“Sobolev-type inequalities in position based cryptography”

Marius Junge (UIUC)

Aleksander M. Kubicki (UCM)

Carlos Palazuelos (UCM-ICMAT)

David Pérez-García (UCM-ICMAT)

This work was funded by the ERC
(grant agreement no. 648913)

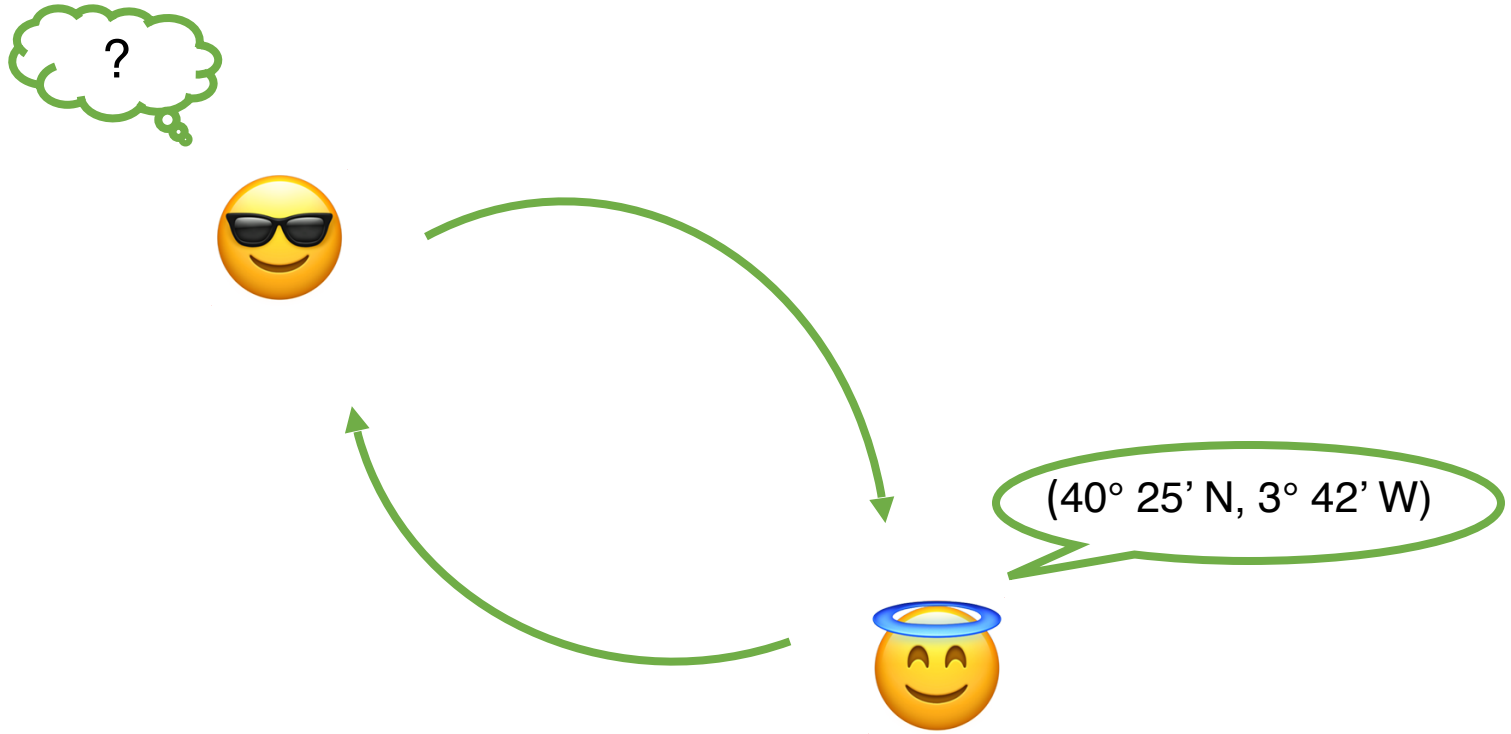
Outline.

1. Position Based-cryptography
2. Summary of main results
3. Some mathematical background
4. Bounds under regularity assumptions
5. Towards unconditional bounds
6. Final remarks

Position based cryptography

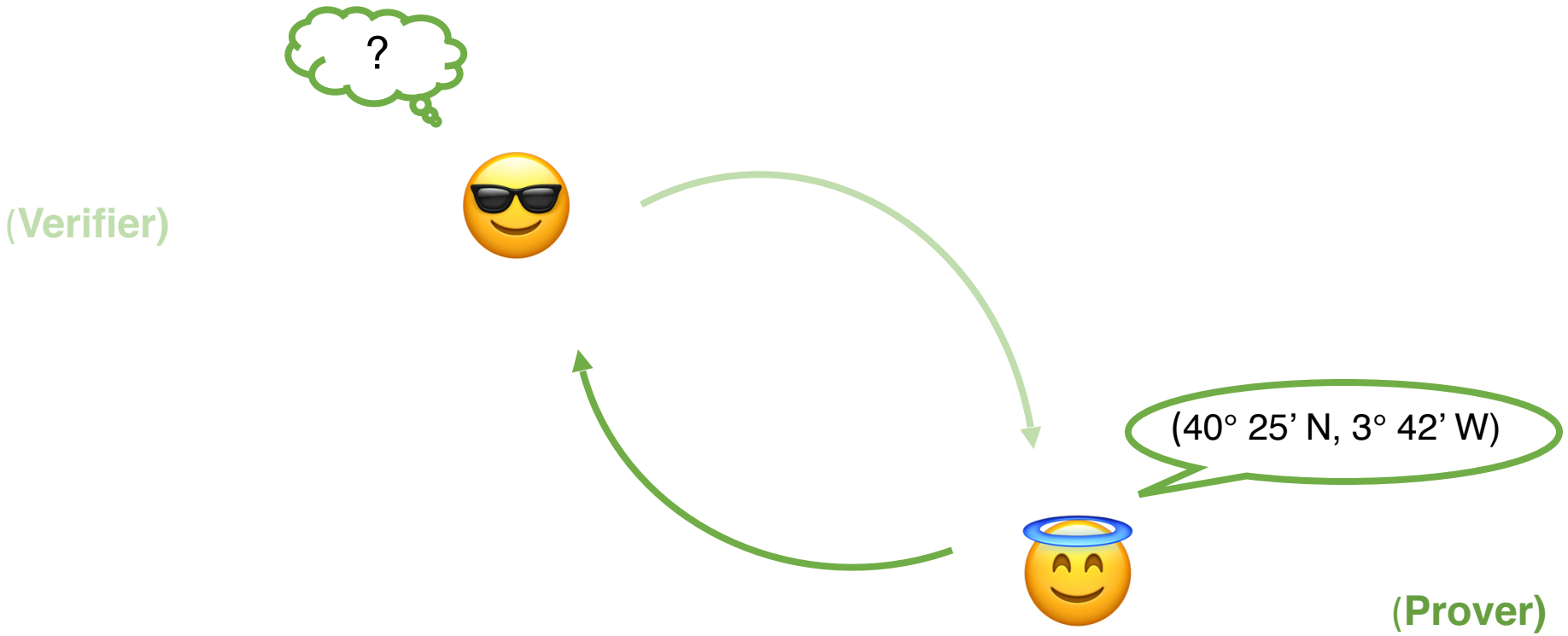
1.

1. Position based cryptography.



PBC: Geographical position as (the only) credencial

1. Position based cryptography. Position Verification.



PV: A prover has to convince a verifier of his position.

1. Position based cryptography. 1-D Position Verification.

1. Position based cryptography. 1-D Position Verification.

1. 1-D Position Verification. Honest protocol.

1. Verifiers prepare questions and send them to prover.

1. 1-D Position Verification. Honest protocol.

1. Verifiers prepare questions and send them to prover.

2. Prover prepares a (bipartite) answer according to the information received and sends it back to verifiers.

1. 1-D Position Verification. Honest protocol.

1. Verifiers prepare questions and send them to prover.

2. Prover prepares a (bipartite) answer according to the information received and sends it back to verifiers.

3. At some later time, verfiers check:
   - Timeliness: answers arrive on time
   - Correctness: answers are correct w.r.t. questions asked.

1. 1-D Position Verification. Honest protocol.

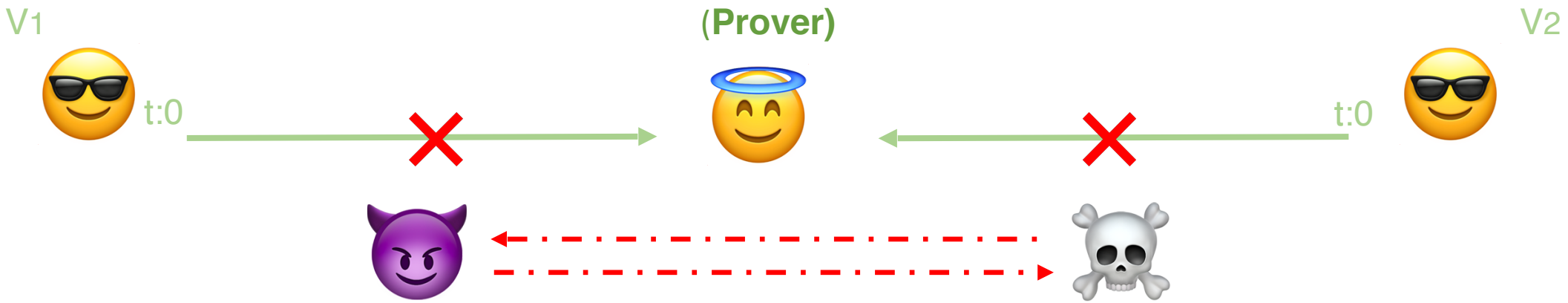
1. Verifiers prepare a state $|\psi\rangle \in \mathcal{H}_{BCV}$ and send registers $\mathcal{H}_{BC}$ to prover.

2. Prover applies a quantum operation $S \in \mathrm{CPTP}(\mathcal{H}_{BC} \to \mathcal{H}_{BC})$ and sends the result back.

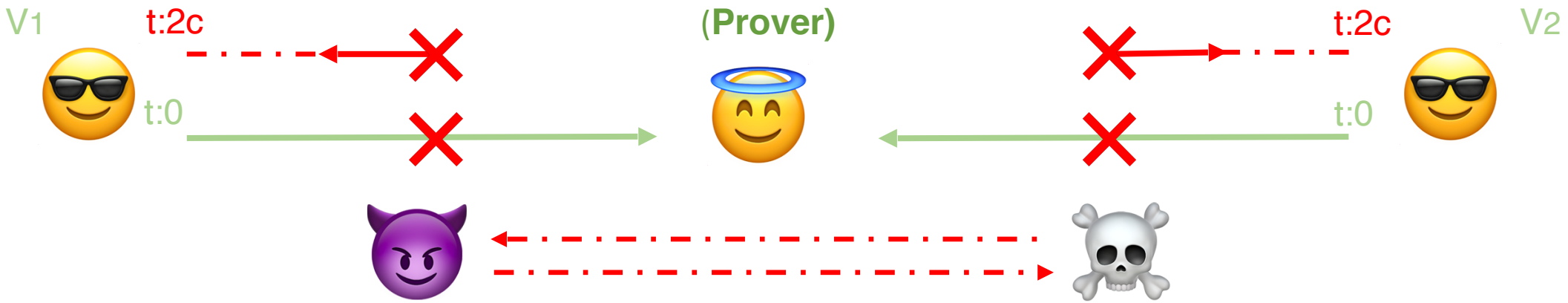
3. At some later time, verifiers check:
   - Timeliness: answers arrive on time
   - Correctness: verifiers check if $\mathrm{Id}_V \otimes S(|\psi\rangle\langle\psi|) \approx T(|\psi\rangle\langle\psi|)$ for a target operation $T \in \mathrm{CPTP}(\mathcal{H}_{BCV} \to \mathcal{H}_{BCV})$

1. 1-D Position Verification. Cheating on PV.

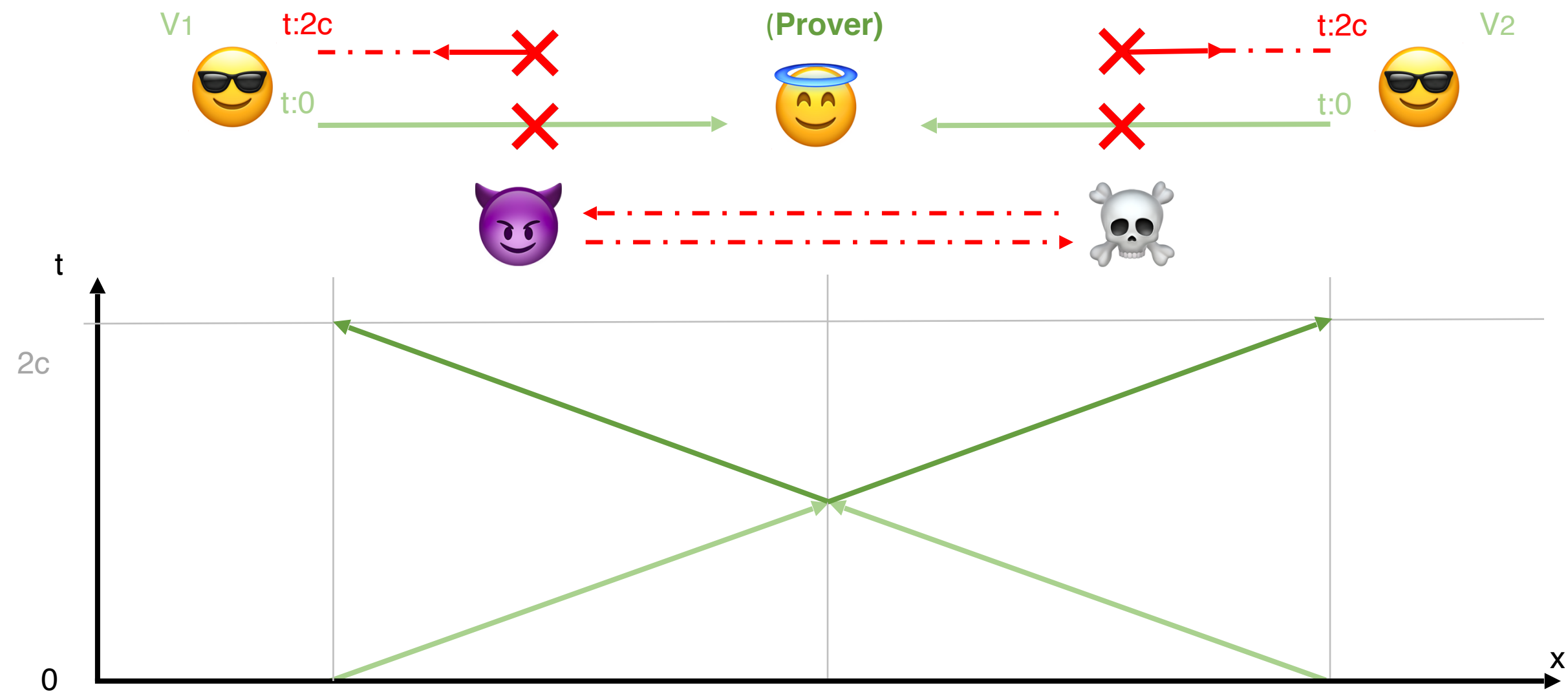
1. 1-D Position Verification. Cheating on PV.



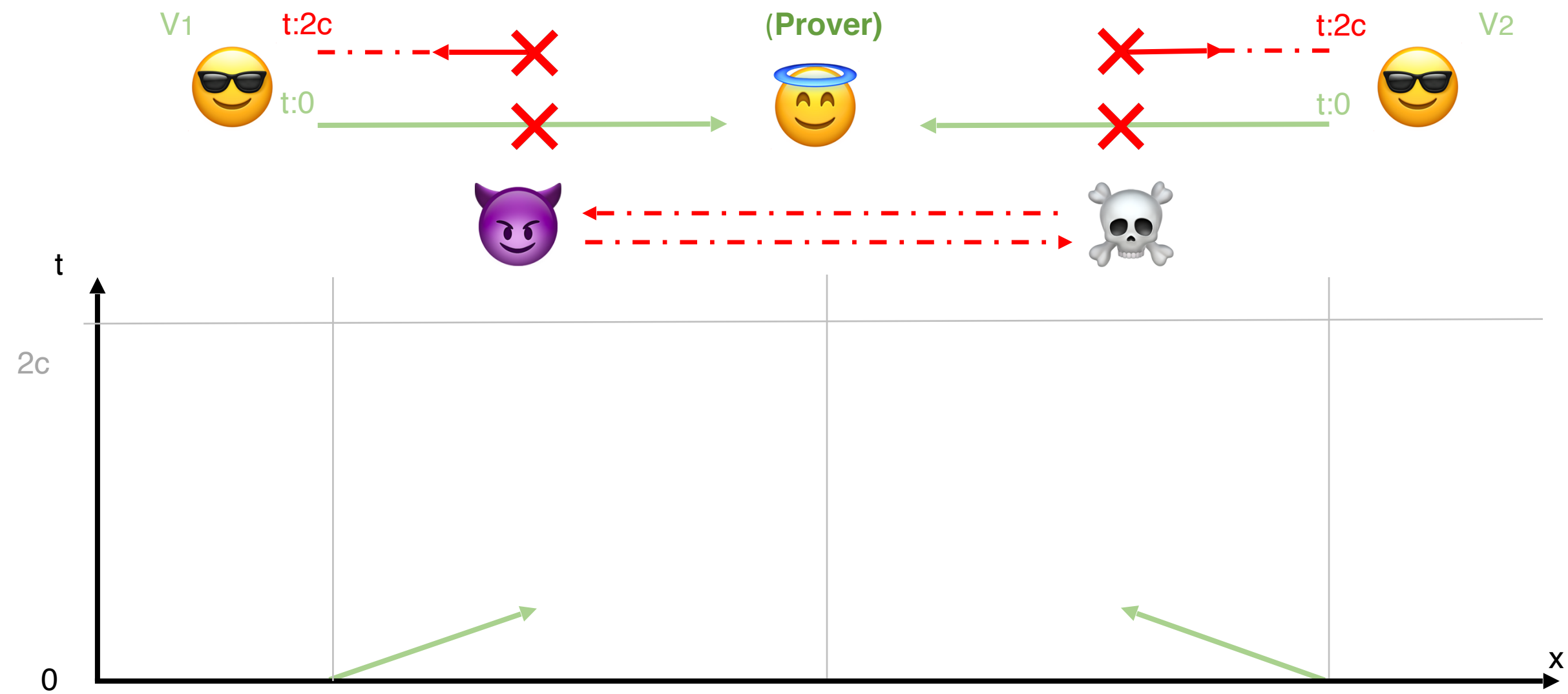
1. 1-D Position Verification. Cheating on PV.



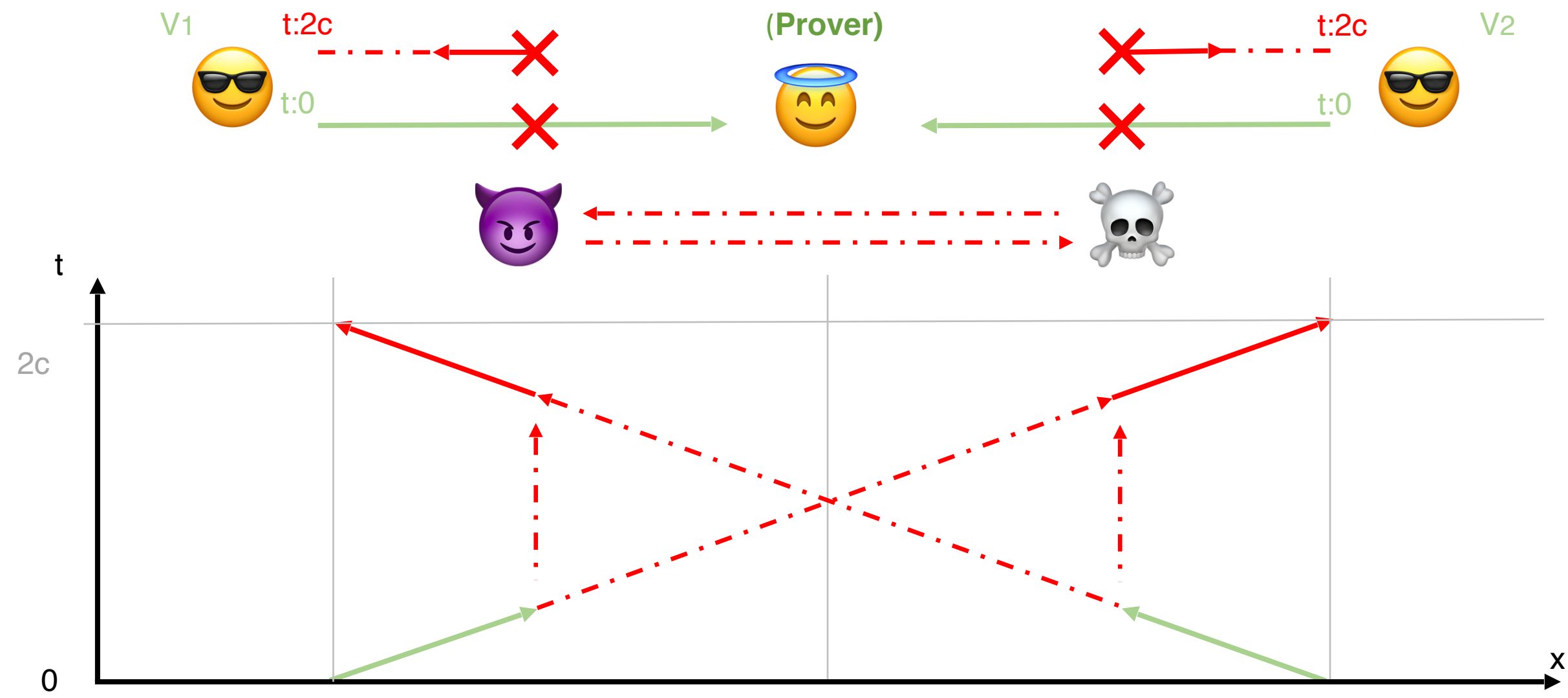
1. 1-D Position Verification. Cheating on PV.



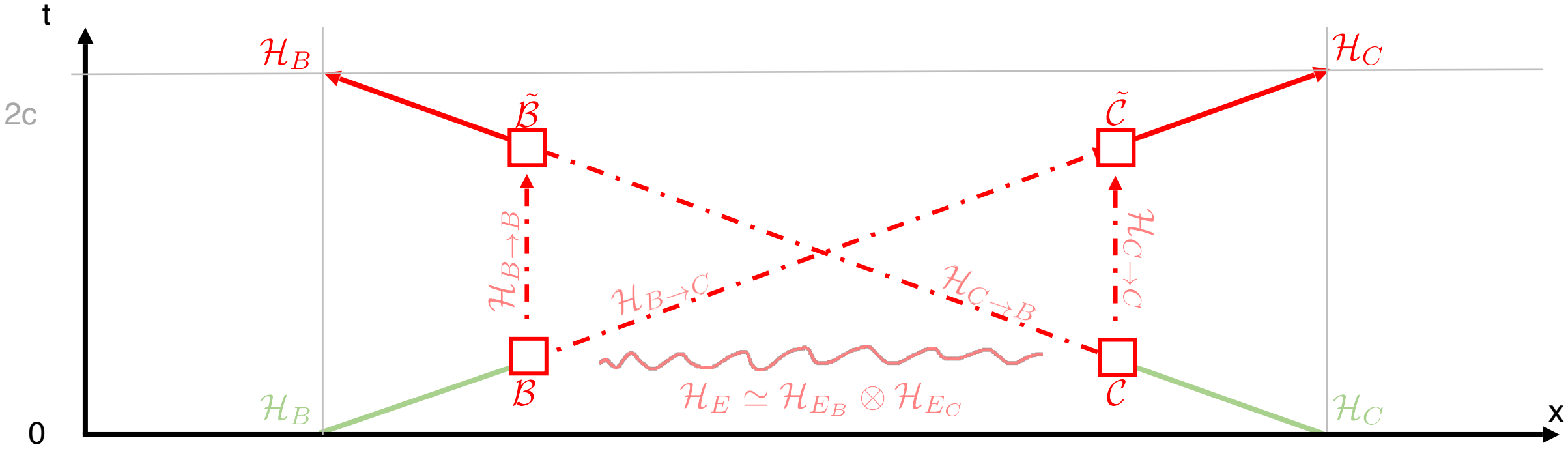
1. 1-D Position Verification. Cheating on PV.



1. 1-D Position Verification. Cheating on PV.

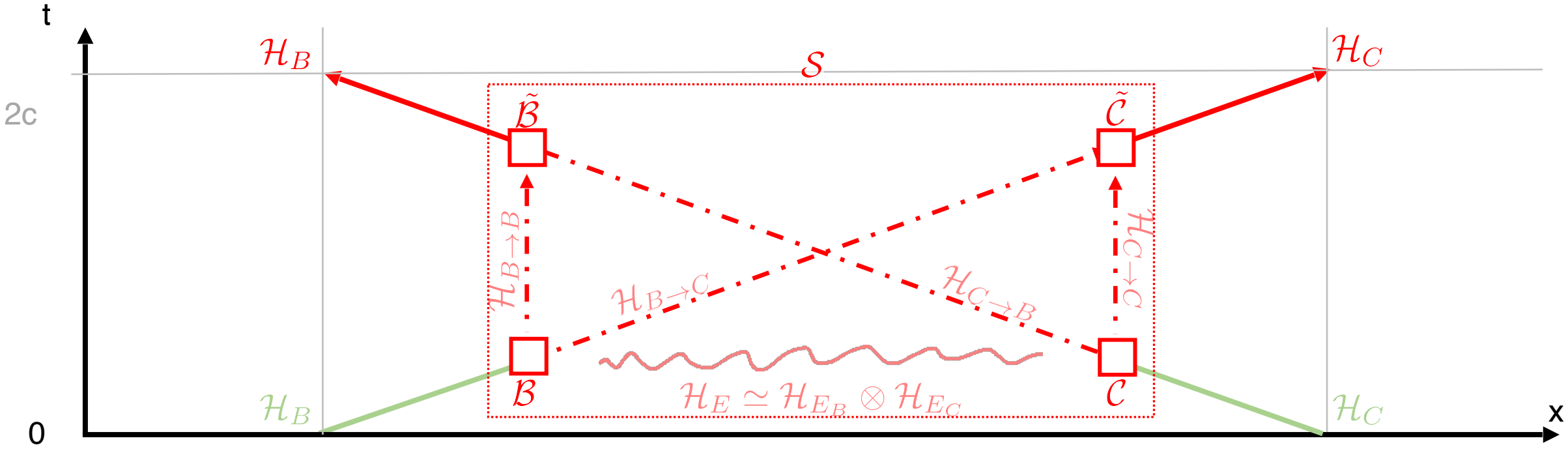


1. 1-D Position Verification. Cheating on PV.



- $\mathcal{B} \in \mathrm{CPTP}(\mathcal{H}_B \otimes \mathcal{H}_{E_B} \longrightarrow \mathcal{H}_{B\to B} \otimes \mathcal{H}_{B\to C})$,
- $\mathcal{C} \in \mathrm{CPTP}(\mathcal{H}_C \otimes \mathcal{H}_{E_C} \longrightarrow \mathcal{H}_{C\to C} \otimes \mathcal{H}_{C\to B})$,
- $\tilde{\mathcal{B}} \in \mathrm{CPTP}(\mathcal{H}_{B\to B} \otimes \mathcal{H}_{C\to B} \longrightarrow \mathcal{H}_B)$,
- $\tilde{\mathcal{C}} \in \mathrm{CPTP}(\mathcal{H}_{C\to C} \otimes \mathcal{H}_{B\to C} \longrightarrow \mathcal{H}_C)$.

1. 1-D Position Verification. Cheating on PV.



Channel implemented by cheaters:

- $\mathcal{S}(\,\cdot\,) \;=\; (\tilde{\mathcal{B}} \otimes \tilde{\mathcal{C}}) \circ (\mathcal{B} \otimes \mathcal{C})(\,\cdot \otimes |\varphi\rangle\langle\varphi|) \in \mathrm{CPTP}(\mathcal{H}_{BC} \longrightarrow \mathcal{H}_{BC}) \quad$ for some $\quad |\varphi\rangle \in \mathcal{H}_E.$

(Simultaneous two-way communication model, s2w)

1. 1-D Position Verification. Cheating on PV.

Previous results:

For any target operation $T \in \mathrm{CPTP}(\mathscr{H}_{BC} \to \mathscr{H}_{BC})$ there exists an s2w channel S approximating T [Bu10]

That is, *information-theoretically secure* quantum PV is imposible.

- [Bu10] Burhman, H. et al, arXiv 1009.2490 (2010)
- [Be11] Beigi, S. and Koenig, R., arXiv 1101.1065 (2011)
- [To13] Tomamichel, M. et al, arXiv 1210.4359 (2013)

1. 1-D Position Verification. Cheating on PV.

Previous results:

For any target operation $T \in \mathrm{CPTP}(\mathscr{H}_{BC} \to \mathscr{H}_{BC})$ there exists an s2w channel S approximating T [Bu10]

That is, *information-theoretically secure* quantum PV is imposible.

However:

Cheaters need to use (an enormous amount of) entanglement [Be11]: $\dim(\mathscr{H}_E) \approx \exp(\dim \mathscr{H}_{BC})$

- [Bu10] Burhman, H. et al, arXiv 1009.2490 (2010)
- [Be11] Beigi, S. and Koenig, R., arXiv 1101.1065 (2011)
- [To13] Tomamichel, M. et al, arXiv 1210.4359 (2013)

1. 1-D Position Verification. Cheating on PV.

Previous results:

For any target operation $T \in \mathrm{CPTP}(\mathscr{H}_{BC} \to \mathscr{H}_{BC})$ there exists an s2w channel S approximating T [Bu10]

That is, *information-theoretically secure* quantum PV is imposible.

However:

Cheaters need to use (an enormous amount of) entanglement [Be11]: $\dim(\mathscr{H}_E) \approx \exp(\dim \mathscr{H}_{BC})$

Open question:

Optimal entanglement dimension necessary to break *any* PV scheme? It is known that:

[To13] [Be11]

$$\Omega(\dim \mathcal{H}) \leq \dim \mathcal{H}_E^{(opt)} \leq O(\exp(\dim \mathcal{H}))$$

- [Bu10] Burhman, H. et al, arXiv 1009.2490 (2010)
- [Be11] Beigi, S. and Koenig, R., arXiv 1101.1065 (2011)
- [To13] Tomamichel, M. et al, arXiv 1210.4359 (2013)

Main results | 2.

2. Main results.

Previous comments:

- Classical resources are free for us.
- We do not consider computational-complexity considerations.

Plan:

1. Construct a specific PV scheme that we call G_{Rad}
2. Prove lower bounds for the entanglement dimension required in attacks to G_{Rad}

2. $G^{(n)}_{Rad}$.

Plan:

1. Construct a specific PV scheme that we call G_{Rad}
2. Prove lower bounds for the entanglement dimension required in attacks to G_{Rad}

2. $G^{(n)}_{Rad}$.

2. $G^{(n)}_{Rad}$.

1. V1 prepares $|\psi\rangle = \frac{1}{n}\sum_{i,j=1}^{n} |ij\rangle_{BC} \otimes |ij\rangle_{V} \in \mathcal{H}_{BCV}$, sends $\mathcal{H}_{BC}$.

   V2 samples a sign-vector $\varepsilon \in \{\pm 1\}^{n^2}$

2. $G^{(n)}_{Rad}$.

1. V1 prepares $|\psi\rangle = \frac{1}{n}\sum_{i,j=1}^{n} |ij\rangle_{BC} \otimes |ij\rangle_V \in \mathcal{H}_{BCV}$, sends $\mathcal{H}_{BC}$.

   V2 samples a sign-vector $\varepsilon \in \{\pm 1\}^{n^2}$

2. Prover applies $S_\varepsilon \in \mathrm{CPTP}(\mathscr{H}_{BC} \to \mathscr{H}_{BC})$ and sends the result back.

2. $G^{(n)}_{Rad}$.

1. V1 prepares $|\psi\rangle = \frac{1}{n}\sum_{i,j=1}^{n} |ij\rangle_{BC} \otimes |ij\rangle_V \in \mathcal{H}_{BCV}$, sends $\mathcal{H}_{BC}$.

   V2 samples a sign-vector $\varepsilon \in \{\pm 1\}^{n^2}$

2. Prover applies $S_\varepsilon \in \mathrm{CPTP}(\mathscr{H}_{BC} \to \mathscr{H}_{BC})$ and sends the result back.

3. Verifiers check:

   - Timeliness.
   - Correctness: $\mathrm{Id}_V \otimes \mathcal{S}_\varepsilon(|\psi\rangle\langle\psi|) \overset{?}{\approx} (\mathrm{Id}_V \otimes U_\varepsilon)\,|\psi\rangle\langle\psi|\,(\mathrm{Id}_V \otimes U_\varepsilon^\dagger)$

where $U_\varepsilon = diag(\varepsilon)$ is the ideal operation to be applied on BC: $U_\varepsilon |ij\rangle = \varepsilon_{ij} |ij\rangle$

2. $G^{(n)}_{Rad}$.

3. Verifiers check:
   - Timeliness.
   - Correctness: $\mathrm{Id}_V \otimes \mathcal{S}_\varepsilon(|\psi\rangle\langle\psi|) \overset{?}{\approx} (\mathrm{Id}_V \otimes U_\varepsilon)\,|\psi\rangle\langle\psi|\,(\mathrm{Id}_V \otimes U_\varepsilon^\dagger)$

     where $U_\varepsilon = diag(\varepsilon)$ is the ideal operation to be applied.

2. $G^{(n)}_{Rad}$.

3. Verifiers check:
   - Timeliness.
   - Correctness: $\mathrm{Id}_V \otimes \mathcal{S}_\varepsilon(|\psi\rangle\langle\psi|) \overset{?}{\approx} (\mathrm{Id}_V \otimes U_\varepsilon)\,|\psi\rangle\langle\psi|\,(\mathrm{Id}_V \otimes U_\varepsilon^\dagger)$

     where $U_\varepsilon = diag(\varepsilon)$ is the ideal operation to be applied.

The challenge is passed or failed depending on the result of the measurement

$$\mathcal{M}_\varepsilon = \{M^0_\varepsilon,\, M^1_\varepsilon\} \in \mathrm{POVM}(\mathcal{H}_{BCV})$$

where $M^0_\varepsilon := (\mathrm{Id}_V \otimes U_\varepsilon)\,|\psi\rangle\langle\psi|\,(\mathrm{Id}_V \otimes U_\varepsilon^\dagger),\ M^1_\varepsilon := \mathrm{Id}_{BCV} - M^0_\varepsilon$

$M^0_\varepsilon \longrightarrow$ pass

$M^1_\varepsilon \longrightarrow$ fail

2. $G_{Rad}^{(n)}$.

3. Verifiers check:
   - Timeliness.
   - Correctness: $\mathrm{Id}_V \otimes \mathcal{S}_\varepsilon(|\psi\rangle\langle\psi|) \overset{?}{\approx} (\mathrm{Id}_V \otimes U_\varepsilon)\,|\psi\rangle\langle\psi|\,(\mathrm{Id}_V \otimes U_\varepsilon^\dagger)$

     where $U_\varepsilon = diag(\varepsilon)$ is the ideal operation to be applied.

The challenge is passed or failed depending on the result of the measurement

$$\mathcal{M}_\varepsilon = \{M_\varepsilon^0,\, M_\varepsilon^1\} \in \mathrm{POVM}(\mathcal{H}_{BCV})$$

where $M_\varepsilon^0 := (\mathrm{Id}_V \otimes U_\varepsilon)\,|\psi\rangle\langle\psi|\,(\mathrm{Id}_V \otimes U_\varepsilon^\dagger),\ M_\varepsilon^1 := \mathrm{Id}_{BCV} - M_\varepsilon^0$

$M_\varepsilon^0 \longrightarrow$ pass

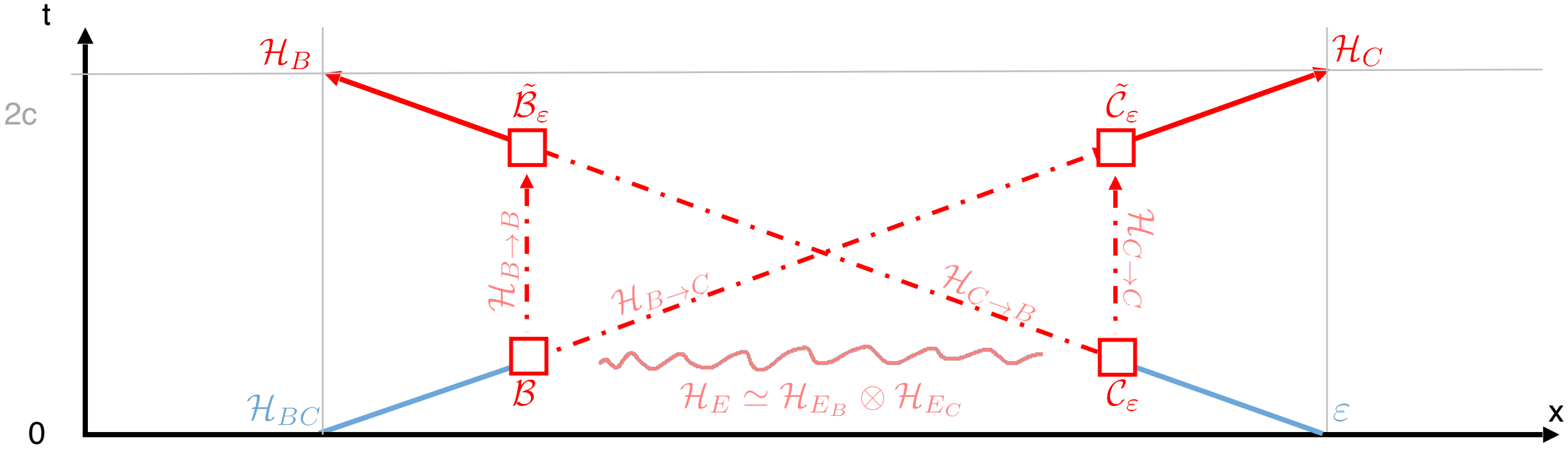
$M_\varepsilon^1 \longrightarrow$ fail

Definition. The *value* achieved by a *strategy* $\{\mathcal{S}_\varepsilon\}_\varepsilon \subset \mathrm{CPTP}(\mathcal{H}_{BC} \to \mathcal{H}_{BC})$ in G_{Rad} is

$$\omega(G_{Rad}; \{\mathcal{S}_\varepsilon\}_\varepsilon) := \mathbb{E}_\varepsilon\ \mathrm{Tr}\, M_\varepsilon^0\, (\mathrm{Id}_V \otimes \mathcal{S}_\varepsilon)(|\psi\rangle\langle\psi|)$$

2. Cheating on $G^{(n)}_{Rad}$.

2. Cheating on $G^{(n)}_{Rad}$.

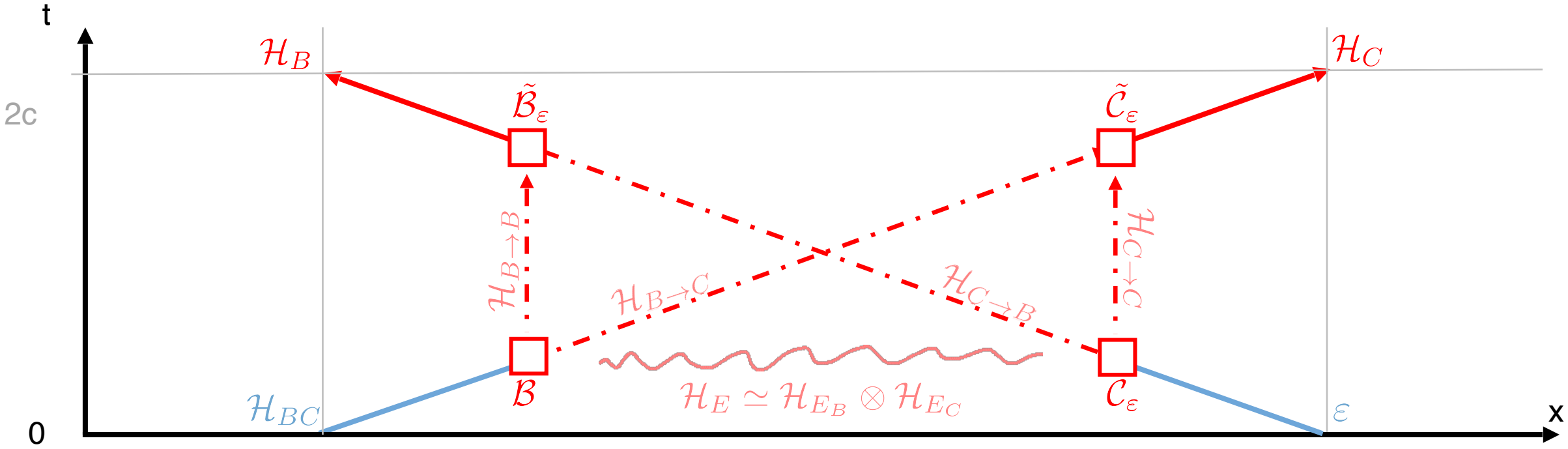


Cheating strategies:

$$\mathcal{S}_\varepsilon(\,\cdot\,) \;=\; (\tilde{\mathcal{B}}_\varepsilon \otimes \tilde{\mathcal{C}}_\varepsilon) \circ (\mathcal{B} \otimes \mathcal{C}_\varepsilon)(\,\cdot \otimes |\varphi\rangle\langle\varphi|) \in \mathrm{CPTP}(\mathcal{H}_{BC} \longrightarrow \mathcal{H}_{BC}) \quad \text{for some} \quad |\varphi\rangle \in \mathcal{H}_E.$$

We call $\mathfrak{S}_{s2w}$ the set of such strategies.

2. Cheating on $G^{(n)}_{Rad}$.



We are interested in the value:

$$\sup_{\mathfrak{S}_{s2w}} \omega(G_{Rad}; \{\mathcal{S}_\varepsilon\}_\varepsilon) = \sup_{\mathfrak{S}_{s2w}} \mathbb{E}_\varepsilon \operatorname{Tr} M^0_\varepsilon (\mathrm{Id}_V \otimes \mathcal{S}_\varepsilon)(|\psi\rangle\langle\psi|).$$

2. Cheating on $G^{(n)}_{Rad}$. Main result.

Main result (informal). *If the cheating strategy depends on* $\varepsilon \in \{\pm 1\}^{n^2}$ *in a sufficiently regular way, then the entanglement needed to pass* $G^{(n)}_{Rad}$ *is exponential in* n.

2. Cheating on $G^{(n)}_{Rad}$. Main result.

A cheating strategy (when "purified") consists of a pair of isometries for both cheaters, corresponding respectively to their first and second operations (after Stinespring dilation).

 $V, \tilde{V}_\varepsilon$  $W_\varepsilon, \tilde{W}_\varepsilon$ and a shared entangled state $|\psi\rangle \in \mathscr{H}_{E_b} \otimes \mathscr{H}_{E_c}$

$$V : \mathcal{H}_{BC} \otimes \mathcal{H}_{E_a} \longrightarrow \mathcal{H}_{B\to B} \otimes \mathcal{H}_{B\to C}, \qquad W_\varepsilon : \mathcal{H}_{E_b} \longrightarrow \mathcal{H}_{C\to C} \otimes \mathcal{H}_{C\to B},$$

$$\tilde{V}_\varepsilon : \mathcal{H}_{B\to B} \otimes \mathcal{H}_{C\to B} \longrightarrow \mathcal{H}_B \otimes \mathcal{H}_{anc}, \qquad \tilde{W}_\varepsilon : \mathcal{H}_{C\to C} \otimes \mathcal{H}_{B\to C} \longrightarrow \mathcal{H}_C \otimes \mathcal{H}_{anc'}.$$

2. Cheating on $G^{(n)}_{Rad}$. Main result.

A cheating strategy (when "purified") consists of a pair of isometries for both cheaters, corresponding respectively to their first and second operations (after Stinespring dilation).

 $V, \tilde{V}_\varepsilon$  $W_\varepsilon, \tilde{W}_\varepsilon$ and a shared entangled state $|\psi\rangle \in \mathscr{H}_{E_b} \otimes \mathscr{H}_{E_c}$

$$V : \mathcal{H}_{BC} \otimes \mathcal{H}_{E_a} \longrightarrow \mathcal{H}_{B\to B} \otimes \mathcal{H}_{B\to C}, \qquad W_\varepsilon : \mathcal{H}_{E_b} \longrightarrow \mathcal{H}_{C\to C} \otimes \mathcal{H}_{C\to B},$$

$$\tilde{V}_\varepsilon : \mathcal{H}_{B\to B} \otimes \mathcal{H}_{C\to B} \longrightarrow \mathcal{H}_B \otimes \mathcal{H}_{anc}, \qquad \tilde{W}_\varepsilon : \mathcal{H}_{C\to C} \otimes \mathcal{H}_{B\to C} \longrightarrow \mathcal{H}_C \otimes \mathcal{H}_{anc'}.$$

k will denote the *maximal local dimension* manipulated in a strategy. That is,

$$\dim(\mathcal{H}_{E_b}),\, \dim(\mathcal{H}_{E_c}) \leq k, \qquad \begin{array}{l} \dim(\mathcal{H}_{B\to B})\, \dim(\mathcal{H}_{C\to B}) \leq k, \\ \dim(\mathcal{H}_{C\to C})\, \dim(\mathcal{H}_{B\to C}) \leq k. \end{array}$$

2. Cheating on $G^{(n)}_{Rad}$. Main result.

Main result (informal). *If the cheating strategy depends on* $\varepsilon \in \{\pm 1\}^{n^2}$ *in a sufficiently regular way, then the entanglement needed to pass* $G^{(n)}_{Rad}$ *is exponential in* n.

2. Cheating on $G_{Rad}^{(n)}$. Main result.

Main result (informal). *If the cheating strategy depends on* $\varepsilon \in \{\pm 1\}^{n^2}$ *in a sufficiently regular way, then the entanglement needed to pass* $G_{Rad}^{(n)}$ *is exponential in* n.

Main result (formal). Given ε, define $\bar{\varepsilon}^{ij} = (\varepsilon_{11}, \ldots, -\varepsilon_{ij}, \ldots, \varepsilon_{nn})$. If there exist $0 < \alpha \leq 1$ s.t.

$$\mathbb{E}_{\varepsilon}\left(\sum_{i,j}\frac{1}{2}\left\|\tilde{V}_{\varepsilon}\otimes\tilde{W}_{\varepsilon}-\tilde{V}_{\bar{\varepsilon}^{ij}}\otimes\tilde{W}_{\bar{\varepsilon}^{ij}}\right\|^{2}\right)^{1/2} \leq \frac{1}{n^{\alpha}}$$

Then $k = \Omega\left(\exp(n^{\alpha})\right)$

2. Cheating on $G_{Rad}^{(n)}$. Main result.

Main result (informal). *If the cheating strategy depends on $\varepsilon \in \{\pm 1\}^{n^2}$ in a sufficiently regular way, then the entanglement needed to pass $G_{Rad}^{(n)}$ is exponential in n.*

Main result (formal). Given ε, define $\bar{\varepsilon}^{ij} = (\varepsilon_{11}, \ldots, -\varepsilon_{ij}, \ldots, \varepsilon_{nn})$. If there exist $0 < \alpha \leq 1$ s.t.

$$\mathbb{E}_{\varepsilon} \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_{\varepsilon} \otimes \tilde{W}_{\varepsilon} - \tilde{V}_{\bar{\varepsilon}^{ij}} \otimes \tilde{W}_{\bar{\varepsilon}^{ij}} \right\|^2 \right)^{1/2} \leq \frac{1}{n^{\alpha}}$$

Then $k = \Omega\left(\exp(n^{\alpha})\right)$

For standard attacks (teleportation and port-based teleportation) LHS = 0

Similar statement for the first operation

Vector valued maps on the Boolean hypercube & type constants

3.

3. Type of Banach spaces.

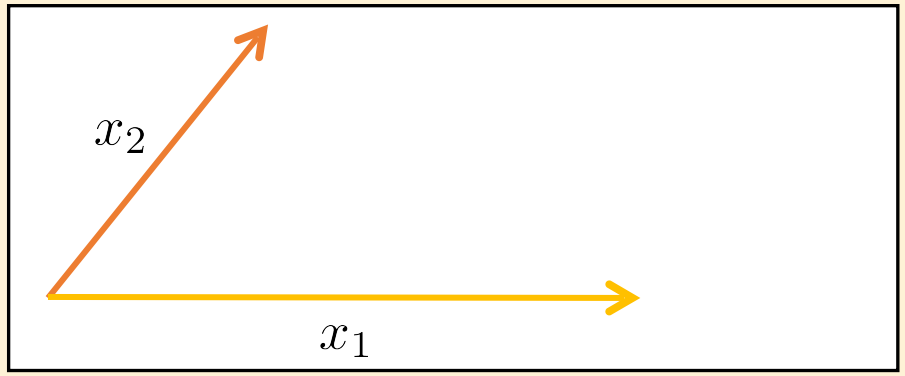
Definition. Given a Banach space X, $\mathrm{T}_2(X)$ is the infimum of the constants T such that

$$\left(\mathbb{E}_\varepsilon \left[\left\|\sum_i \varepsilon_i x_i\right\|_X^2\right]\right)^{1/2} \leq \mathrm{T}\left(\sum_i \|x_i\|_X^2\right)^{1/2},$$

for any finite sequence $\{x_i\}_i$ of elements in X.

Restricting above the cardinal of the sequence $\{x_i\}_i$ to be lower or equal to $m \in \mathbb{N}$, we obtain the type-2 constant of X *with* m *vectors*, $\mathrm{T}_2^{(m)}(X)$.

Example. $m = 2$, X a Hilbert space:



3. Type of Banach spaces.

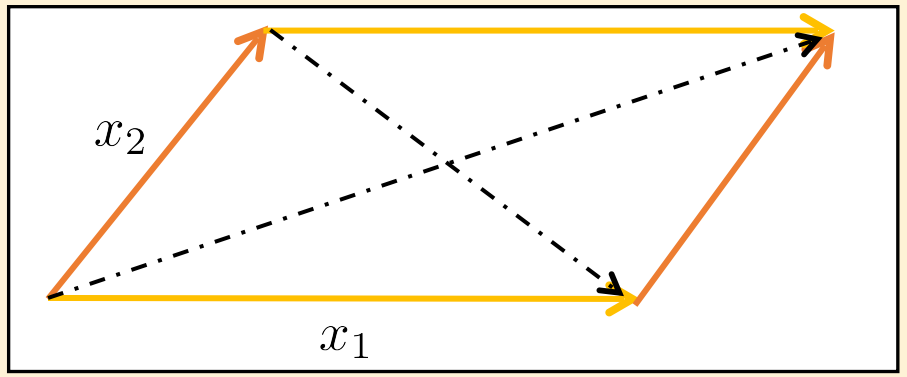
Definition. Given a Banach space X, $\mathrm{T}_2(X)$ is the infimum of the constants T such that

$$\left(\mathbb{E}_\varepsilon \left[\Big\| \sum_i \varepsilon_i x_i \Big\|_X^2\right]\right)^{1/2} \leq \mathrm{T} \left(\sum_i \|x_i\|_X^2\right)^{1/2},$$

for any finite sequence $\{x_i\}_i$ of elements in X.

Restricting above the cardinal of the sequence $\{x_i\}_i$ to be lower or equal to $m \in \mathbb{N}$, we obtain the type-2 constant of X *with* m *vectors*, $\mathrm{T}_2^{(m)}(X)$.

Example. $m = 2$, X a Hilbert space:



$$\|x_1 + x_2\|^2 + \|x_1 - x_2\|^2 = 2\,(\,\|x_1\|^2 + \|x_2\|^2\,)$$

3. Type of Banach spaces.

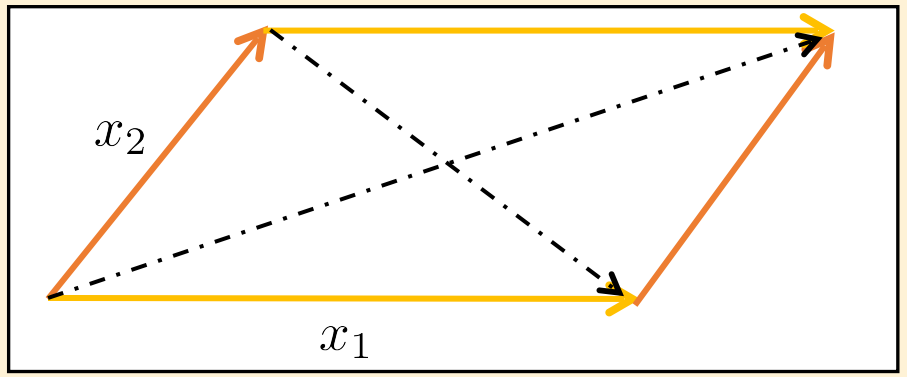
Definition. Given a Banach space X, $\mathrm{T}_2(X)$ is the infimum of the constants T such that

$$\left(\mathbb{E}_\varepsilon \left[\left\|\sum_i \varepsilon_i x_i\right\|_X^2\right]\right)^{1/2} \leq \mathrm{T}\left(\sum_i \|x_i\|_X^2\right)^{1/2},$$

for any finite sequence $\{x_i\}_i$ of elements in X.

Restricting above the cardinal of the sequence $\{x_i\}_i$ to be lower or equal to $m \in \mathbb{N}$, we obtain the type-2 constant of X *with* m *vectors*, $\mathrm{T}_2^{(m)}(X)$.

Example. $m = 2$, X a Hilbert space:



$$\mathbb{E}_\varepsilon \left[\|\varepsilon_1 x_1 + \varepsilon_2 x_2\|^2\right] = \|x_1\|^2 + \|x_2\|^2$$

$$\Downarrow$$

$$\mathrm{T}_2^{(2)}(\mathcal{H}) = 1$$

3. Type of Banach spaces.

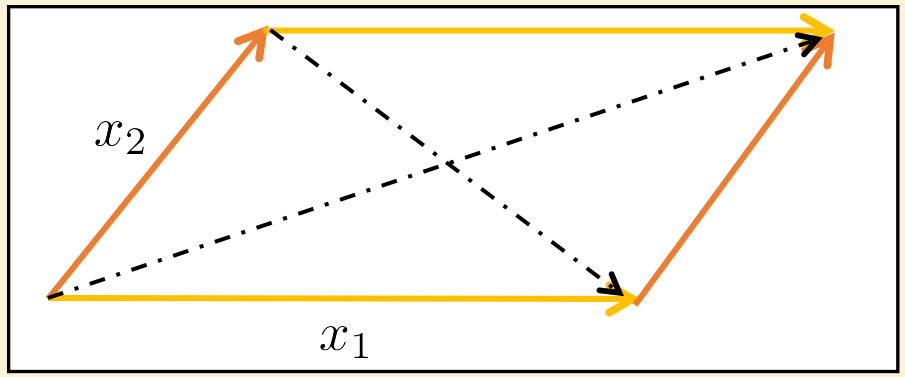
Definition. Given a Banach space X, $\mathrm{T}_2(X)$ is the infimum of the constants T such that

$$\left(\mathbb{E}_\varepsilon \left[\left\|\sum_i \varepsilon_i x_i\right\|_X^2\right]\right)^{1/2} \leq \mathrm{T}\left(\sum_i \|x_i\|_X^2\right)^{1/2},$$

for any finite sequence $\{x_i\}_i$ of elements in X.

Restricting above the cardinal of the sequence $\{x_i\}_i$ to be lower or equal to $m \in \mathbb{N}$, we obtain the type-2 constant of X *with* m *vectors*, $\mathrm{T}_2^{(m)}(X)$.

Example. $m = 2$, X a Hilbert space:



$$\mathrm{T}_2(\mathcal{H}) = 1$$

3. Maps on $\{\pm 1\}^m$.

3. Maps on $\{\pm 1\}^m$.

Definition. Given a map $\Phi : \{\pm 1\}^m \to X$ we define the *regularity* parameter:

$$\sigma_\Phi := \log(m)\, \mathbb{E}_{\varepsilon \in \{\pm 1\}^m} \left(\sum_{i=1}^m \|\partial_i \Phi(\varepsilon)\|_X^2 \right)^{1/2},$$

where $\partial_i \Phi(\varepsilon) := \frac{\Phi(\varepsilon_1,\ldots,\varepsilon_i,\ldots,\varepsilon_m) - \Phi(\varepsilon_1,\ldots,-\varepsilon_i,\ldots,\varepsilon_m)}{2}$ is the discrete derivative on the boolean hypercube in the i-th direction.

3. Maps on $\{\pm 1\}^m$.

Example. Linear maps. Consider $x_1, \dots x_{n^2} \in B_X$ and

$$\begin{array}{rccc} \Phi: & \{\pm 1\}^{n^2} & \longrightarrow & X \\ & \varepsilon & \mapsto & \Phi(\varepsilon) := \frac{1}{n^2} \sum_j \varepsilon_j x_j \end{array} .$$

3. Maps on $\{\pm 1\}^m$.

Example. Linear maps. Consider $x_1, \dots x_{n^2} \in B_X$ and

$$\begin{array}{rccc} \Phi: & \{\pm 1\}^{n^2} & \longrightarrow & X \\ & \varepsilon & \mapsto & \Phi(\varepsilon) := \frac{1}{n^2} \sum_j \varepsilon_j x_j \end{array}.$$

We have that,

$$\partial_i \Phi(\varepsilon) = \frac{1}{2n^2} \left(\sum_j \varepsilon_j x_j - \varepsilon_j (-1)^{\delta_{i,j}} x_j \right) = \frac{1}{n^2} \varepsilon_i \, x_i.$$

And therefore,

$$\sigma_\Phi = \frac{\log(n^2)}{n^2} \left(\sum_i \|x_i\|_X^2 \right)^{\frac{1}{2}} \lesssim \frac{\log(n)}{n}.$$

3. Maps on $\{\pm 1\}^m$.

Definition. Given a map $\Phi : \{\pm 1\}^m \to X$ we define the *regularity* parameter:

$$\sigma_\Phi := \log(m)\, \mathbb{E}_{\varepsilon \in \{\pm 1\}^m} \left(\sum_{i=1}^m \|\partial_i \Phi(\varepsilon)\|_X^2 \right)^{1/2},$$

where $\partial_i \Phi(\varepsilon) := \frac{\Phi(\varepsilon_1,\ldots,\varepsilon_i,\ldots,\varepsilon_m) - \Phi(\varepsilon_1,\ldots,-\varepsilon_i,\ldots,\varepsilon_m)}{2}$ is the discrete derivative on the boolean hypercube in the i-th direction.

3. Maps on $\{\pm 1\}^m$.

Definition. Given a map $\Phi : \{\pm 1\}^m \to X$ we define the *regularity* parameter:

$$\sigma_\Phi := \log(m)\ \mathbb{E}_{\varepsilon\in\{\pm 1\}^m} \left(\sum_{i=1}^m \|\partial_i \Phi(\varepsilon)\|_X^2\right)^{1/2},$$

where $\partial_i \Phi(\varepsilon) := \frac{\Phi(\varepsilon_1,\dots,\varepsilon_i,\dots,\varepsilon_m)-\Phi(\varepsilon_1,\dots,-\varepsilon_i,\dots,\varepsilon_m)}{2}$ is the discrete derivative on the boolean hypercube in the i-th direction.

Lemma (Pisier). Let $p \geq 1$, $\Phi : \{\pm 1\}^m \to X$ and ε, $\tilde{\varepsilon}$ be independent random vectors uniformly distributed on $\{\pm 1\}^m$. Then, for an independent constant C:

$$\mathbb{E}_\varepsilon \left\|\Phi(\varepsilon) - \mathbb{E}_\varepsilon \Phi(\varepsilon)\right\|_X^p \leq (C \log m)^p\ \mathbb{E}_{\varepsilon,\tilde{\varepsilon}} \left\|\sum_i \tilde{\varepsilon}_i \partial_i \Phi(\varepsilon)\right\|_X^p.$$

Corollary *.

$$\mathbb{E}_\varepsilon \left\|\Phi(\varepsilon)\right\|_X \leq \left\|\mathbb{E}_\varepsilon \Phi(\varepsilon)\right\|_X + C\ \sigma_\Phi\ \mathrm{T}_2^{(m)}(X).$$

Bounds under regularity assumptions

4.

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$

Given a cheating strategy $\mathcal{S}$, we define:

$$\begin{array}{rccc} \Phi_{\mathcal{S}}: & \{\pm 1\}^{n^2} & \longrightarrow & M_{k^2} \\ & \varepsilon & \mapsto & \Phi_{\mathcal{S}}(\varepsilon) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \left(\langle i| \tilde{V}_\varepsilon \otimes \langle j| \tilde{W}_\varepsilon \right) \left(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^k} \right) \end{array} .$$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$

Given a cheating strategy $\mathcal{S}$, we define:

$$\begin{array}{rccc} \Phi_{\mathcal{S}}: & \{\pm 1\}^{n^2} & \longrightarrow & M_{k^2} \\ & \varepsilon & \mapsto & \Phi_{\mathcal{S}}(\varepsilon) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \left(\langle i| \tilde{V}_\varepsilon \otimes \langle j| \tilde{W}_\varepsilon \right) \left(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^k} \right) \end{array} .$$

1. $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \mathbb{E}_\varepsilon \left\| \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}}$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$

Given a cheating strategy $\mathcal{S}$, we define:

$$\begin{array}{rccc} \Phi_{\mathcal{S}}: & \{\pm 1\}^{n^2} & \longrightarrow & M_{k^2} \\ & \varepsilon & \mapsto & \Phi_{\mathcal{S}}(\varepsilon) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \left(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon\right)(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^k}) \end{array} .$$

1. $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \mathbb{E}_\varepsilon \left\| \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}}$
2. According to **Corollary ***: $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}} + C\, \sigma_{\Phi_{\mathcal{S}}} T_2^{(n^2)}(M_{k^2})$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$

Given a cheating strategy $\mathcal{S}$, we define:

$$\begin{array}{rccc} \Phi_{\mathcal{S}}: & \{\pm 1\}^{n^2} & \longrightarrow & M_{k^2} \\ & \varepsilon & \mapsto & \Phi_{\mathcal{S}}(\varepsilon) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \left(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon\right)\left(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^k}\right) \end{array} .$$

1. $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \mathbb{E}_\varepsilon \left\| \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}}$
2. According to **Corollary ***: $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}} + C\, \sigma_{\Phi_{\mathcal{S}}} T_2^{(n^2)}(M_{k^2})$
3. $T_2^{(n^2)}(M_{k^2}) \leq T_2(M_{k^2}) \approx \sqrt{\log(k)}$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$

Given a cheating strategy $\mathcal{S}$, we define:

$$\begin{array}{rccc} \Phi_{\mathcal{S}}: & \{\pm 1\}^{n^2} & \longrightarrow & M_{k^2} \\ & \varepsilon & \mapsto & \Phi_{\mathcal{S}}(\varepsilon) = \frac{1}{n^2} \sum_{ij} \varepsilon_{ij} \left(\langle i|\tilde{V}_\varepsilon \otimes \langle j|\tilde{W}_\varepsilon\right)(V|ij\rangle \otimes \mathrm{Id}_{\ell_2^k}) \end{array} .$$

1. $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \mathbb{E}_\varepsilon \left\| \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}}$
2. According to **Corollary ***: $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}} + C\, \sigma_{\Phi_{\mathcal{S}}} T_2^{(n^2)}(M_{k^2})$
3. $T_2^{(n^2)}(M_{k^2}) \leq T_2(M_{k^2}) \approx \sqrt{\log(k)}$
4. **Lemma**: For any cheating strategy $\left\| \mathbb{E}_\varepsilon \Phi_{\mathcal{S}}(\varepsilon) \right\|_{M_{k^2}} \leq \frac{3}{4} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right)$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$.

Combining those estimates, we get

$$\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \frac{3}{4} + C\sqrt{\log(k)}\ \sigma_{\Phi_{\mathcal{S}}} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right)$$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$.

Combining those estimates, we get

$$\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \frac{3}{4} + C\sqrt{\log(k)}\ \sigma_{\Phi_{\mathcal{S}}} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right)$$

So if $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \geq 1 - \delta$, then

$$k = \Omega\left(\ \exp\left(\frac{1}{\sigma_{\Phi_{\mathcal{S}}}}\right)\right)$$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$.

Combining those estimates, we get

$$\omega(G_{\mathrm{Rad}}, \mathcal{S}) \leq \frac{3}{4} + C\sqrt{\log(k)}\ \sigma_{\Phi_{\mathcal{S}}} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right)$$

So if $\omega(G_{\mathrm{Rad}}, \mathcal{S}) \geq 1 - \delta$, then

$$k = \Omega\left(\ \exp\left(\frac{1}{\sigma_{\Phi_{\mathcal{S}}}}\right)\right)$$

The final ingredient is the following **lemma** (we neglect log-factors):

$$\sigma_{\Phi_{\mathcal{S}}} \leq \mathbb{E}_{\varepsilon}\left(\sum_{i,j}\frac{1}{2}\ \left\|\ \tilde{V}_{\varepsilon}\otimes\tilde{W}_{\varepsilon} - \tilde{V}_{\overline{\varepsilon}^{ij}}\otimes\tilde{W}_{\overline{\varepsilon}^{ij}}\ \right\|^2\right)^{1/2} + \mathrm{O}\left(\frac{1}{n}\right)$$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$.

$$k = \Omega\left(\exp\left(\frac{1}{\sigma_{\Phi_{\mathcal{S}}}} \right) \right) \quad , \quad \sigma_{\Phi_{\mathcal{S}}} \leq \mathbb{E}_{\varepsilon} \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_{\varepsilon} \otimes \tilde{W}_{\varepsilon} - \tilde{V}_{\overline{\varepsilon}^{ij}} \otimes \tilde{W}_{\overline{\varepsilon}^{ij}} \right\|^2 \right)^{1/2} + \mathrm{O}\left(\frac{1}{n} \right)$$

4. Cheating strategies as maps on $\{\pm 1\}^{n^2}$

$$k = \Omega\left(\exp\left(\frac{1}{\sigma_{\Phi_{\mathcal{S}}}} \right) \right) \quad , \quad \sigma_{\Phi_{\mathcal{S}}} \leq \mathbb{E}_{\varepsilon} \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_{\varepsilon} \otimes \tilde{W}_{\varepsilon} - \tilde{V}_{\bar{\varepsilon}^{ij}} \otimes \tilde{W}_{\bar{\varepsilon}^{ij}} \right\|^2 \right)^{1/2} + \mathrm{O}\left(\frac{1}{n} \right)$$

Main result. Given ε, define $\bar{\varepsilon}^{ij} = (\varepsilon_{11}, \ldots, -\varepsilon_{ij}, \ldots, \varepsilon_{nn})$. If there exist $0 < \alpha \leq 1$ s.t.

$$\mathbb{E}_{\varepsilon} \left(\sum_{i,j} \frac{1}{2} \left\| \tilde{V}_{\varepsilon} \otimes \tilde{W}_{\varepsilon} - \tilde{V}_{\bar{\varepsilon}^{ij}} \otimes \tilde{W}_{\bar{\varepsilon}^{ij}} \right\|^2 \right)^{1/2} = \mathrm{O}\left(\frac{1}{n^{\alpha}} \right)$$

Then $k = \Omega\left(\exp(n^{\alpha}) \right)$

Towards unconditional bounds | 5.

5. Type constants and tensor norms.

Let us consider the Banach space

$$X_{n,k} = \left[\left(\ell_2^n \otimes_\pi \ell_2^k \right) \otimes_{g_2} \left(\ell_2^n \otimes_\pi \ell_2^k \right) \right] \otimes_\epsilon \ell_2^{k^2}$$

Where ℓ_2^N stands for the N dimensional complex Hilbert space, and π, ϵ, g_2 are three of Grothendieck's natural tensor norms. In particular, those associated to the operator ideals of nuclear, bounded and 2-summing operators respectively.

5. Type constants and tensor norms.

Let us consider the Banach space

$$X_{n,k} = \left[\left(\ell_2^n \otimes_\pi \ell_2^k \right) \otimes_{g_2} \left(\ell_2^n \otimes_\pi \ell_2^k \right) \right] \otimes_\epsilon \ell_2^{k^2}$$

Where ℓ_2^N stands for the N dimensional complex Hilbert space, and π, ϵ, g_2 are three of Grothendieck's natural tensor norms. In particular, those associated to the operator ideals of nuclear, bounded and 2-summing operators respectively.

Lemma:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}) \leq \log(n) \frac{T_2^{(n^2)}(X_{n,k})}{n}$$

5. Type constants and tensor norms.

Let us consider the Banach space

$$X_{n,k} = \left[\left(\ell_2^n \otimes_\pi \ell_2^k \right) \otimes_{g_2} \left(\ell_2^n \otimes_\pi \ell_2^k \right) \right] \otimes_\epsilon \ell_2^{k^2}$$

Where ℓ_2^N stands for the N dimensional complex Hilbert space, and π, ϵ, g_2 are three of Grothendieck's natural tensor norms. In particular, those associated to the operator ideals of nuclear, bounded and 2-summing operators respectively.

Lemma:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}) \leq \log(n) \frac{T_2^{(n^2)}(X_{n,k})}{n}$$

Conjecture:

$$T_2(X_{n,k}) = \mathrm{O}\left(n^\beta \ \mathrm{polylog}(k) \right) \text{ for some } \beta < 1$$

5. Type constants and tensor norms.

Let us consider the Banach space

$$X_{n,k} = \left[\left(\ell_2^n \otimes_\pi \ell_2^k \right) \otimes_{g_2} \left(\ell_2^n \otimes_\pi \ell_2^k \right) \right] \otimes_\epsilon \ell_2^{k^2}$$

Where ℓ_2^N stands for the N dimensional complex Hilbert space, and π, ϵ, g_2 are three of Grothendieck's natural tensor norms. In particular, those associated to the operator ideals of nuclear, bounded and 2-summing operators respectively.

Lemma:

$$\omega(G_{\mathrm{Rad}}; \mathcal{S}) \leq \log(n) \frac{T_2^{(n^2)}(X_{n,k})}{n}$$

$$k = \Omega\left(\exp(n^\alpha)\right)$$

Conjecture:

$$T_2(X_{n,k}) = \mathrm{O}\left(n^\beta \ \mathrm{polylog}(k)\right) \text{ for some } \beta < 1$$

5. Type constants and tensor norms.

Conjecture:

$$T_2(X_{n,k}) = \mathrm{O}\left(n^{\beta}\ \mathrm{polylog}(k)\right) \text{ for some } \beta < 1$$

Supporting evidence. Volume ratio of the dual space $X^*_{n,k}$

Proposition:

$$\mathrm{vrad}\left(X^*_{n,k}\right) = \mathrm{O}\left(n^{\frac{3}{4}}\right)$$

In the context of tensor products of ℓ_p spaces, no known example for which the type-2 constant and the volume ratio of the dual deviates more than a log-factor.

Final remarks | 6.

6. Final remarks.

-. Our Main Theorem implies previous bounds on Programmable Quantum Proccessors [Ku19].

-. PBC was connected with questions about quantum teleportation, complexity theory [Bu13] and even the holographic duality AdS/CFT [Ma20].

Claim [Ma20] (using physics-like reasoning exploiting the properties expected for a good holographic correspondence):

PBC can be broken with k=poly(n)

Which are the implications of our result (conjecture) in holographic duality models of quantum gravity?

- [Ku19] Kubicki, A., Palazuelos, C., Pérez-García, D., arXiv 1805.00756 (2019)
- [Bu13] Burhman, H. etal, arXiv: 1109.2563 (2013)
- [Ma20] May, A., Pennington, G., Sorce, J., arXiv 1912.05649 (2020)

Thank you for your attention.