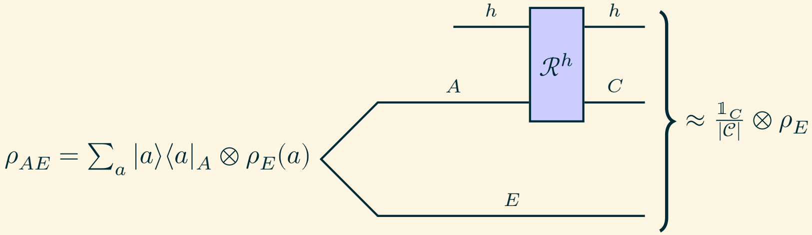
Privacy amplification and decoupling without smoothing

Frédéric Dupuis *Université de Montréal*

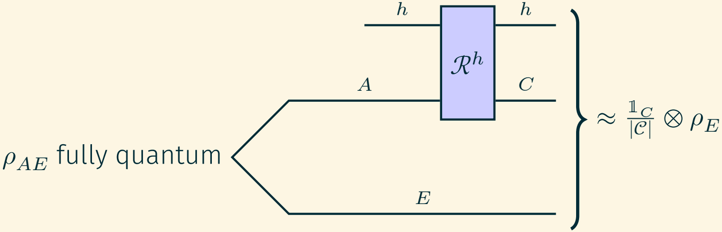
August 17, 2021

Privacy amplification



- $\{h : \mathcal{A} \to \mathcal{C} | h \in \mathcal{H}\}$.
- $\mathcal{R}^h_{A\to C}(\theta_A) = \sum_a \langle a|\theta_A|a\rangle |h(a)\rangle\langle h(a)|$
- Want: $\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \rho_E \right\|_1 \leq$ small.
- Depends on randomness in ρ and size of $\mathcal{C}$
- Important case: ρ is iid: $\rho_{A_1^n E_1^n} = \tau_{AE}^{\otimes n}$.

Decoupling



- $\{U_h : \mathcal{A} \to \mathcal{C} | h \in \mathcal{H}\}$
- $\mathcal{R}^h_{A\to C}(\theta_A) = U_h \theta_A U_h^\dagger$
- Want: $\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \rho_E \right\|_1 \leq$ small.
- Can be used to prove a wide range of achievability results in quantum Shannon theory via Uhlmann's theorem.

Entropy measures

- von Neumann: $2^{-H(A|E)_\rho} = \mathrm{Tr}[\rho_{AE}(\log \rho_{AE} - \log \rho_E)]$
  - Lots of nice properties (chain rules, etc), right quantity for anything iid
  - Too good to be true in general
- Min-entropy: $2^{-H_{\min}(A|E)_\rho} = \mathrm{Pr}[\text{Guessing } A \text{ by measuring } E]$
  - Semidefinite program, well understood
  - Needs smoothing to be useful in most cases
- "Sandwiched" Rényi entropy: $2^{-H_\alpha(A|E)_\rho} = \min_{\sigma_E} \mathrm{Tr}\left[\left(\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE} \sigma_E^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right]$
  - $\alpha \in [\frac{1}{2}, \infty]$
  - Recently defined, starting to understand it better
  - Generalizes both above quantities

Privacy amplification: achievability result

Theorem (Renner 2005)

Let h be drawn from a 2-universal family of hash functions. Then,

$$\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \rho_E \right\|_1 \leq 2^{\frac{1}{2}(\log|\mathcal{C}| - H_2(A|E)_\rho)}$$

- Not so good for iid: $H_2(A|E)_\rho < H(A|E)_\rho$

Smoothing

- Use min-entropy, rather than 2-entropy: better understood
- ε-smooth min-entropy: $H^{\varepsilon}_{\min}(A|E)_{\rho} := \max_{D(\tilde{\rho},\rho)\leq\varepsilon} H_{\min}(A|E)_{\tilde{\rho}}$
- Use this version:

$$\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \rho_E \right\|_1 \leq 2\varepsilon + 2^{\frac{1}{2}(\log|\mathcal{C}| - H^{\varepsilon}_{\min}(A|E)_{\rho})}$$

Smoothing of iid states

- FQAEP: for $\rho_{A_1^n E_1^n} = \tau^{\otimes n}$,

$$H_{\min}^{\varepsilon}(A_1^n|E_1^n)_\rho \geq nH(A|E)_\tau - O(\sqrt{n})$$

- Core of proof:

$$\begin{aligned} H_{\min}^{\varepsilon}(A_1^n|E_1^n)_\rho &\geq H_\alpha(A_1^n|E_1^n) - \frac{1}{\alpha-1}\log\frac{2}{\varepsilon^2} \\ &= nH_\alpha(A|E)_\tau - \frac{1}{\alpha-1}\log\frac{2}{\varepsilon^2} \\ &\geq nH(A|E)_\tau - n(\alpha-1)V^2 - \frac{1}{\alpha-1}\log\frac{2}{\varepsilon^2} \end{aligned}$$

  Then picking $\alpha = 1 + \sqrt{\frac{\log\frac{2}{\varepsilon^2}}{nV}}$ yields the theorem.
- EAT works in a similar way

Previous work

Fully classical case[1]:

$$\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \rho_E \right\|_1 \leq 3 \times 2^{\frac{\alpha-1}{\alpha}(\log|\mathcal{C}| - H_\alpha(A|E)_\rho)}.$$

Optimizing over α yields a good error exponent.

[1] M. Hayashi, "Tight Exponential Analysis of Universally Composable Privacy Amplification and Its Applications, "arXiv: 1010.1358

Previous work

CQ case[2]:

$$\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \sigma_E \right\|_1 \lesssim (4 + \sqrt{\varepsilon v(\sigma_E)}) 2^{\frac{\alpha-1}{2}(\log|\mathcal{C}| - H_{\alpha,\mathrm{Petz}}(A|E)_{\rho|\sigma})}.$$

- $v(\sigma_E)$: number of distinct eigenvalues $\Rightarrow$ good for iid, bad in general
- Also a version involving the ratio between largest and smallest eigenvalue

[2] M. Hayashi, "Large Deviation Analysis for Quantum Security Via Smoothing of Renyi Entropy of Order 2, "arXiv: `1202.0322`

Previous work

Fully quantum case (i.e. decoupling)[3]:

$$\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \sigma_E \right\|_1 \leq 4 \times 2^{\frac{\alpha-1}{2\alpha}(\log v(\sigma_E) + \log|\mathcal{C}| - H_\alpha(A|E)_{\rho|\sigma})}$$

- $v(\sigma_E)$: number of distinct eigenvalues $\Rightarrow$ good for iid, bad in general
- Can be used to get error exponents for lots of iid tasks.

[3] N. Sharma, *Random Coding Exponents Galore Via Decoupling*, arXiv: `1504.07075`

Main result

Theorem (Main result)

$$\mathbb{E}_h \left\| \mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|} \otimes \rho_E \right\|_1 \leq 2^{\frac{2}{\alpha}-1} \cdot 2^{\frac{\alpha-1}{\alpha}(\log|\mathcal{C}| - H_\alpha(A|E)_\rho)}$$

for $\alpha \in (1, 2]$.

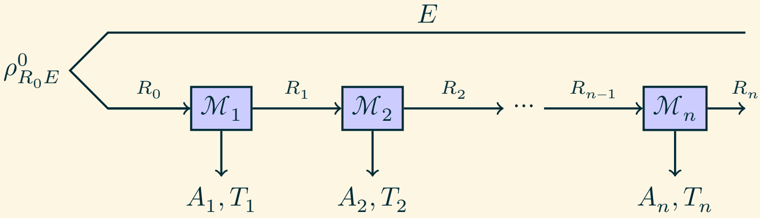
We can replace the "core of the proof" above by:

$$\begin{aligned} H_\alpha(A_1^n|E_1^n)_\rho &= nH_\alpha(A|E)_\tau \\ &\geq nH(A|E)_\tau - n(\alpha-1)V^2. \end{aligned}$$

Optimizing over α yields an error exponent of $\geq \frac{1}{2}\left(\frac{H(A|E) - \frac{1}{n}\log|\mathcal{C}|}{V}\right)^2$.

Combining main result with entropy accumulation

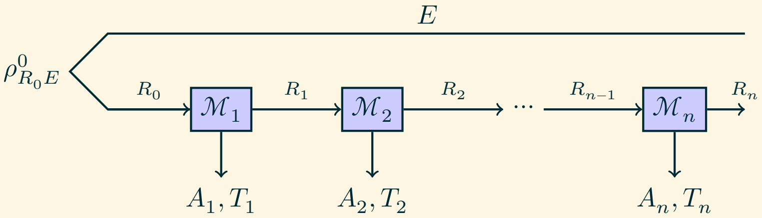
Entropy accumulation[4]:



- T_1^n: test bits (think of win/lose in CHSH)
- Event observed: $\mathrm{wt}(T_1^n) = w$.
- Tradeoff function: $f(w)$: amount of Shannon entropy per round consistent with statistics
- Useful for proving security of DI protocols

[4] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation, "arXiv: `1607.01796`

Combining main result with entropy accumulation



Theorem

$$\Pr\left[\mathrm{wt}(T_1^n) = w\right] \cdot \mathbb{E}_h \left\| \mathcal{R}^h(\rho_{A_1^n E | \mathrm{wt}(T_1^n)=w}) - \frac{1}{2^{nR}} \otimes \rho_{E | \mathrm{wt}(T_1^n)=w} \right\|_1 \leq 2 \cdot 2^{-nE(R)},$$

where $E(R) = \frac{1}{2}\left(\frac{f(w)-R}{V}\right)^2$.

Proof idea

Proof idea: norm interpolation

- Riesz-Thorin theorem: $\|f\|_{p_\theta} \leq \|f\|_{p_0}^{1-\theta}\|f\|_{p_1}^{\theta}$ for $\frac{1}{p_\theta} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$.
- Can write
$$2^{\frac{\alpha-1}{\alpha}H_\alpha(A|E)_{\rho|\sigma}} = \left\|\sigma_E^{\frac{1-\alpha}{2\alpha}}\rho_{AE}\sigma_E^{\frac{1-\alpha}{2\alpha}}\right\|_\alpha .$$
- Use a similar technique to interpolation between:

$$\mathbb{E}_h\left\|\mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|}\otimes\rho_E\right\|_1 \leq 2^{\frac{2}{2}-1}\cdot 2^{\frac{2-1}{2}(\log|\mathcal{C}|-H_2(A|E)_\rho)}$$
$$\mathbb{E}_h\left\|\mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|}\otimes\rho_E\right\|_1 \leq 2^{\frac{2}{1}-1}\cdot 2^{\frac{1-1}{1}(\log|\mathcal{C}|-H(A|E)_\rho)} = 2$$

to get

$$\mathbb{E}_h\left\|\mathcal{R}^h(\rho_{AE}) - \frac{\mathbb{1}_C}{|\mathcal{C}|}\otimes\rho_E\right\|_1 \leq 2^{\frac{2}{\alpha}-1}\cdot 2^{\frac{\alpha-1}{\alpha}(\log|\mathcal{C}|-H_\alpha(A|E)_\rho)}.$$

Conclusion and open problems

- Question: can we "Rényify" all of one-shot quantum information theory?
    - Decoupling gets us part of the way there.
- Simultaneous smoothing

The end

The paper:

- "Privacy amplification and decoupling without smoothing", `arXiv:2105.05342`

Thanks!