The zoo of semi-DI assumptions and the path to redemption

Jef Pauwels

Joint work with Armin Tavakoli and Stefano Pironio

arXiv:2405.07231

UNIVERSITÉ
DE GENÈVE

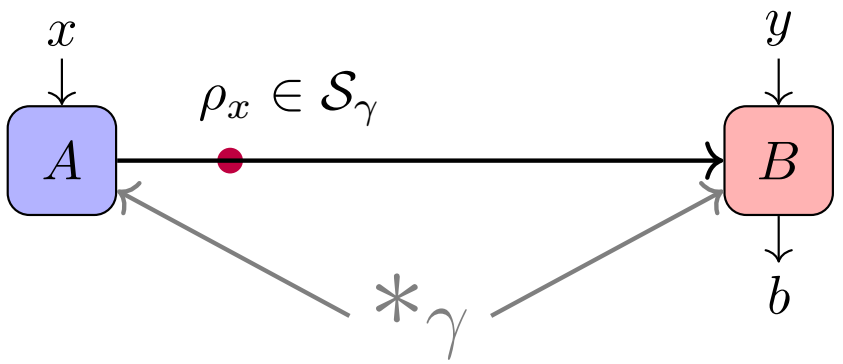
Quantum communication with partially characterised devices

Communication in **prepare-and-measure scenario**

Relaxed trust on devices

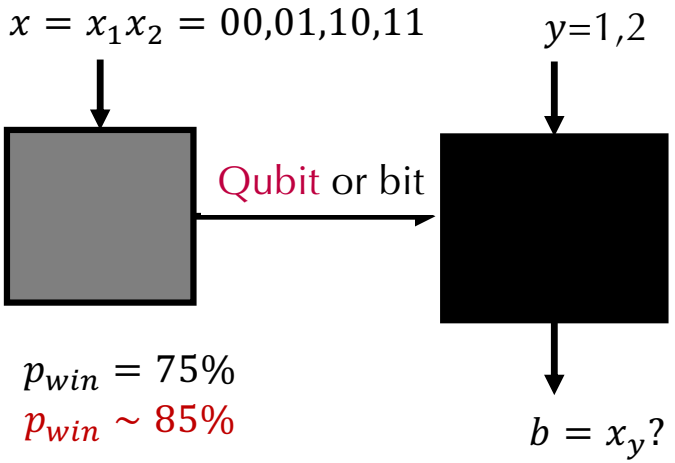
Contrary to Bell scenario some assumptions $\boldsymbol{\gamma}$ needed

Practical motivation: → **semi**-device-independent schemes are easier to implement

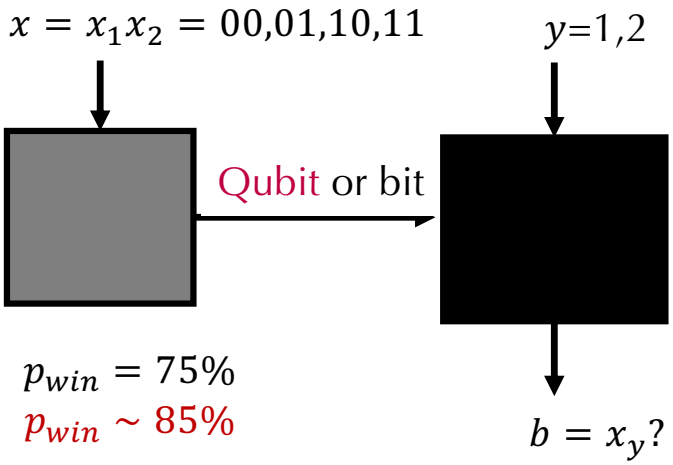


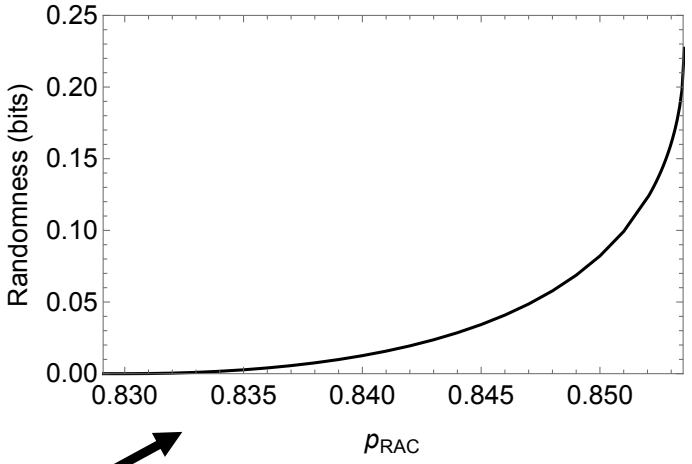
Simple example: dimension restriction

Random Access Coding



Random Access Coding





Quantum-over-classical advantage with self-testing properties

➔ can be used for QKD, QRNG, self-testing, certification,…

A zoo of alternative assumptions

1. **Dimension** [Brunner et al. 2008 PRL]

   $\rho \in C^d$

2. **Entanglement-assisted dimension** [AT, JP, EW, SP 2022 PRXQ]

   $\rho \in C^d$, shared entanglement

3. **Almost dimension** [JP, AT, EW, SP 2023 PRL]

   $tr(\rho \Pi_d) \geq 1 - \epsilon$

A zoo of alternative assumptions

1. **Dimension** [Brunner et al. 2008 PRL]

   $\rho \in C^d$

2. **Entanglement-assisted dimension** [AT, JP, EW, SP 2022 PRXQ]

   $\rho \in C^d$, shared entanglement

3. **Almost dimension** [JP, AT, EW, SP 2023 PRL]

   $tr(\rho \Pi_d) \geq 1 - \epsilon$

Foundationally interesting
$\log(d)$ ~ units of information

A zoo of alternative assumptions

1. **Dimension** [Brunner et al. 2008 PRL]

   $\rho \in C^d$

2. **Entanglement-assisted dimension** [AT, JP, EW, SP 2022 PRXQ]

   $\rho \in C^d$, shared entanglement

3. **Almost dimension** [JP, AT, EW, SP 2023 PRL]

   $tr(\rho \Pi_d) \geq 1 - \epsilon$

} Address some (practical) shortcomings, retaining fundamental interest of dimension

A zoo of alternative assumptions

1. **Dimension** [Brunner et al. 2008 PRL]

   $\rho \in C^d$

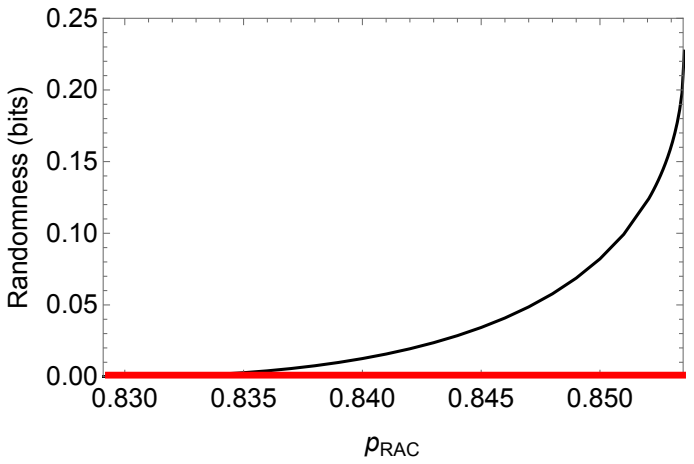
2. **Entanglement-assisted dimension** [AT, JP, EW, SP 2022 PRXQ]

   $\rho \in C^d$, shared entanglement

3. **Almost dimension** [JP, AT, EW, SP 2023 PRL]

   $tr(\rho \Pi_d) \geq 1 - \epsilon$

(Accidental) and (short-lived) entanglement radically changes correlations
→ Compromised protocols



A zoo of alternative assumptions

1. **Dimension** [Brunner et al. 2008 PRL]

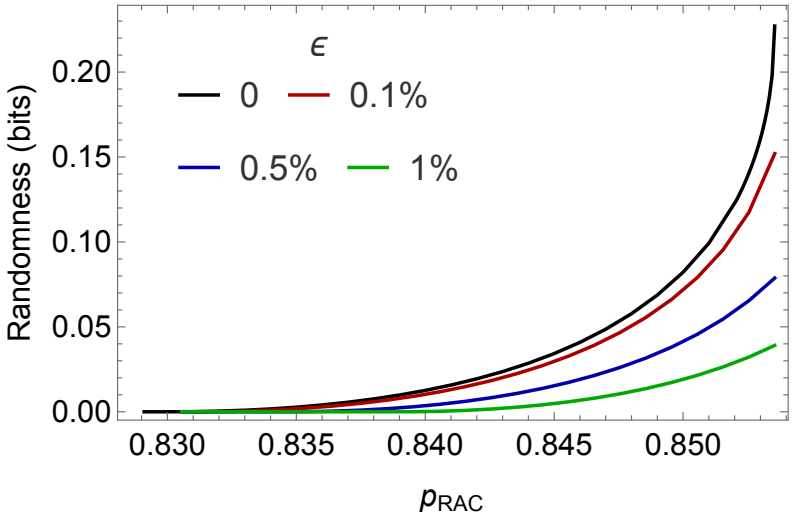
   $\rho \in C^d$

2. **Entanglement-assisted dimension** [AT, JP, EW, SP 2022 PRXQ]

   $\rho \in C^d$, shared entanglement

3. **Almost dimension** [JP, AT, EW, SP 2023 PRL]

   $tr(\rho \Pi_d) \geq 1 - \epsilon$



Tiny higher-dimensional components radically affect semi-DI security

A zoo of alternative assumptions

4. **Vacuum component** [Van Himbeeck, SP 2017 Quantum]

   $\mathrm{tr}(\rho H) \geq \omega$, where $\mathrm{H} = Id - |0\rangle\langle 0|$

5. **Overlaps** [Brask et al. 2017 Phys. Rev. Applied]

   - $\left|\langle \psi_x | \psi_{x'} \rangle\right| \geq a_{xx'}$

6. **Distrust** [AT 2023 PRL]

   - Alice wants to prepare $|\psi\rangle$, but her device is imperfect
   - The fidelity of the actual state ρ is bounded $\langle \psi | \rho | \psi \rangle \geq 1 - \epsilon$

Assumptions without reference to dimension

A zoo of alternative assumptions

4. **Vacuum component** [Van Himbeeck et al. 2017 Quantum]

   $\mathrm{tr}(\rho H) \geq \omega$, where $\mathrm{H} = Id - |0\rangle\langle 0|$

Natural for optical systems, trusted energy measurement

5. **Overlaps** [Brask et al. Phys. Rev. Applied 2017]

   - $\left|\langle\psi_x|\psi_{x'}\rangle\right| \geq a_{xx'}$

6. **Distrust** [AT PRL 2023]

   - Alice wants to prepare $|\psi\rangle$, but her device is imperfect
   - The fidelity of the actual state ρ is bounded $\langle\psi|\rho|\psi\rangle \geq 1 - \epsilon$

A zoo of alternative assumptions

4. **Vacuum component** [Van Himbeeck et al. 2017 Quantum]

   $\mathrm{tr}(\rho H) \geq \omega$, where $\mathrm{H} = Id - |0\rangle\langle 0|$

5. **Overlaps** [Brask et al. Phys. Rev. Applied 2017]

   - $\left|\langle\psi_x|\psi_{x'}\rangle\right| \geq a_{xx'}$

Also common for optical systems

6. **Distrust** [AT PRL 2023]

   - Alice wants to prepare $|\psi\rangle$, but her device is imperfect
   - The fidelity of the actual state ρ is bounded $\langle\psi|\rho|\psi\rangle \geq 1 - \epsilon$

A zoo of alternative assumptions

4. **Vacuum component** [Van Himbeeck et al. 2017 Quantum]

   $\mathrm{tr}(\rho H) \geq \omega$, where $\mathrm{H} = Id - |0\rangle\langle 0|$

5. **Overlaps** [Brask et al. Phys. Rev. Applied 2017]

   - $\left|\langle\psi_x|\psi_{x'}\rangle\right| \geq a_{xx'}$

6. **Distrust** [AT PRL 2023]

   - Alice wants to prepare $|\psi\rangle$, but her device is imperfect
   - The fidelity of the actual state ρ is bounded $\langle\psi|\rho|\psi\rangle \geq 1 - \epsilon$

Platform independent

Capacity constraint

(*) **Information** [AT et al. 2022 Quantum]

Information-theoretic assumption, without reference to Hilbert space

Bound the "accesible information" through the min-entropy:

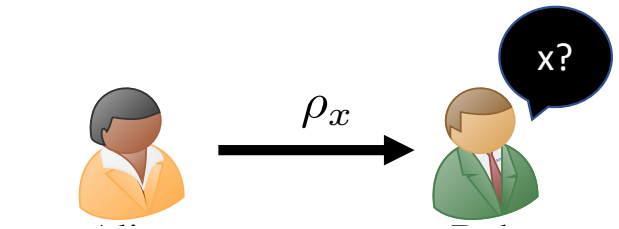
$$I = H_{min}(X) - H_{min}(X|B) = \log n + \log P_g$$

where

$$P_g = \max \frac{1}{n} \sum_x tr(\rho_x N_x)$$

inputs Alice

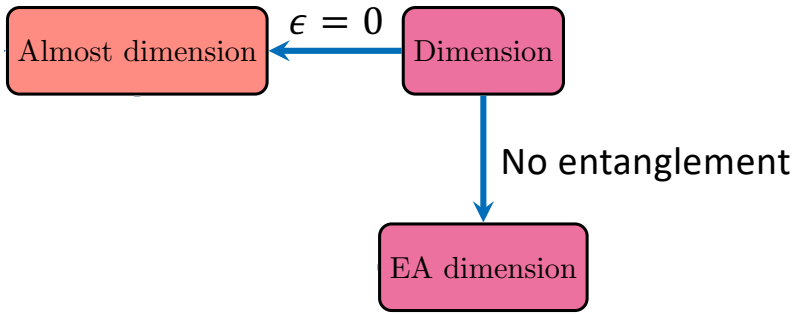
Optimal extraction POVM

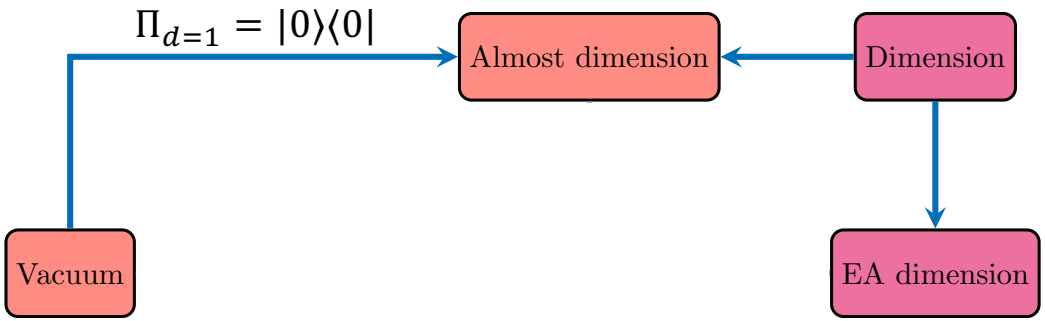


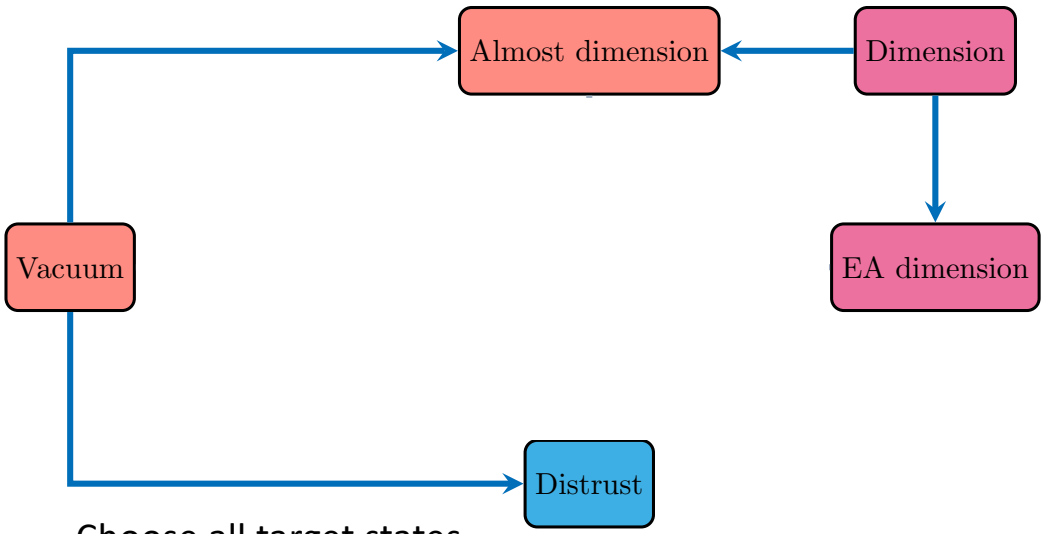
$\mathcal{B} = \{p_x, \rho_x\}$

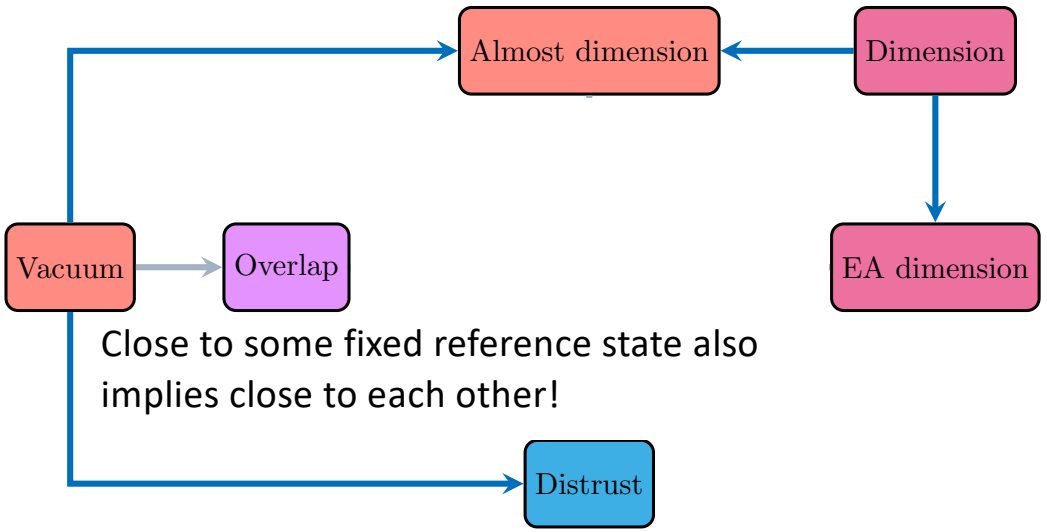
How are all these assumptions connected?

The path to redemption…



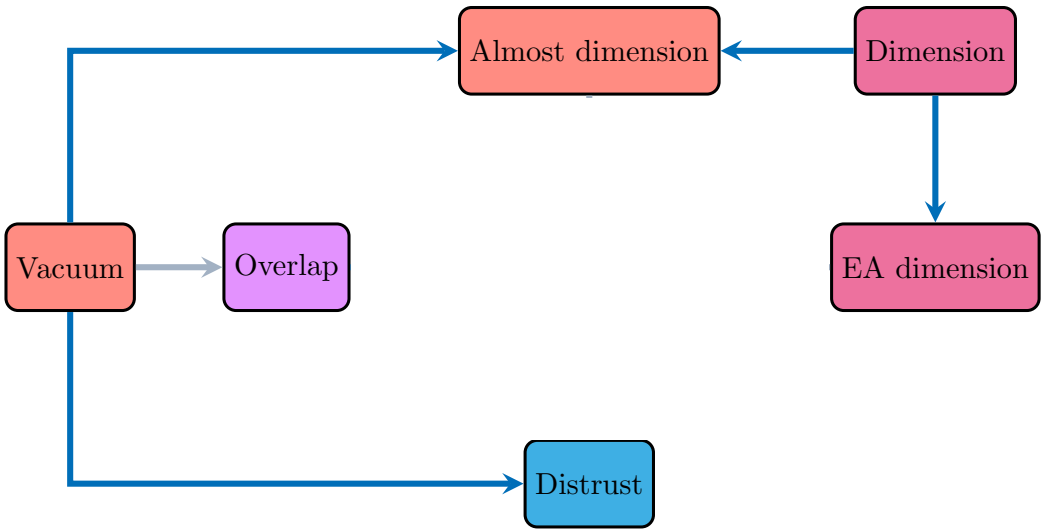

$\Pi_{d=1} = |0\rangle\langle 0|$
Almost dimension
Dimension
Vacuum
EA dimension


Almost dimension
Dimension
Vacuum
EA dimension
Distrust
Choose all target states
$|\psi_x\rangle = |0\rangle$


Almost dimension
Dimension
Vacuum
Overlap
EA dimension
Close to some fixed reference state also
implies close to each other!
Distrust

Methods for characterising correlations for some assumptions can be applied to others in limiting cases

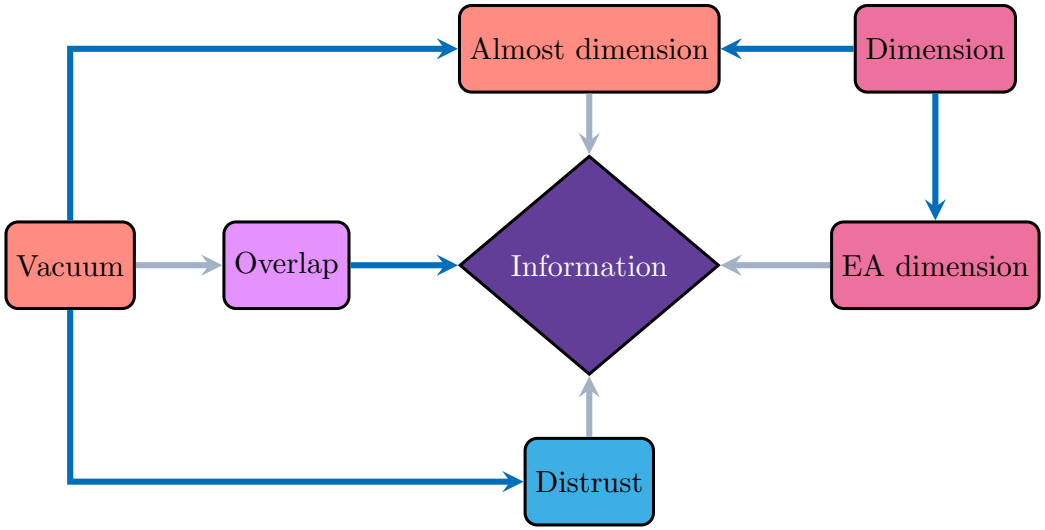
No complete hierarchy of assumptions…



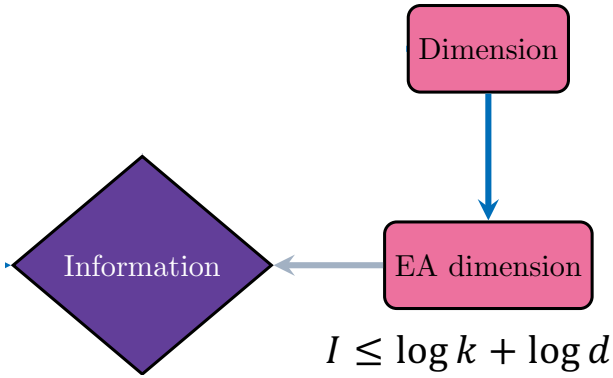
The path to redemption… a unifying assumption

All assumptions imply a capacity constraint!

Not a surprise: this is why they were introduced in the first place



Information in entanglement-assisted dimension



[AT, JP, EW, SP 2022 PRXQ]

The energy cost of information

- Assume pure states, w.l.g. real (infinite dimensional)
- Energy assumption:

$$tr(\rho_x H) \leq \omega \;\rightarrow\; \langle\psi_x|0\rangle \leq \sqrt{1-\omega}$$

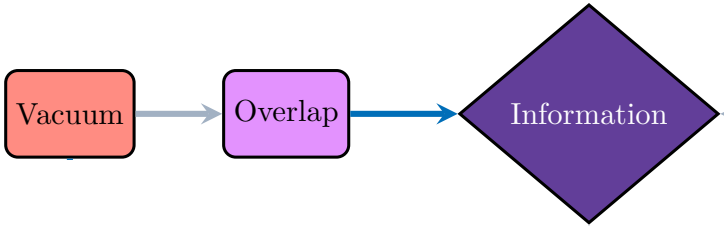
The states lie in a **cone around the vacuum**

- Choose them **equidistant** $\langle\psi_x|\psi_{x'}\rangle = \mathbf{a}$

on the cone $\langle\psi_x|0\rangle = \sqrt{1-\omega}$

- How distinguishable can I choose the states?

$min\ a$ s.t. $G \geq 0$



$$G = \begin{pmatrix} 1 & a & a & \dots & a & \sqrt{1-\omega} \\ a & 1 & a & \dots & a & \sqrt{1-\omega} \\ a & a & \ddots & \dots & a & \sqrt{1-\omega} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a & a & a & \dots & 1 & \sqrt{1-\omega} \\ \sqrt{1-\omega} & \sqrt{1-\omega} & \sqrt{1-\omega} & \dots & \sqrt{1-\omega} & 1 \end{pmatrix}$$

The energy cost of information

- Assume pure states, w.l.g. real (infinite dimensional)
- Energy assumption:

$$tr(\rho_x H) \leq \omega \rightarrow \langle\psi_x|0\rangle \leq \sqrt{1-\omega}$$

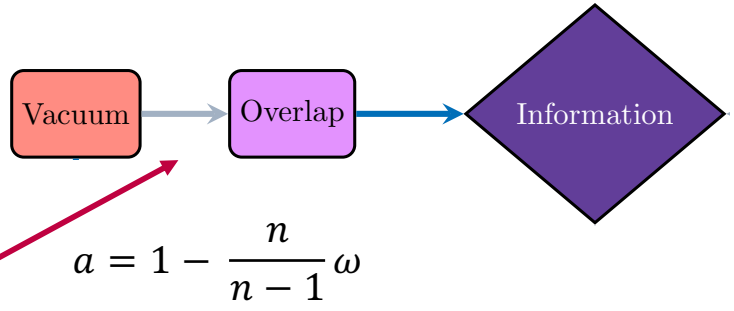
The states lie in a **cone around the vacuum**

- Choose them **equidistant** $\langle\psi_x|\psi_{x'}\rangle = \mathbf{a}$

on the cone $\langle\psi_x|0\rangle = \sqrt{1-\omega}$

- How distinguishable can I choose the states?

$min\ a$ s.t. $G \geq 0$



$$a = 1 - \frac{n}{n-1}\omega$$

$$G = \begin{pmatrix} 1 & a & a & \dots & a & \sqrt{1-\omega} \\ a & 1 & a & \dots & a & \sqrt{1-\omega} \\ a & a & \ddots & \dots & a & \sqrt{1-\omega} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a & a & a & \dots & 1 & \sqrt{1-\omega} \\ \sqrt{1-\omega} & \sqrt{1-\omega} & \sqrt{1-\omega} & \dots & \sqrt{1-\omega} & 1 \end{pmatrix}$$

The energy cost of information

- Assume pure states, w.l.g. real (infinite dimensional)
- Energy assumption:

$$tr(\rho_x H) \leq \omega \;\rightarrow\; \langle\psi_x|0\rangle \leq \sqrt{1-\omega}$$

The states lie in a **cone around the vacuum**

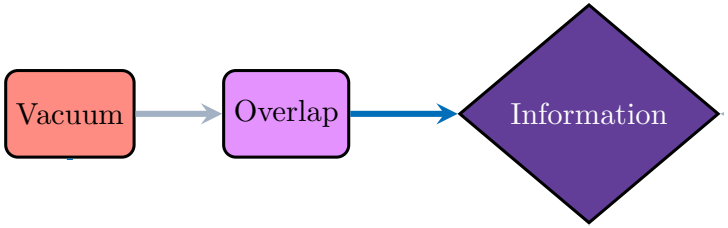
- Choose them **equidistant** $\langle\psi_x|\psi_{x'}\rangle = \mathbf{a}$

on the cone $\langle\psi_x|0\rangle = \sqrt{1-\omega}$

- How distinguishable can I choose the states?

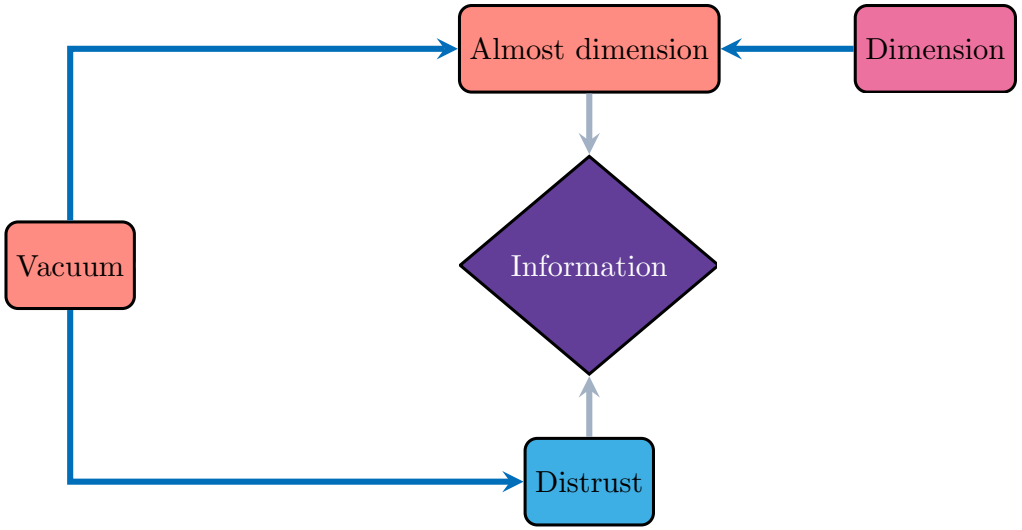
$min\ a$ s.t. $G \geq 0$

- **Optimal states** → equianglular → **Pretty good measurement is optimal**

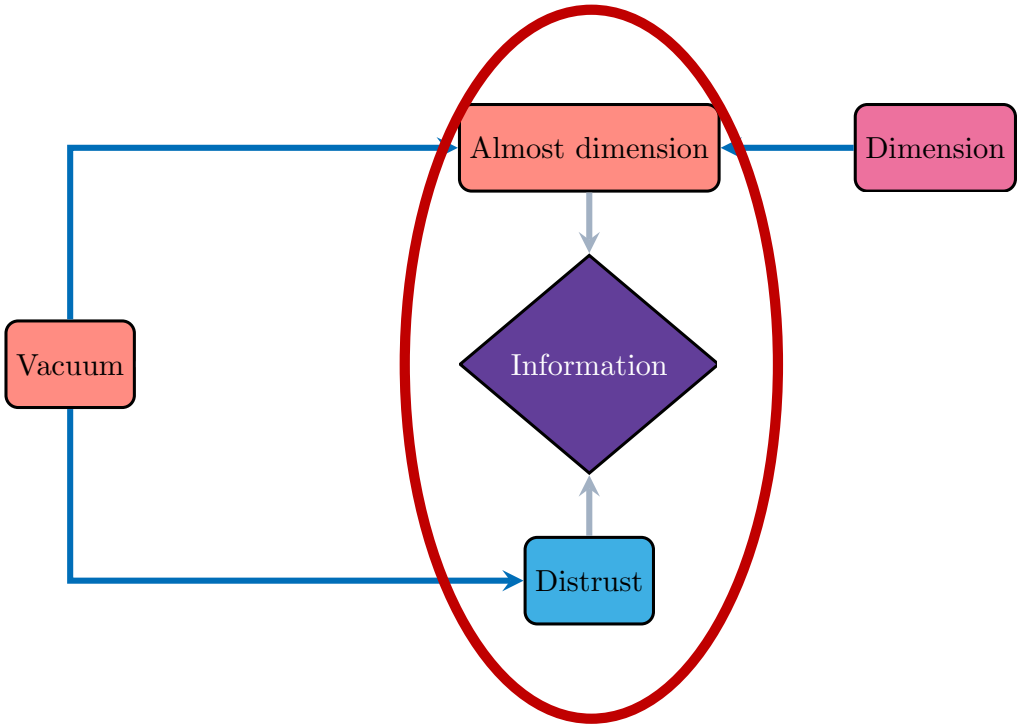


$$I \leq 2\log\sqrt{\omega(n-1)} + \sqrt{1-\omega}$$

Information cost of SDI: a general method



Information cost of SDI: a general method



Sketch: method for bounded subspace

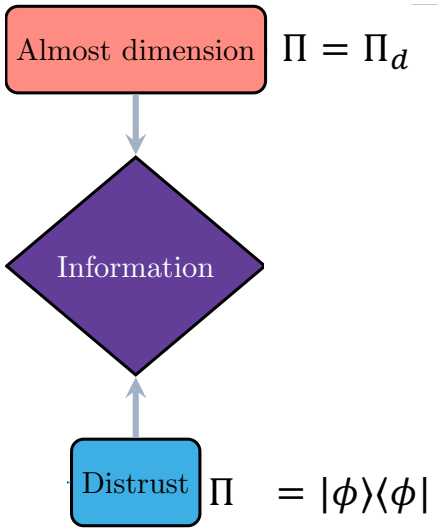
- Assume pure states (can relax later) $|\psi\rangle$
- Both assumptions take the form $\langle\psi|\Pi|\psi\rangle \geq 1-\epsilon$
- This implies $|\psi\rangle\langle\psi| \leq (1-\mu)\tilde{\psi} + \mathrm{h}(\epsilon,\mu)I$ for all $\mu \geq -1$

Projection on Π

Correction

- Plug this into expression for P_g

$$P_g^{\epsilon} \leq P_g^0 + \left(1-2P_g^0\right)\epsilon + 2\sqrt{P_g^0\left(1-P_g^0\right)\epsilon(1-\epsilon)}$$



Sketch: method for bounded subspace

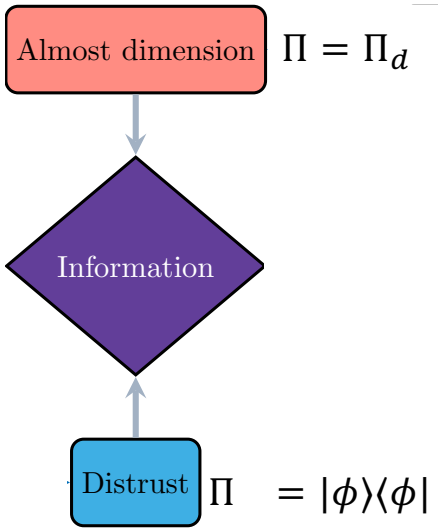
- Assume pure states (can relax later) $|\psi\rangle$
- Both assumptions take the form $\langle\psi|\Pi|\psi\rangle \geq 1-\epsilon$
- This implies $|\psi\rangle\langle\psi| \leq (1-\mu)\tilde{\psi} + \mathrm{h}(\epsilon,\mu)I$ for all $\mu \geq -1$

Projection on Π Correction

- Plug this into expression for P_g

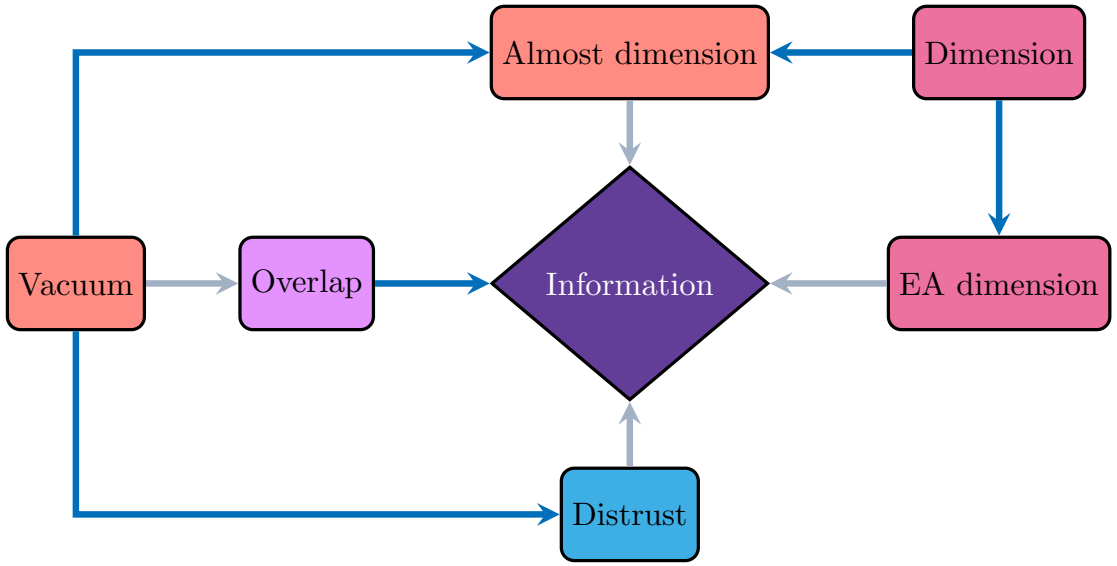
$$P_g^{\epsilon} \leq P_g^0 + \left(1-2P_g^0\right)\epsilon + 2\sqrt{P_g^0\left(1-P_g^0\right)\epsilon(1-\epsilon)}$$

TIGHT for almost qudits!



Summary

- Two classes of SDI assumptions:
  1. Bounded subspace constraints
  2. Information (capacity) constraints
- Tight bounds on information capacity under bounded subspace constraints
- Not nesecarily a useful relaxation to study correlations



Summary

- Two classes of SDI assumptions:
  1. Bounded subspace constraints
  2. Information (capacity) constraints
- Tight bounds on information capacity under bounded subspace constraints
- Not nesecarily a useful relaxation to study correlations

arXiv:2405.07231