Variational bounds on the relative entropy and their applications

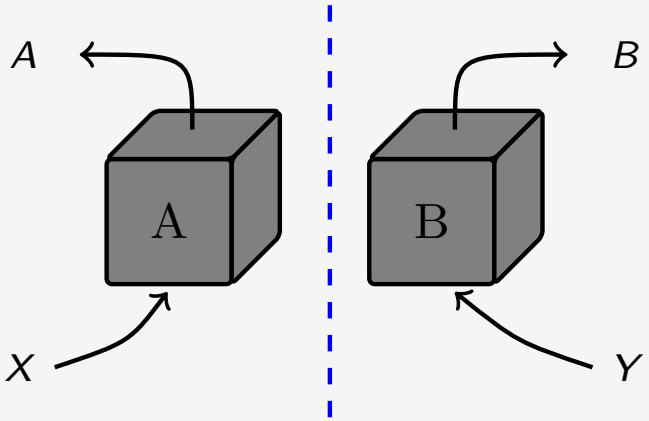
Peter Brown, Hamza Fawzi and Omar Fawzi

Paper 1: arXiv:2106.13692
Paper 2: arXiv this week

Mar 07 2022

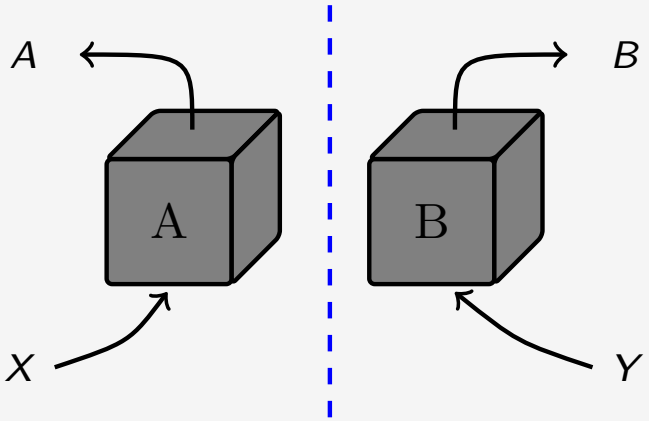
Motivation – Device-independence

Bell-nonlocality



Motivation – Device-independence

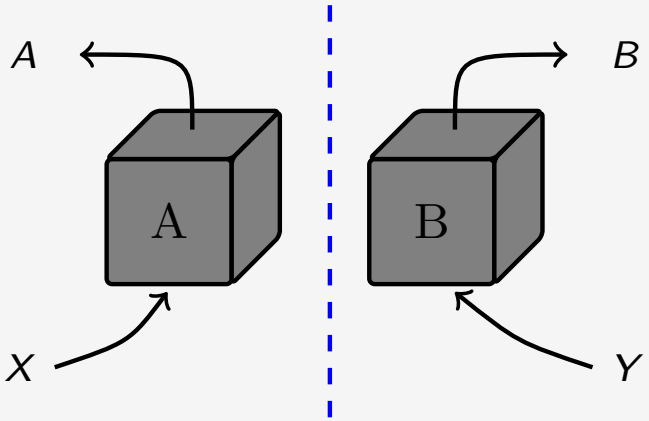
Bell-nonlocality



- Nonlocal correlations are inherently random.

Motivation – Device-independence

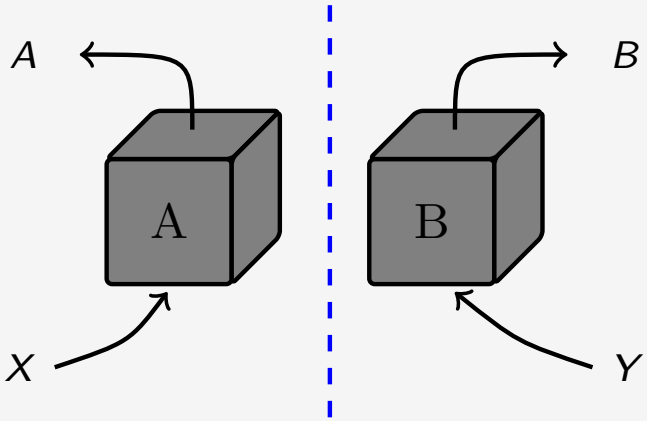
Bell-nonlocality



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

Motivation – Device-independence

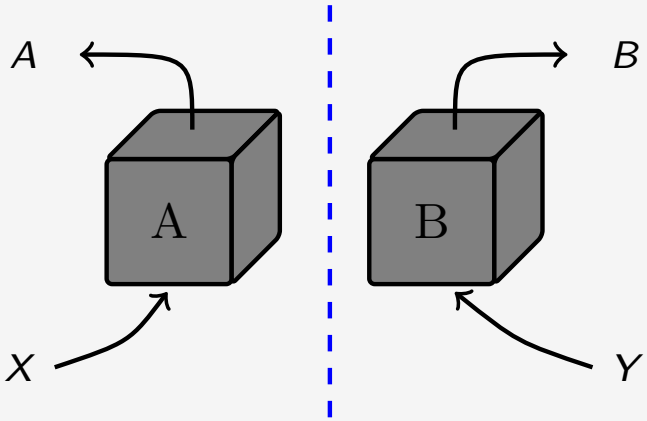
Bell-nonlocality



- 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

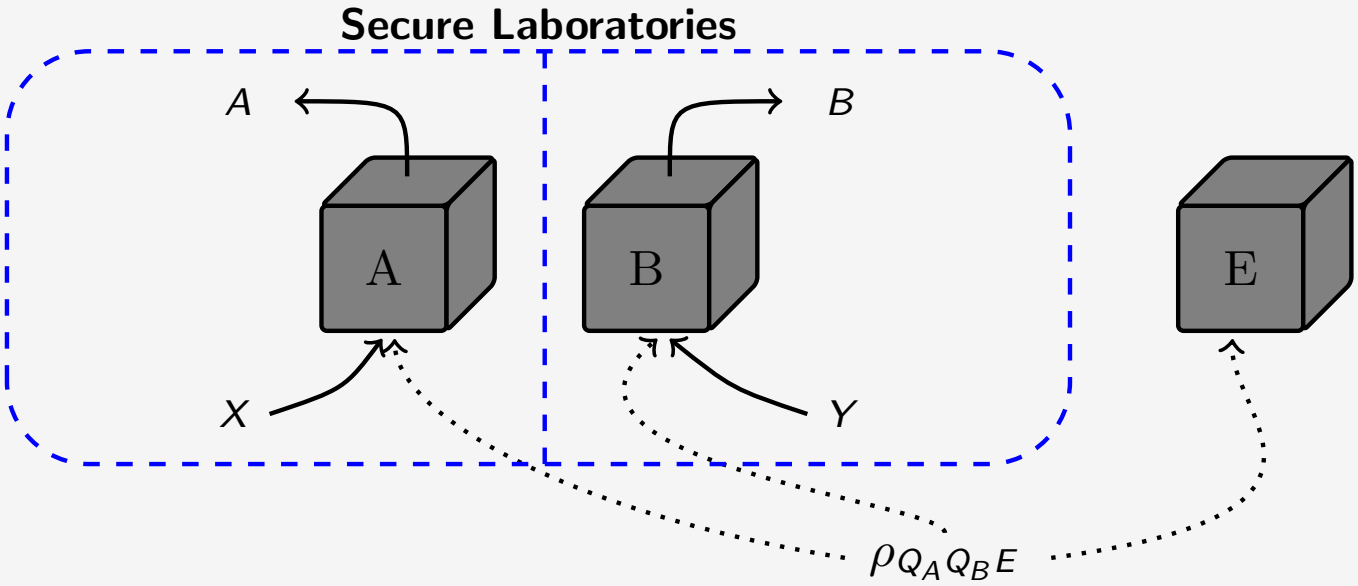
Bell-nonlocality



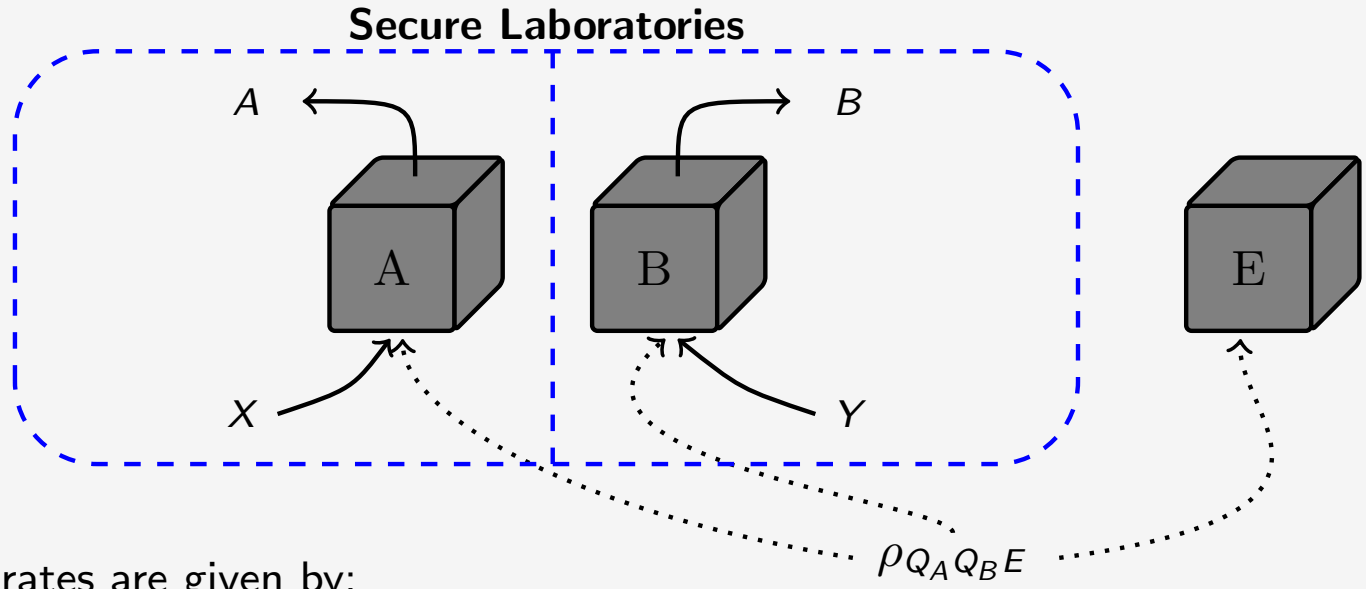
- Nonlocal correlations are inherently random.
- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on the *rate* (bits per round).

Optimization of von Neumann entropies

Randomness generated per round



Randomness generated per round



Asymptotic rates are given by:

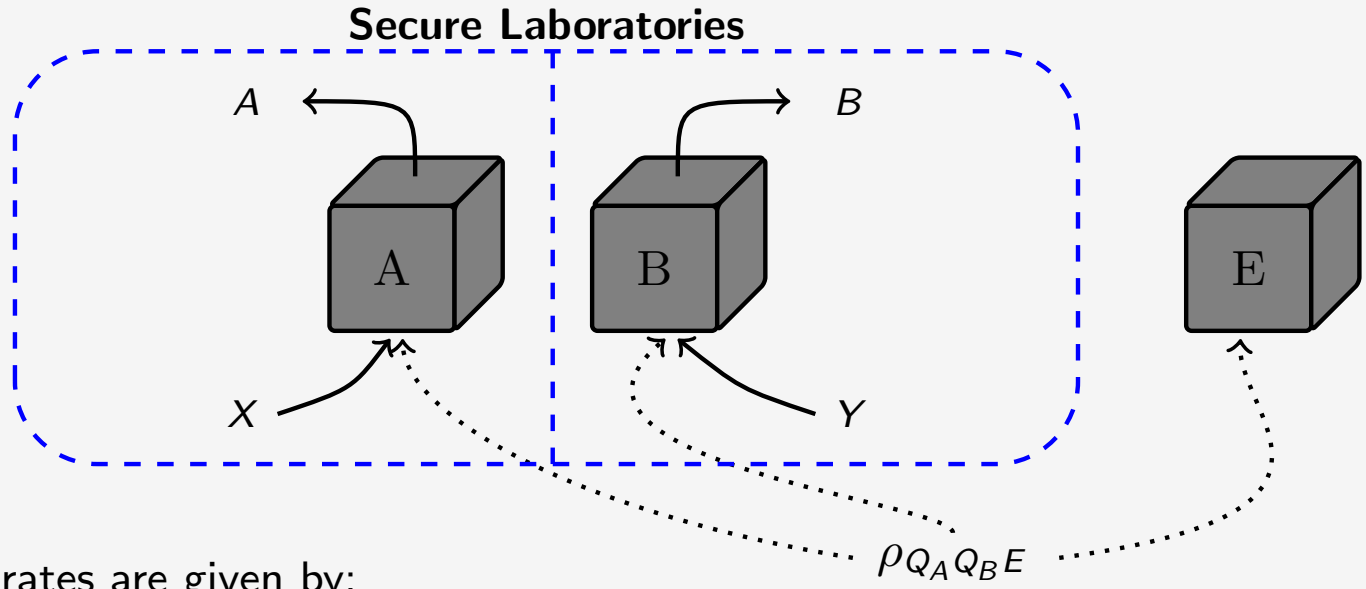
- **Randomness expansion**

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

- **QKD**

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

Randomness generated per round



Asymptotic rates are given by:

- **Randomness expansion**

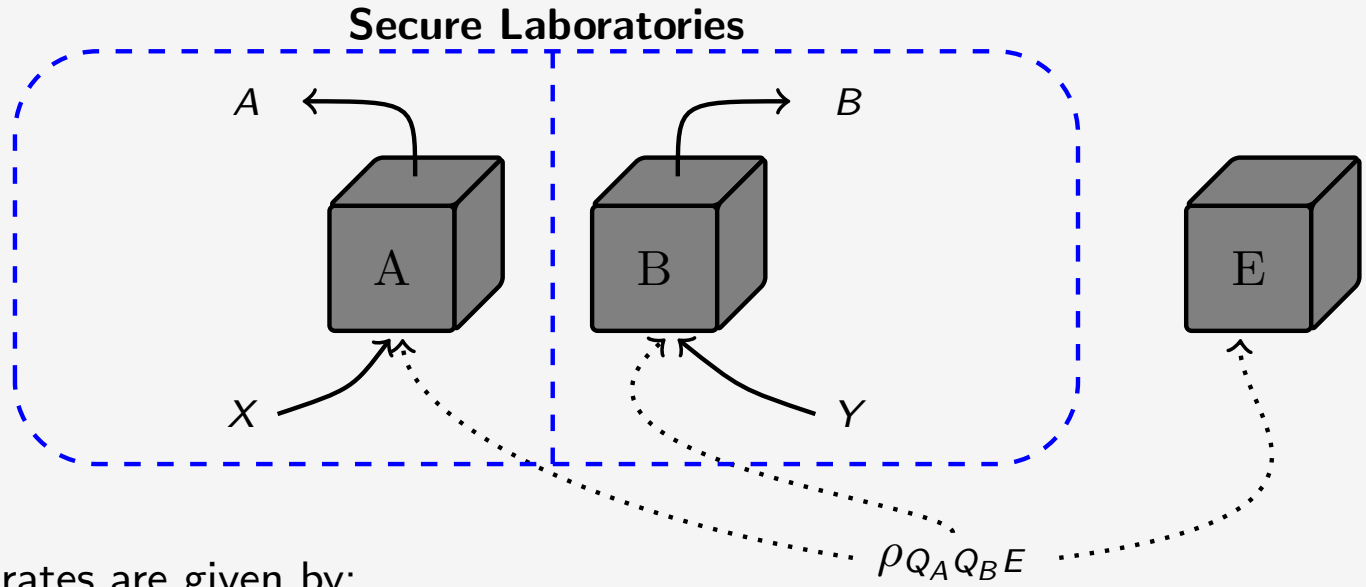
$$H(AB|X=x^*, Y=y^*, E)$$

- **QKD**

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

Want device-independent lower bounds

Randomness generated per round



Asymptotic rates are given by:

- **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

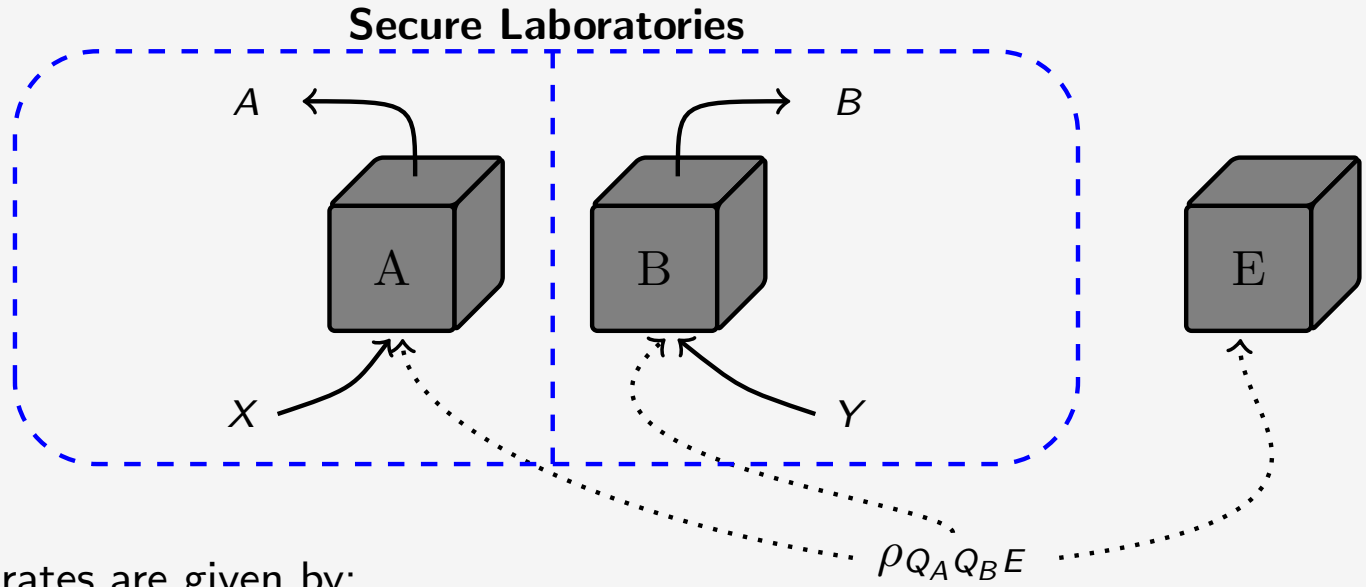
DI bounds

Want to compute

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

where inf over all devices compatible with P.

Randomness generated per round



Asymptotic rates are given by:

- **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

DI bounds

Want to compute

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

where inf over all devices compatible with P.

Difficult to solve
nonconvex / unbounded dimension

Variational forms and NCPOPs

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

Variational forms and NCPOPs

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 NCPOPs

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 NCPOPs

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 NCPOP form.

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

$$D(\rho\|\sigma) \leq \sum_{i=1}^{m} \sup_{Z} \mathrm{Tr}\left[\rho p_i(Z)\right] + \mathrm{Tr}\left[\sigma q_i(Z)\right]$$

with p_i and q_i 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

$$D(\rho\|\sigma) \leq \sum_{i=1}^{m} \sup_{Z} \mathrm{Tr}\left[\rho p_i(Z)\right] + \mathrm{Tr}\left[\sigma q_i(Z)\right]$$

with p_i and q_i 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 $f_t(x) = \frac{x-1}{t(x-1)+1}$ (RHS converges 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 $f_t(x) = \frac{x-1}{t(x-1)+1}$ (RHS converges as $m \to \infty$).

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 $f_t(x) = \frac{x-1}{t(x-1)+1}$ (RHS converges as $m \to \infty$).

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

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

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

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

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 $f_t(x) = \frac{x-1}{t(x-1)+1}$ (RHS converges as $m \to \infty$).

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

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

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

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

Main Result

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

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

Application: Device-independence

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

Theorem

The rate $\inf H(A|X = x^*, Q_E)$ *is never smaller than*

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

Application: Device-independence

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

Theorem

The rate $\inf H(A|X = x^*, Q_E)$ *is never smaller than*

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

Remarks

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

Application: Device-independence

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

Theorem

The rate $\inf H(A|X = x^*, Q_E)$ *is never smaller than*

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

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

Remarks

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

Application: Device-independence

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

Theorem

The rate $\inf H(A|X = x^*, Q_E)$ *is never smaller than*

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

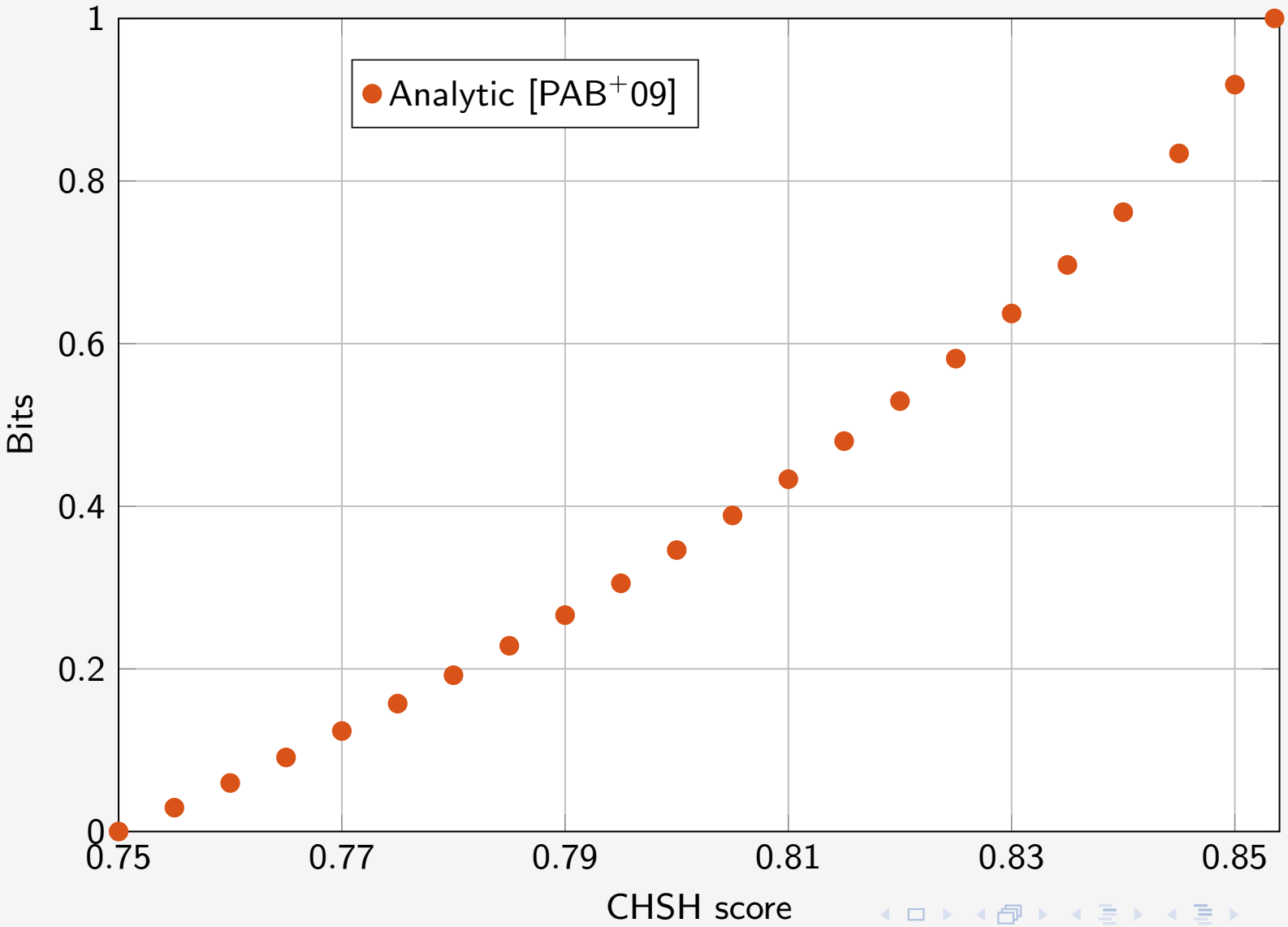
Drop $\otimes$ and impose $[M, Z] = 0$.

Remarks

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

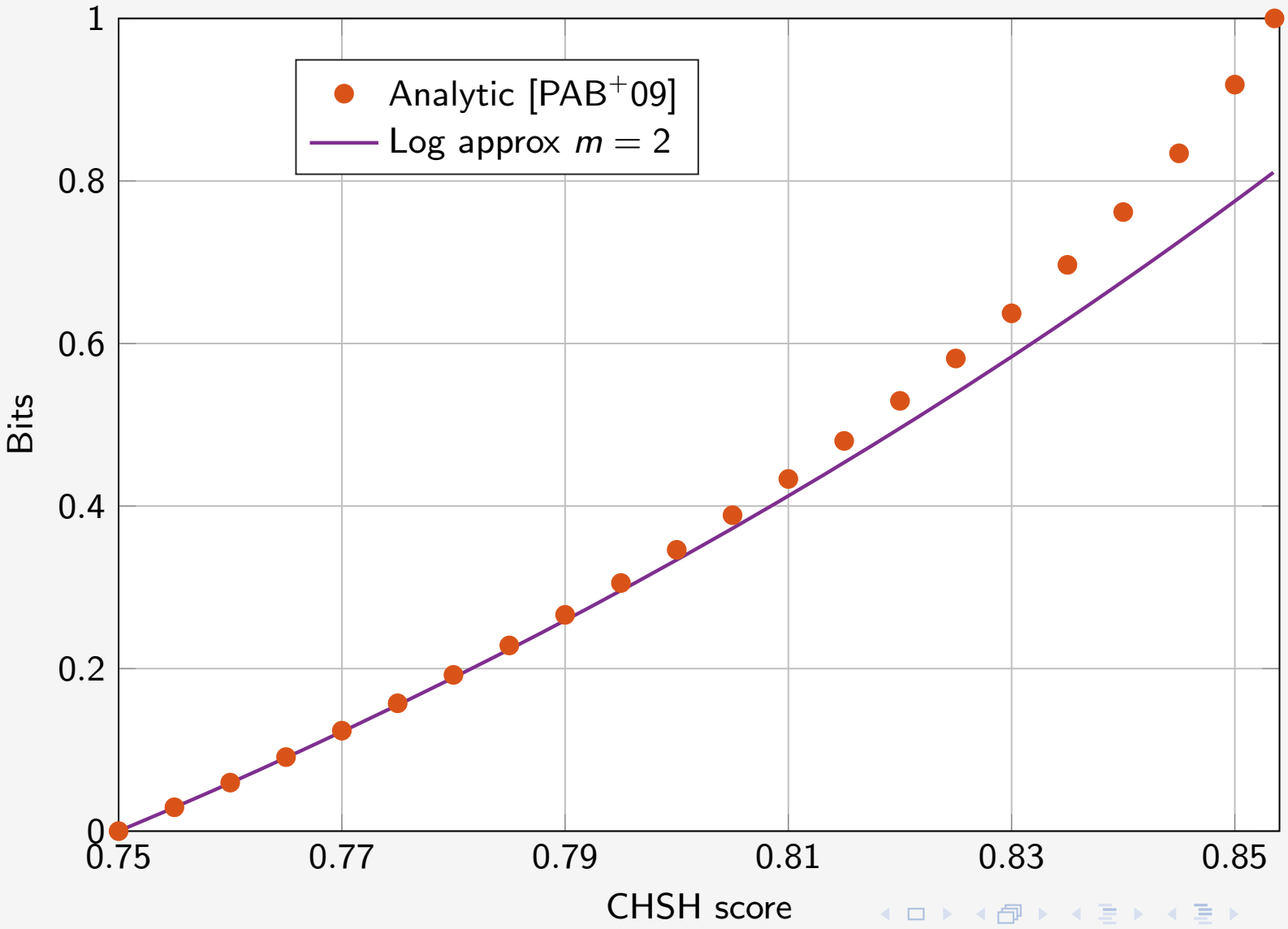
Results I – Recovering tight bounds for the CHSH game

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



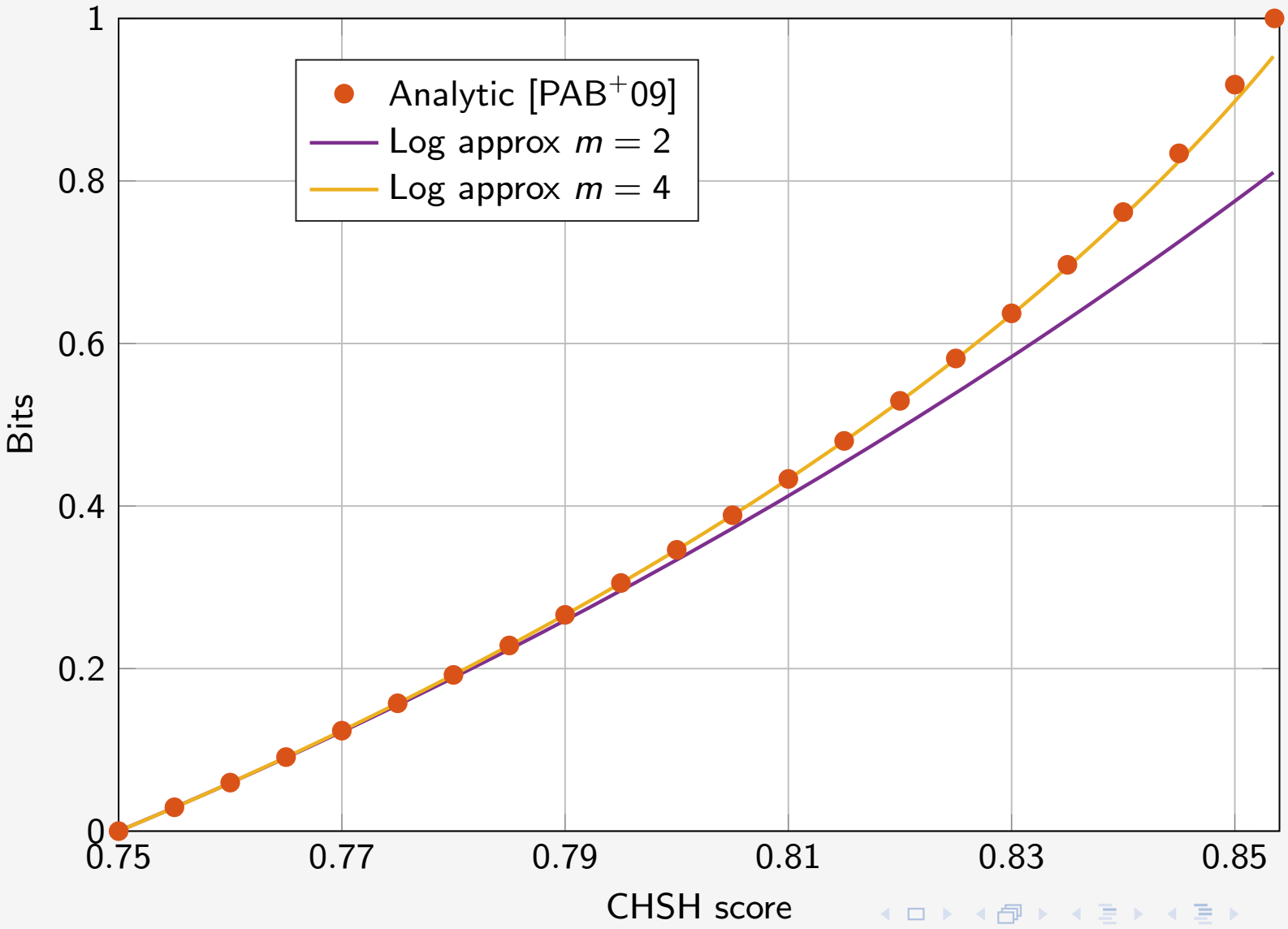
Results I – Recovering tight bounds for the CHSH game

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



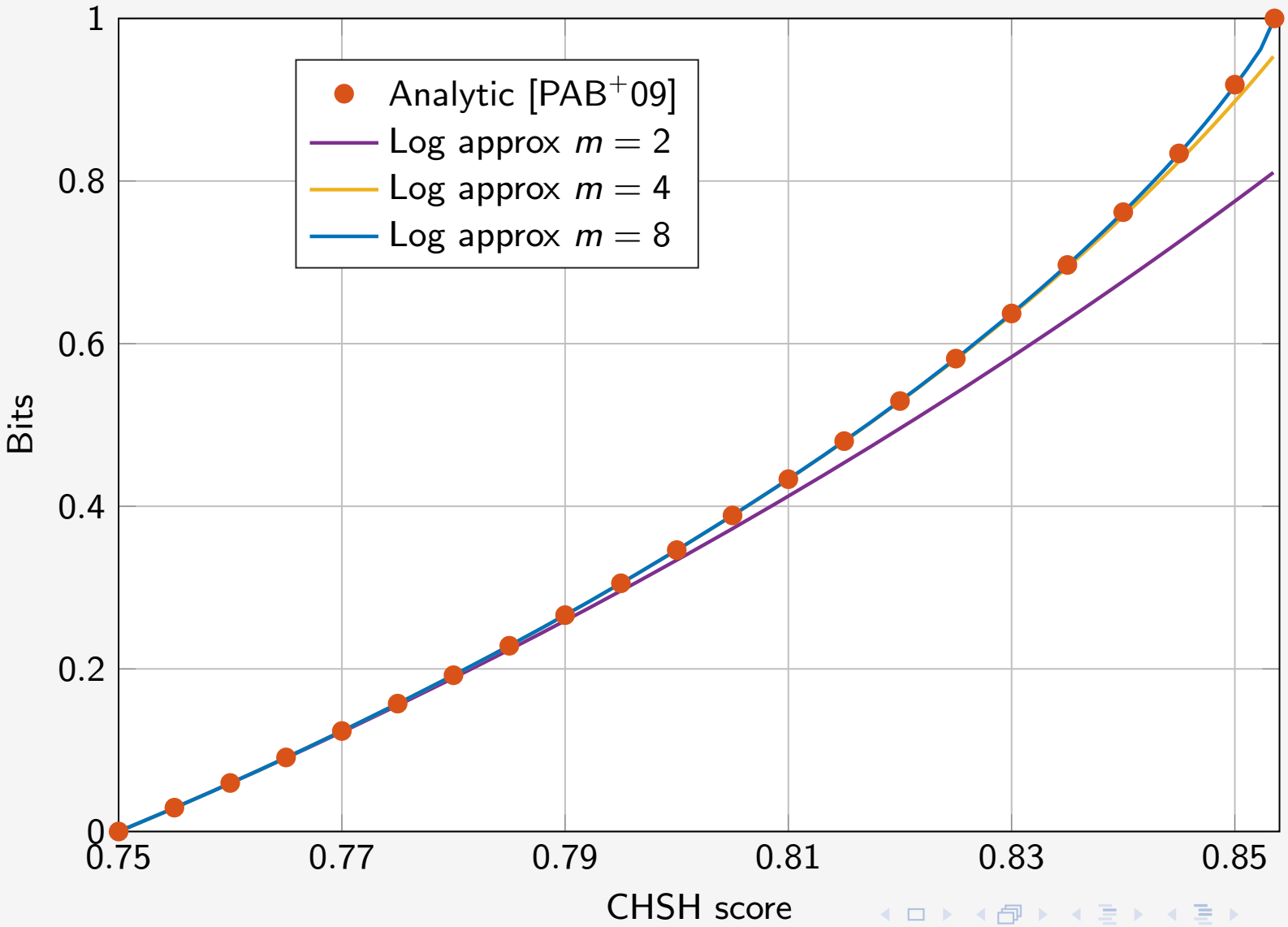
Results I – Recovering tight bounds for the CHSH game

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



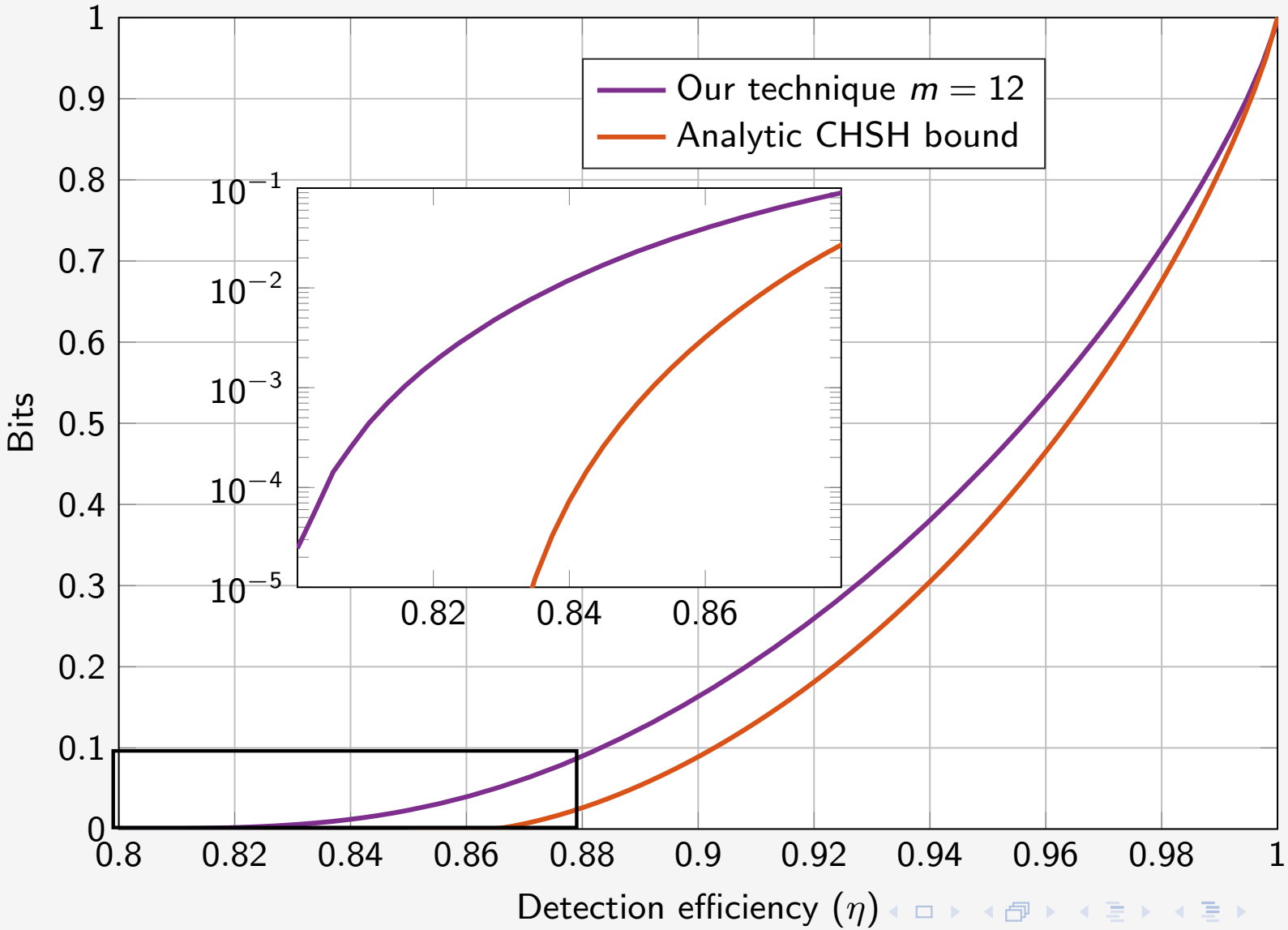
Results I – Recovering tight bounds for the CHSH game

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



Results II – Improved DIQKD rates

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



Application: squashed entanglement

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: squashed entanglement

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: squashed entanglement

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: squashed entanglement

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: squashed entanglement

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: squashed entanglement

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: squashed entanglement

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: squashed entanglement

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

- Can derive bounds:

$$E_m(A:B) \leq E(A:B) \leq E_m(A:B) + \frac{2d_A - 2}{m^2 \ln 2}$$

Application: squashed entanglement

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

- Can derive bounds:

$$E_m(A:B) \leq E(A:B) \leq E_m(A:B) + \frac{2d_A - 2}{m^2 \ln 2}$$

- 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

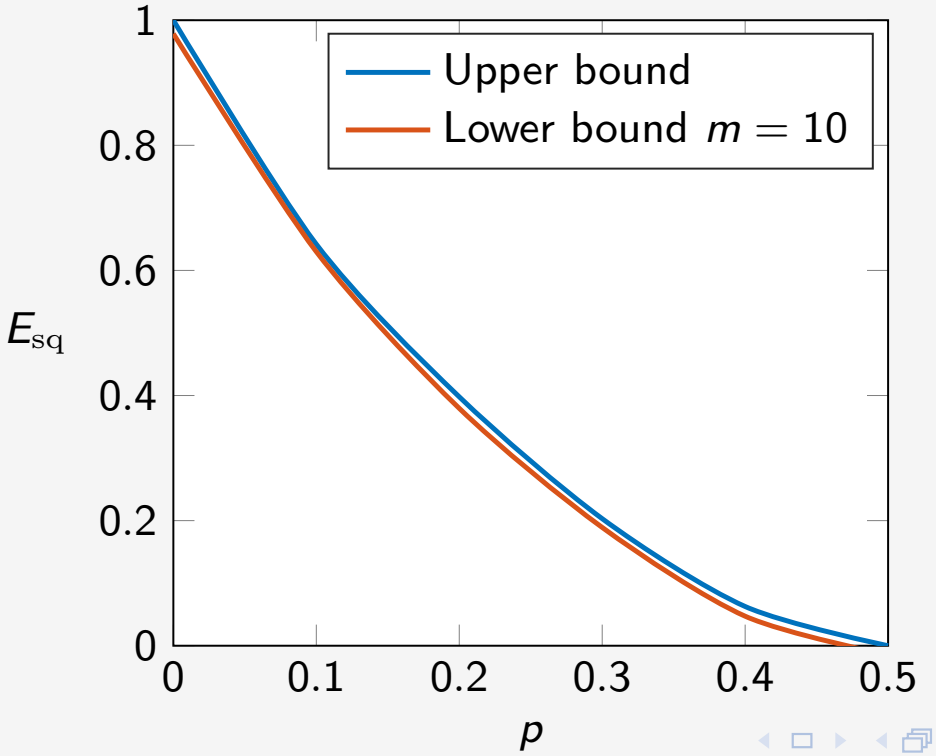
Consider a two-qubit Werner state

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

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 1: Improved lower bounds on DI protocol rates.

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application 1: Improved lower bounds on DI protocol rates.
- Application 2: SDP lower bounds on squashed entanglement.

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application 1: Improved lower bounds on DI protocol rates.
- Application 2: SDP lower bounds on squashed entanglement.

Outlook

- More efficient computations?

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application 1: Improved lower bounds on DI protocol rates.
- Application 2: SDP lower bounds on squashed entanglement.

Outlook

- More efficient computations?
- Convergence of the numerics?

Conclusion

Summary

- Technical result: convergent variational upper bounds on $D(\rho\|\sigma)$.
- Application 1: Improved lower bounds on DI protocol rates.
- Application 2: SDP lower bounds on squashed entanglement.

Outlook

- More efficient computations?
- Convergence of the numerics?
- Other applications?

Bibliography

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.

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.
Convergent relaxations of polynomial optimization problems with noncommuting variables.
SIAM Journal on Optimization, 20(5):2157–2180, 2010.

Mark M Wilde.
Squashed entanglement and approximate private states.
Quantum Information Processing, 15(11):4563–4580, 2016.

Device-independent lower bounds

Fix some linear constraint(s) C on the joint probability distribution of the devices $p_{AB|XY}$. 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 the joint probability distribution of the devices $p_{AB|XY}$. 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 the joint probability distribution of the devices $p_{AB|XY}$. 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.

Through the 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 the joint probability distribution of the devices $p_{AB|XY}$. 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.

Through the 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 the joint probability distribution of the devices $p_{AB|XY}$. 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.

Through the 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

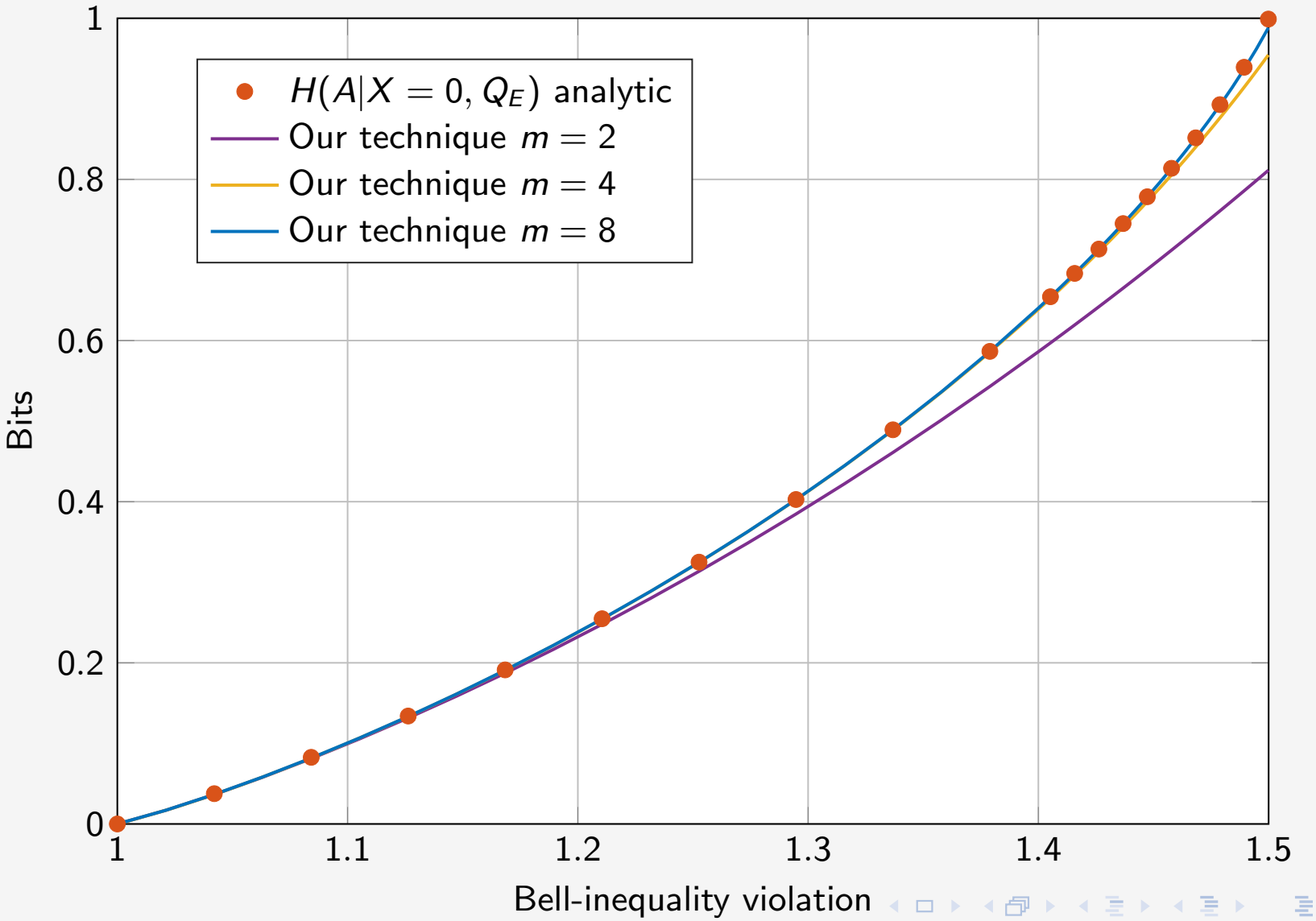
$$r(C) = \inf \quad H(A|X=x^*, E)$$

where inf over all strategies compatible with C.

Difficult to solve
nonconvex / unbounded dimension

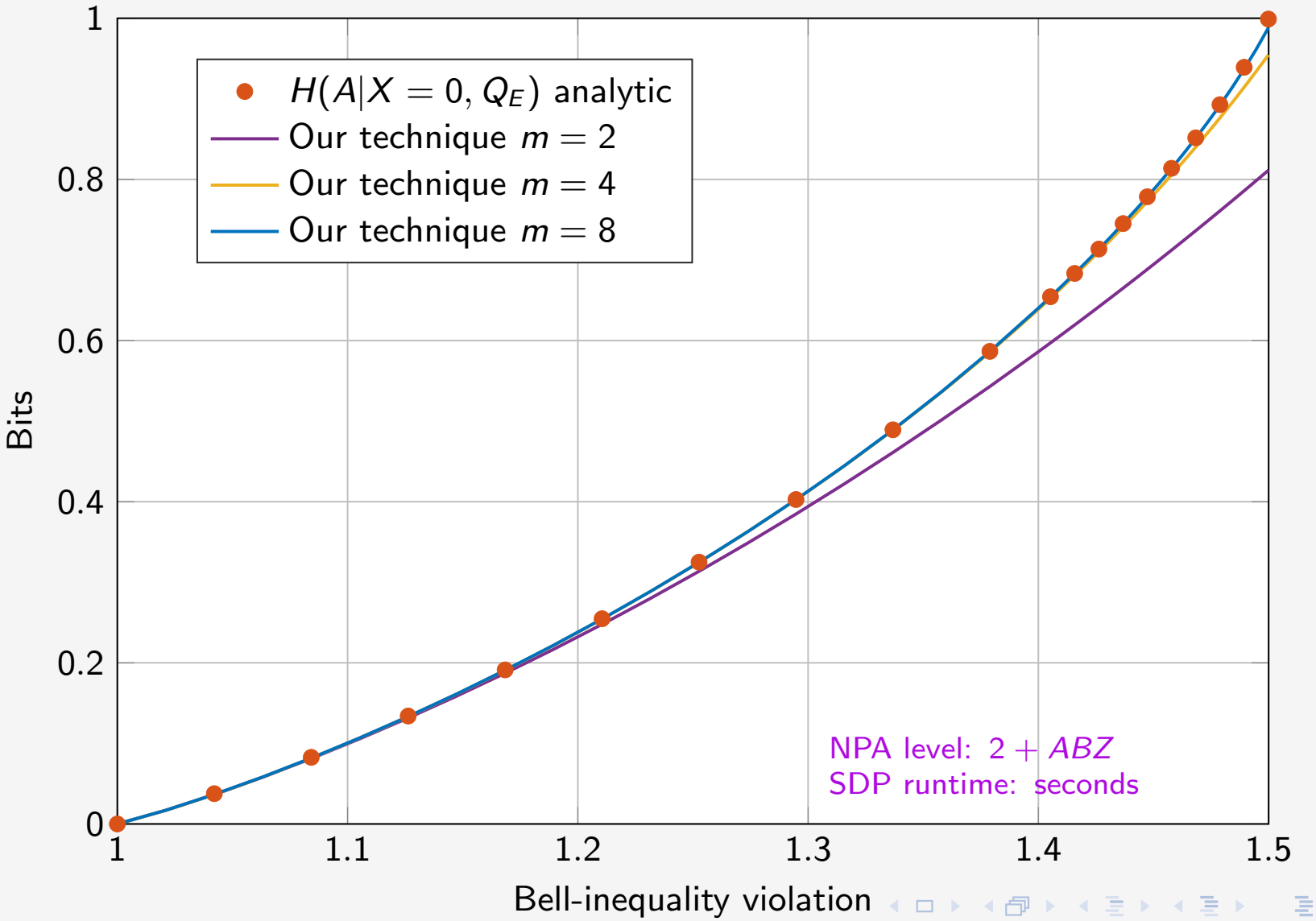
Bonus results – DICKA setting (Holz inequality)

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



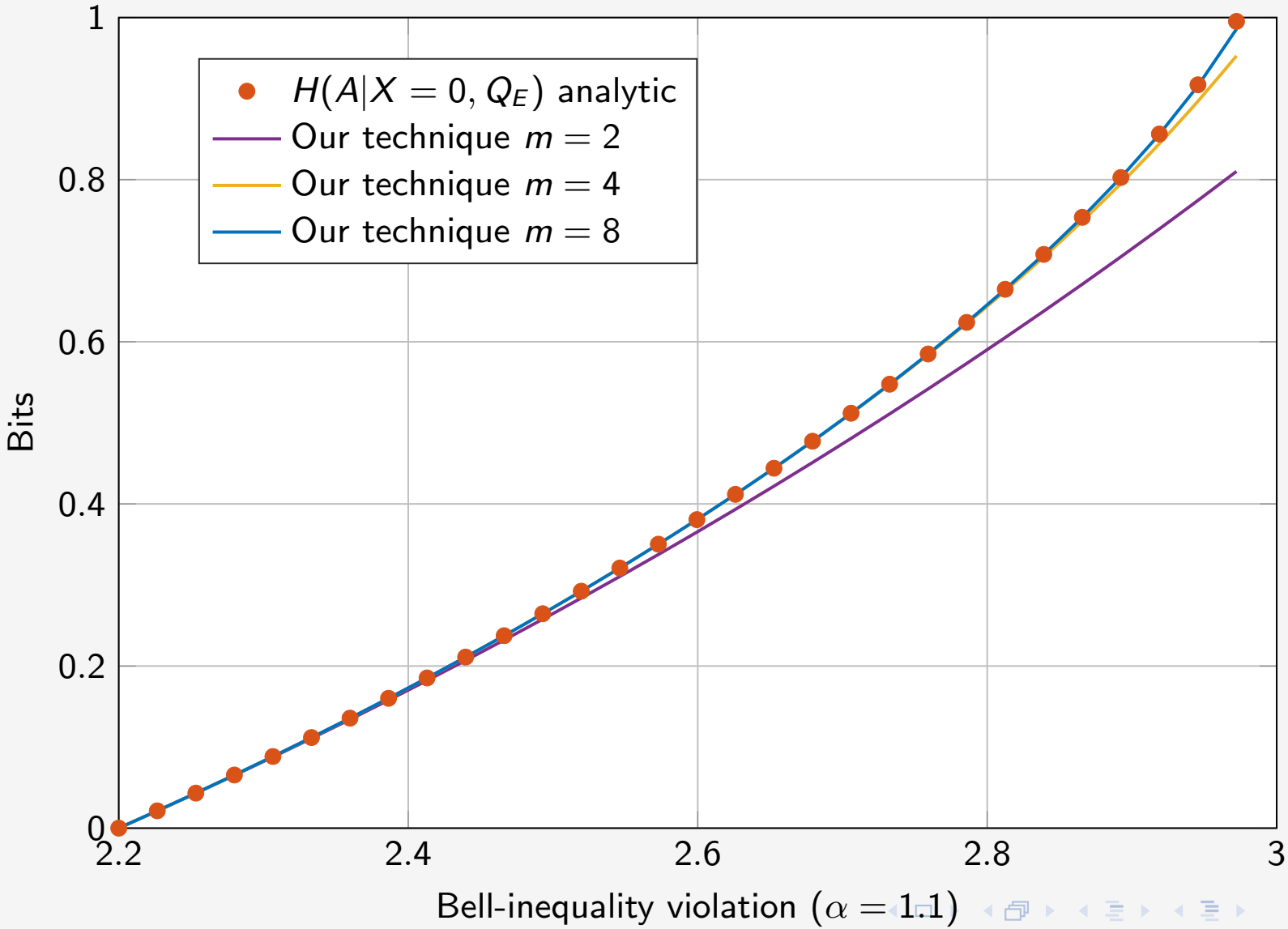
Bonus results – DICKA setting (Holz inequality)

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



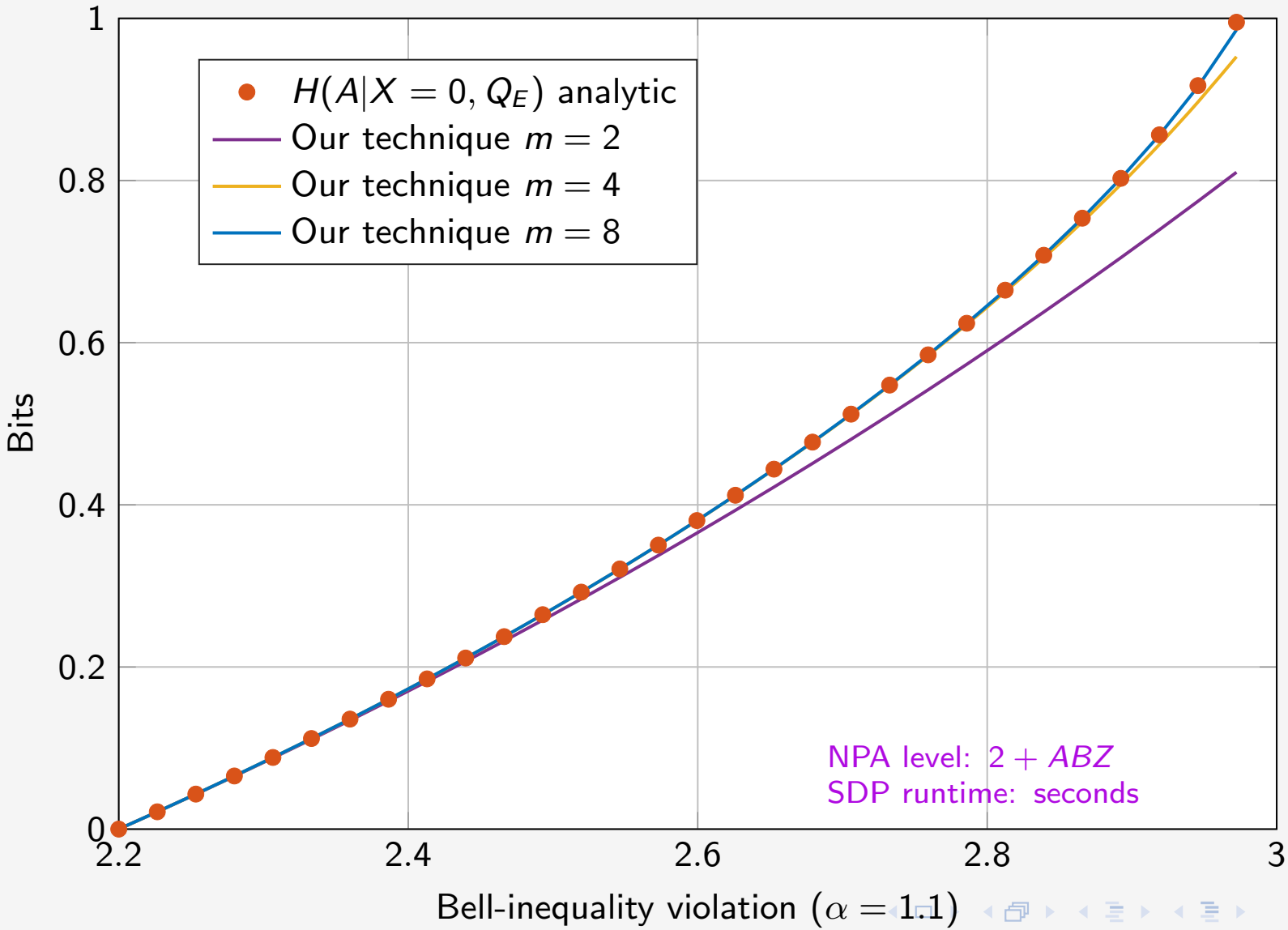
Bonus results – Generalized CHSH ($\alpha = 1.1$)

Bounding inf $H(A|X=0,Q_E)$ $\qquad B_\alpha = \alpha(\langle A_0B_0\rangle + \langle A_0B_1\rangle) + \langle A_1B_0\rangle - \langle A_1B_1\rangle$



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

Bounding inf $H(A|X=0,Q_E)$ $\qquad$ $B_\alpha = \alpha(\langle A_0B_0\rangle + \langle A_0B_1\rangle) + \langle A_1B_0\rangle - \langle A_1B_1\rangle$



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

Bounding inf $H(A|X=0,Q_E)$ $\qquad$ $B_\alpha = \alpha(\langle A_0B_0\rangle + \langle A_0B_1\rangle) + \langle A_1B_0\rangle - \langle A_1B_1\rangle$