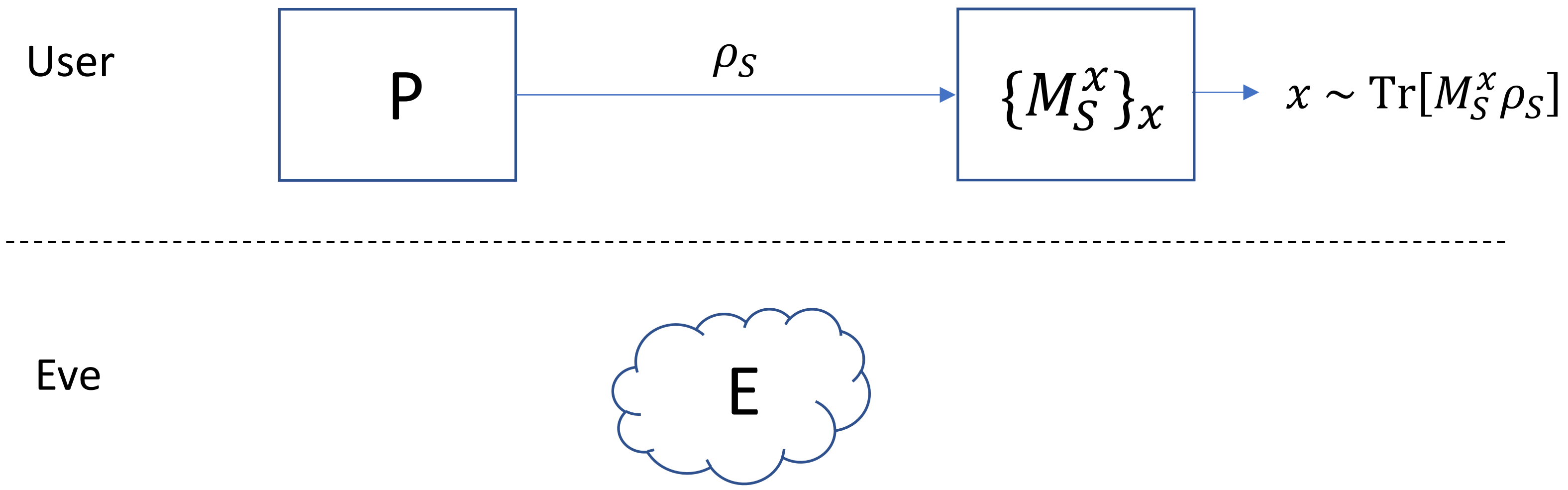
Quantifying the intrinsic randomness of quantum measurements

Gabriel Senno, Thomas Strohm and Antonio Acín.

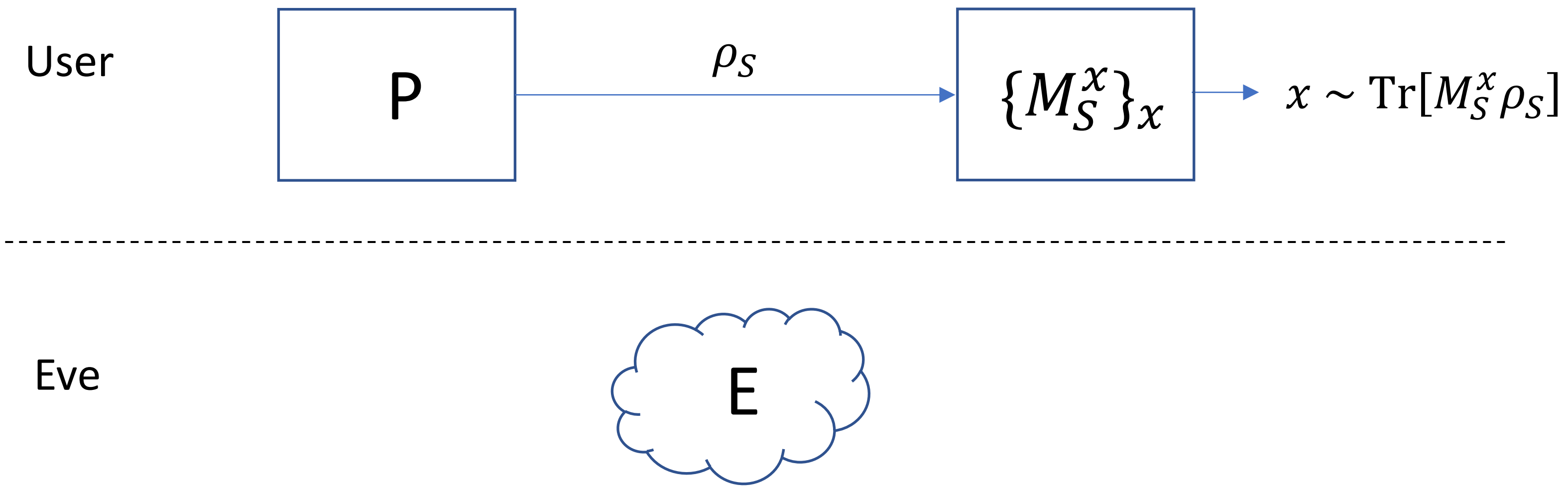
Phys. Rev. Lett. 131, 130202 (2023).

ICFO Quside QRANGE

Setting

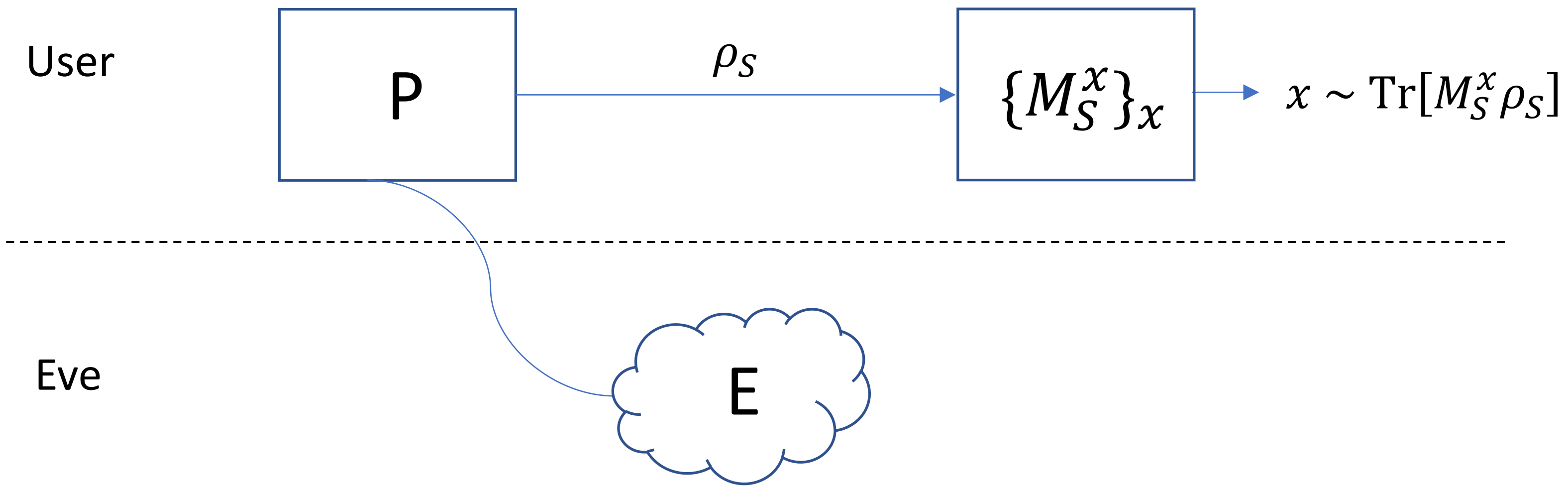


Setting



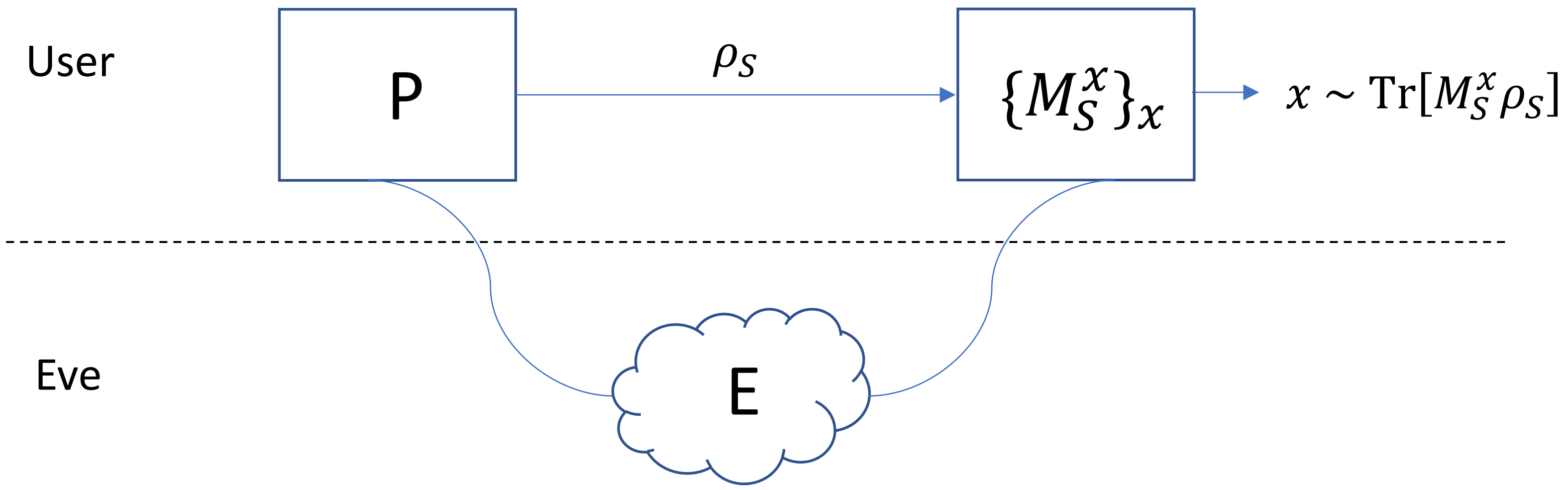
p_{guess}: "probability that Eve guesses the outcome of a measurement described by the POVM $\{M_S^x\}_x$ on a system S in the state ρ_S, about which she holds side information *E*"

Setting



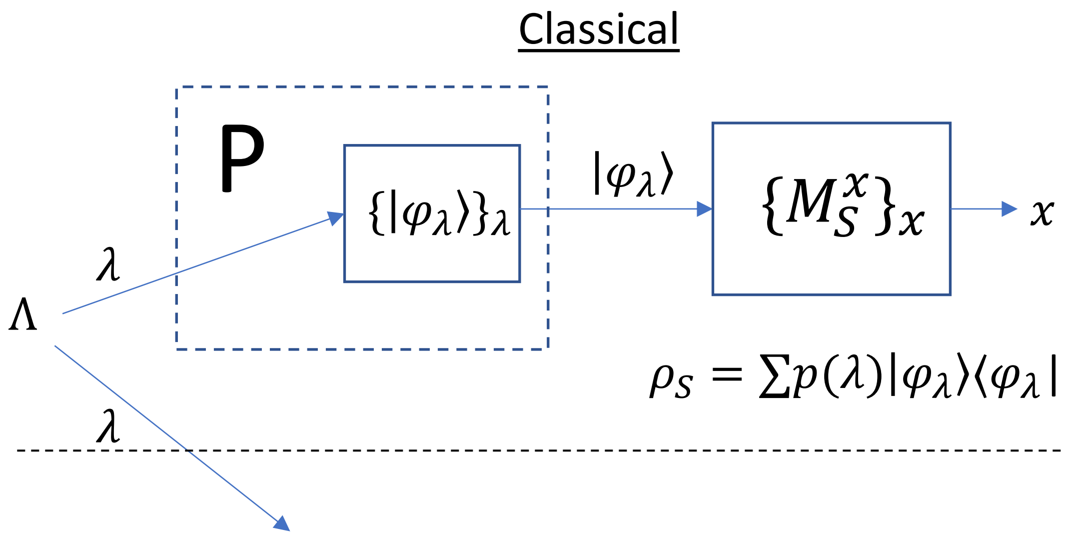
p_{guess}: "probability that Eve guesses the outcome of a measurement described by the POVM $\{M_S^x\}_x$ on a system S in the state ρ_S, about which she holds side information *E*"

Setting



p_{guess}: "probability that Eve guesses the outcome of a measurement described by the POVM $\{M_S^x\}_x$ on a system S in the state ρ_S, about which she holds side information *E*"

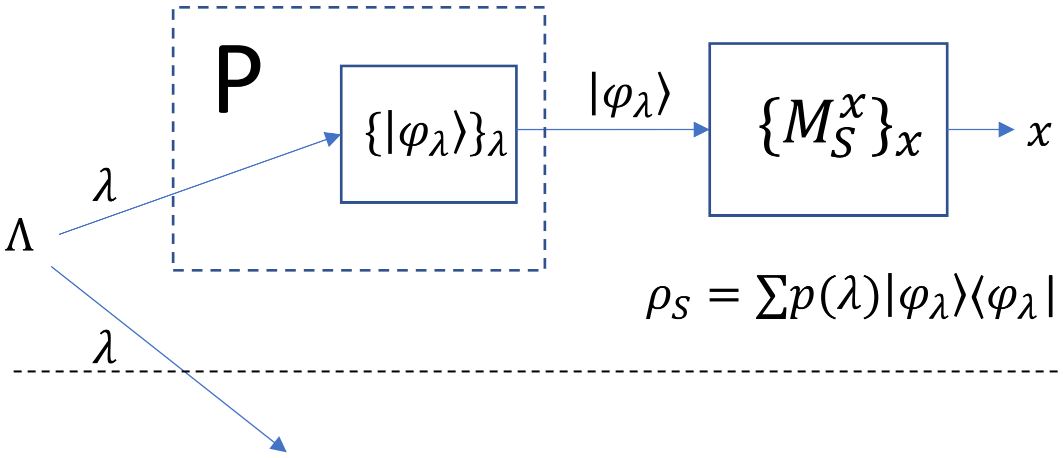
Correlations with the state



Quantum

Correlations with the state

Classical



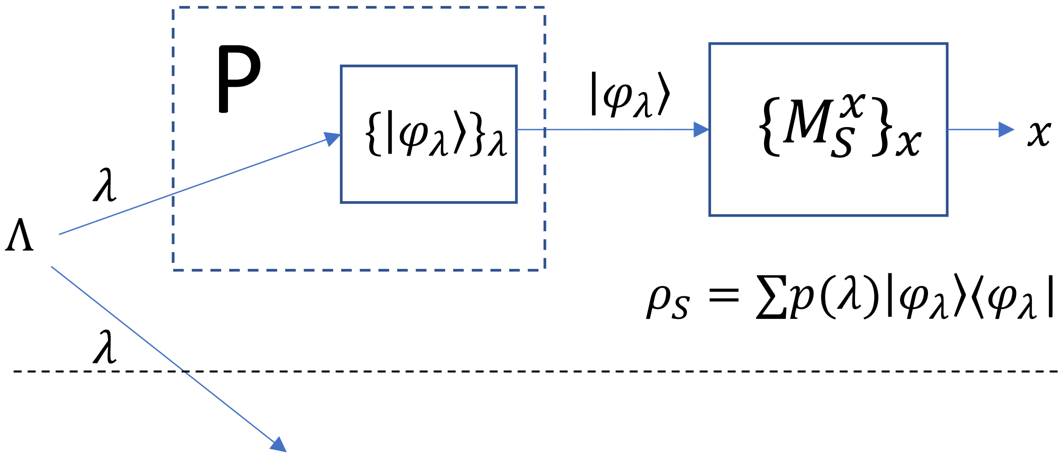
$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

Quantum

Correlations with the state

Classical



$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$

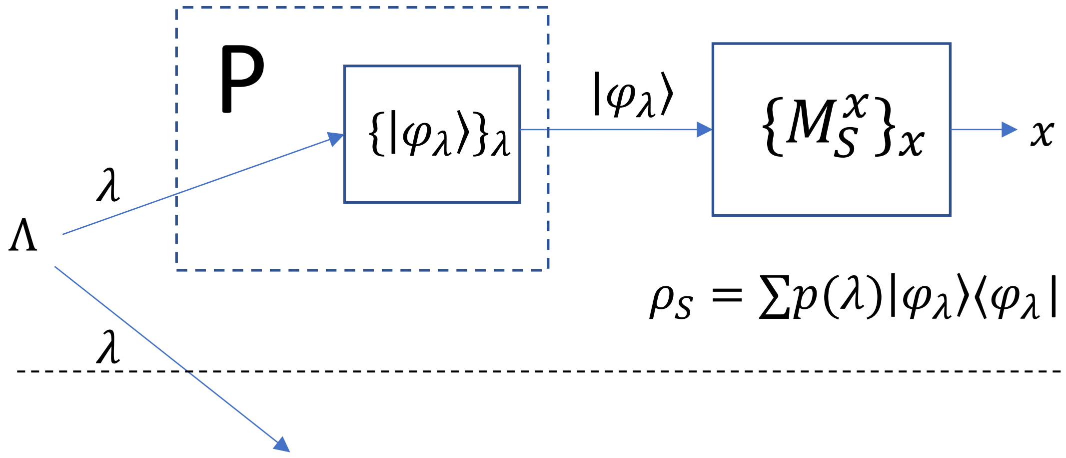
$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$

$\max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$

Quantum

Correlations with the state

<u>Classical</u>



$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

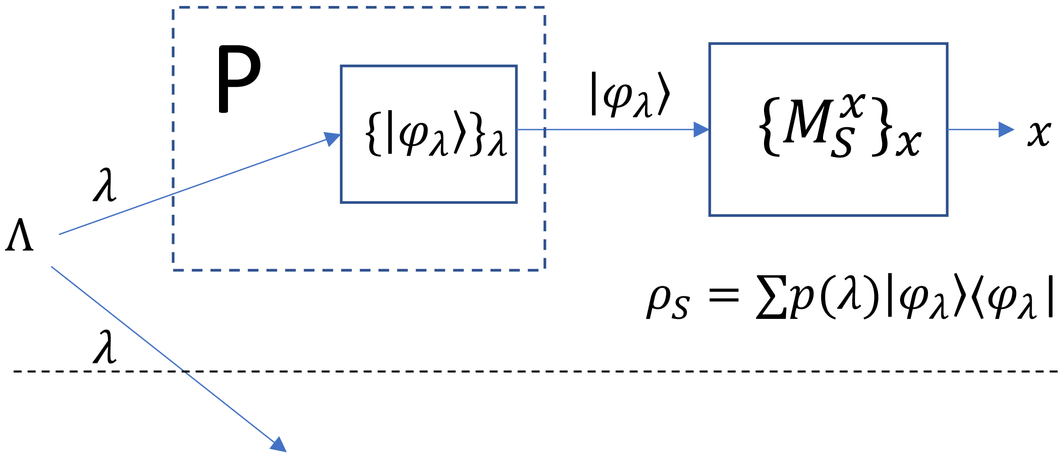
$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

$$\sum_\lambda p(\lambda)\max_x\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

<u>Quantum</u>

Correlations with the state

<u>Classical</u>



$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

$$p_{\text{guess}}(X|\Lambda) \coloneqq \max_{p(\lambda),|\varphi\rangle_\lambda} \sum_\lambda p(\lambda) \max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

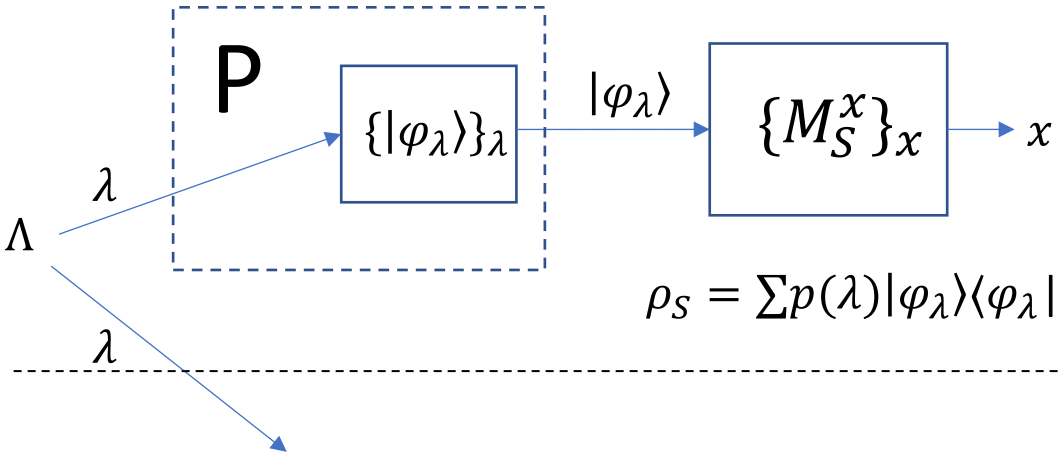
subject to

$$\sum_\lambda p(\lambda)|\varphi\rangle\langle\varphi| = \rho_S$$

<u>Quantum</u>

Correlations with the state

<u>Classical</u>



$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

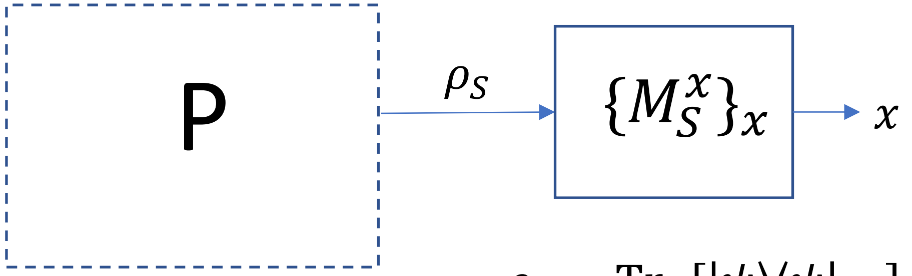
$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

$$p_{\text{guess}}(X|\Lambda) \coloneqq \max_{p(\lambda),|\varphi\rangle_\lambda} \sum_\lambda p(\lambda) \max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

subject to

$$\sum_\lambda p(\lambda)|\varphi\rangle\langle\varphi| = \rho_S$$

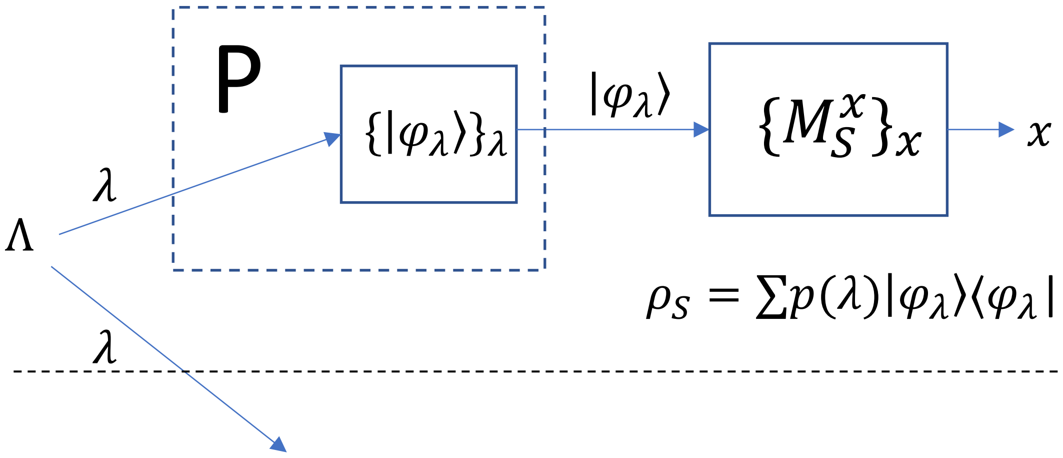
<u>Quantum</u>



$$\rho_S = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{SE}]$$

Correlations with the state

<u>Classical</u>



$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

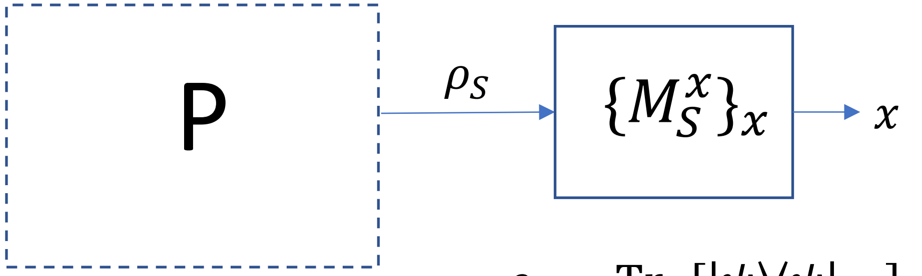
$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

$$p_{\text{guess}}(X|\Lambda) := \max_{p(\lambda),|\varphi\rangle_\lambda} \sum_\lambda p(\lambda) \max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

subject to

$$\sum_\lambda p(\lambda)|\varphi\rangle\langle\varphi| = \rho_S$$

<u>Quantum</u>



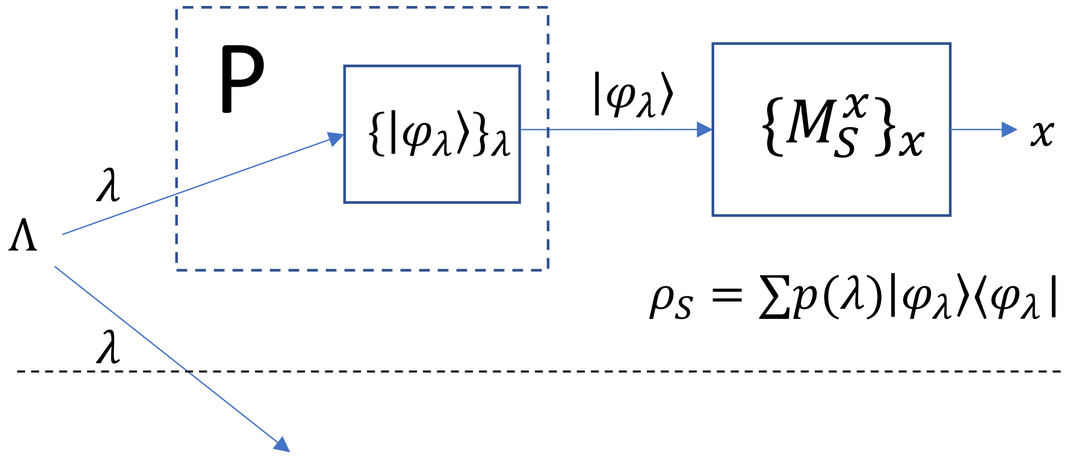
$$\rho_S = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{SE}]$$

$$\rho_{XE} := \sum_x |x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

with $\tilde{\rho}_E^x := \mathrm{Tr}_S[(M_S^x \otimes I)|\psi\rangle\langle\psi|]$

Correlations with the state

Classical



$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

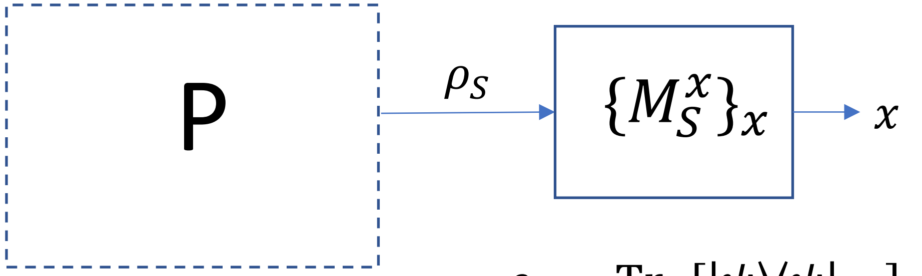
$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

$$p_{\text{guess}}(X|\Lambda) \coloneqq \max_{p(\lambda),|\varphi\rangle_\lambda} \sum_\lambda p(\lambda) \max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

subject to

$$\sum_\lambda p(\lambda)|\varphi\rangle\langle\varphi| = \rho_S$$

Quantum



$$\rho_S = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{SE}]$$

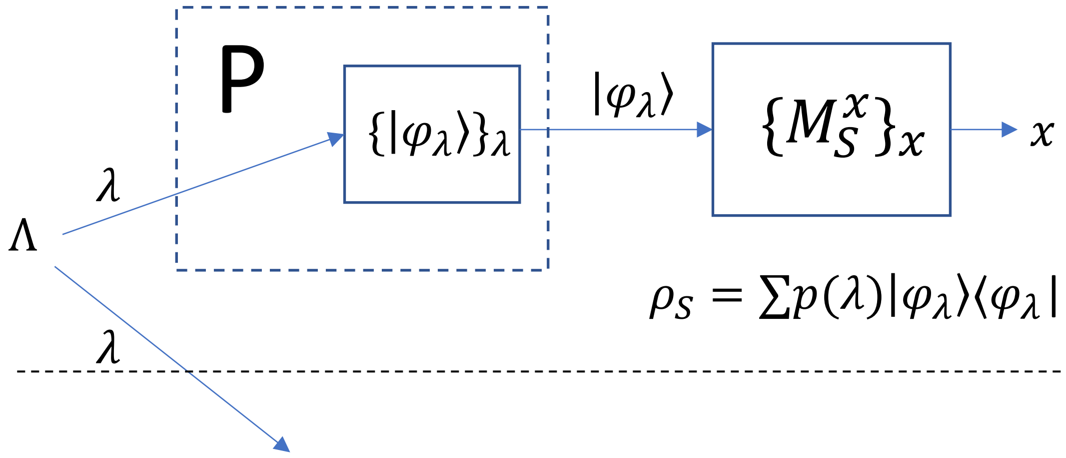
$$\rho_{XE} \coloneqq \sum_x |x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

with $\tilde{\rho}_E^x \coloneqq \mathrm{Tr}_S[(M_S^x \otimes I)|\psi\rangle\langle\psi|]$

$$p_{\text{guess}}(X|E) = \max_{\{M_E^x\}_x} \sum_x \langle\psi|M_S^x \otimes M_E^x|\psi\rangle_{SE}$$

Correlations with the state

Classical



$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

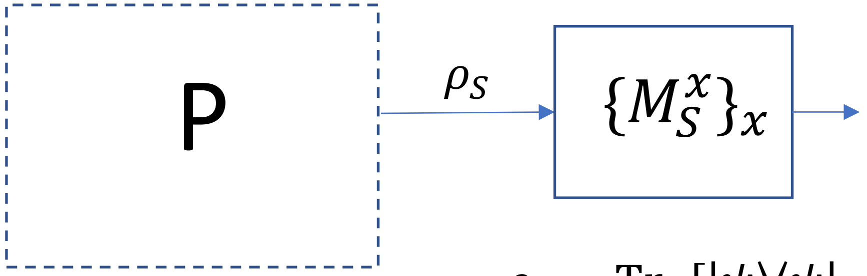
$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

$$p_{\text{guess}}(X|\Lambda) \coloneqq \max_{p(\lambda),|\varphi\rangle_\lambda} \sum_\lambda p(\lambda) \max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

subject to

$$\sum_\lambda p(\lambda)|\varphi\rangle\langle\varphi| = \rho_S$$

Quantum



$$\rho_S = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{SE}]$$

$$\rho_{XE} \coloneqq \sum_x |x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

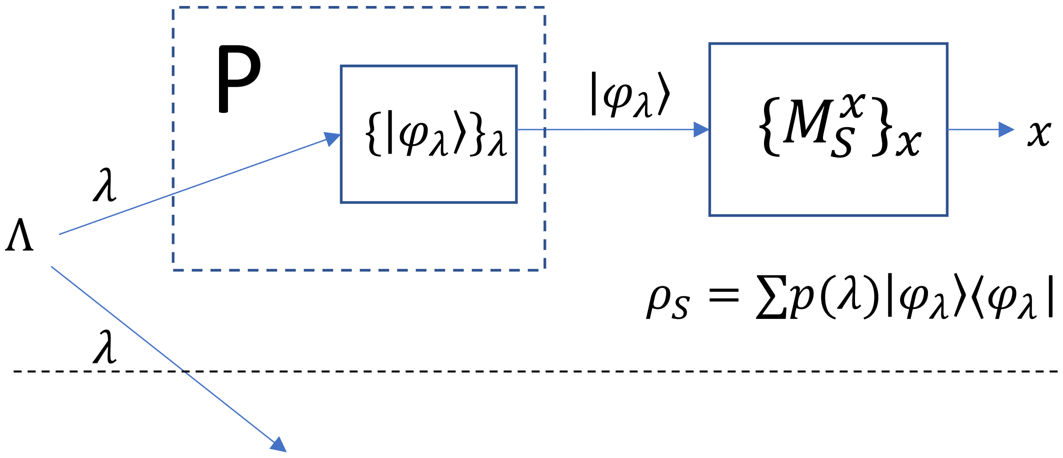
with $\tilde{\rho}_E^x \coloneqq \mathrm{Tr}_S[(M_S^x \otimes I)|\psi\rangle\langle\psi|]$

$$p_{\text{guess}}(X|E) = \max_{\{M_E^x\}_x} \sum_x \langle\psi|M_S^x \otimes M_E^x|\psi\rangle_{SE}$$

$$= \max_{\{M_E^x\}_x} \sum_x p_X(x)\mathrm{Tr}[M_E^x \rho_E^x]$$

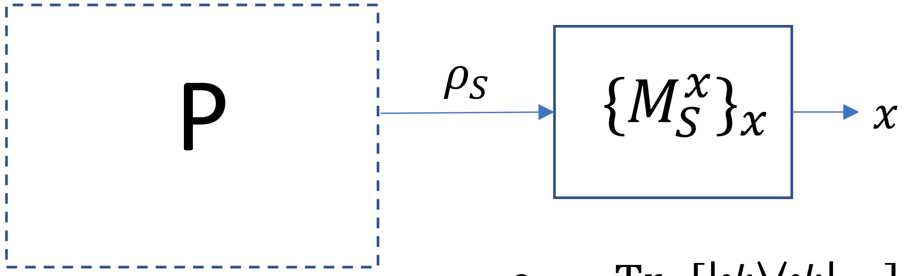
Correlations with the state

Classical



$$\rho_S = \sum p(\lambda)|\varphi_\lambda\rangle\langle\varphi_\lambda|$$

Quantum



$$\rho_S = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{SE}]$$

$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

$$\rho_{XE} := \sum_x |x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

with $\tilde{\rho}_E^x := \mathrm{Tr}_S[(M_S^x \otimes I)|\psi\rangle\langle\psi|]$

$$p_{\text{guess}}(X|\Lambda) := \max_{p(\lambda),|\varphi\rangle_\lambda} \sum_\lambda p(\lambda) \max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

subject to

$$\sum_\lambda p(\lambda)|\varphi\rangle\langle\varphi| = \rho_S$$

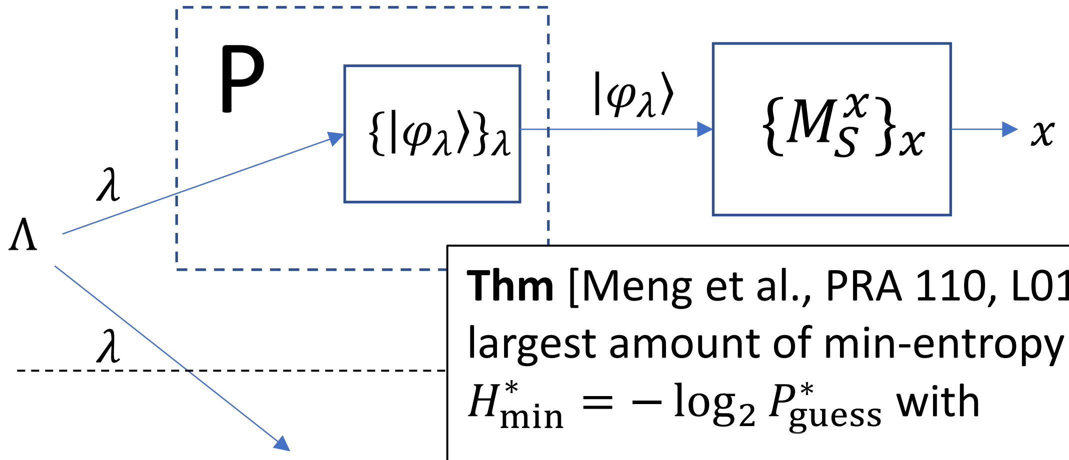
=

$$p_{\text{guess}}(X|E) = \max_{\{M_E^x\}_x} \sum_x \langle\psi|M_S^x \otimes M_E^x|\psi\rangle_{SE}$$

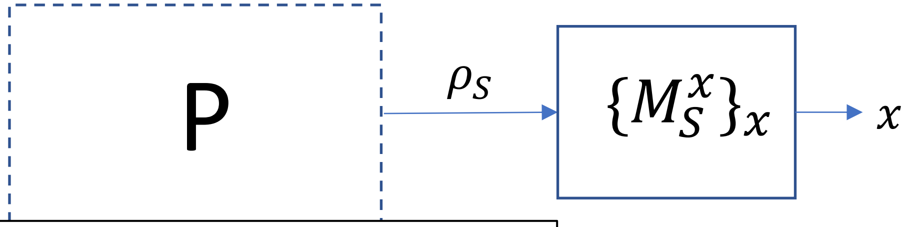
$$= \max_{\{M_E^x\}_x} \sum_x p_X(x)\mathrm{Tr}[M_E^x \rho_E^x]$$

Correlations with the state

<u>Classical</u>



<u>Quantum</u>



$= \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{SE}]$

Thm [Meng et al., PRA 110, L010403]: For a given state ρ, the largest amount of min-entropy that can be extracted from it is $H_{\min}^* = -\log_2 P_{\text{guess}}^*$ with

Fionnuala's talk

$p_{X\Lambda}(x,\lambda) =$

with $\tilde{\rho}_E^x \coloneqq \mathrm{Tr}_S[(M_S^x \otimes I)|\psi\rangle\langle\psi|]$

$$p_{\text{guess}}(X|\Lambda) \coloneqq \max_{p(\lambda),|\varphi\rangle_\lambda} \sum_\lambda p(\lambda) \max_x \langle\varphi_\lambda|M_S^x|\varphi_\lambda\rangle$$

subject to

$$\sum_\lambda p(\lambda)|\varphi\rangle\langle\varphi| = \rho_S$$

$=$

$$p_{\text{guess}}(X|E) = \max_{\{M_E^x\}_x} \sum_x \langle\psi|M_S^x \otimes M_E^x|\psi\rangle_{SE}$$

$$= \max_{\{M_E^x\}_x} \sum_x p_X(x)\mathrm{Tr}[M_E^x \rho_E^x]$$

Correlations with the measurement (motivating example)

Let $M_S = \{M_S^0, M_S^1\}$ with $M_S^1 = \eta|1\rangle\langle 1|$ and $|\phi\rangle_S = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$

Correlations with the measurement (motivating example)

Let $M_S = \{M_S^0, M_S^1\}$ with $M_S^1 = \eta|1\rangle\langle 1|$ and $|\phi\rangle_S = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$

Notice that $M_S^0 = I - \eta|1\rangle\langle 1|$

$= [|0\rangle\langle 0| + |1\rangle\langle 1|] - \eta|1\rangle\langle 1| + \eta|0\rangle\langle 0| - \eta|0\rangle\langle 0|$

$= (1-\eta)I + \eta|0\rangle\langle 0|$

Correlations with the measurement (motivating example)

Let $M_S = \{M_S^0, M_S^1\}$ with $M_S^1 = \eta|1\rangle\langle 1|$ and $|\phi\rangle_S = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$

Notice that $M_S^0 = I - \eta|1\rangle\langle 1|$

$= [|0\rangle\langle 0| + |1\rangle\langle 1|] - \eta|1\rangle\langle 1| + \eta|0\rangle\langle 0| - \eta|0\rangle\langle 0|$

$= (1-\eta)I + \eta|0\rangle\langle 0|$

and $M_S^1 = (1-\eta) * \mathbf{0} + \eta|1\rangle\langle 1|$

Correlations with the measurement (motivating example)

Let $M_S = \{M_S^0, M_S^1\}$ with $M_S^1 = \eta|1\rangle\langle 1|$ and $|\phi\rangle_S = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$

Notice that $M_S^0 = I - \eta|1\rangle\langle 1|$

$= [|0\rangle\langle 0| + |1\rangle\langle 1|] - \eta|1\rangle\langle 1| + \eta|0\rangle\langle 0| - \eta|0\rangle\langle 0|$

$= (1-\eta)I + \eta|0\rangle\langle 0|$

and $M_S^1 = (1-\eta) * \mathbf{0} + \eta|1\rangle\langle 1|$

Measuring M_S is sampling $\Lambda \sim \text{Bernoulli}(\eta)$ and
then measuring M_S^λ with $M_S^0 = \{I, \mathbf{0}\}$ and $M_S^1 = \{|0\rangle, |1\rangle\}$.

Correlations with the measurement (motivating example)

Let $M_S = \{M_S^0, M_S^1\}$ with $M_S^1 = \eta|1\rangle\langle 1|$ and $|\phi\rangle_S = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$

Notice that $M_S^0 = I - \eta|1\rangle\langle 1|$

$= [|0\rangle\langle 0| + |1\rangle\langle 1|] - \eta|1\rangle\langle 1| + \eta|0\rangle\langle 0| - \eta|0\rangle\langle 0|$

$= (1-\eta)I + \eta|0\rangle\langle 0|$

and $M_S^1 = (1-\eta) * \mathbf{0} + \eta|1\rangle\langle 1|$

Measuring M_S is sampling $\Lambda \sim \text{Bernoulli}(\eta)$ and
then measuring M_S^λ with $M_S^0 = \{I, \mathbf{0}\}$ and $M_S^1 = \{|0\rangle, |1\rangle\}$.

If Eve sees $\lambda = 0$, she guesses $x = 0$
else she guesses $x = \arg\max_y |\langle y|\phi\rangle|^2$.

Correlations with the measurement (motivating example)

Let $M_S = \{M_S^0, M_S^1\}$ with $M_S^1 = \eta|1\rangle\langle 1|$ and $|\phi\rangle_S = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$

Notice that $M_S^0 = I - \eta|1\rangle\langle 1|$

$= [|0\rangle\langle 0| + |1\rangle\langle 1|] - \eta|1\rangle\langle 1| + \eta|0\rangle\langle 0| - \eta|0\rangle\langle 0|$

$= (1-\eta)I + \eta|0\rangle\langle 0|$

and $M_S^1 = (1-\eta) * \mathbf{0} + \eta|1\rangle\langle 1|$

Measuring M_S is sampling $\Lambda \sim \mathrm{Bernoulli}(\eta)$ and
then measuring M_S^λ with $M_S^0 = \{I, \mathbf{O}\}$ and $M_S^1 = \{|0\rangle, |1\rangle\}$.

If Eve sees $\lambda = 0$, she guesses x =0
else she guesses $x = \arg\max_y |\langle y|\phi\rangle|^2$.

She's correct with prob $p_{\text{guess}} = (1-\eta) + \eta \max_y |\langle y|\phi\rangle|^2$

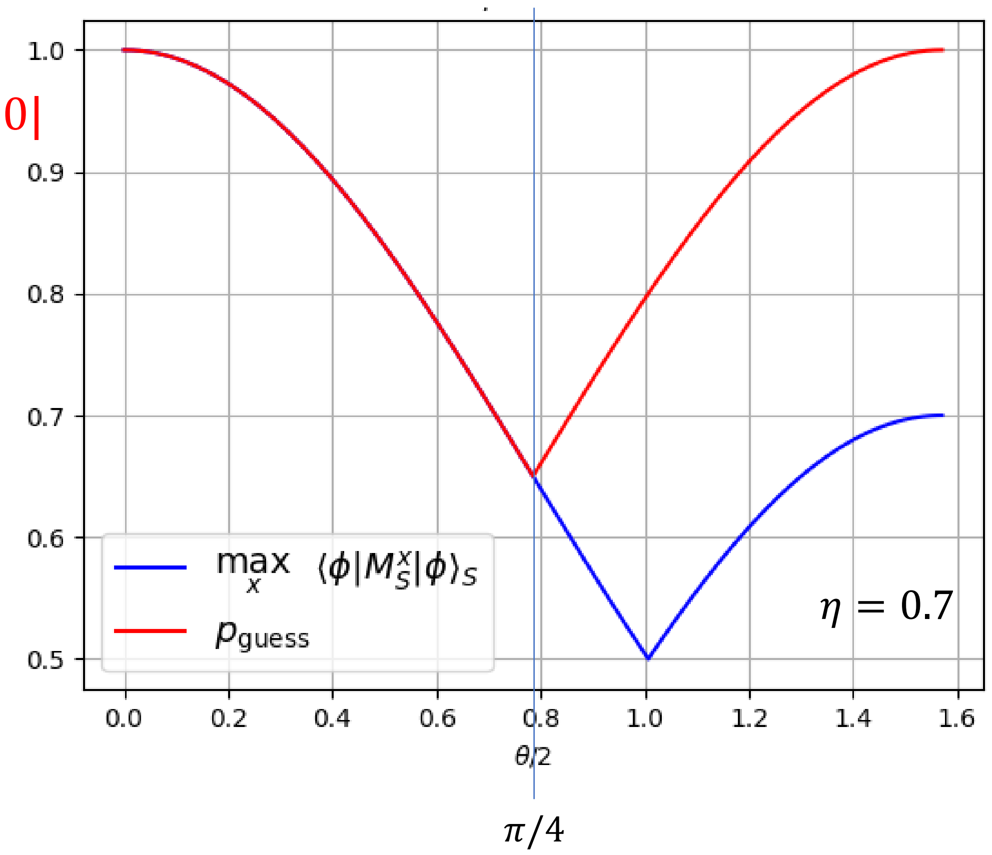
Correlations with the measurement (motivating example)

Let $M_S = \{M_S^0, M_S^1\}$ with $M_S^1 = \eta|1\rangle\langle 1|$ and $|\phi\rangle_S = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$

Notice that $M_S^0 = I - \eta|1\rangle\langle 1|$

$$= [|0\rangle\langle 0| + |1\rangle\langle 1|] - \eta|1\rangle\langle 1| + \eta|0\rangle\langle 0| - \eta|0\rangle\langle 0|$$
$$= (1-\eta)I + \eta|0\rangle\langle 0|$$

and $M_S^1 = (1-\eta) * \mathbf{0} + \eta|1\rangle\langle 1|$

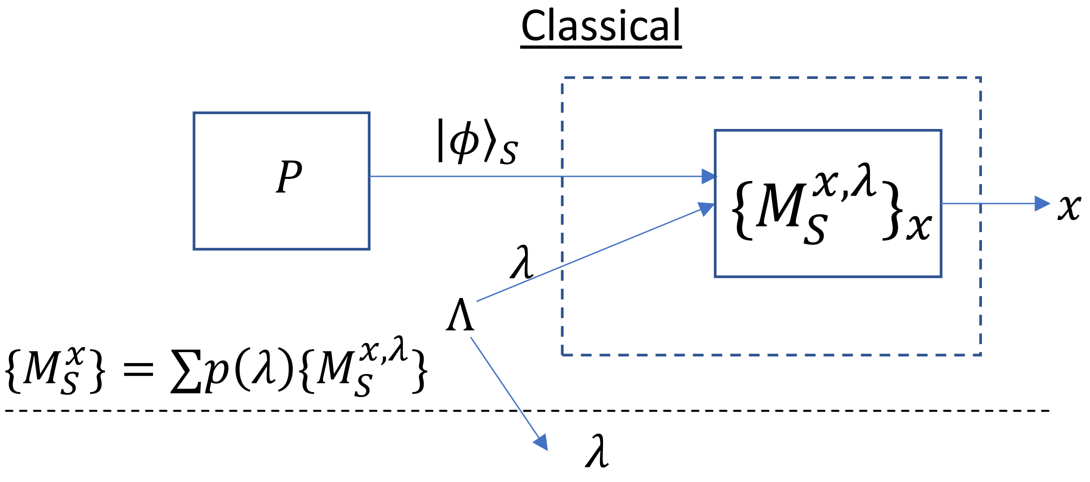


Measuring M_S is sampling $\Lambda \sim \text{Bernoulli}(\eta)$ and then measuring M_S^λ with $M_S^0 = \{I, \mathbf{O}\}$ and $M_S^1 = \{|0\rangle, |1\rangle\}$.

If Eve sees $\lambda = 0$, she guesses $x = 0$
else she guesses $x = \arg\max_y |\langle y|\phi\rangle|^2$.

She's correct with prob $p_{\text{guess}} = (1-\eta) + \eta \max_y |\langle y|\phi\rangle|^2$

Correlations with the measurement



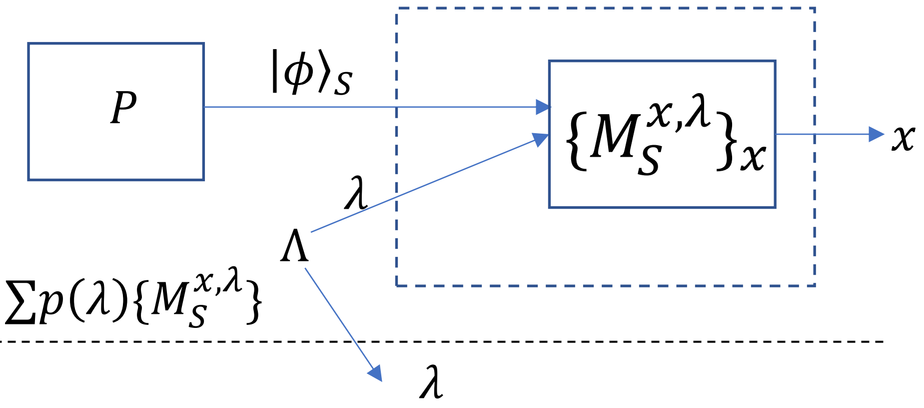
$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

$$p_{\text{guess}}(X|\Lambda) := \max_{p(\lambda),\{M_S^{x,\lambda}\}_x} \sum_\lambda p(\lambda) \max_x \langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

subject to $\sum_\lambda p(\lambda) M_S^{x,\lambda} = M_S^x$ for all x

Correlations with the measurement

<u>Classical</u>



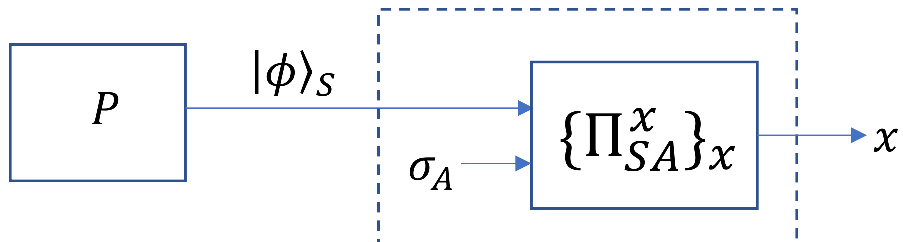
$\{M_S^x\} = \sum p(\lambda)\{M_S^{x,\lambda}\}$

$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

$$p_{\text{guess}}(X|\Lambda) \coloneqq \max_{p(\lambda),\{M_S^{x,\lambda}\}_x} \sum_\lambda p(\lambda) \max_x \langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

subject to $\sum_\lambda p(\lambda) M_S^{x,\lambda} = M_S^x$ for all x

<u>Quantum</u>[1]

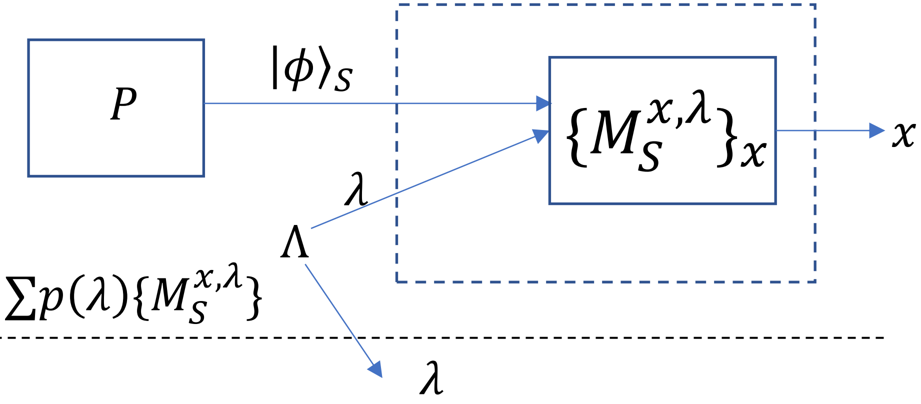


$\sigma_A = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AE}]$

[1] D. Frauchiger, M. Troyer and R. Renner, “True randomness from realistic quantum devices”, arXiv:1311.4547.

Correlations with the measurement

<u>Classical</u>



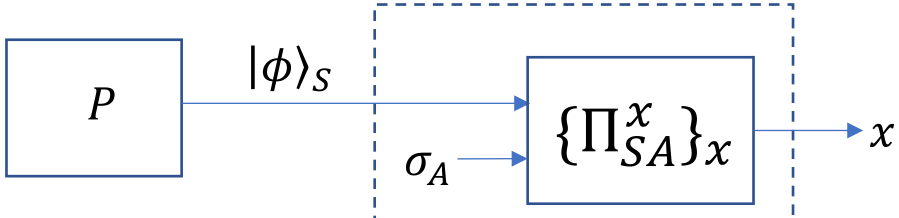
$\{M_S^x\} = \sum p(\lambda)\{M_S^{x,\lambda}\}$

$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

$$p_{\text{guess}}(X|\Lambda) := \max_{p(\lambda),\{M_S^{x,\lambda}\}_x} \sum_\lambda p(\lambda) \max_x \langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

subject to $\sum_\lambda p(\lambda) M_S^{x,\lambda} = M_S^x$ for all x

<u>Quantum</u>[1]



$\sigma_A = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AE}]$

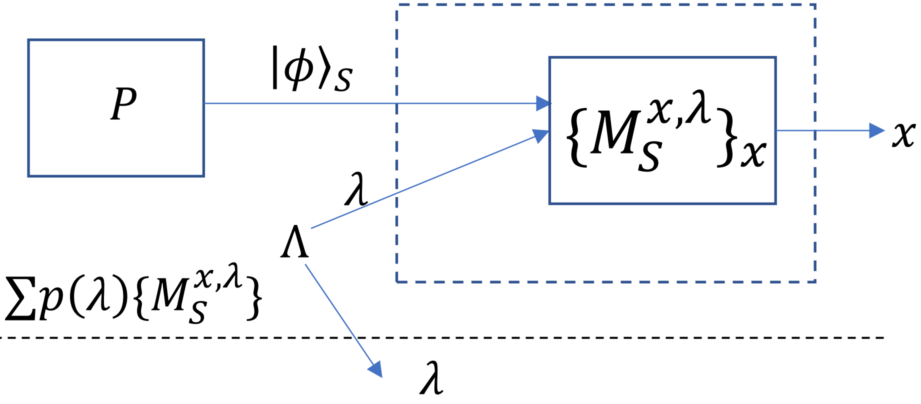
$$\rho_{XE} := \sum_x |x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

with $\tilde{\rho}_E^x := \mathrm{Tr}_{SA}[(\Pi_{SA}^x \otimes I)|\phi,\psi\rangle\langle\phi,\psi|]$

[1] D. Frauchiger, M. Troyer and R. Renner, "True randomness from realistic quantum devices", arXiv:1311.4547.

Correlations with the measurement

Classical



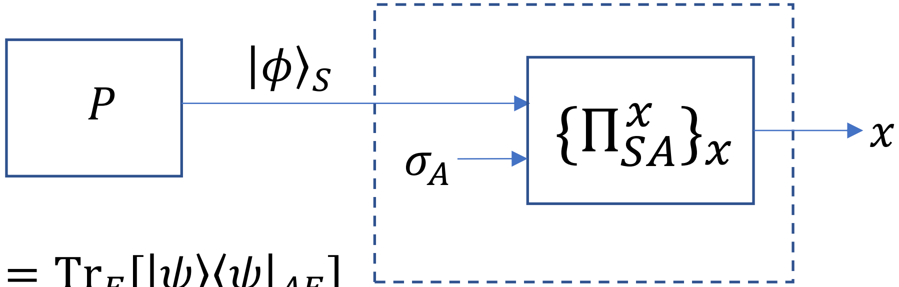
$$\{M_S^x\} = \sum p(\lambda)\{M_S^{x,\lambda}\}$$

$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

$$p_{\text{guess}}(X|\Lambda) := \max_{p(\lambda),\{M_S^{x,\lambda}\}_x} \sum_\lambda p(\lambda) \max_x \langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

subject to $\sum_\lambda p(\lambda) M_S^{x,\lambda} = M_S^x$ for all x

Quantum[1]



$$\sigma_A = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AE}]$$

$$\rho_{XE} := \sum_x |x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

with $\tilde{\rho}_E^x := \mathrm{Tr}_{SA}[(\Pi_{SA}^x \otimes I)|\phi,\psi\rangle\langle\phi,\psi|]$

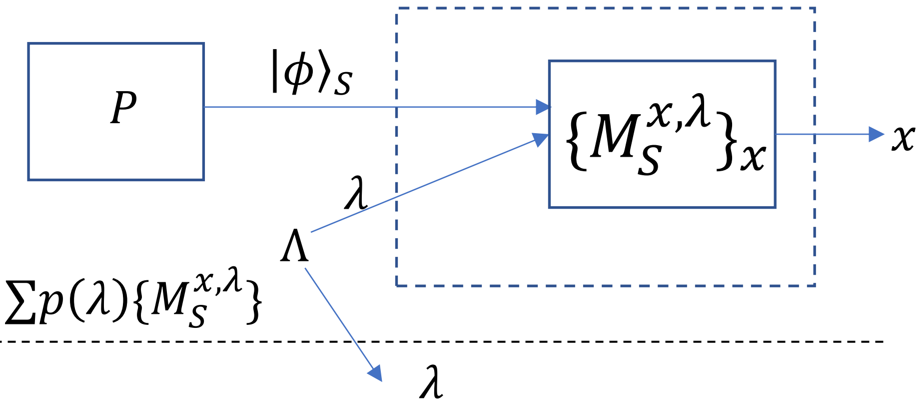
$$p_{\text{guess}}(X|E) = \max_{\{M_E^x\}_x,\{\Pi_{SA}^x\}_x,\sigma_A} \sum_x \langle\psi|\Pi_{SA}^x \otimes M_E^x|\psi\rangle_{SE}$$

subject to $\mathrm{Tr}_A[\Pi_{SA}^x(\mathrm{I} \otimes \sigma_A)] = M_S^x$ for all x

[1] D. Frauchiger, M. Troyer and R. Renner, “True randomness from realistic quantum devices”, arXiv:1311.4547.

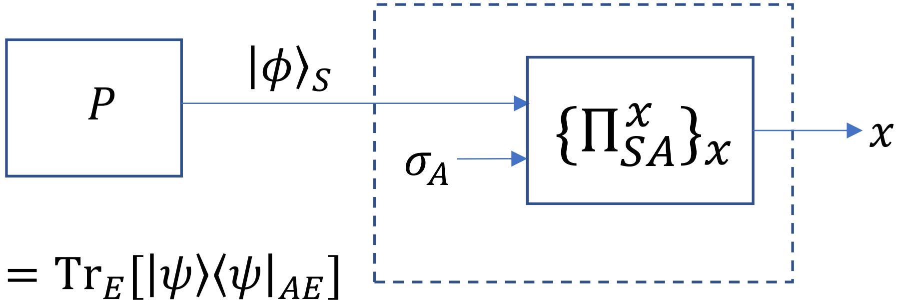
Correlations with the measurement

Classical



$\{M_S^x\} = \sum p(\lambda)\{M_S^{x,\lambda}\}$

Quantum[1]



$\sigma_A = \mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AE}]$

$$p_{X\Lambda}(x,\lambda) = p(\lambda)\langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

$$\rho_{XE} := \sum_x |x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

with $\tilde{\rho}_E^x := \mathrm{Tr}_{SA}[(\Pi_{SA}^x \otimes I)|\phi,\psi\rangle\langle\phi,\psi|]$

$$p_{\text{guess}}(X|\Lambda) := \max_{p(\lambda),\{M_S^{x,\lambda}\}_x} \sum_\lambda p(\lambda) \max_x \langle\psi|M_S^{x,\lambda}|\psi\rangle_S$$

subject to $\sum_\lambda p(\lambda) M_S^{x,\lambda} = M_S^x$ for all x

$=$[2]

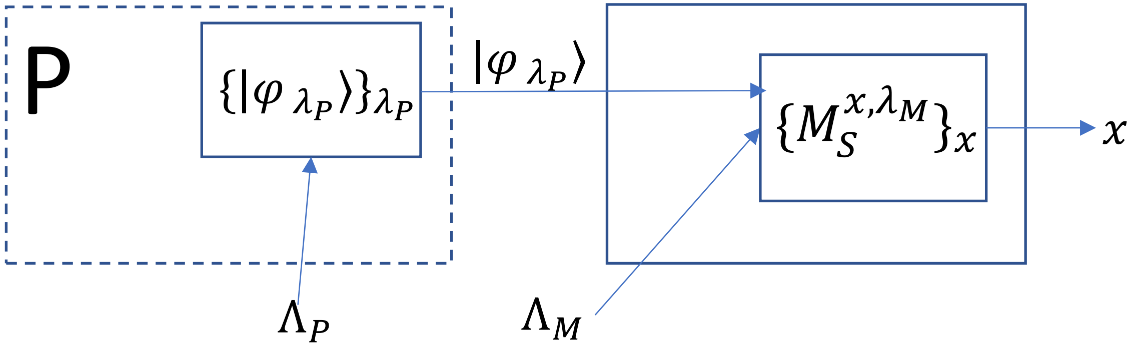
$$p_{\text{guess}}(X|E) = \max_{\{M_E^x\}_x,\{\Pi_{SA}^x\}_x,\sigma_A} \sum_x \langle\psi|\Pi_{SA}^x \otimes M_E^x|\psi\rangle_{SE}$$

subject to $\mathrm{Tr}_A[\Pi_{SA}^x(\mathrm{I} \otimes \sigma_A)] = M_S^x$ for all x

[1] D. Frauchiger, M. Troyer and R. Renner, “True randomness from realistic quantum devices”, arXiv:1311.4547.
[2] GS, T. Strohm and A. Acín, Phys. Rev. Lett. 131, 130202 (2023).

General scenario

Classical



$$p_{X\Lambda_P\Lambda_M}(x,\lambda_P,\lambda_M) = p(\lambda_P,\lambda_M)\langle\varphi_{\lambda_P}|M_S^{x,\lambda_M}|\varphi_{\lambda_P}\rangle$$

$$p_{\text{guess}}(X|\Lambda,\rho_S,\{M_S^x\}_x) \coloneqq$$

$$\max_{p(\lambda_P,\lambda_M),|\varphi_{\lambda_P}\rangle,\{M_S^{x,\lambda_M}\}_x} \sum_{\lambda_P,\lambda_M} p(\lambda_P,\lambda_M) \max_x \langle\varphi_{\lambda_P}|M_S^{x,\lambda_M}|\varphi_{\lambda_P}\rangle$$

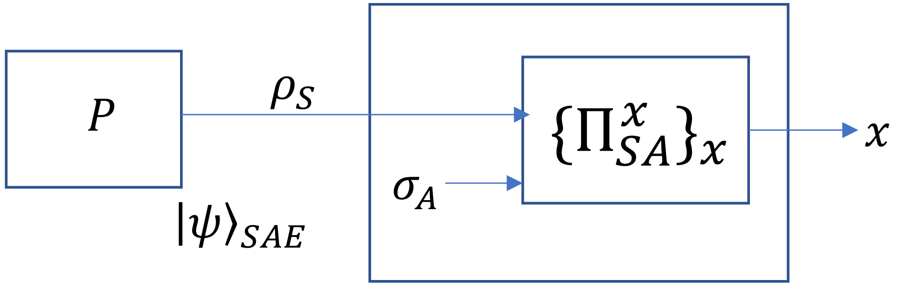
subject to

$$\sum p(\lambda_M)M_S^{x,\lambda_M} = M_S^x$$

$$\sum p(\lambda_P)|\varphi_{\lambda_P}\rangle\langle\varphi_{\lambda_P}| = \rho_S$$

$$\sum p(\lambda_P,\lambda_M)\langle\varphi_{\lambda_P}|M_S^{x,\lambda_M}|\varphi_{\lambda_P}\rangle = \text{Tr}[M_S^x\rho_S]$$

Quantum



$$\rho_{XE} \coloneqq \sum(x)|x\rangle\langle x| \otimes \tilde{\rho}_E^x$$

with $\tilde{\rho}_E^x \coloneqq \text{Tr}_{SA}[(\Pi_{SA}^x \otimes I)|\psi\rangle\langle\psi|]$

$$p_{\text{guess}}(X|E,\rho_S,\{M_S^x\}_x) := $$

$$\max_{\{M_E^x\}_x,\{\Pi_{SA}^x\}_x,\rho_{SA}} \sum_x \langle\psi|\Pi_{SA}^x \otimes M_E^x|\psi\rangle_{SAE}$$

subject to

$$\text{Tr}_A[\Pi_{SA}^x(\text{I} \otimes \sigma_A)] = M_S^x$$

$$\text{Tr}_A[\rho_{SA}] = \rho_S$$

$$\text{Tr}[\Pi_{SA}^x\rho_{SA}] = \text{Tr}[M_S^x\rho_S]$$

Results (1/2)

Thm: For every state ρ_S and every POVM $\{M_S^x\}_x$ it holds that

1. $p_{guess}(X|\Lambda, \rho_S, \{M_S^x\}_x) \leq p_{guess}(X|E, \rho_S, \{M_S^x\}_x)$ and

2. If $p_{guess}(X|E, \rho_S, \{M_S^x\}_x)$ has an optimal solution $\langle \{M_E^x\}_x, \{\Pi_{SA}^x\}_x, \rho_{SA} \rangle$ such that the postmeasurement states on SA

$$\tilde{\rho}_{SA}^x = \mathrm{Tr}_E[(I_{SA} \otimes M_E^x)|\psi\rangle\langle\psi|]$$

are all separable, then $p_{guess}(X|E, \rho_S, \{M_S^x\}_x) \leq p_{guess}(X|\Lambda, \rho_S, \{M_S^x\}_x)$

Results (1/2)

Thm: For every state ρ_S and every POVM $\{M_S^x\}_x$ it holds that

1. $p_{guess}(X|\Lambda, \rho_S, \{M_S^x\}_x) \leq p_{guess}(X|E, \rho_S, \{M_S^x\}_x)$ and
2. If $p_{guess}(X|E, \rho_S, \{M_S^x\}_x)$ has an optimal solution $\langle\{M_E^x\}_x, \{\Pi_{SA}^x\}_x, \rho_{SA}\rangle$ such that the postmeasurement states on SA

$$\tilde{\rho}_{SA}^x = \mathrm{Tr}_E[(I_{SA} \otimes M_E^x)|\psi\rangle\langle\psi|]$$

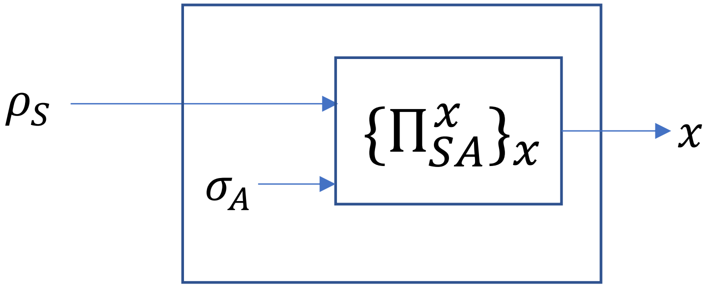
are all separable, then $p_{guess}(X|E, \rho_S, \{M_S^x\}_x) \leq p_{guess}(X|\Lambda, \rho_S, \{M_S^x\}_x)$

Observe that equality for the case of ρ_S pure follows as a corollary.

Restricted adversarial setting

In [1], intrinsic randomness quantification was studied under the assumptions:

1. System A and ancilla S are uncorrelated and,



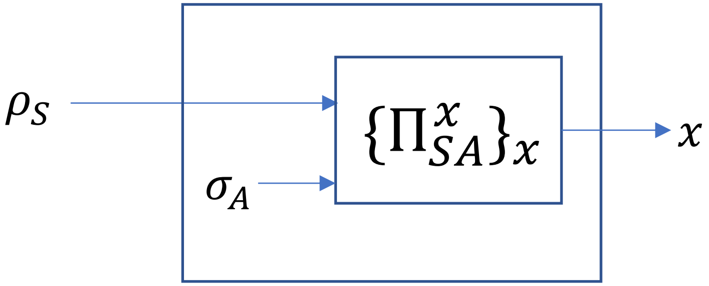
$$|\psi\rangle_{SAE} = |\phi\rangle_{SE_1} |\varphi\rangle_{AE_2}$$

[1] H. Dai, B. Chen, X. Zhang and X. Ma (2023), “Intrinsic randomness under general quantum measurements”, Phys. Rev. Research 5, 033081.

Restricted adversarial setting

In [1], intrinsic randomness quantification was studied under the assumptions:

1. System A and ancilla S are uncorrelated and,
2. Eve is restricted to act on their purifications *individually*.



$$|\psi\rangle_{SAE} = |\phi\rangle_{SE_1}|\varphi\rangle_{AE_2}$$

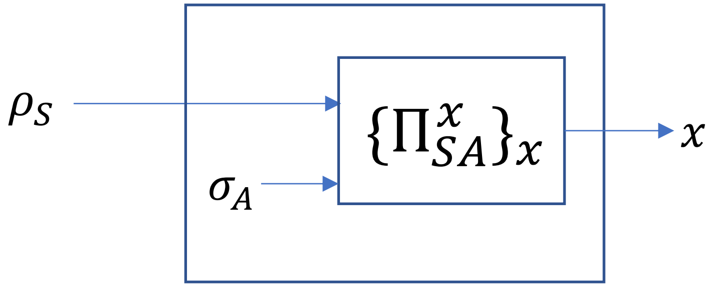
$$M_E^x = M_{E_1}^x \otimes M_{E_2}^x$$

[1] H. Dai, B. Chen, X. Zhang and X. Ma (2023), “Intrinsic randomness under general quantum measurements”, Phys. Rev. Research 5, 033081.

Restricted adversarial setting

In [1], intrinsic randomness quantification was studied under the assumptions:

1. System A and ancilla S are uncorrelated and,
2. Eve is restricted to act on their purifications *individually*.



$$|\psi\rangle_{SAE} = |\phi\rangle_{SE_1}|\varphi\rangle_{AE_2}$$

$$M^x_E = M^x_{E_1} \otimes M^x_{E_2}$$

Thm. 1 implies that no separation between the guessing probabilities in the classical and quantum pictures can be seen under this restrictions.

[1] H. Dai, B. Chen, X. Zhang and X. Ma (2023), “Intrinsic randomness under general quantum measurements”, Phys. Rev. Research 5, 033081.

Results (2/2)

Thm: There exists a 4-outcome qubit POVM $\{F_S^x\}_x$ such that

$$p_{guess}(X|\Lambda, I/2, \{F_S^x\}_x) < p_{guess}(X|E, I/2, \{F_S^x\}_x) = 1.$$

Results (2/2)

Thm: There exists a 4-outcome qubit POVM $\{F_S^x\}_x$ such that

$$p_{guess}(X|\Lambda, I/2, \{F_S^x\}_x) < p_{guess}(X|E, I/2, \{F_S^x\}_x) = 1.$$

Proof (sketch):

Results (2/2)

Thm: There exists a 4-outcome qubit POVM $\{F_S^x\}_x$ such that

$$p_{guess}(X|\Lambda, I/2, \{F_S^x\}_x) < p_{guess}(X|E, I/2, \{F_S^x\}_x) = 1.$$

Proof (sketch):

1. Let $\rho_{SA} = \frac{1}{4}\sum|\psi^x\rangle\langle\psi^x|$ with $\{|\psi^x\rangle\}_x$ be the entangled basis for two qubits from [1] and let $F_S^x = \mathrm{Tr}[\Pi_{SA}^x(\mathrm{I} \otimes \rho_A)]$ with $\Pi_{SA}^x = |\psi^x\rangle\langle\psi^x|$. Quantum guessing probability is then unity by construction.

Results (2/2)

Thm: There exists a 4-outcome qubit POVM $\{F_S^x\}_x$ such that

$$p_{guess}(X|\Lambda, I/2, \{F_S^x\}_x) < p_{guess}(X|E, I/2, \{F_S^x\}_x) = 1.$$

Proof (sketch):

1. Let $\rho_{SA} = \frac{1}{4}\sum|\psi^x\rangle\langle\psi^x|$ with $\{|\psi^x\rangle\}_x$ be the entangled basis for two qubits from [1] and let $F_S^x = \mathrm{Tr}[\Pi_{SA}^x(\mathrm{I} \otimes \rho_A)]$ with $\Pi_{SA}^x = |\psi^x\rangle\langle\psi^x|$. Quantum guessing probability is then unity by construction.
2. We show that for qubit POVMs,

$$p_{guess}(X|\Lambda, \rho, \{M_S^x\}_x) = 1 \;\Rightarrow\; \{M_S^x\}_x \text{ is a convex combination of projective measurements.}$$

Results (2/2)

Thm: There exists a 4-outcome qubit POVM $\{F_S^x\}_x$ such that

$$p_{guess}(X|\Lambda, I/2, \{F_S^x\}_x) < p_{guess}(X|E, I/2, \{F_S^x\}_x) = 1.$$

Proof (sketch):

1. Let $\rho_{SA} = \frac{1}{4}\sum|\psi^x\rangle\langle\psi^x|$ with $\{|\psi^x\rangle\}_x$ be the entangled basis for two qubits from [1] and let $F_S^x = \mathrm{Tr}[\Pi_{SA}^x(\mathrm{I} \otimes \rho_A)]$ with $\Pi_{SA}^x = |\psi^x\rangle\langle\psi^x|$. Quantum guessing probability is then unity by construction.
2. We show that for qubit POVMs,

   $$p_{guess}(X|\Lambda, \rho, \{M_S^x\}_x) = 1 \;\Rightarrow\; \{M_S^x\}_x \text{ is a convex combination of projective measurements.}$$
3. Finally, using tools from [2], we show that $\{F_S^x\}_x$ is not a convex combination of projective measurements.

[1] A. Tavakoli et al., “Bilocal Bell inequalities violated by the quantum elegant joint measurement”, Phys. Rev. Lett. 126, 220401 (2021).

[2] M. Oszmaniec et al., “Simulating positive-operator-valued measures with projective measurements”, Phys. Rev. Lett. 119, 190501 (2017).

Discussion

Discussion

- If a given POVM $\{M_S^x\}_x$ is not a convex combination of projective measurements, then, in order to measure it, one necessarily must implement a Naimark dilation.

Discussion

- If a given POVM $\{M_S^x\}_x$ is not a convex combination of projective measurements, then, in order to measure it, one necessarily must implement a Naimark dilation.
- The information about the dilation is not being given to classical Eve. Therefore, it seems to make sense that her guessing probability is below that of quantum Eve.

Discussion

- If a given POVM $\{M_S^x\}_x$ is not a convex combination of projective measurements, then, in order to measure it, one necessarily must implement a Naimark dilation.
- The information about the dilation is not being given to classical Eve. Therefore, it seems to make sense that her guessing probability is below that of quantum Eve.
- However, that cannot be the whole explanation, because this already happens in the setting of pure states in which we do have equality.

Discussion

- If a given POVM $\{M_S^x\}_x$ is not a convex combination of projective measurements, then, in order to measure it, one necessarily must implement a Naimark dilation.
- The information about the dilation is not being given to classical Eve. Therefore, it seems to make sense that her guessing probability is below that of quantum Eve.
- However, that cannot be the whole explanation, because this already happens in the setting of pure states in which we do have equality.

Future work

- Characterize the set of states and measurements for which the classical and quantum *pguesses* coincide.
- Find ways to compute (or to, at least, computably approximate from above) $p_{guess}(X|E, \rho_S, \{M_S^x\}_x)$.

¡Gracias!

¡Gracias!

Questions?