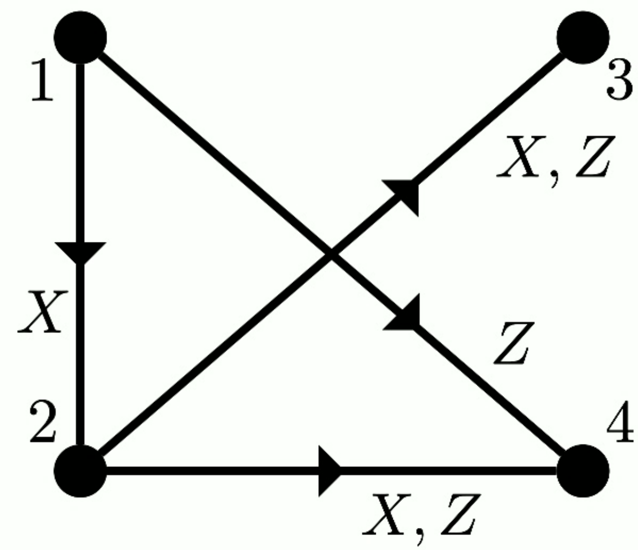




23

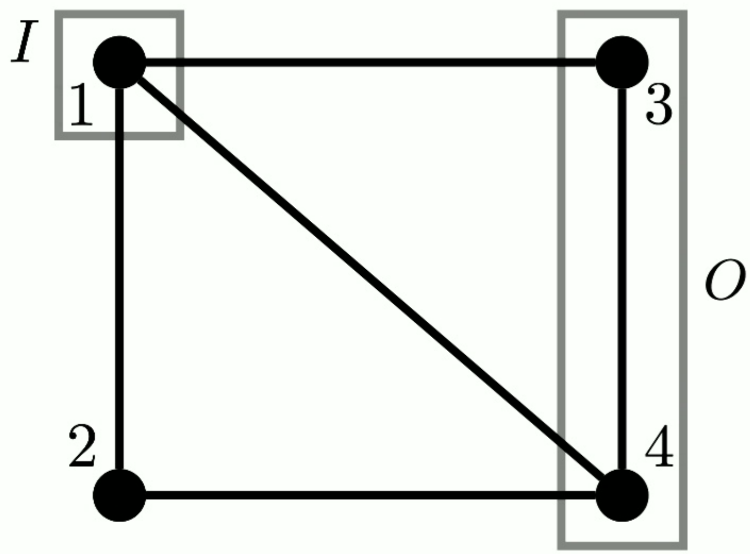
Testing Corrections

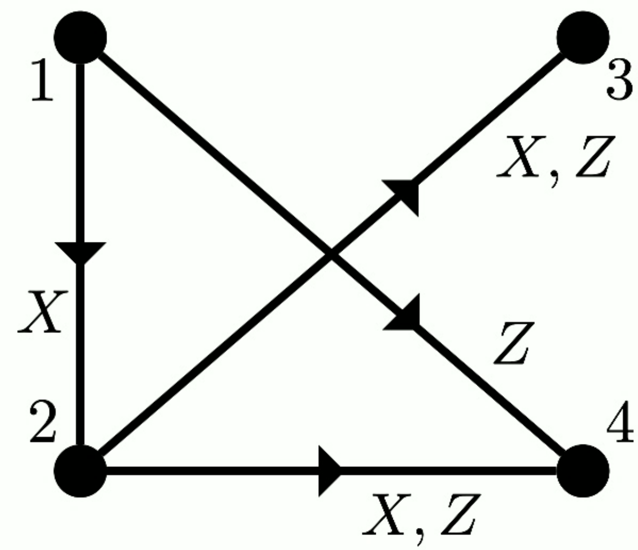




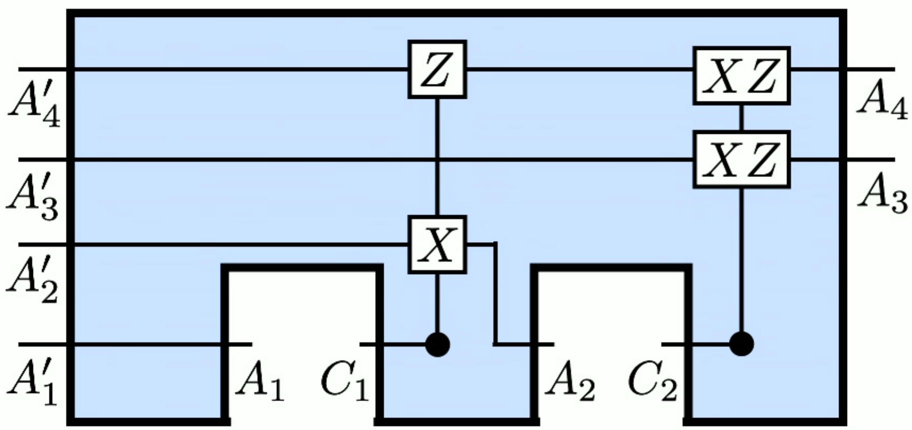
22

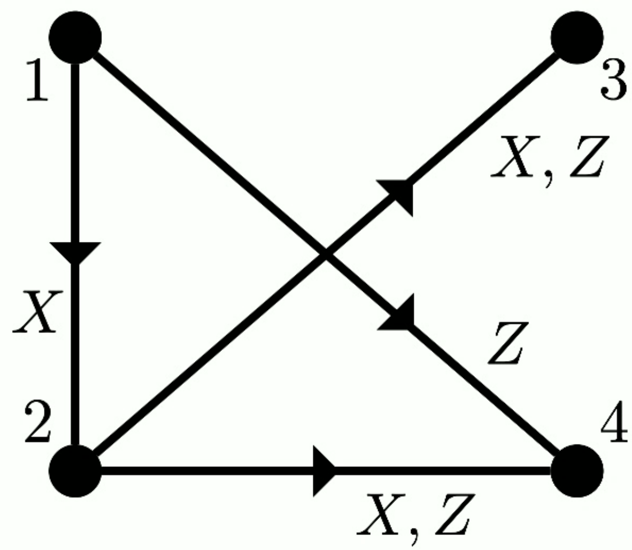
Testing Corrections





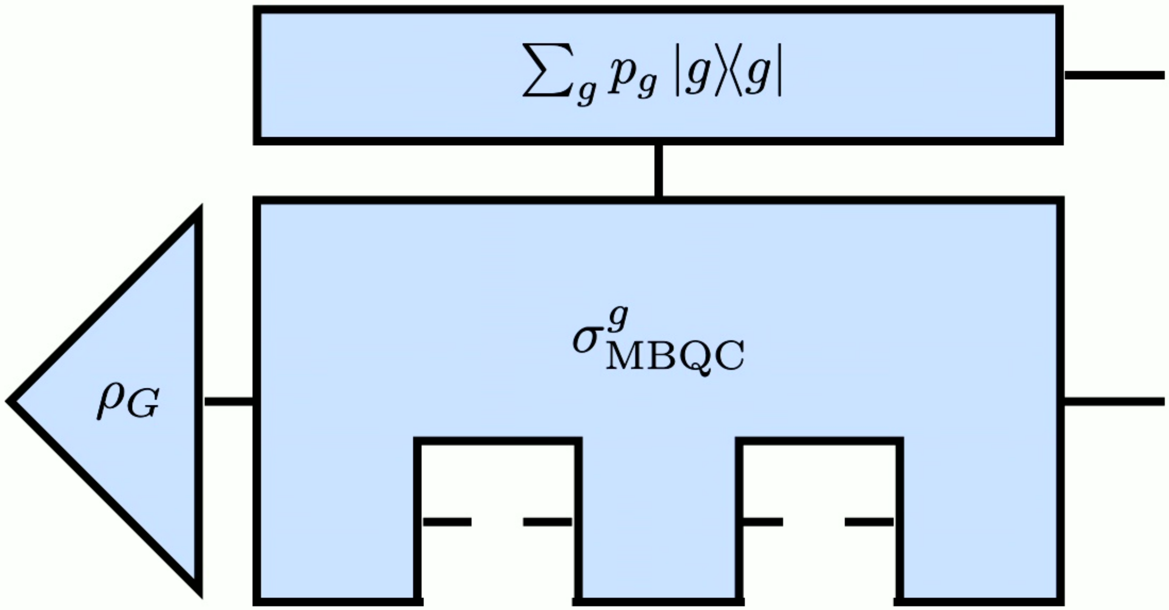
Testing Corrections





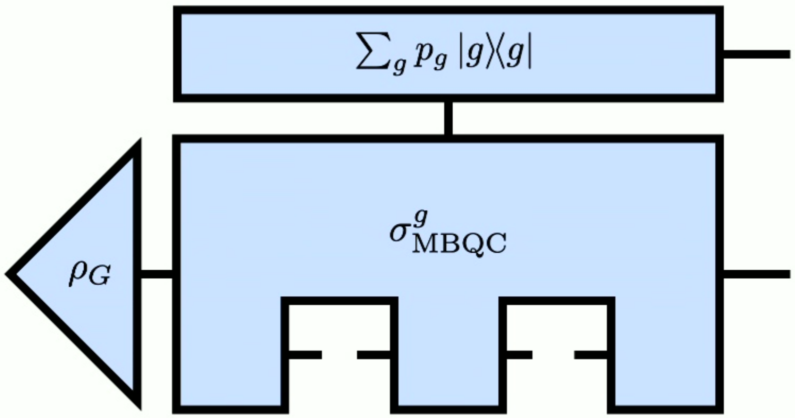
22

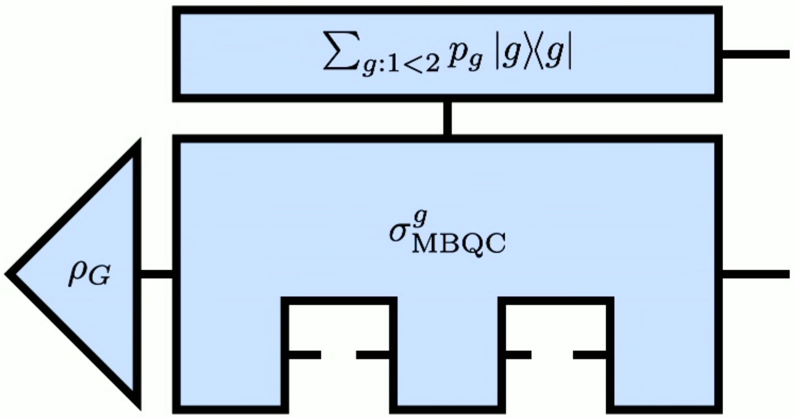
Testing Corrections



27

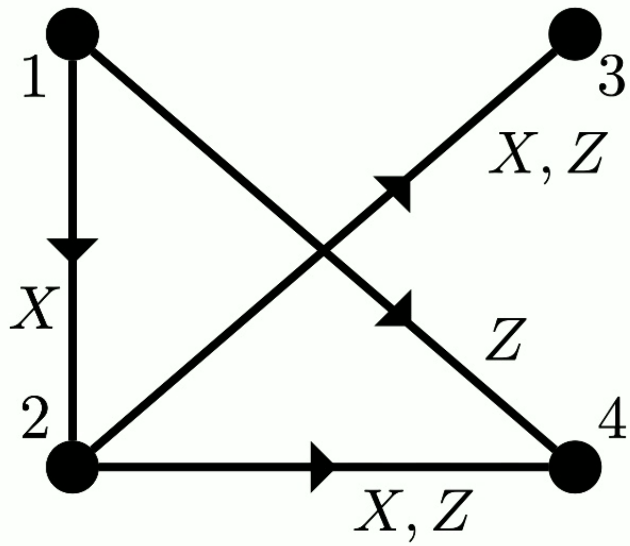
Testing Corrections

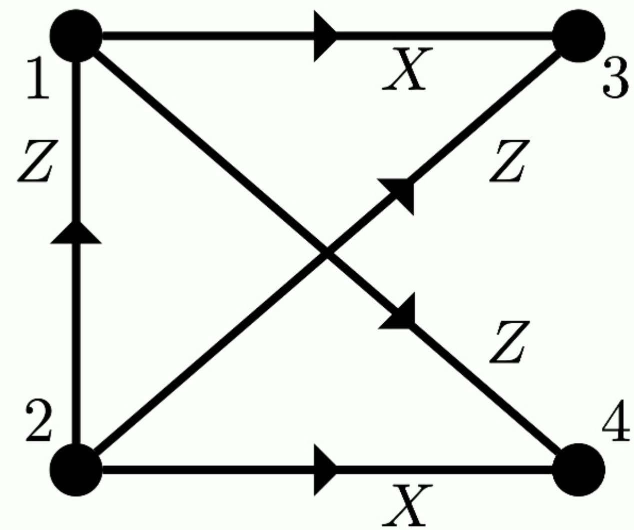




28

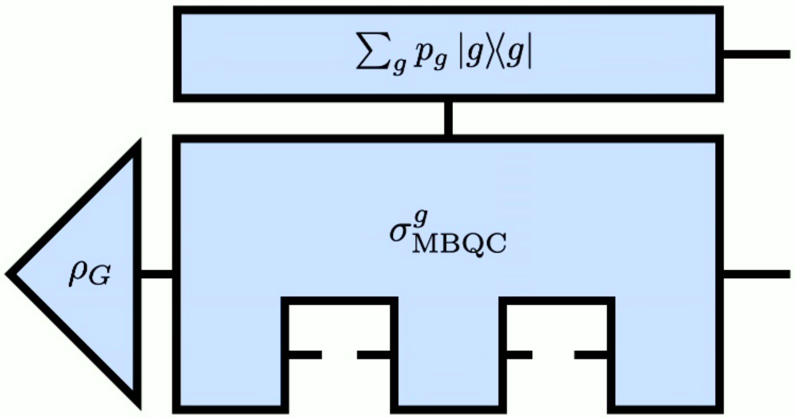
Testing Corrections

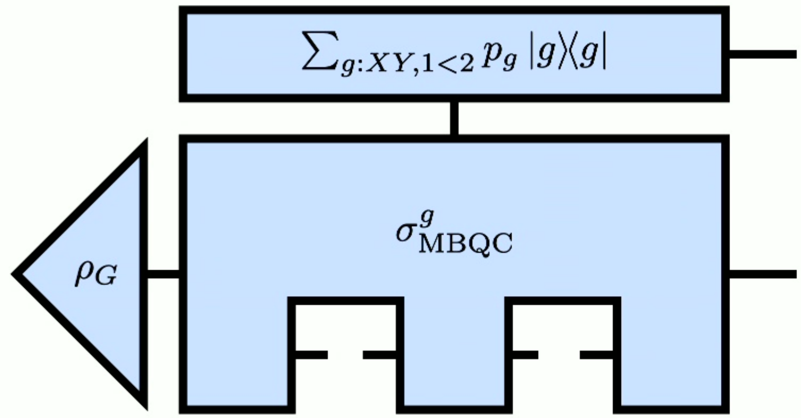




29

Testing Corrections

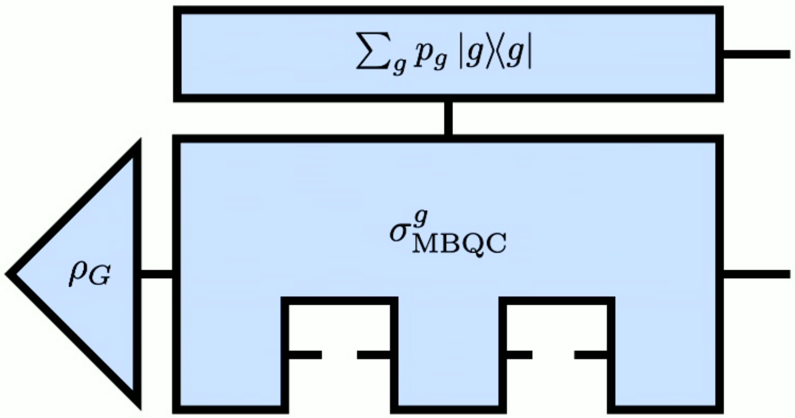




$$\max_{\mathcal{D}} \mathcal{C} * \mathcal{D} = 0.373$$

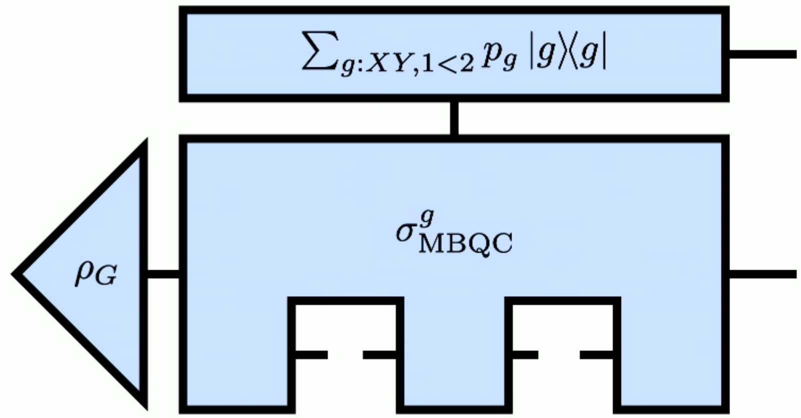
$$\frac{1}{15} \approx 0.067$$

Testing Corrections



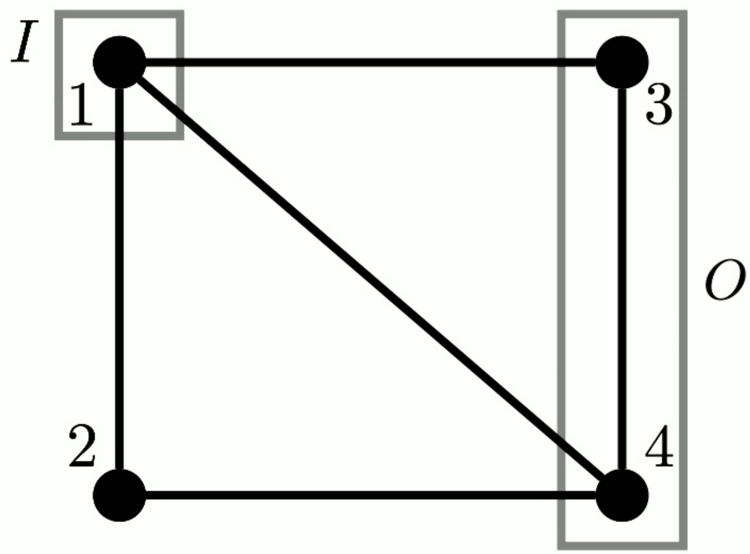
$$\max_{\mathcal{D}} \mathcal{C} * \mathcal{D} = 0.373$$

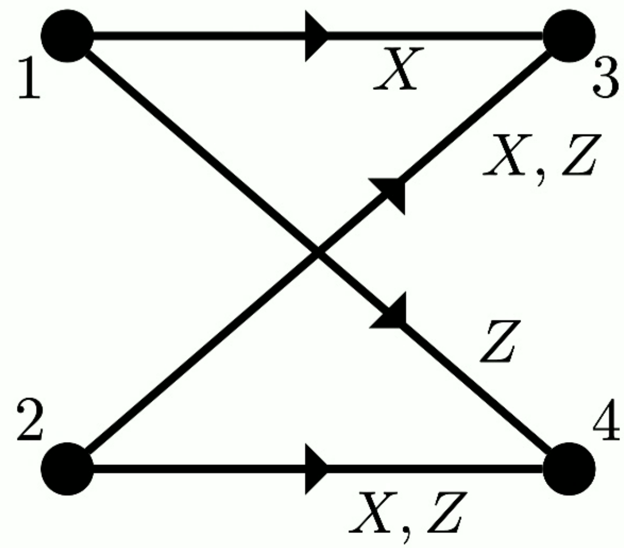
$$\frac{1}{15} \approx 0.067$$



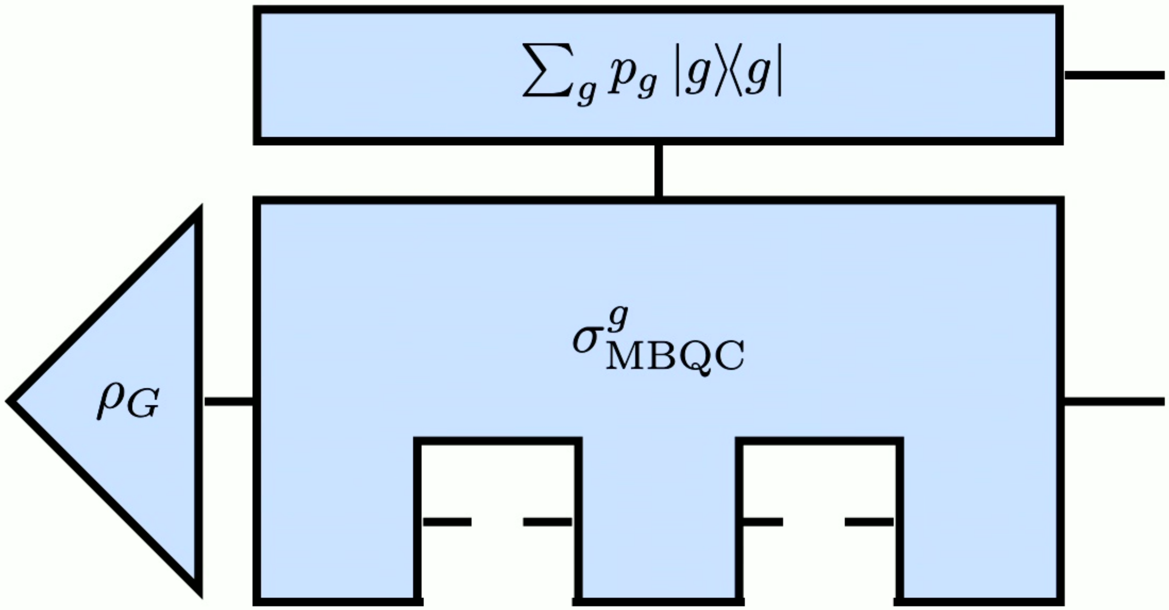
$$\max_{\mathcal{D}} \mathcal{C} * \mathcal{D} = 0.250$$

Testing Corrections

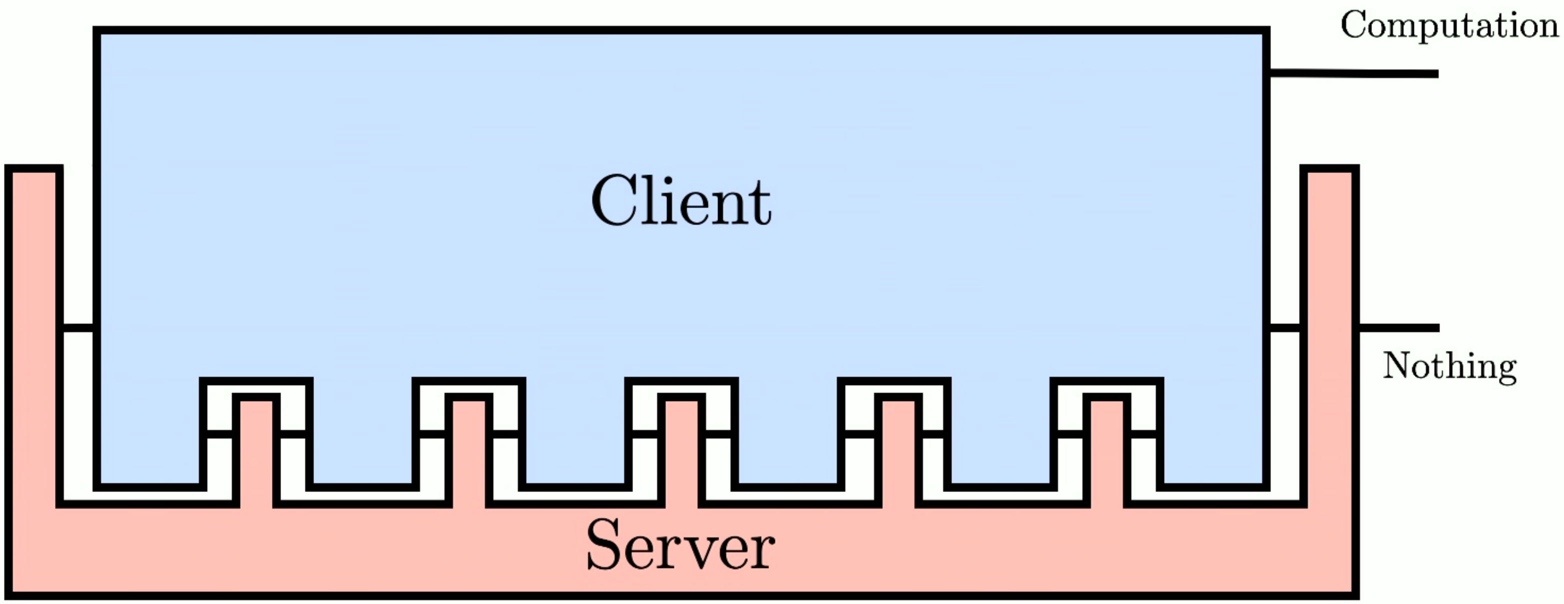




Testing Corrections

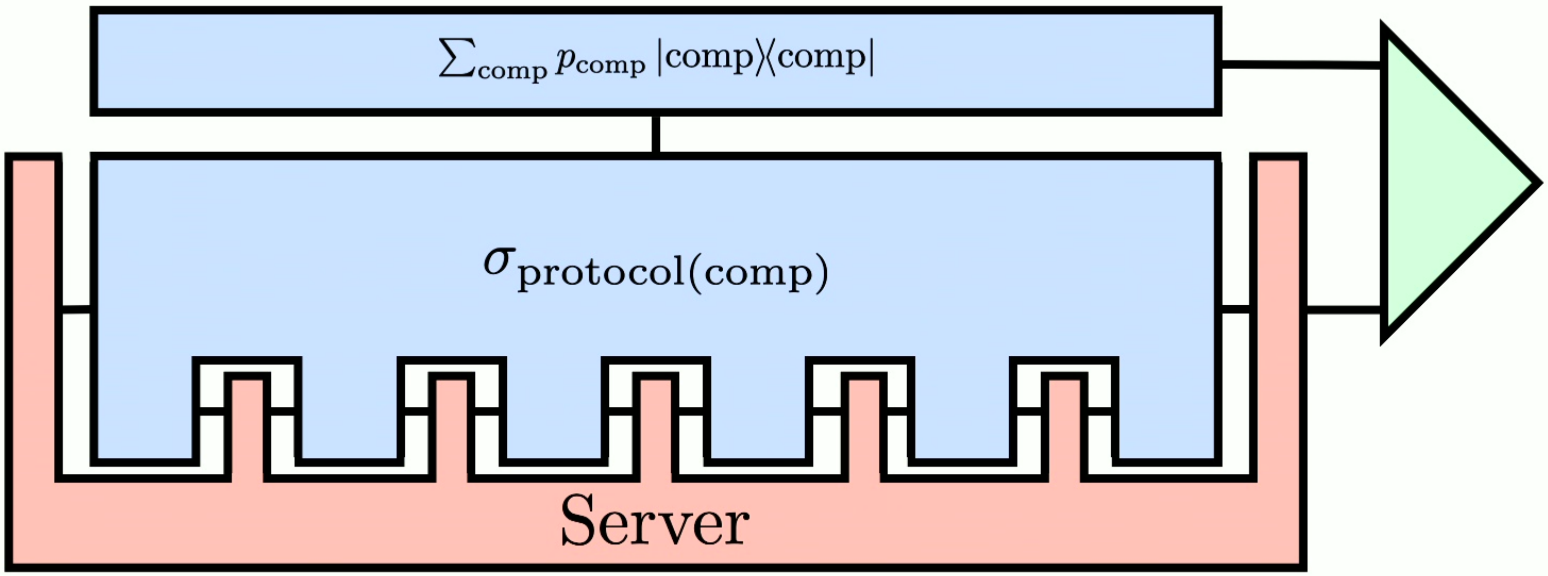


Blind Quantum Computation



31

Blind Quantum Computation



Mantri, A. *PRX* 7, no. 3 (2017): 031004.

Blind Quantum Computation

$$|+_\alpha\rangle\langle+_\alpha| \;:\; |\psi\rangle \mapsto U_\alpha |\psi\rangle$$

$$|-_\alpha\rangle\langle-_\alpha| \;:\; |\psi\rangle \mapsto U_{\alpha+\pi} |\psi\rangle$$

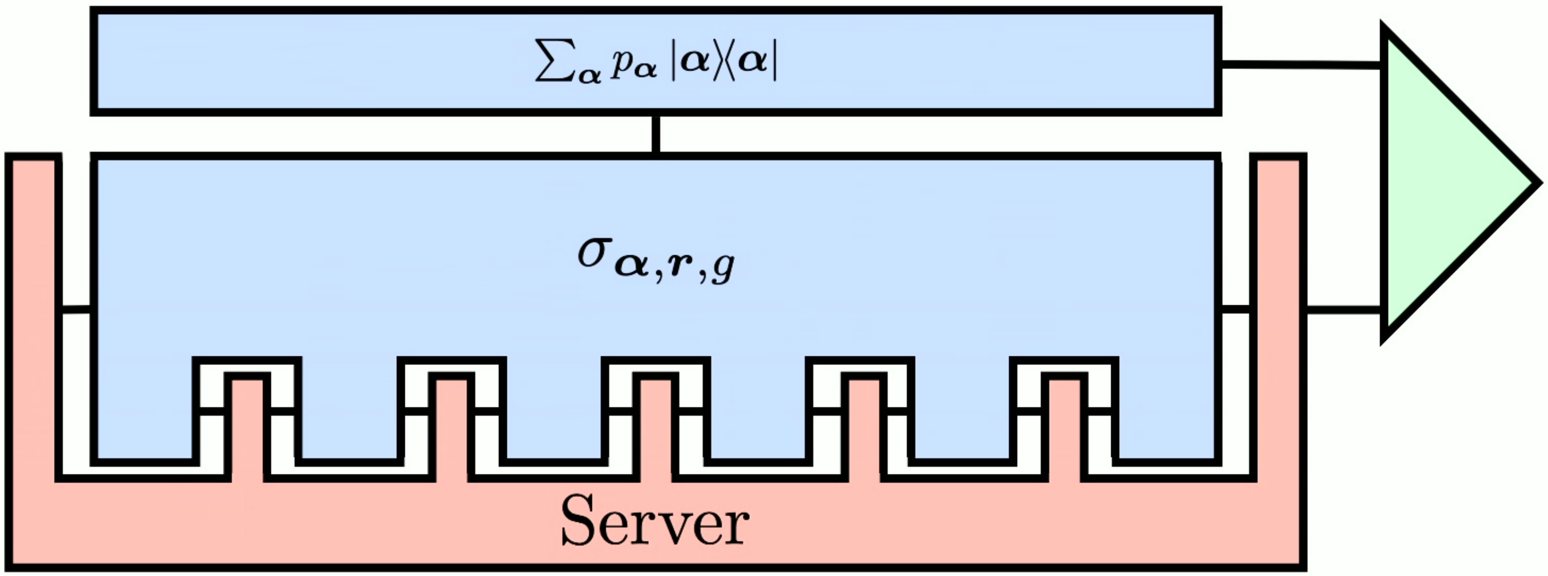
$$|||$$

$$|-_{\alpha+\pi}\rangle\langle-_{\alpha+\pi}|$$

	Angles	Outcomes
Computation:	$\boldsymbol{\alpha}$	$\mathbf{0}$
	$\boldsymbol{\alpha} + \boldsymbol{r}\pi$	$\boldsymbol{r}$

Mantri, A. *PRX* 7, no. 3 (2017): 031004.

Blind Quantum Computation



Mantri, A. *PRX* 7, no. 3 (2017): 031004.

Blind Quantum Computation

$\mathcal{C}_1 := \sum_{\boldsymbol{\alpha}} p_{\boldsymbol{\alpha}} \, |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \otimes \sigma_{\boldsymbol{\alpha},\boldsymbol{r},g}$ $\qquad$ $H_{\min}(\boldsymbol{\alpha}|\sigma_{\boldsymbol{\alpha},\boldsymbol{r},g})_{\mathcal{C}_1} > 0$

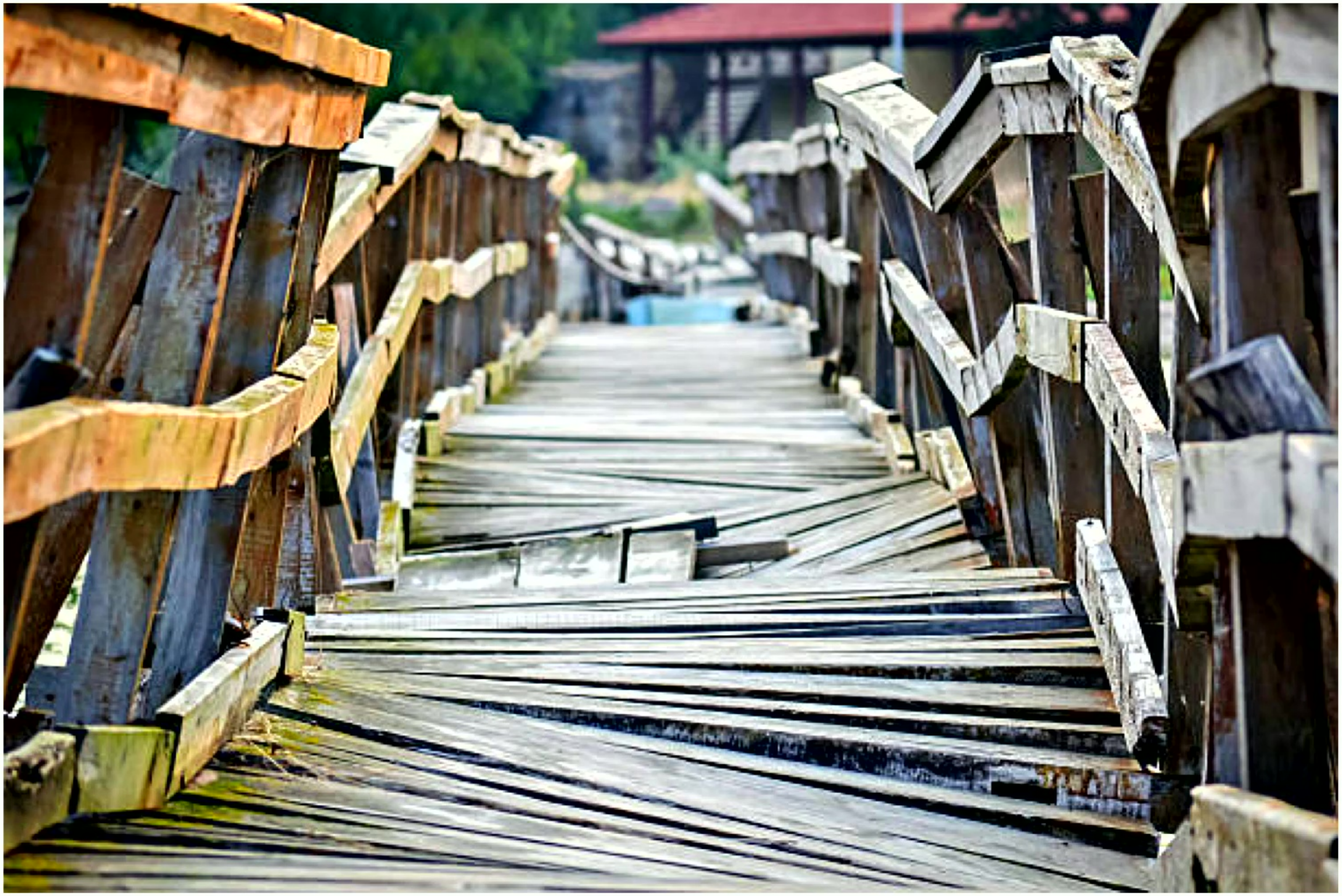
$\mathcal{C}_m := \sum_{\boldsymbol{\alpha}} p_{\boldsymbol{\alpha}} \, |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \otimes \sigma_{\boldsymbol{\alpha},\boldsymbol{r},g}^{\otimes m}$ $\qquad$ $H_{\min}(\boldsymbol{\alpha}|\sigma_{\boldsymbol{\alpha},\boldsymbol{r},g}^{\otimes m})_{\mathcal{C}_m} > 0$

Blind Quantum Computation

$\mathcal{C}_1 := \sum_{\boldsymbol{\alpha}} p_{\boldsymbol{\alpha}} \, |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \otimes \sigma_{\boldsymbol{\alpha},\boldsymbol{r},g}$ $\qquad$ $H_{\min}(\boldsymbol{\alpha}|\sigma_{\boldsymbol{\alpha},\boldsymbol{r},g})_{\mathcal{C}_1} > 0$

$\mathcal{C}_m := \sum_{\boldsymbol{\alpha}} p_{\boldsymbol{\alpha}} \, |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \otimes \sigma_{\boldsymbol{\alpha},\boldsymbol{r},g}^{\otimes m}$ $\qquad$ $H_{\min}(\boldsymbol{\alpha}|\sigma_{\boldsymbol{\alpha},\boldsymbol{r},g}^{\otimes m})_{\mathcal{C}_m} > 0$

Example, numerically: $\qquad$ $H_{\min}(\boldsymbol{\alpha}|\sigma_{\boldsymbol{\alpha},\boldsymbol{r},g})_{\mathcal{C}_1} > H_{\min}(\boldsymbol{\alpha}|\sigma_{\boldsymbol{\alpha},\boldsymbol{r},g}^{\otimes 2})_{\mathcal{C}_2}$



36

Hypothesis Testing Causal Structure

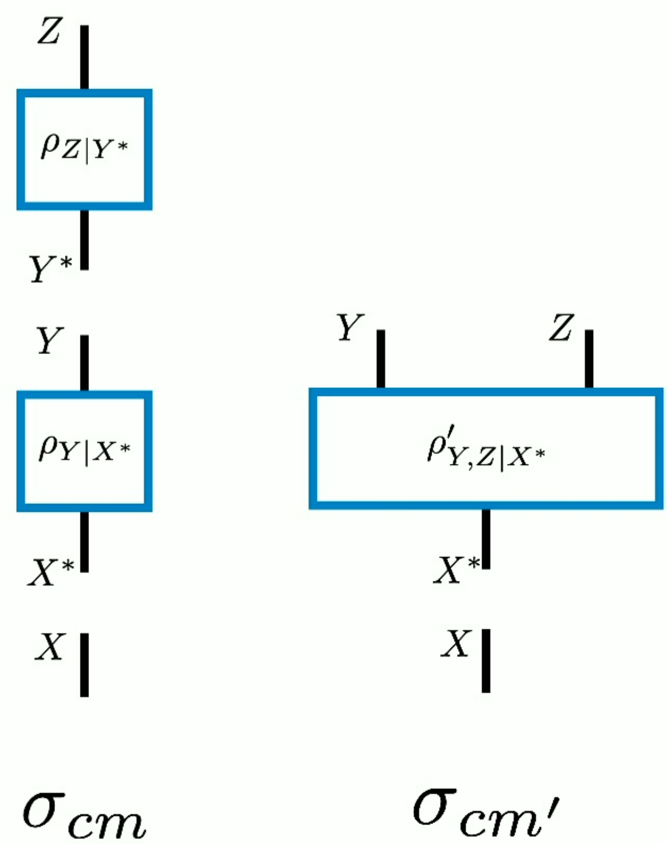
$$\mathcal{C}_{CM} := \sum_{cm \in \mathbb{CM}} p_{cm} \, |cm\rangle\langle cm| \otimes \sigma_{cm}$$

$$\mathbb{CM} := \text{set of causal models}$$

Hypothesis Testing Causal Structure

$$\mathcal{C}_{CM} := \sum_{cm \in \mathbb{CM}} p_{cm} \, |cm\rangle\langle cm| \otimes \sigma_{cm}$$

$$\mathbb{CM} := \text{set of causal models}$$



37

Hypothesis Testing Causal Structure

$$\mathcal{C}_{CM} := \sum_{cm \in \mathbb{CM}} p_{cm} \, |cm\rangle\langle cm| \otimes \sigma_{cm}$$

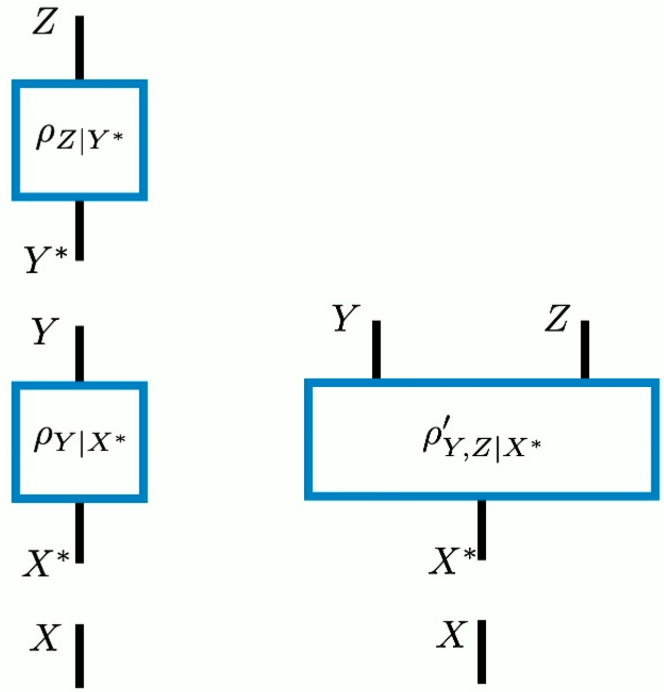
$\mathbb{CM}$:= set of causal models

if all $cm \in \mathbb{CM}$ have a compatible total order:

$\mathcal{C}_{CM}$ is a valid comb

can use $H_{\min}$ as is

When are the cm distinguishable?



σ_{cm} $\sigma_{cm'}$

37

Hypothesis Testing Causal Structure

Recall:

$$\{\rho_x\} \longrightarrow \begin{array}{c}\text{orthogonality} \leftrightsquigarrow \text{distinguishability} \\ \text{adaptivity not useful for } m \text{ copies}\end{array}$$

$$\{\mathcal{F}_x\} \longrightarrow \begin{array}{c}\text{disjoint, condition on Kraus operators} \leftrightsquigarrow \text{distinguishability} \\ \text{adaptivity } \textit{is} \text{ useful}\end{array}$$

$$\{\sigma_x\} \longrightarrow ?$$

Duan, R. et al. *PRL* 103, no. 21 (2009): 210501

Chiribella, G + Ebler, D. *Nature communications* 10, no. 1 (2019): 1472.

Hypothesis Testing Causal Structure

if *not* all $cm \in \mathbb{CM}$ have a compatible total order:

$\mathcal{C}_{CM}$ is not a comb - process matrix?

can we use a modified $H_{\min}$?

Bavaresco, J. et al. *PRL* 127, no. 20 (2021): 200504.

Objectivity of Causal Structure

Thm 1:

Objective existence $\Leftarrow$ Spectrum broadcast structure,

$$\begin{pmatrix}\text{Objective}\\ \text{existence}\end{pmatrix} + \begin{pmatrix}\text{Strong}\\ \text{independence}\end{pmatrix} \Rightarrow \begin{pmatrix}\text{Spectrum}\\ \text{broadcast}\\ \text{structure}\end{pmatrix}.$$

$$\Updownarrow$$

$$\rho_{S:E_1,\ldots,E_N} := \sum_i p_i \, |i\rangle\langle i| \otimes \rho_i^{E_1} \otimes \ldots \otimes \rho_i^{E_N}$$

Horodecki, R, et al. *PRA* 91, no. 3 (2015): 032122.

Thanks!