Device-independent lower bounds on the conditional von Neumann entropy

Peter Brown, Hamza Fawzi and Omar Fawzi

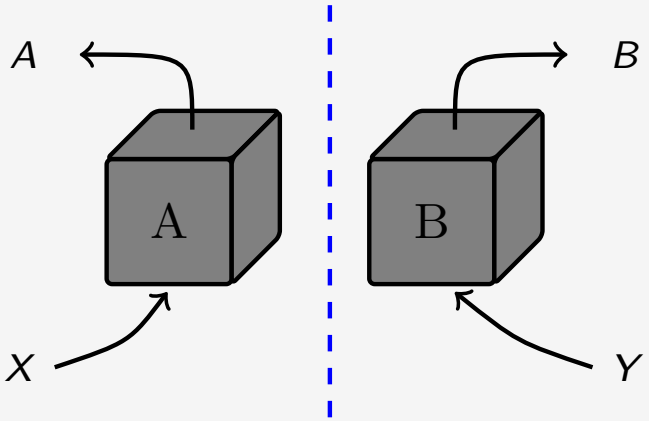
arXiv:2106.13692

April 05 2022

Code available: github.com/peterjbrown519/DI-rates

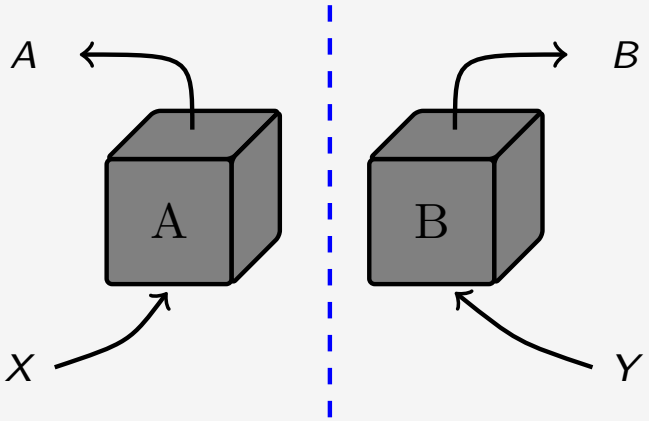
Motivation – Device-independence

Bell-nonlocality



Motivation – Device-independence

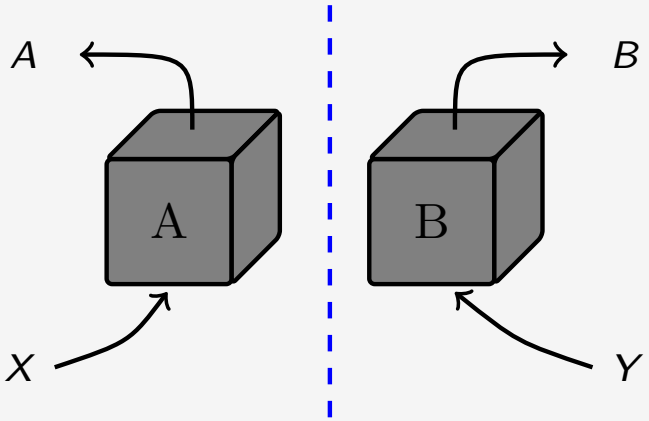
Bell-nonlocality



- Nonlocal correlations are inherently random.

Motivation – Device-independence

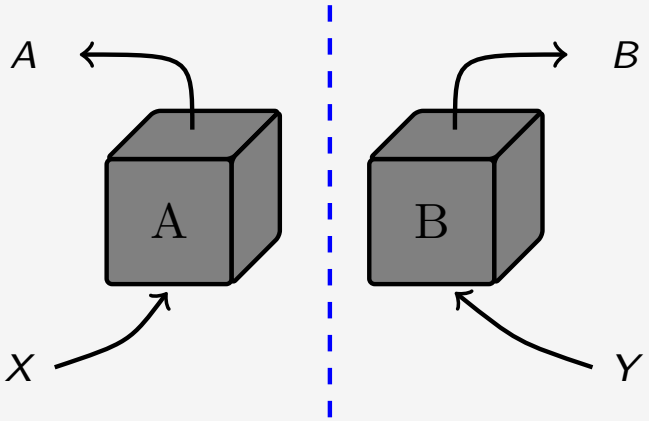
Bell-nonlocality



- Nonlocal correlations are inherently random.
- Foundation for randomness expansion / key-distribution protocols!

Motivation – Device-independence

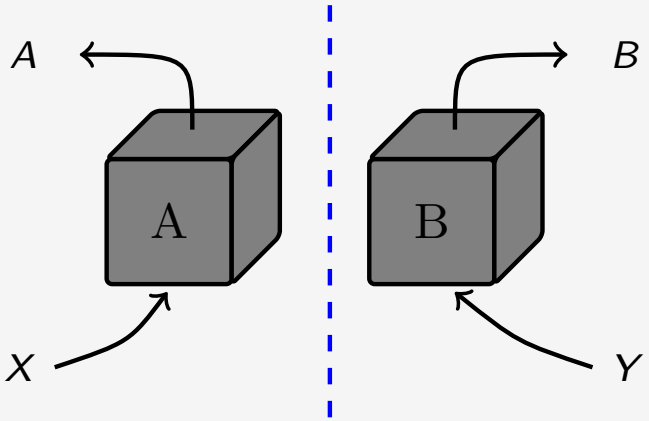
Bell-nonlocality



- Nonlocal correlations are inherently random.
- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on the *rate* (bits per round).

Motivation – Device-independence

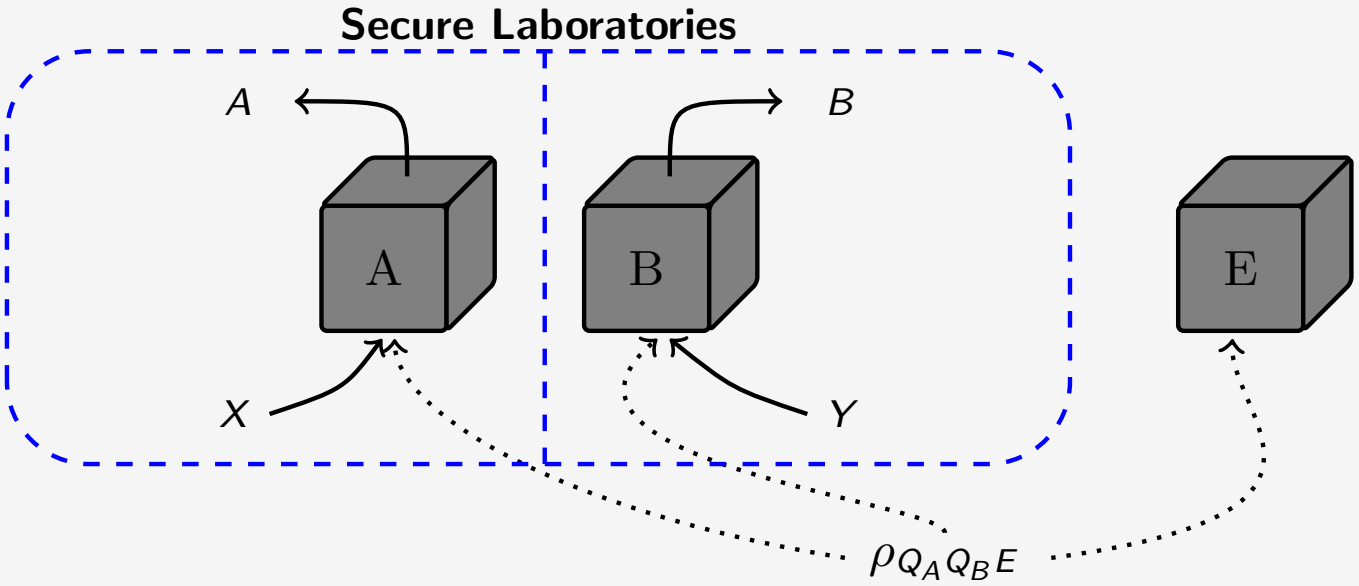
Bell-nonlocality



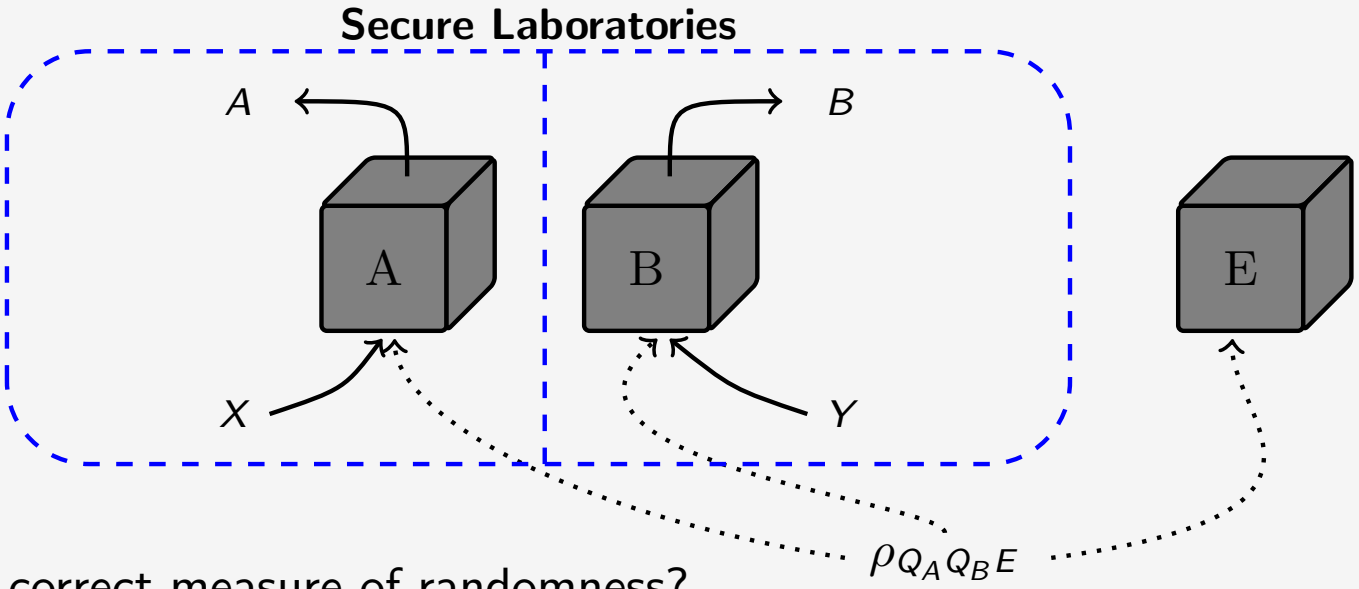
- Nonlocal correlations are inherently random.
- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on the *rate* (bits per round).

Main focus of this work

Randomness generated per round

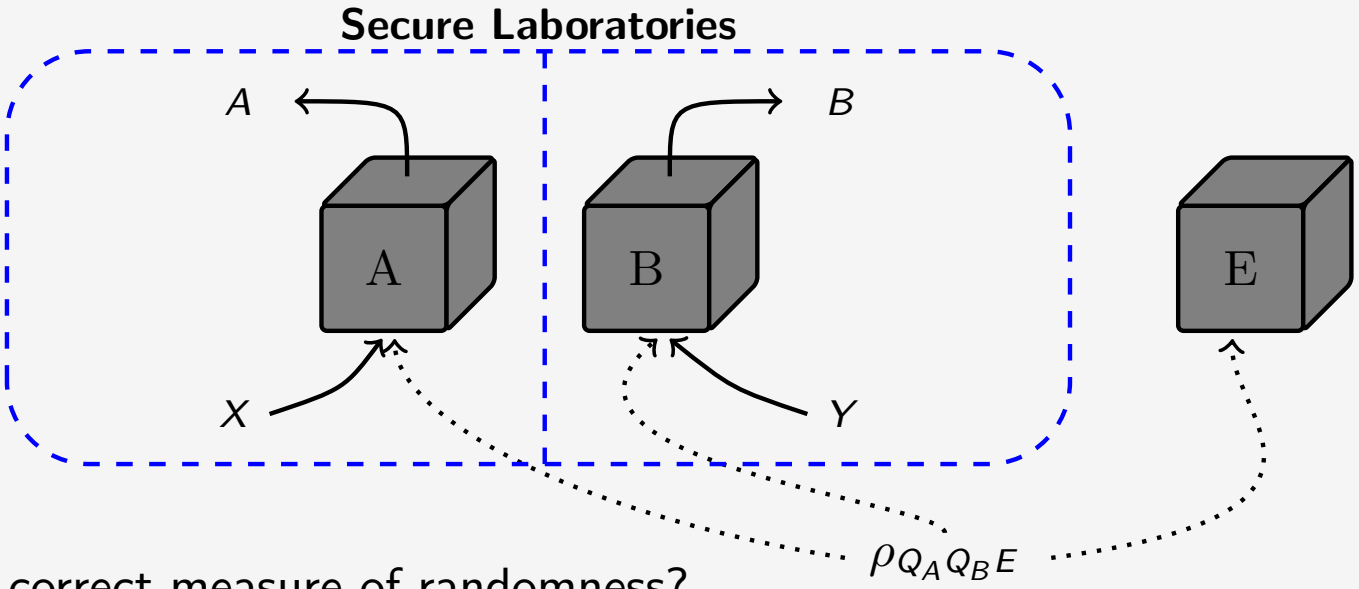


Randomness generated per round



What's the correct measure of randomness?

Randomness generated per round



What's the correct measure of randomness?

(Non-)Asymptotic rates in terms of:

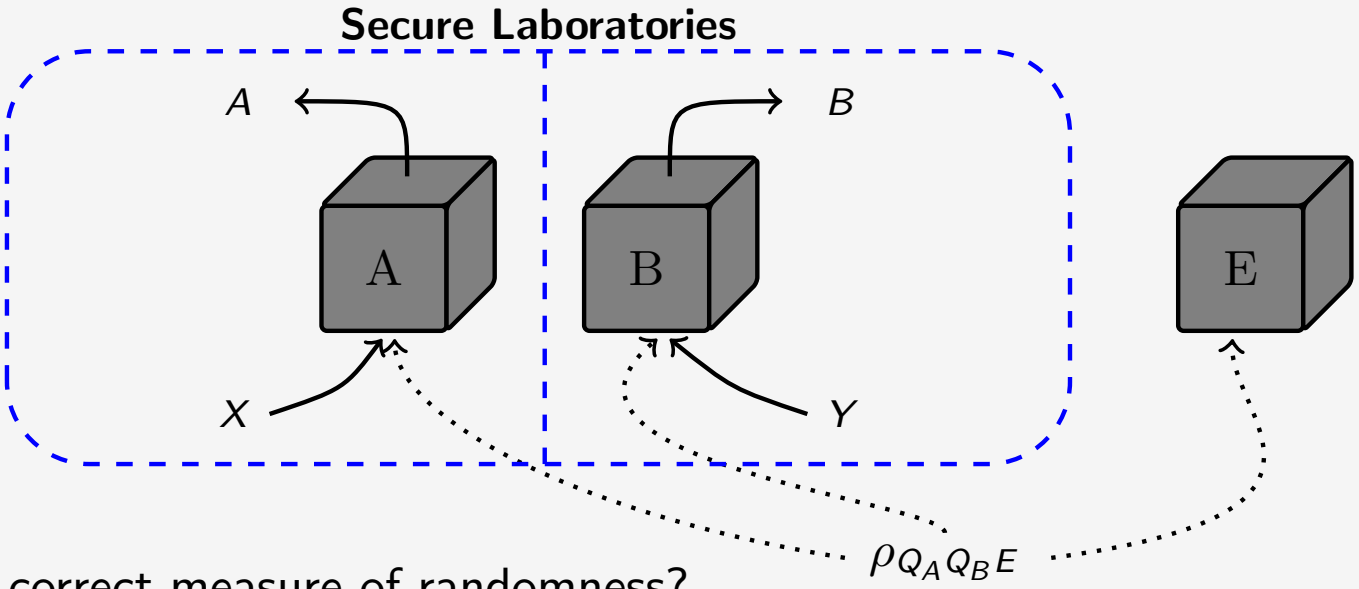
- **Randomness expansion**

$$H(AB|X = x^*, Y = y^*, E)$$

- **QKD**

$$H(A|X = x^*, E) - H(A|X = x^*, Y = y^*, B)$$

Randomness generated per round



What's the correct measure of randomness?

(Non-)Asymptotic rates in terms of:

- **Randomness expansion**

$$H(AB|X = x^*, Y = y^*, E)$$

- **QKD**

$$H(A|X = x^*, E) - H(A|X = x^*, Y = y^*, B)$$

Want device-independent lower bounds

Device-independent lower bounds

Fix some linear constraint(s) C on $p_{AB|XY}$. E.g.

$$\frac{1}{4} \sum_{xy=a\oplus b} p(ab|xy) \geq 0.8\,.$$

Device-independent lower bounds

Fix some linear constraint(s) C on $p_{AB|XY}$. E.g.

$$\frac{1}{4}\sum_{xy=a\oplus b} p(ab|xy) \geq 0.8\,.$$

A **strategy** for C is a tuple $(Q_A Q_B Q_E, \rho, \{\{M_{a|x}\}_a\}_x, \{\{N_{b|y}\}_b\}_y)$ such that

$$p(ab|xy) = \mathrm{Tr}\left[\rho(M_{a|x} \otimes N_{b|y} \otimes I_E)\right]$$

satisfies the constraints in C.

Device-independent lower bounds

Fix some linear constraint(s) C on $p_{AB|XY}$. E.g.

$$\frac{1}{4}\sum_{xy=a\oplus b} p(ab|xy) \geq 0.8\,.$$

A **strategy** for C is a tuple $(Q_A Q_B Q_E, \rho, \{\{M_{a|x}\}_a\}_x, \{\{N_{b|y}\}_b\}_y)$ such that

$$p(ab|xy) = \mathrm{Tr}\left[\rho(M_{a|x} \otimes N_{b|y} \otimes I_E)\right]$$

satisfies the constraints in C.

Post-measurement state

$$\rho_{AQ_E} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}\left[(M_{a|x^*} \otimes I)\rho\right] \longrightarrow H(A|X = x^*, Q_E)$$

Device-independent lower bounds

Fix some linear constraint(s) C on $p_{AB|XY}$. E.g.

$$\frac{1}{4}\sum_{xy=a\oplus b} p(ab|xy) \geq 0.8\,.$$

A **strategy** for C is a tuple $(Q_A Q_B Q_E, \rho, \{\{M_{a|x}\}_a\}_x, \{\{N_{b|y}\}_b\}_y)$ such that

$$p(ab|xy) = \mathrm{Tr}\left[\rho(M_{a|x} \otimes N_{b|y} \otimes I_E)\right]$$

satisfies the constraints in C.

Post-measurement state

$$\rho_{AQ_E} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}\left[(M_{a|x^*} \otimes I)\rho\right] \longrightarrow H(A|X = x^*, Q_E)$$

DI bounds

Want to compute

$$r(C) = \inf \quad H(A|X = x^*, E)$$

where inf over all strategies compatible with C.

Device-independent lower bounds

Fix some linear constraint(s) C on $p_{AB|XY}$. E.g.

$$\frac{1}{4}\sum_{xy=a\oplus b} p(ab|xy) \geq 0.8\,.$$

A **strategy** for C is a tuple $(Q_A Q_B Q_E, \rho, \{\{M_{a|x}\}_a\}_x, \{\{N_{b|y}\}_b\}_y)$ such that

$$p(ab|xy) = \mathrm{Tr}\left[\rho(M_{a|x}\otimes N_{b|y}\otimes I_E)\right]$$

satisfies the constraints in C.

Post-measurement state

$$\rho_{AQ_E} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}\left[(M_{a|x^*}\otimes I)\rho\right] \longrightarrow H(A|X=x^*, Q_E)$$

DI bounds

Want to compute

$$r(C) = \inf \quad H(A|X=x^*, E)$$

where inf over all strategies compatible with C.

Difficult to solve
nonconvex / unbounded dimension

Previous works

Approaches

- Analytical bounds [PAB+09, GMKB21, MPW21]
  - Reduce to qubits and solve explicitly
  - tight bounds / restricted scope

Previous works

Approaches

- Analytical bounds [PAB+09, GMKB21, MPW21]
  - Reduce to qubits and solve explicitly
  - tight bounds / restricted scope
- The min-entropy $H_{\min}$
  - Write as a noncommutative polynomial optimization problem (NPO) and apply NPA.
  - easy to compute / poor bounds

Previous works

Approaches

- Analytical bounds [PAB+09, GMKB21, MPW21]
  - Reduce to qubits and solve explicitly
  - tight bounds / restricted scope
- The min-entropy $H_{\min}$
  - Write as a noncommutative polynomial optimization problem (NPO) and apply NPA.
  - easy to compute / poor bounds
- Recent works [TSG+19, BFF21]
  - Different lower bounding NPOs.
  - Better than $H_{\min}$ / room for improvement

Previous works

Approaches

- Analytical bounds [PAB+09, GMKB21, MPW21]
  - Reduce to qubits and solve explicitly
  - tight bounds / restricted scope
- The min-entropy $H_{\min}$
  - Write as a noncommutative polynomial optimization problem (NPO) and apply NPA.
  - easy to compute / poor bounds
- Recent works [TSG+19, BFF21]
  - Different lower bounding NPOs.
  - Better than $H_{\min}$ / room for improvement
- Our new approach
  - Define a sequence

$$H_m(\rho) = \inf_{Z_1,\ldots,Z_m \in B(H)} \mathrm{Tr}\left[\rho\ q(Z_1,\ldots,Z_m)\right] \tag{1}$$

    such that $H_m \leq H$ and $H_m \to H$ as $m \to \infty$.
  - close to optimal / more efficient / wider scope

Variational forms and NPOs

Idea: Relax to a problem we can approximate...

Variational forms and NPOs

Idea: Relax to a problem we can approximate...

Noncommutative polynomial optimization problems

$$\begin{aligned} \inf \quad & \mathrm{Tr}\left[\rho P(Z_1, \ldots, Z_n)\right] \\ \text{s.t.} \quad & \mathrm{Tr}\left[\rho Q_i(Z_1, \ldots Z_n)\right] \geq w_i \\ & R_i(Z_1, \ldots, Z_n) \geq 0 \end{aligned}$$

infimum over $(\mathcal{H}, \rho, Z_1, \ldots, Z_n)$.

Variational forms and NPOs

Idea: Relax to a problem we can approximate...

Noncommutative polynomial optimization problems

$$\begin{aligned} \inf \quad & \mathrm{Tr}\left[\rho P(Z_1, \ldots, Z_n)\right] \\ \text{s.t.} \quad & \mathrm{Tr}\left[\rho Q_i(Z_1, \ldots Z_n)\right] \geq w_i \\ & R_i(Z_1, \ldots, Z_n) \geq 0 \end{aligned}$$

infimum over $(\mathcal{H}, \rho, Z_1, \ldots, Z_n)$.

Why?

(Convergent) SDP hierarchy gives lower bounds (NPA hierarchy [PNA10]).

Variational forms and NPOs

Idea: Relax to a problem we can approximate...

Noncommutative polynomial optimization problems

$$\begin{aligned} \inf \quad & \mathrm{Tr}\left[\rho P(Z_1, \ldots, Z_n)\right] \\ \text{s.t.} \quad & \mathrm{Tr}\left[\rho Q_i(Z_1, \ldots Z_n)\right] \geq w_i \\ & R_i(Z_1, \ldots, Z_n) \geq 0 \end{aligned}$$

infimum over $(\mathcal{H}, \rho, Z_1, \ldots, Z_n)$.

Why?

(Convergent) SDP hierarchy gives lower bounds (NPA hierarchy [PNA10]).

Goal:

Search for variational bounds on entropies with an NPO form.

Example: Min-entropy

Consider $H_{\min}(A|E) := -\log P_{\mathrm{guess}}(A|E)$

$H_{\min}(A|E) \leq H(A|E)$

Example: Min-entropy

Consider $H_{\min}(A|E) := -\log P_{\mathrm{guess}}(A|E)$

$H_{\min}(A|E) \leq H(A|E)$

1. For cq-state arising from nonlocal test we have

$$P_{\mathrm{guess}}(A|E) = \max_{Z_a} \sum_a \mathrm{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

Example: Min-entropy

Consider $H_{\min}(A|E) := -\log P_{\text{guess}}(A|E)$

$H_{\min}(A|E) \leq H(A|E)$

1. For cq-state arising from nonlocal test we have

$$P_{\text{guess}}(A|E) = \max_{Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

2. Note $\inf_{strategies} H(A|E) \geq \inf_{strategies} H_{\min}(A|E)$ so compute

$$\max_{strategies + Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

Example: Min-entropy

Consider $H_{\min}(A|E) := -\log P_{\text{guess}}(A|E)$ $\qquad H_{\min}(A|E) \leq H(A|E)$

1. For cq-state arising from nonlocal test we have

$$P_{\text{guess}}(A|E) = \max_{Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

2. Note $\inf_{strategies} H(A|E) \geq \inf_{strategies} H_{\min}(A|E)$ so compute

$$\max_{strategies + Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

3. Relax tensor product to get NPO

$$\begin{aligned} \max_{strategies + Z_a} \quad & \sum_a \text{Tr}\left[\rho_{Q_A E} M_a Z_a\right] \\ \text{s.t.} \quad & [M_a, Z_a] = 0 \\ & + \text{ other constraints} \end{aligned}$$

Example: Min-entropy

Consider $H_{\min}(A|E) := -\log P_{\text{guess}}(A|E)$ $\qquad H_{\min}(A|E) \leq H(A|E)$

1. For cq-state arising from nonlocal test we have

$$P_{\text{guess}}(A|E) = \max_{Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

2. Note $\inf_{strategies} H(A|E) \geq \inf_{strategies} H_{\min}(A|E)$ so compute

$$\max_{strategies + Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

3. Relax tensor product to get NPO

$$\begin{aligned} \max_{strategies + Z_a} \quad & \sum_a \text{Tr}\left[\rho_{Q_A E} M_a Z_a\right] \\ \text{s.t.} \quad & [M_a, Z_a] = 0 \\ & + \text{ other constraints} \end{aligned}$$

4. Apply NPA and compute some SDPs!

Example: Min-entropy

Consider $H_{\min}(A|E) := -\log P_{\text{guess}}(A|E)$

$H_{\min}(A|E) \leq H(A|E)$

1. For cq-state arising from nonlocal test we have

$$P_{\text{guess}}(A|E) = \max_{Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

2. Note $\inf_{strategies} H(A|E) \geq \inf_{strategies} H_{\min}(A|E)$ so compute

$$\max_{strategies + Z_a} \sum_a \text{Tr}\left[\rho_{Q_A E}(M_a \otimes Z_a)\right]$$

3. Relax tensor product to get NPO

$$\begin{aligned} \max_{strategies + Z_a} \quad & \sum_a \text{Tr}\left[\rho_{Q_A E} M_a Z_a\right] \\ \text{s.t.} \quad & [M_a, Z_a] = 0 \\ & + \text{ other constraints} \end{aligned}$$

4. Apply NPA and compute some SDPs!

Rule of thumb:
$H_{\min}$ applicable $\implies$ Our bounds applicable
(not iff)

Generalization: relative entropy bounds

We actually work with the relative entropy

$$D(\rho\|\sigma) = \mathrm{Tr}\left[\rho(\log\rho - \log\sigma)\right].$$

Generalization: relative entropy bounds

We actually work with the relative entropy

$$D(\rho\|\sigma) = \mathrm{Tr}\left[\rho(\log\rho - \log\sigma)\right].$$

Can use it for conditional entropy

$$H(A|B) = -D(\rho_{AB}\|I_A \otimes \rho_B).$$

Generalization: relative entropy bounds

We actually work with the relative entropy

$$D(\rho\|\sigma) = \mathrm{Tr}\left[\rho(\log\rho - \log\sigma)\right].$$

Can use it for conditional entropy

$$H(A|B) = -D(\rho_{AB}\|I_A \otimes \rho_B).$$

The goal

Derive something of the form

$$D(\rho\|\sigma) \leq c_m + \sup_Z \mathrm{Tr}\left[\rho p_m(Z)\right] + \mathrm{Tr}\left[\sigma q_m(Z)\right]$$

with p_m and q_m some polynomials and with the RHS converging as $m \to \infty$.

Generalization: relative entropy bounds

We actually work with the relative entropy

$$D(\rho\|\sigma) = \mathrm{Tr}\left[\rho(\log\rho - \log\sigma)\right].$$

Can use it for conditional entropy

$$H(A|B) = -D(\rho_{AB}\|I_A \otimes \rho_B).$$

The goal

Know $D(\rho\|\sigma) = \sup_{(X,Y,z)\in\mathcal{F}} \mathrm{Tr}\left[\rho X\right] + \mathrm{Tr}\left[\sigma Y\right] + z$

Derive something of the form

$$D(\rho\|\sigma) \leq c_m + \sup_Z \mathrm{Tr}\left[\rho p_m(Z)\right] + \mathrm{Tr}\left[\sigma q_m(Z)\right]$$

with p_m and q_m some polynomials and with the RHS converging as $m \to \infty$.

Derivation overview

1. Gauss-Radau approximation of the logarithm

$$\ln(x) = \int_0^1 \frac{x-1}{t(x-1)+1} \mathrm{d}t \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

where $f_t(x) = \frac{x-1}{t(x-1)+1}$.

Derivation overview

1. Gauss-Radau approximation of the logarithm

$$\ln(x) = \int_0^1 \frac{x-1}{t(x-1)+1} \mathrm{d}t \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

   where $f_t(x) = \frac{x-1}{t(x-1)+1}$.

2. Apply approximation to logarithm in $D(\rho\|\sigma)$

$$D(\rho\|\sigma) \leq \sum_{i=1}^{m} \frac{w_i}{\ln 2} D_{-f_{t_i}}(\rho\|\sigma).$$

Derivation overview

1. Gauss-Radau approximation of the logarithm

$$\ln(x) = \int_0^1 \frac{x-1}{t(x-1)+1}\mathrm{d}t \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

where $f_t(x) = \frac{x-1}{t(x-1)+1}$.

2. Apply approximation to logarithm in $D(\rho\|\sigma)$

$D(\rho\|\sigma) = -\sum_{ij} p_i \log(q_j/p_i)|\langle\psi_i,\phi_j\rangle|^2$

$$D(\rho\|\sigma) \leq \sum_{i=1}^{m} \frac{w_i}{\ln 2} D_{-f_{t_i}}(\rho\|\sigma).$$

Derivation overview

1. Gauss-Radau approximation of the logarithm

$$\ln(x) = \int_0^1 \frac{x-1}{t(x-1)+1} \mathrm{d}t \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

where $f_t(x) = \frac{x-1}{t(x-1)+1}$.

2. Apply approximation to logarithm in $D(\rho\|\sigma)$

$D(\rho\|\sigma) = -\sum_{ij} p_i \log(q_j/p_i)|\langle\psi_i,\phi_j\rangle|^2$

$$D(\rho\|\sigma) \leq \sum_{i=1}^{m} \frac{w_i}{\ln 2} D_{-f_{t_i}}(\rho\|\sigma).$$

3. Each $D_{-f_t}(\rho\|\sigma)$ admits a variational form

$$D_{-f_t}(\rho\|\sigma) = -\frac{1}{t} \inf_{Z\in B(H)} \{\mathrm{Tr}\,[\rho(I + Z + Z^* + (1-t)Z^*Z)] + t\,\mathrm{Tr}\,[\sigma ZZ^*]\}$$

Derivation overview

1. Gauss-Radau approximation of the logarithm

$$\ln(x) = \int_0^1 \frac{x-1}{t(x-1)+1} \mathrm{d}t \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

where $f_t(x) = \frac{x-1}{t(x-1)+1}$.

2. Apply approximation to logarithm in $D(\rho\|\sigma)$

$D(\rho\|\sigma) = -\sum_{ij} p_i \log(q_j/p_i) |\langle \psi_i, \phi_j \rangle|^2$

$$D(\rho\|\sigma) \leq \sum_{i=1}^{m} \frac{w_i}{\ln 2} D_{-f_{t_i}}(\rho\|\sigma).$$

3. Each $D_{-f_t}(\rho\|\sigma)$ admits a variational form

$$D_{-f_t}(\rho\|\sigma) = -\frac{1}{t} \inf_{Z \in B(H)} \{\mathrm{Tr}\,[\rho(I + Z + Z^* + (1-t)Z^*Z)] + t\,\mathrm{Tr}\,[\sigma Z Z^*]\}$$

Main Result

$$D(\rho\|\sigma) \leq -\sum_{i=1}^{m} \frac{w_i}{t_i \ln 2} \inf_{Z \in B(H)} \{\mathrm{Tr}\,[\rho(I + Z + Z^* + (1-t_i)Z^*Z)] + t_i\,\mathrm{Tr}\,[\sigma Z Z^*]\}$$

and RHS converges as $m \to \infty$.

Application: Device-independence

1. Approximate von Neumann entropy with m-th level variational form

$$H(A|B) \geq \inf_{Z_i} \sum_{i=1}^{m} \kappa_i (\mathrm{Tr}\left[\rho_{AB} p_i(Z_i)\right] + \mathrm{Tr}\left[(I_A \otimes \rho_B) q_i(Z_i)\right])$$

Application: Device-independence

1. Approximate von Neumann entropy with m-th level variational form

$$H(A|B) \geq \inf_{Z_i} \sum_{i=1}^{m} \kappa_i (\mathrm{Tr}\left[\rho_{AB} p_i(Z_i)\right] + \mathrm{Tr}\left[(I_A \otimes \rho_B) q_i(Z_i)\right])$$

2. Rate optimization $\inf_{\mathrm{strategies}} H(A|X = x^*, Q_E)$ lower bounded by

$$\inf_{\substack{\textit{strategies} \\ +Z_i}} \sum_{i=1}^{m} \frac{w_i}{t_i \ln 2} \sum_a \mathrm{Tr}\left[\rho_{Q_A Q_E} (M_{a|x^*} \otimes (Z_{a,i} + Z_{a,i}^* + (1-t_i) Z_{a,i}^* Z_{a,i}) + t_i Z_{a,i} Z_{a,i}^*)\right] .$$

Application: Device-independence

1. Approximate von Neumann entropy with m-th level variational form

$$H(A|B) \geq \inf_{Z_i} \sum_{i=1}^{m} \kappa_i(\mathrm{Tr}\left[\rho_{AB} p_i(Z_i)\right] + \mathrm{Tr}\left[(I_A \otimes \rho_B) q_i(Z_i)\right])$$

2. Rate optimization $\inf_{\mathrm{strategies}} H(A|X = x^*, Q_E)$ lower bounded by

$$\inf_{\substack{\mathit{strategies} \\ +Z_i}} \sum_{i=1}^{m} \frac{w_i}{t_i \ln 2} \sum_a \mathrm{Tr}\left[\rho_{Q_A Q_E}(M_{a|x^*} \otimes (Z_{a,i} + Z_{a,i}^* + (1-t_i) Z_{a,i}^* Z_{a,i}) + t_i Z_{a,i} Z_{a,i}^*)\right] .$$

Remarks

- Can now be easily relaxed to an NPO and solved using NPA [PNA10].

Application: Device-independence

1. Approximate von Neumann entropy with m-th level variational form

$$H(A|B) \geq \inf_{Z_i} \sum_{i=1}^{m} \kappa_i(\mathrm{Tr}\left[\rho_{AB} p_i(Z_i)\right] + \mathrm{Tr}\left[(I_A \otimes \rho_B) q_i(Z_i)\right])$$

2. Rate optimization $\inf_{\mathrm{strategies}} H(A|X = x^*, Q_E)$ lower bounded by

$$\inf_{\substack{\textit{strategies} \\ +Z_i}} \sum_{i=1}^{m} \frac{w_i}{t_i \ln 2} \sum_a \mathrm{Tr}\left[\rho_{Q_A Q_E}(M_{a|x^*} \otimes (Z_{a,i} + Z_{a,i}^* + (1-t_i) Z_{a,i}^* Z_{a,i}) + t_i Z_{a,i} Z_{a,i}^*)\right] .$$

Drop $\otimes$ and impose $[M, Z] = 0$.

Remarks

- Can now be easily relaxed to an NPO and solved using NPA [PNA10].

Application: Device-independence

1. Approximate von Neumann entropy with m-th level variational form

$$H(A|B) \geq \inf_{Z_i} \sum_{i=1}^{m} \kappa_i(\mathrm{Tr}\left[\rho_{AB} p_i(Z_i)\right] + \mathrm{Tr}\left[(I_A \otimes \rho_B) q_i(Z_i)\right])$$

2. Rate optimization $\inf_{\mathrm{strategies}} H(A|X = x^*, Q_E)$ lower bounded by

$$\inf_{\substack{\textit{strategies} \\ +Z_i}} \sum_{i=1}^{m} \frac{w_i}{t_i \ln 2} \sum_a \mathrm{Tr}\left[\rho_{Q_A Q_E}(M_{a|x^*} \otimes (Z_{a,i} + Z_{a,i}^* + (1-t_i) Z_{a,i}^* Z_{a,i}) + t_i Z_{a,i} Z_{a,i}^*)\right] .$$

Drop $\otimes$ and impose $[M, Z] = 0$.

Remarks

- Can now be easily relaxed to an NPO and solved using NPA [PNA10].
- NPA hierarchy converges as $\|Z\|$ can be bounded.

Application: Device-independence

1. Approximate von Neumann entropy with m-th level variational form

$$H(A|B) \geq \inf_{Z_i} \sum_{i=1}^{m} \kappa_i(\mathrm{Tr}\left[\rho_{AB} p_i(Z_i)\right] + \mathrm{Tr}\left[(I_A \otimes \rho_B) q_i(Z_i)\right])$$

2. Rate optimization $\inf_{\text{strategies}} H(A|X = x^*, Q_E)$ lower bounded by

$$\inf_{\substack{\text{strategies} \\ +Z_i}} \sum_{i=1}^{m} \frac{w_i}{t_i \ln 2} \sum_a \mathrm{Tr}\left[\rho_{Q_A Q_E}(M_{a|x^*} \otimes (Z_{a,i} + Z_{a,i}^* + (1-t_i) Z_{a,i}^* Z_{a,i}) + t_i Z_{a,i} Z_{a,i}^*)\right] .$$

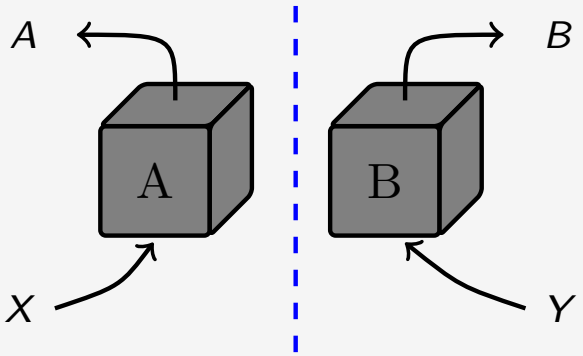
Drop $\otimes$ and impose $[M, Z] = 0$.

Remarks

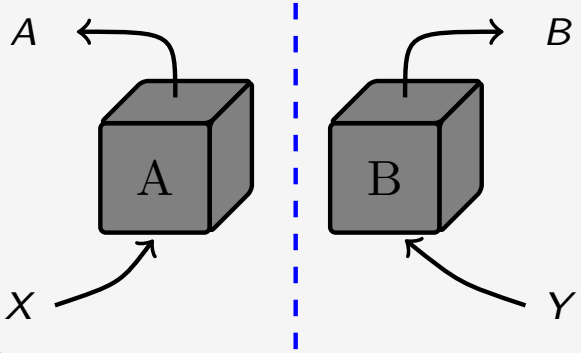
- Can now be easily relaxed to an NPO and solved using NPA [PNA10].
- NPA hierarchy converges as $\|Z\|$ can be bounded.
- Similar results for $H(AB|X = x, Y = y, Q_E)$ or $H(A|XQ_E)$ and others.

Results

- Applied our method to compute rates for DIRNG and DIQKD.



Results



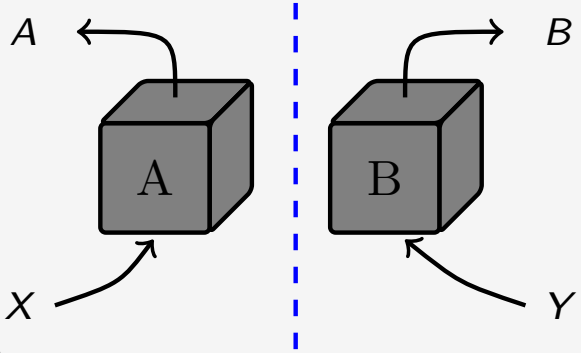
- Applied our method to compute rates for DIRNG and DIQKD.
- Looked at different constraint sets C:
  - CHSH score

$$\frac{1}{4} \sum_{xy=a\oplus b} p(ab|xy) \geq \omega$$

  - Full distribution

$$p(ab|xy) = c_{abxy} \qquad \forall (a, b, x, y)$$

Results



- Applied our method to compute rates for DIRNG and DIQKD.
- Looked at different constraint sets C:
  - CHSH score

$$\frac{1}{4} \sum_{xy=a\oplus b} p(ab|xy) \geq \omega$$

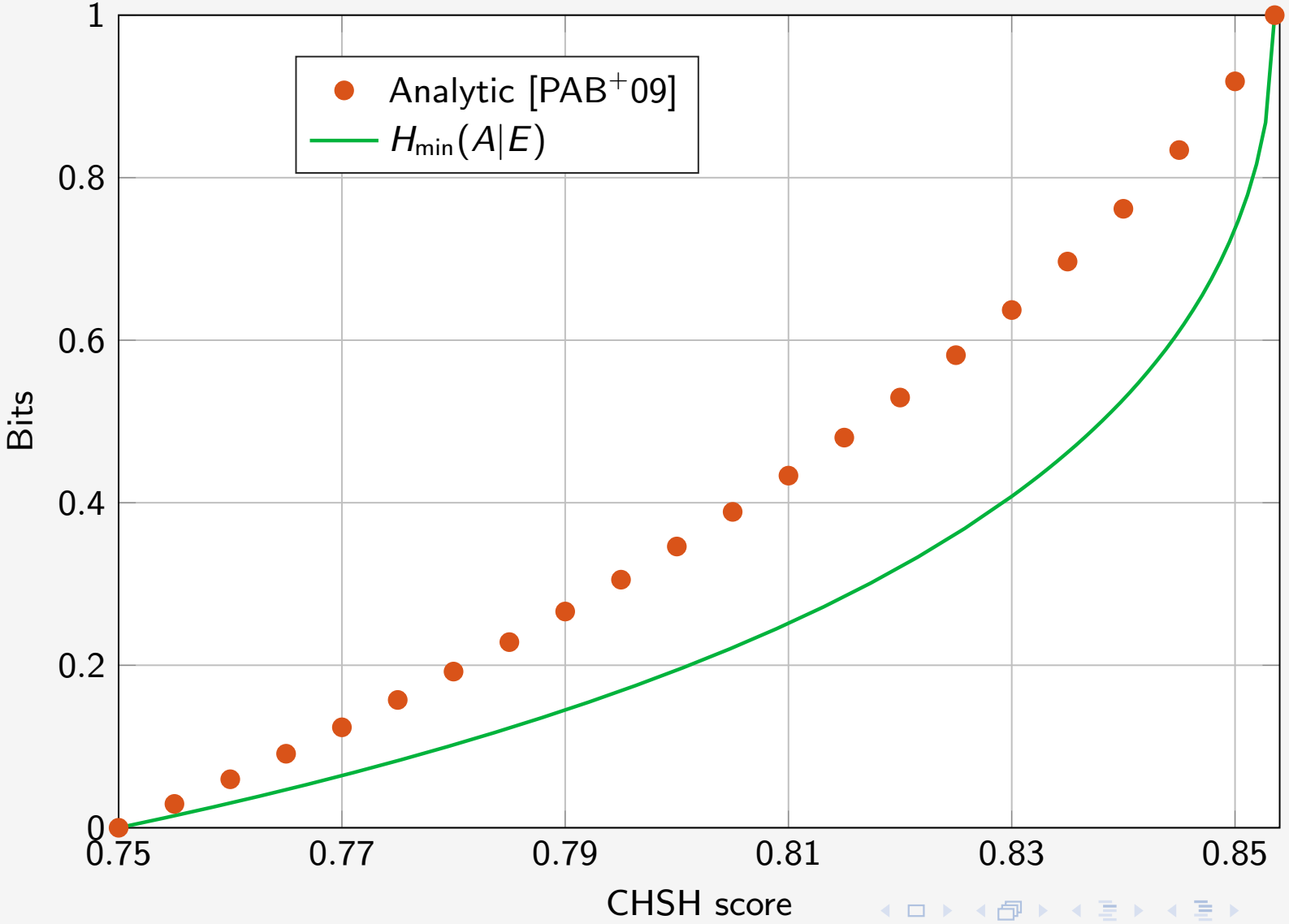
  - Full distribution

$$p(ab|xy) = c_{abxy} \qquad \forall (a,b,x,y)$$

- Investigated *detection efficiency* noise model.
  - Independent probability $\eta \in [0,1]$ that each device *succeeds*.
  - Device failures recorded as a particular outcome.

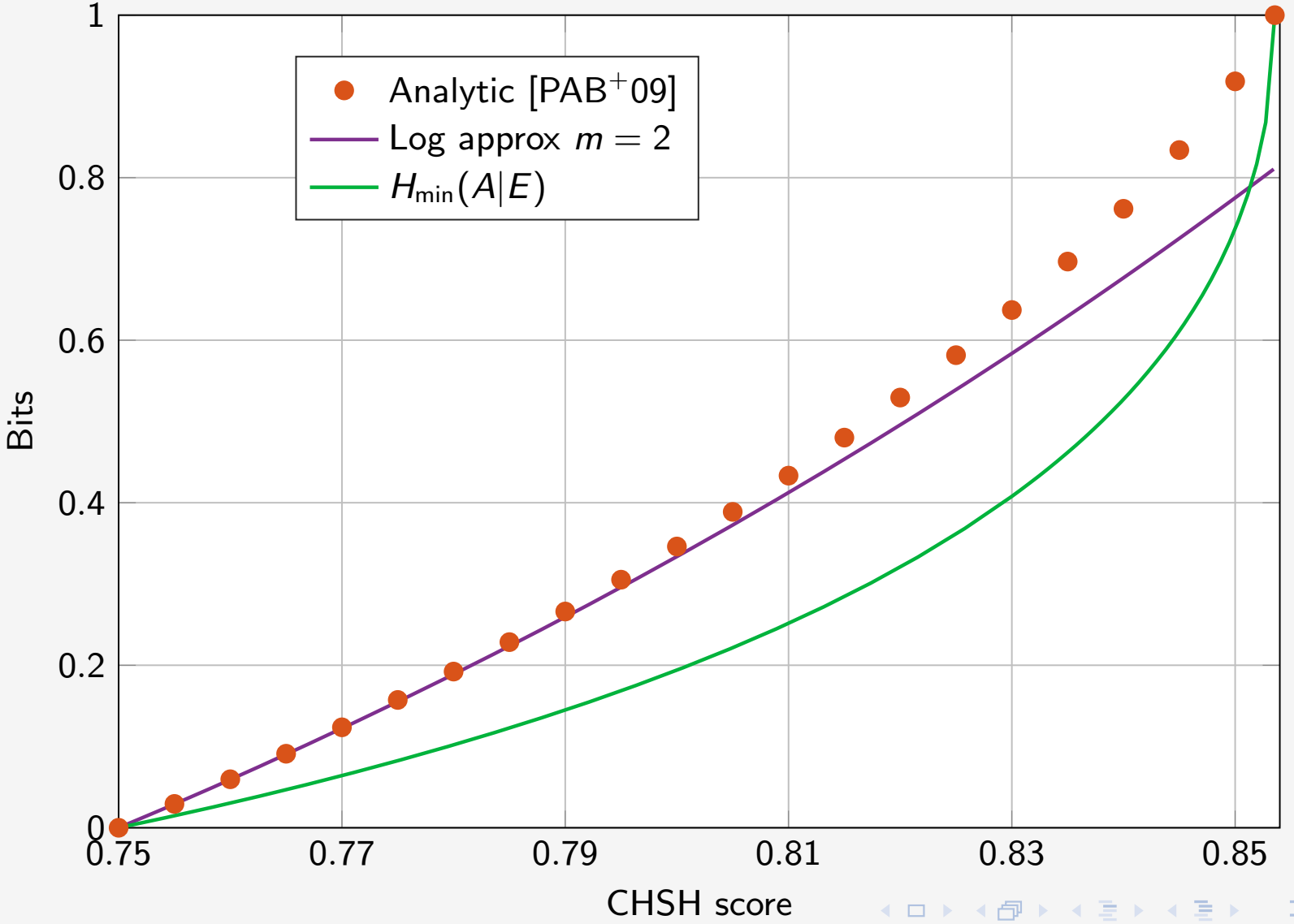
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0, Q_E)$



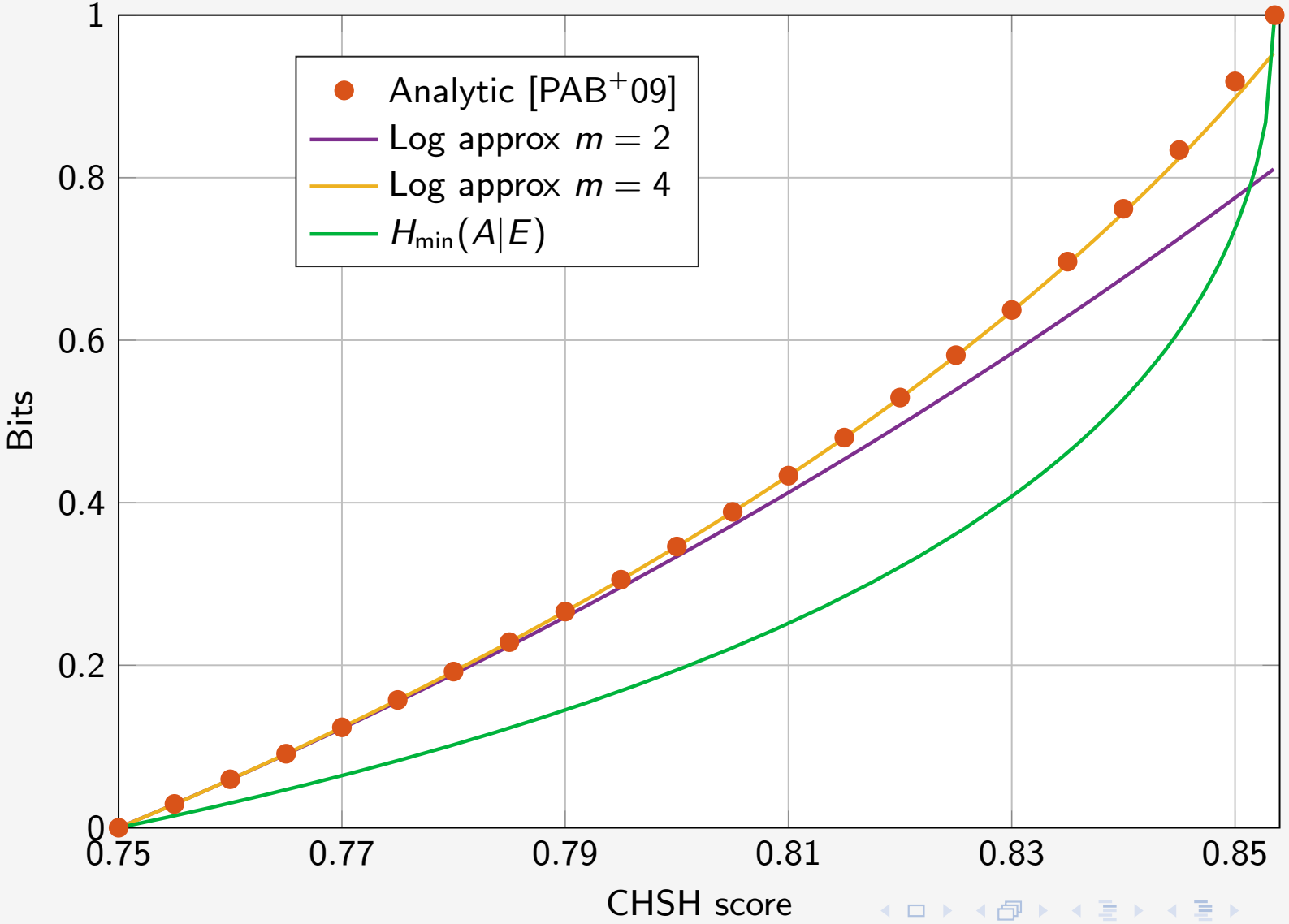
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0, Q_E)$



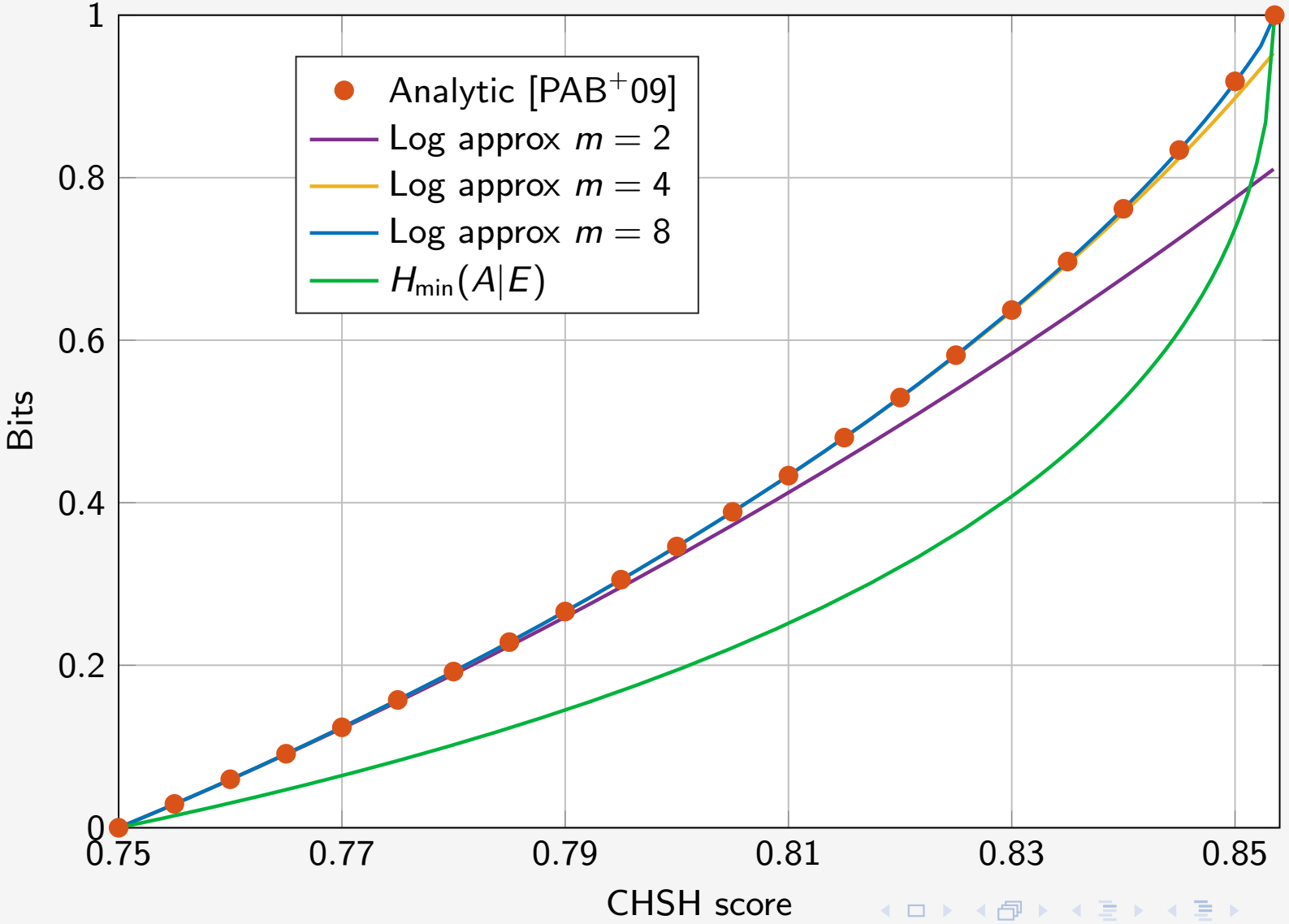
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0, Q_E)$



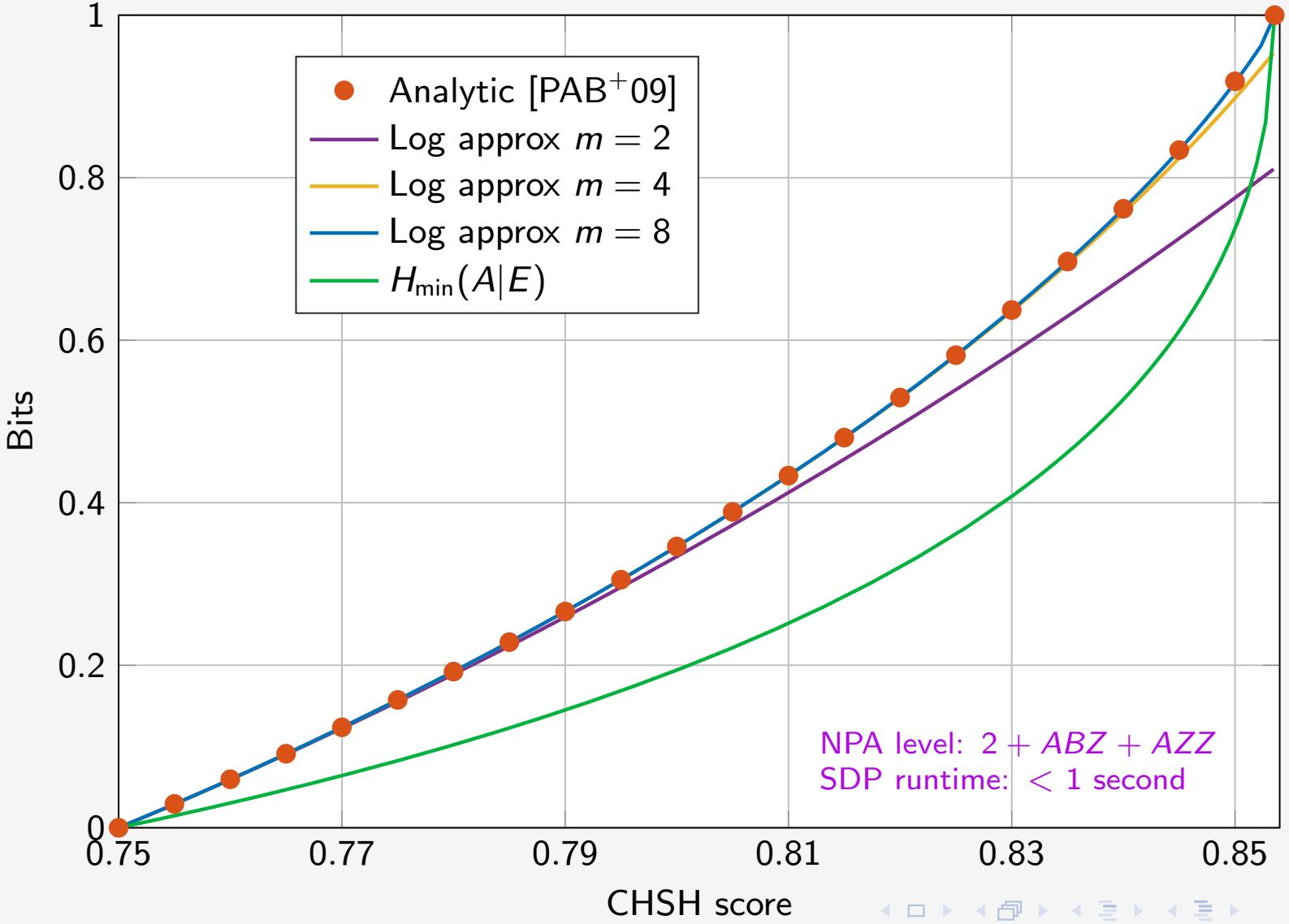
Results I – Recovering tight bounds for the CHSH game

Bounding inf $H(A|X=0, Q_E)$



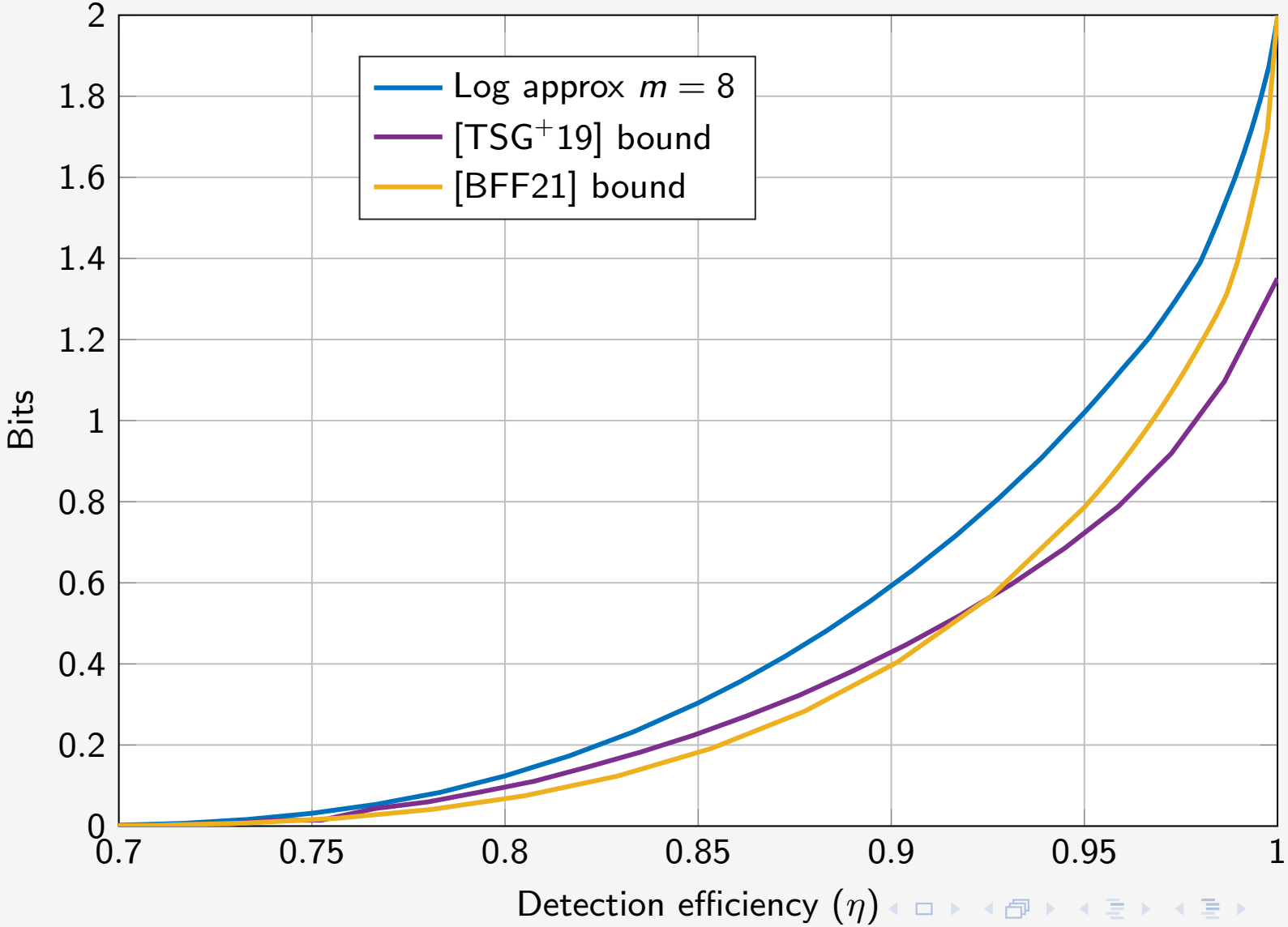
Results I – Recovering tight bounds for the CHSH game

Bounding $\inf H(A|X=0, Q_E)$



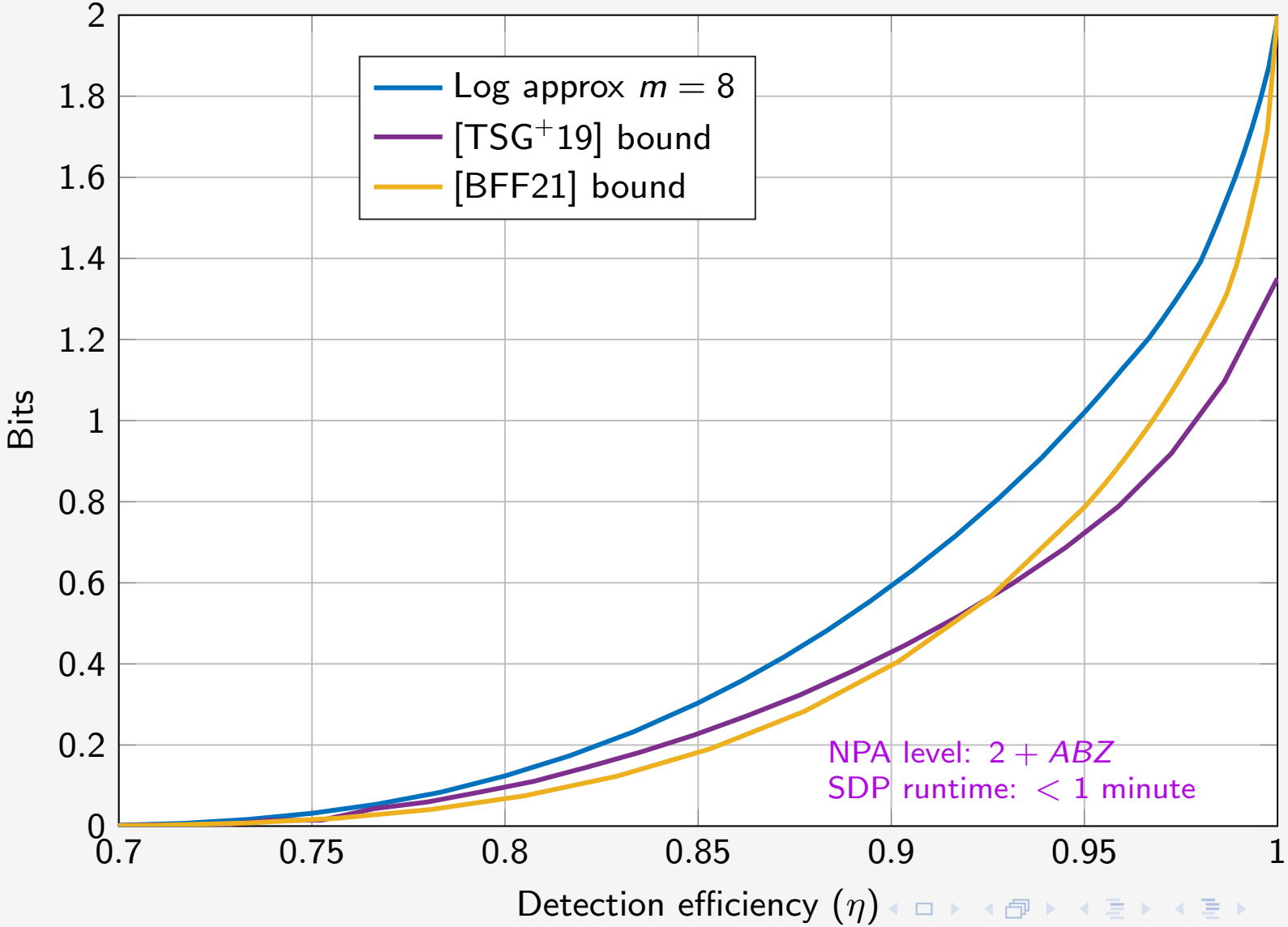
Results II – Improved randomness expansion rates

Bounding $\inf H(AB|X=0, Y=0, Q_E)$



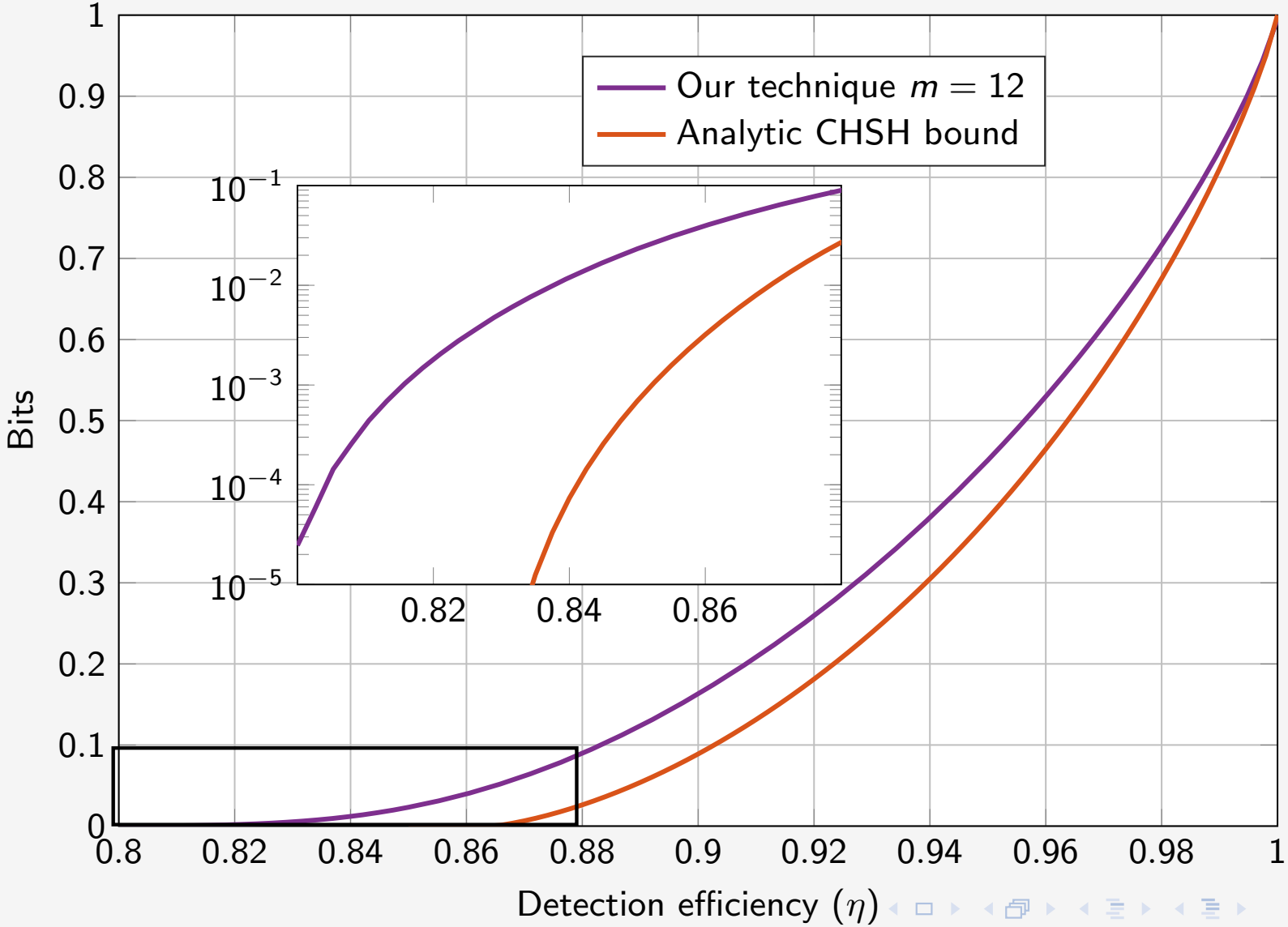
Results II – Improved randomness expansion rates

Bounding $\inf H(AB|X=0, Y=0, Q_E)$



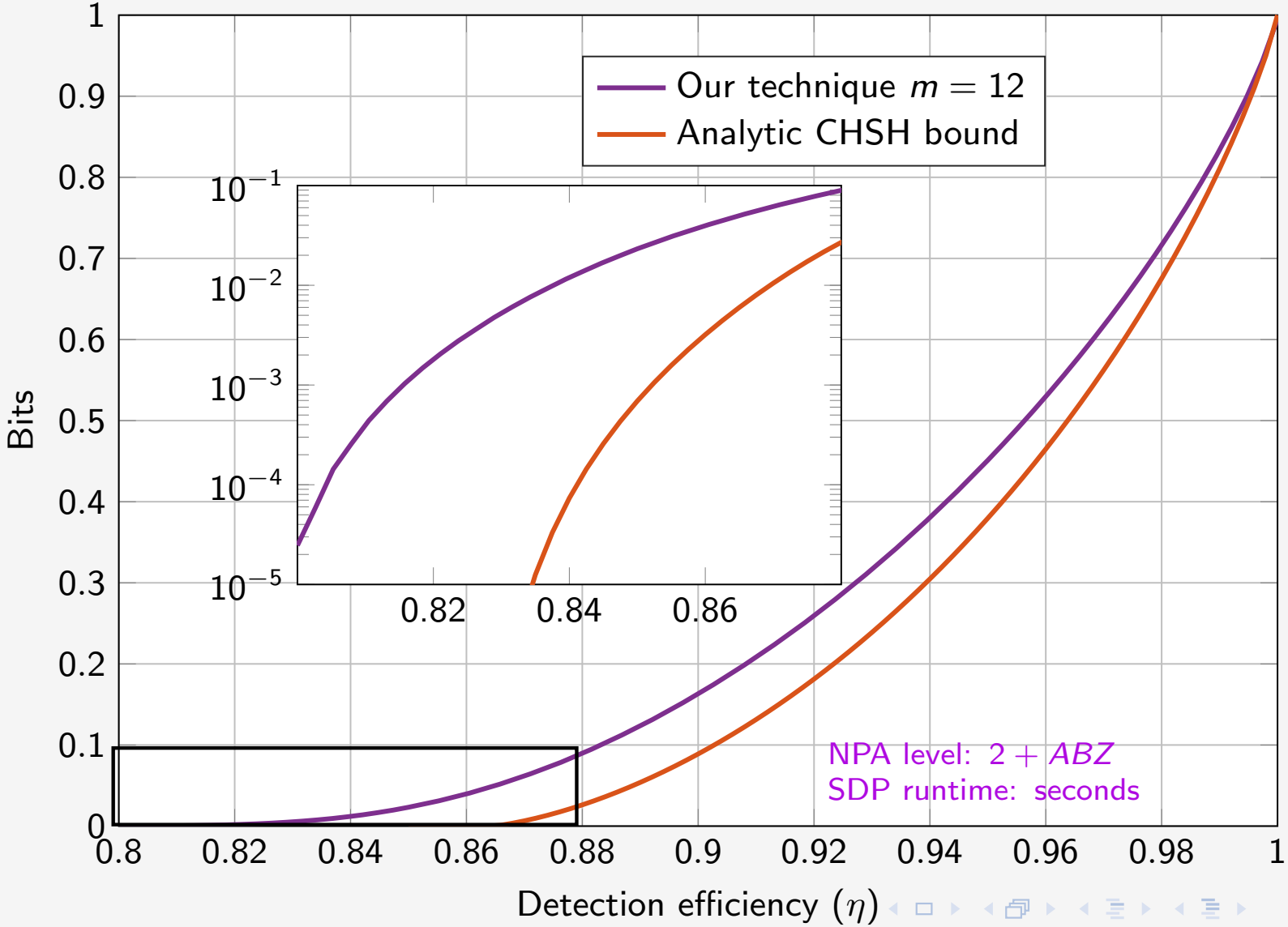
Results III – Improved DIQKD rates

Bounding $\inf H(A|X=0, Q_E) - H(A|X=0, Y=2, B)$



Results III – Improved DIQKD rates

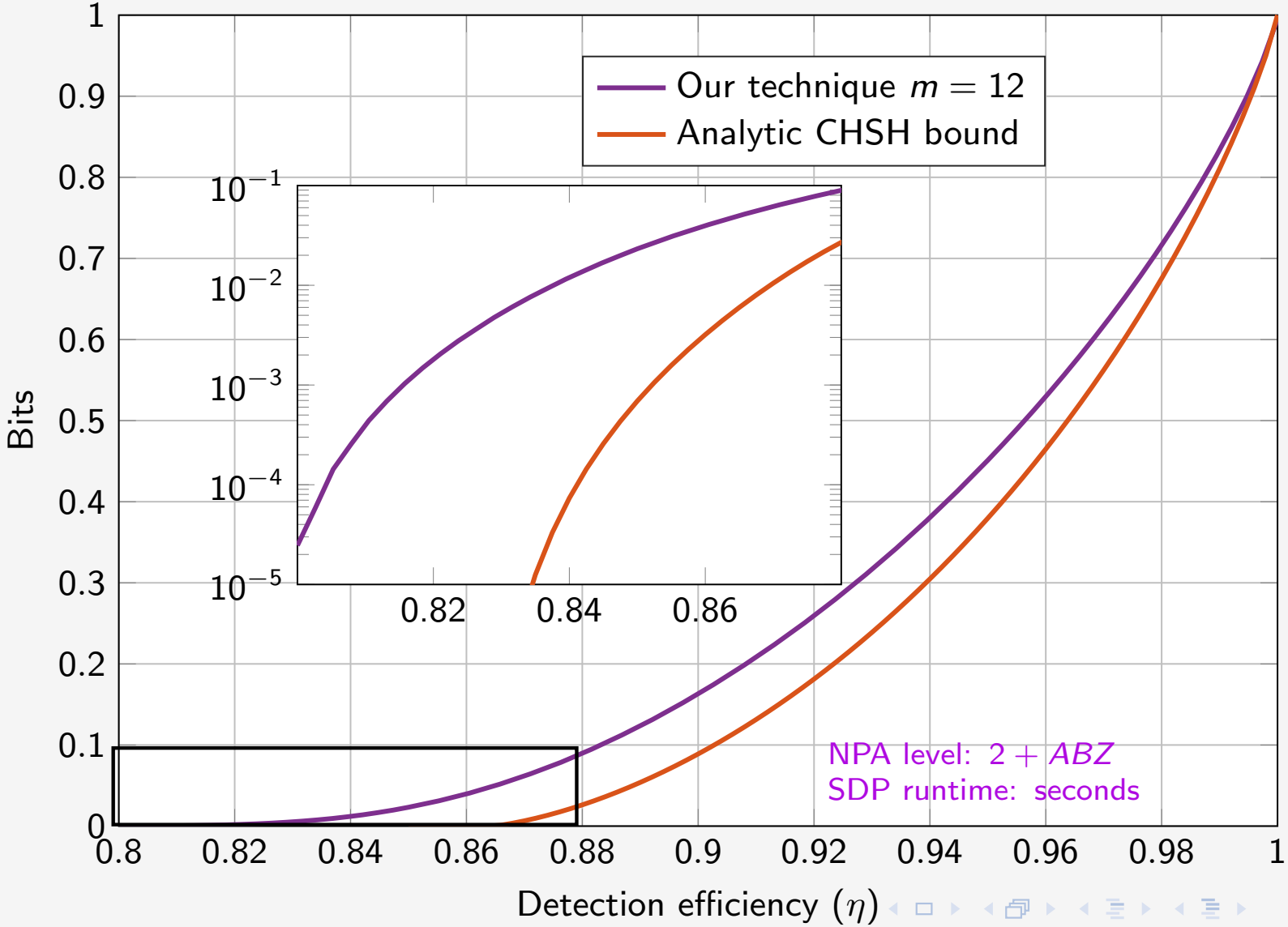
Bounding $\inf H(A|X=0, Q_E) - H(A|X=0, Y=2, B)$



Results III – Improved DIQKD rates

Bounding $\inf H(A|X=0, Q_E) - H(A|X=0, Y=2, B)$

Analytical results
with similar thresholds [MPW21]



Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E)\,.$$

Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E)\,.$$

- Operationally relevant quantity: upper bounds on distillable entanglement / key [Chr06, CEH+07, CSW12, Wil16].

Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E)\,.$$

- Operationally relevant quantity: upper bounds on distillable entanglement / key [Chr06, CEH+07, CSW12, Wil16].
- Many desirable properties: additivity, monotonicity under LOCC, monogamy...

Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E).$$

Difficult to solve
nonconvex / unbounded dimension

- Operationally relevant quantity: upper bounds on distillable entanglement / key [Chr06, CEH+07, CSW12, Wil16].
- Many desirable properties: additivity, monotonicity under LOCC, monogamy...

Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E).$$

Difficult to solve
nonconvex / unbounded dimension

- Operationally relevant quantity: upper bounds on distillable entanglement / key [Chr06, CEH+07, CSW12, Wil16].
- Many desirable properties: additivity, monotonicity under LOCC, monogamy...

Suppose ρ_{ABED} is pure, then

$$I(A:B|E) = H(A|D) + H(A|E)$$

Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E).$$

Difficult to solve
nonconvex / unbounded dimension

- Operationally relevant quantity: upper bounds on distillable entanglement / key [Chr06, CEH+07, CSW12, Wil16].
- Many desirable properties: additivity, monotonicity under LOCC, monogamy...

Suppose ρ_{ABED} is pure, then

$$I(A:B|E) = H(A|D) + H(A|E)$$

$$E_m(A:B) = \inf_{\rho_{ABDE}} H_m(A|D) + H_m(A|E)$$

Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E).$$

Difficult to solve
nonconvex / unbounded dimension

- Operationally relevant quantity: upper bounds on distillable entanglement / key [Chr06, CEH+07, CSW12, Wil16].
- Many desirable properties: additivity, monotonicity under LOCC, monogamy...

Suppose ρ_{ABED} is pure, then

$$I(A:B|E) = H(A|D) + H(A|E)$$

$$E_m(A:B) = \inf_{\rho_{ABDE}} H_m(A|D) + H_m(A|E)$$

m-th variational
lower bound

Application 2: Beyond DI

The squashed entanglement [CW04] for a bipartite state ρ_{AB} is defined as

$$E(A:B) := \inf_{\mathrm{Tr}_E[\rho_{ABE}]=\rho_{AB}} I(A:B|E).$$

Difficult to solve
nonconvex / unbounded dimension

- Operationally relevant quantity: upper bounds on distillable entanglement / key [Chr06, CEH+07, CSW12, Wil16].
- Many desirable properties: additivity, monotonicity under LOCC, monogamy...

Suppose ρ_{ABED} is pure, then

$$I(A:B|E) = H(A|D) + H(A|E)$$

$$E_m(A:B) = \inf_{\rho_{ABDE}} H_m(A|D) + H_m(A|E)$$

m-th variational
lower bound

- SDP lower bounds via NPA hierarchy!

Results - Werner state squashed entanglement

Consider a two-qubit Werner state

$$\rho = p\frac{\Pi_{\mathrm{sym}}}{\mathrm{Tr}\left[\Pi_{\mathrm{sym}}\right]} + (1-p)\frac{\Pi_{\mathrm{asym}}}{\mathrm{Tr}\left[\Pi_{\mathrm{asym}}\right]}$$

with $p \in [0,1]$.

Results - Werner state squashed entanglement

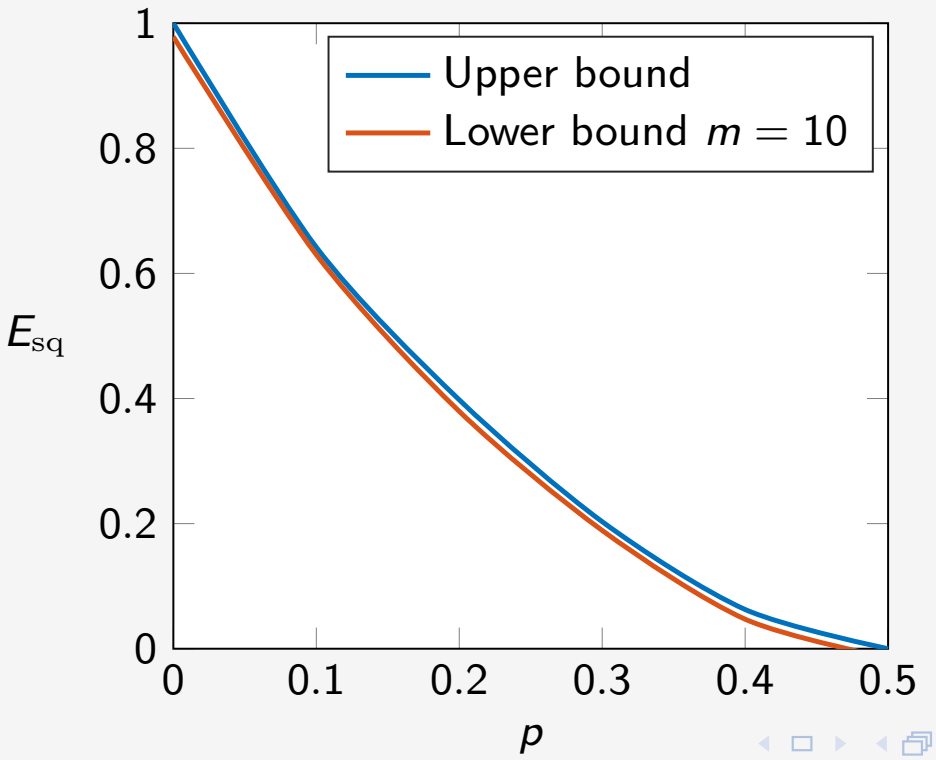
Consider a two-qubit Werner state

$$\rho = p\frac{\Pi_{\mathrm{sym}}}{\mathrm{Tr}\left[\Pi_{\mathrm{sym}}\right]} + (1-p)\frac{\Pi_{\mathrm{asym}}}{\mathrm{Tr}\left[\Pi_{\mathrm{asym}}\right]}$$

with $p \in [0,1]$.

Using variational lower bounds and heuristic upper bounds we find

$$d_A = d_B = 2$$



Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application: Improved lower bounds on DI protocol rates.

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application: Improved lower bounds on DI protocol rates.
- Outperforms previous numerical methods (+ faster).

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application: Improved lower bounds on DI protocol rates.
- Outperforms previous numerical methods (+ faster).
- Can be applied directly to existing security proof techniques

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application: Improved lower bounds on DI protocol rates.
- Outperforms previous numerical methods (+ faster).
- Can be applied directly to existing security proof techniques
- Other applications: Lower bounds on squashed measures

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application: Improved lower bounds on DI protocol rates.
- Outperforms previous numerical methods (+ faster).
- Can be applied directly to existing security proof techniques
- Other applications: Lower bounds on squashed measures

Outlook

- More efficient computations? (symmetries?)

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application: Improved lower bounds on DI protocol rates.
- Outperforms previous numerical methods (+ faster).
- Can be applied directly to existing security proof techniques
- Other applications: Lower bounds on squashed measures

Outlook

- More efficient computations? (symmetries?)
- Convergence of the numerics? (tensor vs commuting)

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application: Improved lower bounds on DI protocol rates.
- Outperforms previous numerical methods (+ faster).
- Can be applied directly to existing security proof techniques
- Other applications: Lower bounds on squashed measures

Outlook

- More efficient computations? (symmetries?)
- Convergence of the numerics? (tensor vs commuting)
- Other applications?

Thanks for your attention

Bibliography

Peter Brown, Hamza Fawzi, and Omar Fawzi.
Computing conditional entropies for quantum correlations.
Nature communications, 12(1):1–12, 2021.

Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Renato Renner.
Unifying classical and quantum key distillation.
In *Theory of Cryptography Conference*, pages 456–478. Springer, 2007.

Matthias Christandl.
The structure of bipartite quantum states-insights from group theory and cryptography.
arXiv preprint quant-ph/0604183, 2006.

Matthias Christandl, Norbert Schuch, and Andreas Winter.
Entanglement of the antisymmetric state.
Communications in Mathematical Physics, 311(2):397–422, 2012.

Matthias Christandl and Andreas Winter.
"squashed entanglement": an additive entanglement measure.
Journal of mathematical physics, 45(3):829–840, 2004.

Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruß.
In preparation.
2021.

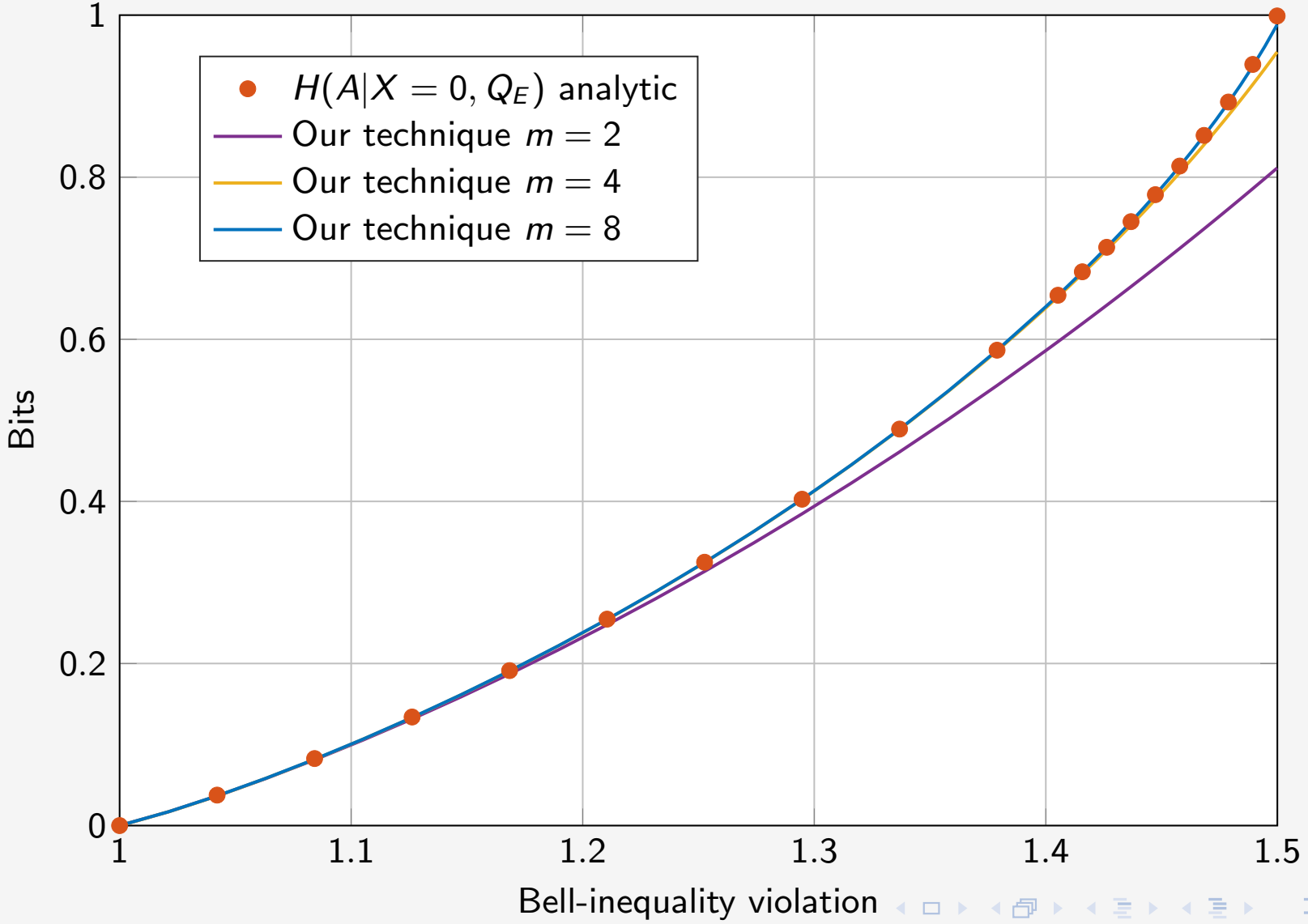
Michele Masini, Stefano Pironio, and Erik Woodhead.
Simple and practical diqkd security analysis via bb84-type uncertainty relations and pauli correlation constraints.
arXiv preprint arXiv:2107.08894, 2021.

Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani.
Device-independent quantum key distribution secure against collective attacks.
New Journal of Physics, 11(4):045021, 2009.

Stefano Pironio, Miguel Navascués, and Antonio Acín.

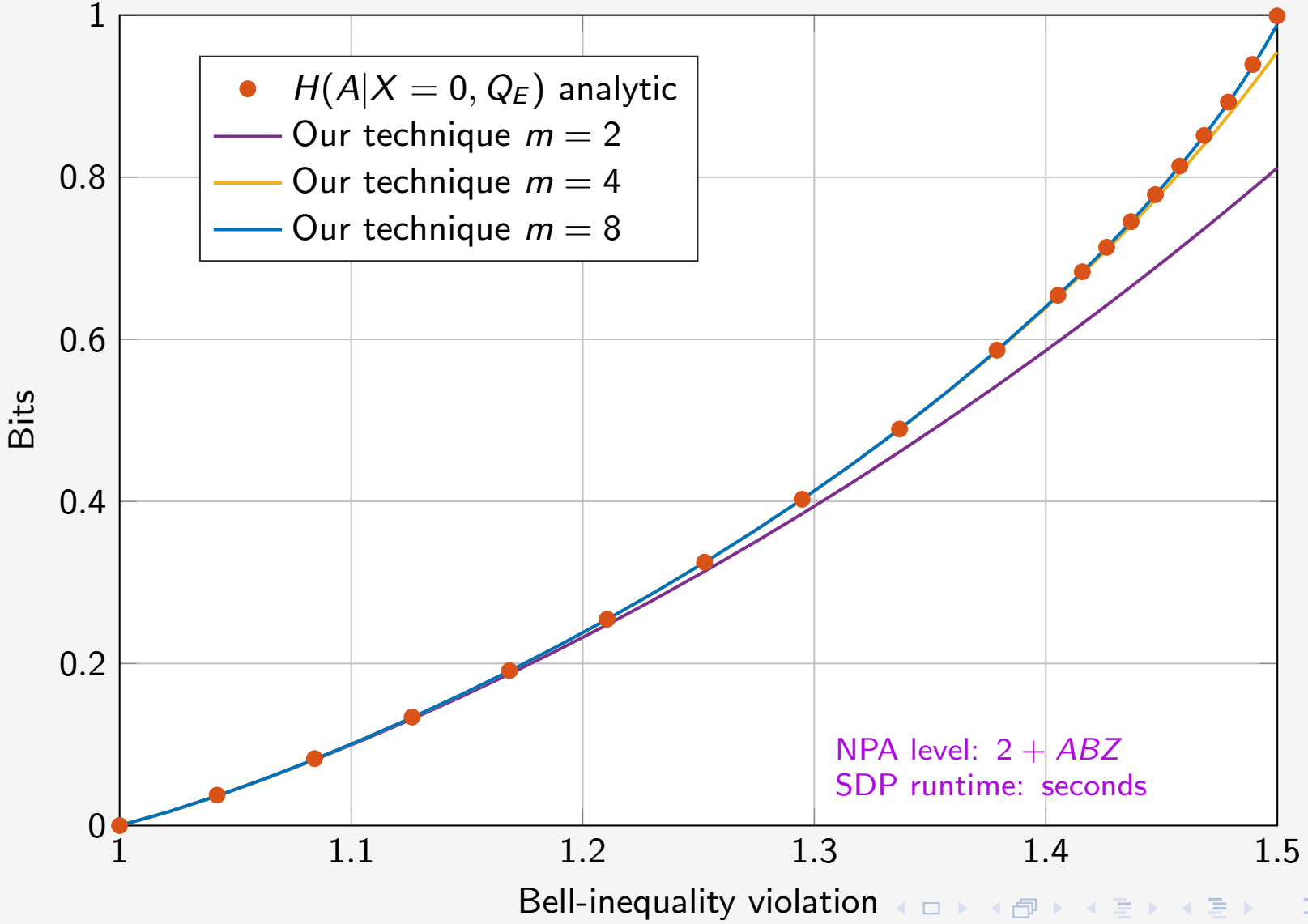
Bonus results – DICKA setting (Holz inequality)

Bounding inf $H(A|X=0, Q_E)$



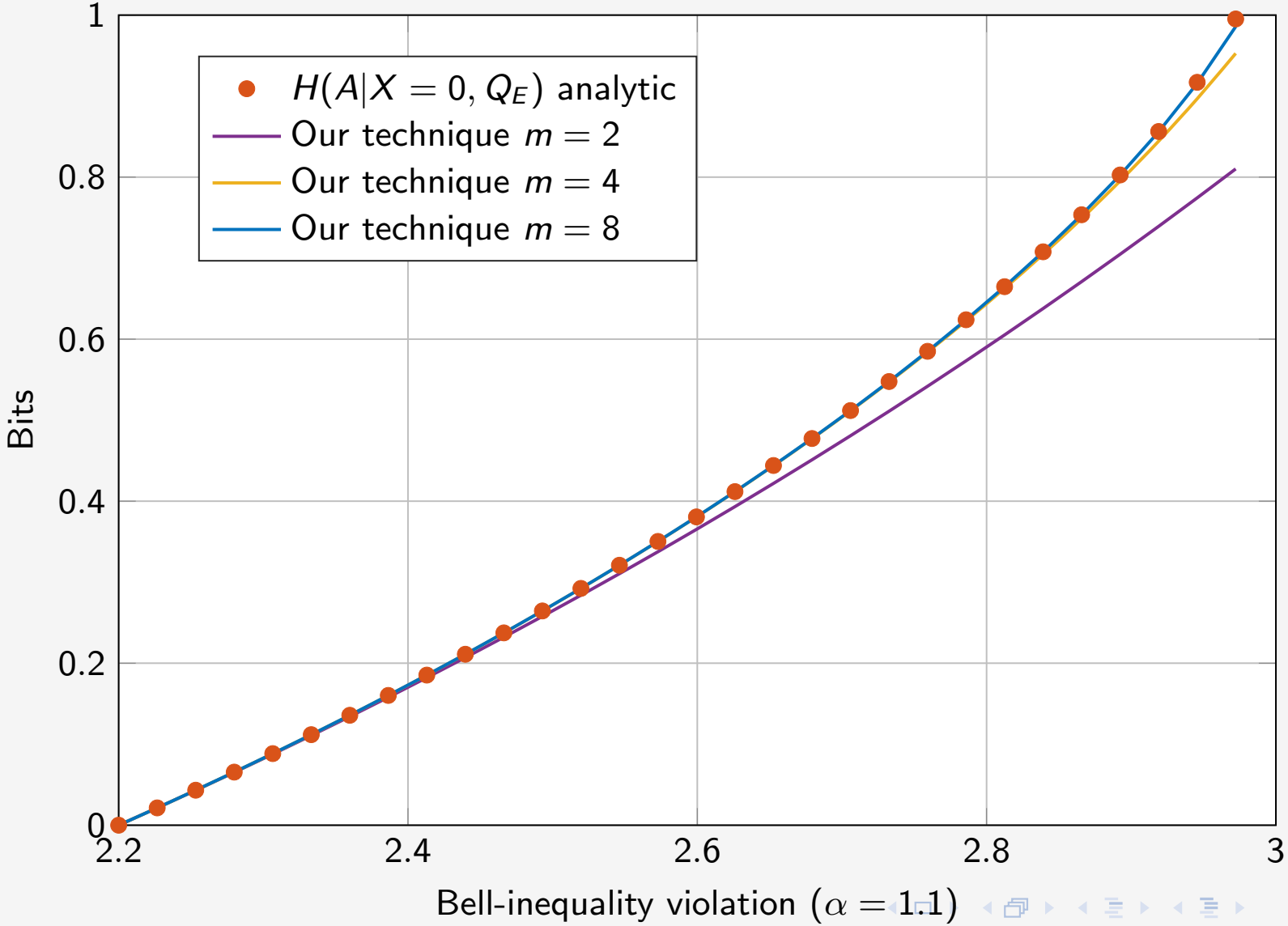
Bonus results – DICKA setting (Holz inequality)

Bounding inf $H(A|X=0, Q_E)$



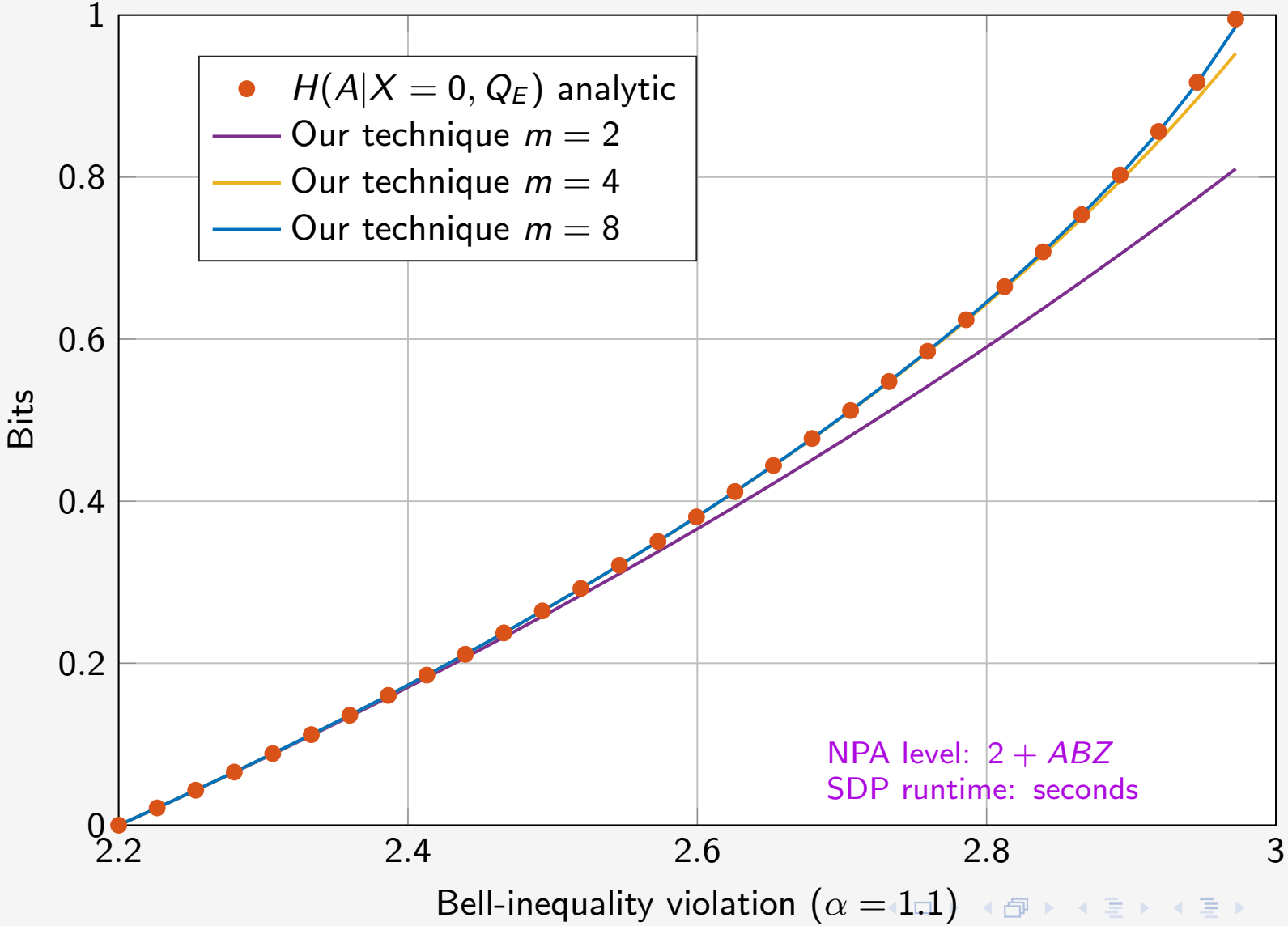
Bonus results – Generalized CHSH ($\alpha = 1.1$)

Bounding inf $H(A|X=0, Q_E)$ $\qquad$ $B_\alpha = \alpha(\langle A_0 B_0\rangle + \langle A_0 B_1\rangle) + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle$



Bonus results – Generalized CHSH ($\alpha = 1.1$)

Bounding inf $H(A|X=0, Q_E)$ $\qquad$ $B_\alpha = \alpha(\langle A_0 B_0\rangle + \langle A_0 B_1\rangle) + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle$



Bonus results – Generalized CHSH ($\alpha = 0.9$)

Bounding inf $H(A|X=0, Q_E)$ $\qquad B_\alpha = \alpha(\langle A_0 B_0\rangle + \langle A_0 B_1\rangle) + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle$