Device-independent lower bounds on the conditional von Neumann entropy

Peter Brown, Hamza Fawzi and Omar Fawzi

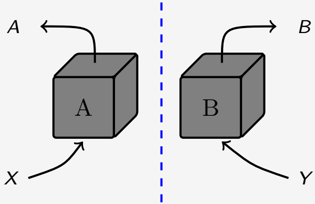
arXiv:2106.13692

Aug 25, 2021

Motivation I

Bell-nonlocality

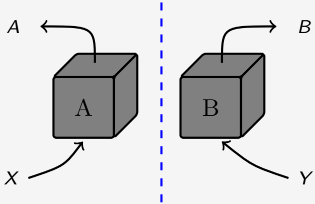
Observe $P_{AB|XY}$



Motivation I

Bell-nonlocality

Observe $P_{AB|XY}$

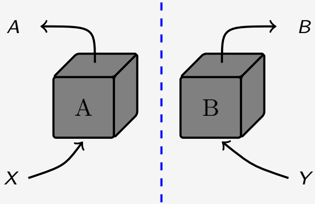


- Nonlocal correlations are inherently random.

Motivation I

Bell-nonlocality

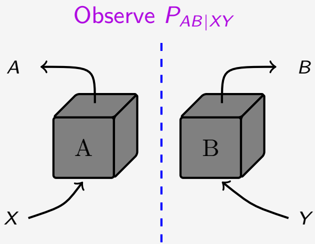
Observe $P_{AB|XY}$



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

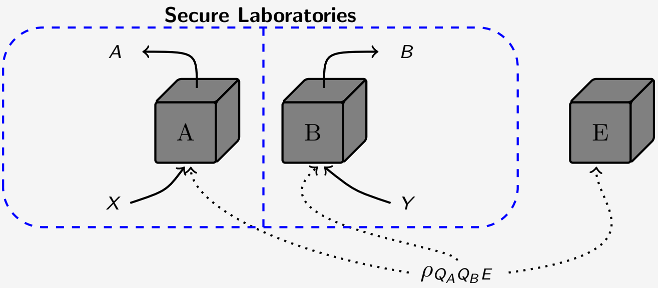
Motivation I

Bell-nonlocality

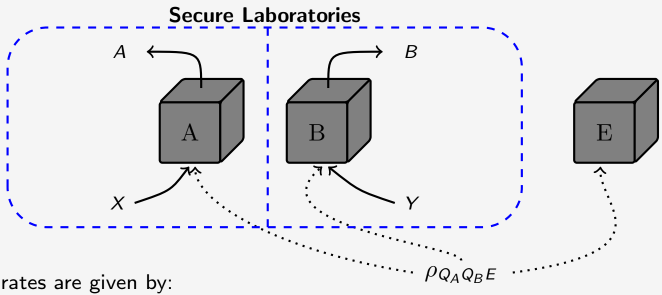


- Nonlocal correlations are inherently random.
- Foundation for randomness expansion / key-distribution protocols!
- Security and analysis relies on being able to calculate the *rates* of such protocols (bits per round).

Randomness generated per round



Randomness generated per round



Asymptotic rates are given by:

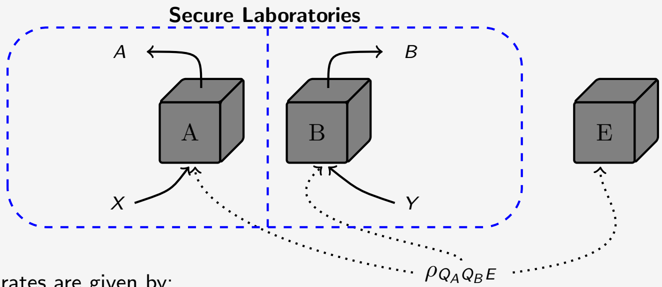
- **Randomness expansion**

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

- **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

Device-independent lower bounds

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

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

A **strategy** for C is a tuple $(\rho, \{M_{a|x}\}, \{N_{b|y}\})$ 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 $p_{AB|XY}$ (observations). E.g.

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

A **strategy** for C is a tuple $(\rho, \{M_{a|x}\}, \{N_{b|y}\})$ 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 $p_{AB|XY}$ (observations). E.g.

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

A **strategy** for C is a tuple $(\rho, \{M_{a|x}\}, \{N_{b|y}\})$ 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 $p_{AB|XY}$ (observations). E.g.

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

A **strategy** for C is a tuple $(\rho, \{M_{a|x}\}, \{N_{b|y}\})$ 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

Previous works

Known approaches

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

Previous works

Known approaches

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

$\inf \mathrm{Tr}\left[\rho p(Z)\right]$

Previous works

Known approaches

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

$\inf \mathrm{Tr}\left[\rho p(Z)\right]$

- Recent works [TSG⁺19, BFF21]
  - Different lower bounding NCPOPs.
  - Better than $H_{\min}$ / room for improvement

Previous works

Known approaches

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

$\inf \mathrm{Tr}\left[\rho p(Z)\right]$

- Recent works [TSG+19, BFF21]
  - Different lower bounding NCPOPs.
  - Better than $H_{\min}$ / room for improvement

Our 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 $m \to \infty$.

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

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

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

$$\ln(x) \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

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

$$\ln(x) \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

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

$$\ln(x) \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

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

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

Derivation overview

1. Gauss-Radau approximation of the logarithm

$$\ln(x) \geq \sum_{i=1}^{m} w_i f_{t_i}(x)$$

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

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

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 $m \to \infty$.

Lower bound on $H(A|X = x^*, Q_E)$

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

Theorem

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

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

Lower bound on $H(A|X = x^*, Q_E)$

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

Theorem

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

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

Remarks

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

Lower bound on $H(A|X = x^*, Q_E)$

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

Theorem

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

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

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

Remarks

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

Lower bound on $H(A|X = x^*, Q_E)$

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

Theorem

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

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

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

Remarks

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

Lower bound on $H(A|X = x^*, Q_E)$

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

Theorem

The rate $\inf H(A|X = x^*, Q_E)$ *is never larger 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].
- 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.

Lower bound on $H(A|X = x^*, Q_E)$

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

Theorem

The rate $\inf H(A|X = x^*, Q_E)$ *is never larger 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].
- 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.

Caveats

- Number of operators grows with m.

Lower bound on $H(A|X = x^*, Q_E)$

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

Theorem

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

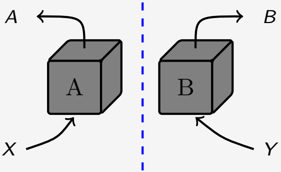
- Can now be easily relaxed to an NCPOP and solved using NPA [PNA10].
- NPA hierarchy converges as $\|Z\|$ can be bounded.
- Similar results for $H(AB|X = x, Y = y, Q_E)$ or $H(A|XQ_E)$ and others.

Caveats

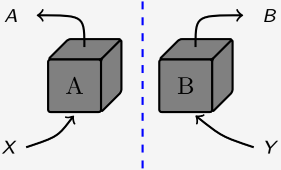
- Number of operators grows with m. Use $\inf \sum_i \cdots \geq \sum_i \inf \ldots$ to stop such scaling

Results

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



Results



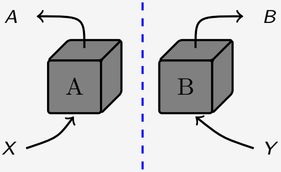
- Applied our method to compute rates for DIRNG and DIQKD.
- Looked at different constraint sets C:
  - CHSH score

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

  - 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

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

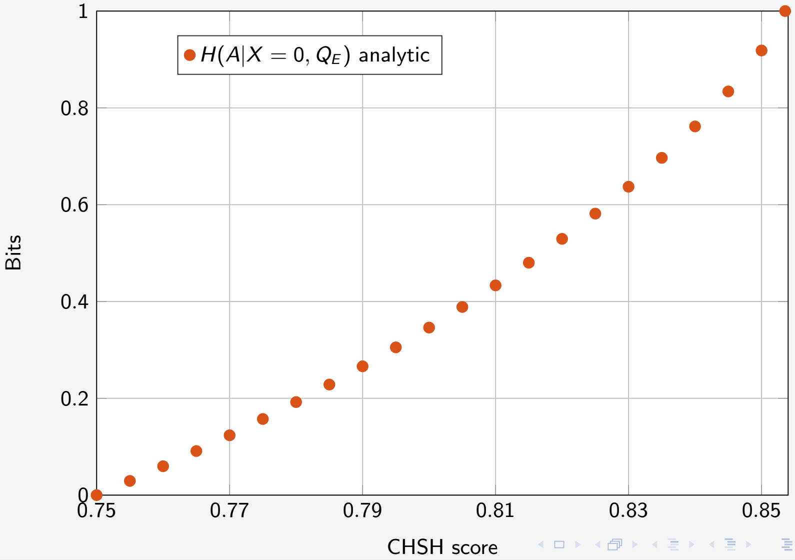
  - Full distribution

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

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

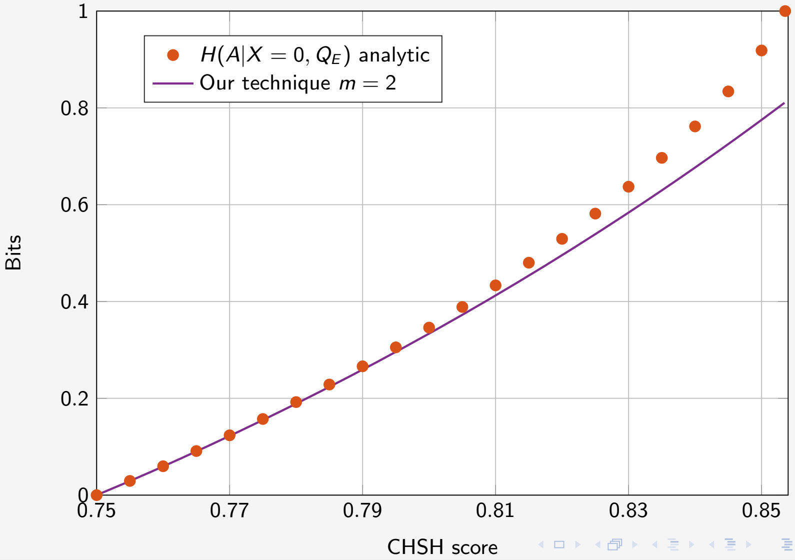
Results I – Recovering tight bounds for the CHSH game

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



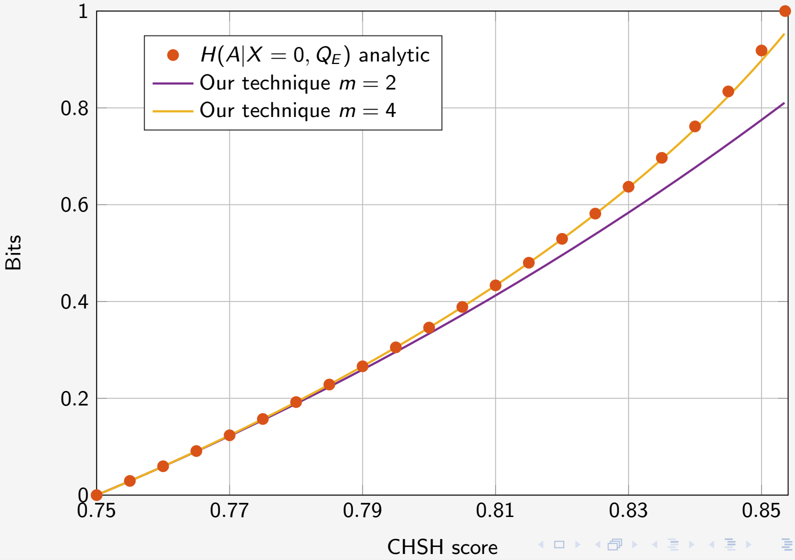
Results I – Recovering tight bounds for the CHSH game

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



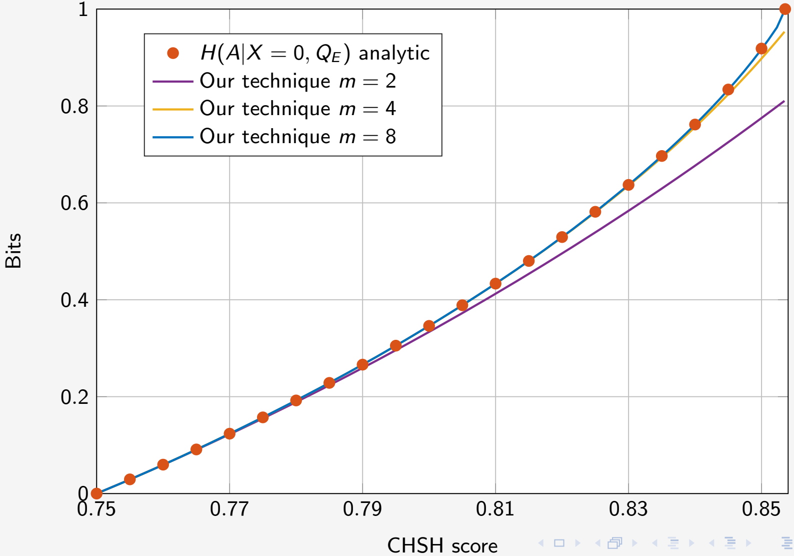
Results I – Recovering tight bounds for the CHSH game

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



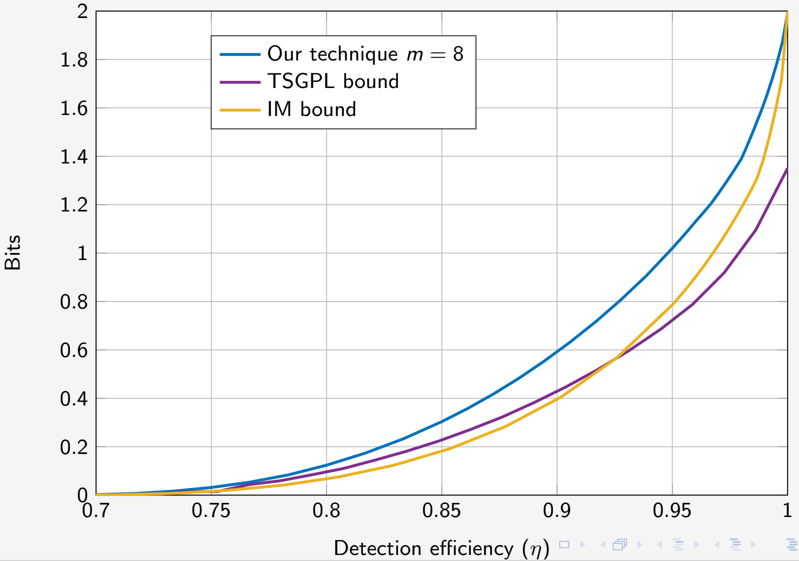
Results I – Recovering tight bounds for the CHSH game

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



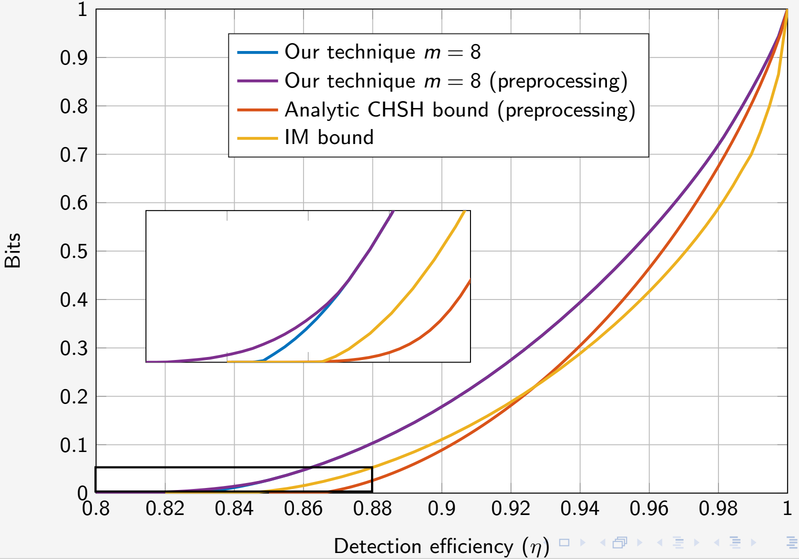
Results II – Improved randomness expansion rates

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



Results III – Improved DIQKD rates

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



Conclusion

Summary

- New general method to compute rates of DI protocols.

Conclusion

Summary

- New general method to compute rates of DI protocols.
- Convergent (in a sense) – observe practical convergence also.

Conclusion

Summary

- New general method to compute rates of DI protocols.
- Convergent (in a sense) – observe practical convergence also.
- Outperforms all previous methods (+ faster)

Conclusion

Summary

- New general method to compute rates of DI protocols.
- Convergent (in a sense) – observe practical convergence also.
- Outperforms all previous methods (+ faster)
- Applies to infinite dimensional systems and can be used directly with EAT to prove security.

Conclusion

Summary

- New general method to compute rates of DI protocols.
- Convergent (in a sense) – observe practical convergence also.
- Outperforms all previous methods (+ faster)
- Applies to infinite dimensional systems and can be used directly with EAT to prove security.

Outlook

- Better understand convergence? (commuting operator vs tensor product).

Conclusion

Summary

- New general method to compute rates of DI protocols.
- Convergent (in a sense) – observe practical convergence also.
- Outperforms all previous methods (+ faster)
- Applies to infinite dimensional systems and can be used directly with EAT to prove security.

Outlook

- Better understand convergence? (commuting operator vs tensor product).
- Is DIQKD feasible now?

Conclusion

Summary

- New general method to compute rates of DI protocols.
- Convergent (in a sense) – observe practical convergence also.
- Outperforms all previous methods (+ faster)
- Applies to infinite dimensional systems and can be used directly with EAT to prove security.

Outlook

- Better understand convergence? (commuting operator vs tensor product).
- Is DIQKD feasible now?
- Other entropic quantities?

Bibliography

Peter Brown, Hamza Fawzi, and Omar Fawzi.
Computing conditional entropies for quantum correlations.
Nature communications, 12(1):1–12, 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.
Convergent relaxations of polynomial optimization problems with noncommuting variables.
SIAM Journal on Optimization, 20(5):2157–2180, 2010.

Ernest Y-Z Tan, René Schwonnek, Koon Tong Goh, Ignatius William Primaatmaja, and Charles C-W Lim.
Computing secure key rates for quantum key distribution with untrusted devices.
e-print arXiv:1908.11372, 2019.