Smooth min-entropy lower bounds for approximation chains

Presentation for Beyond i.i.d 2023

Ashutosh Marwah
(work with Frédéric Dupuis)
Université de Montréal

github.com/goforashutosh/approx-chains

Smooth min-entropy

Min-entropy for a state ρ_{AB} is defined as

$$H_{min}(A|B)_\rho := -\log \inf\{\lambda \in \mathbb{R} : \text{there exists a state } \sigma_B \text{ such that } \rho_{AB} \leq \lambda\, I_A \otimes \sigma_B\}.$$

Smooth min-entropy is defined as

$$H_{min}^{\epsilon}(A|B)_\rho := \sup_{\tilde{\rho}} H_{min}(A|B)_{\tilde{\rho}}$$

where the optimization is over states $\tilde{\rho}$ which are ϵ close to ρ (in purified distance).

The smooth min-entropy characterizes the amount of randomness one can extract from a state when part of it is correlated with a register held by the adversary.

Rényi entropies

For $\alpha \in [{}^1/_2, 1) \cup (1, \infty]$, the (optimised) sandwiched Rényi entropy is defined as:

$$H_\alpha(A|B)_\rho = \sup_{\sigma_B} \frac{1}{1-\alpha} \log \mathrm{tr} \left(\sigma_B^{\frac{1-\alpha}{2\alpha}} \rho_{AB}\, \sigma_B^{\frac{1-\alpha}{2\alpha}} \right)^\alpha$$

for where σ_B is density operator.

These α-Rényi conditional entropies interpolate between min-entropy and the von-Neumann entropy and help produce tight bounds.

Smooth max-relative entropy

The max-relative entropy between states ρ and σ is defined as:

$$D_{max}(\rho||\sigma) \coloneqq \inf\{\lambda \in \mathbb{R} : \rho \leq 2^{\lambda}\sigma\}.$$

The ϵ-smooth max-relative entropy between states ρ and σ is defined as:

$$D_{max}^{\epsilon}(\rho||\sigma) \coloneqq \inf_{\tilde{\rho}} D_{max}(\tilde{\rho}||\sigma)$$

where the optimization is over states $\tilde{\rho}$ which are ϵ close to ρ (in purified distance).

Approximation chains

For a *(big)* state $\rho_{A_1^n B}$, we define a sequence of states $(\sigma^{(k)}_{A_1^k B})_{k=1}^n$ as an ϵ-approximation chain of $\rho_{A_1^n B}$ if for every $1 \leq k \leq n$,

$$\|\rho_{A_1^k B} - \sigma^{(k)}_{A_1^k B}\|_1 \leq \epsilon,$$

that is, the partial state $\rho_{A_1^k B}$ can be approximated by $\sigma^{(k)}_{A_1^k B}$.

Notation:
A_1^n denotes the registers $A_1, A_2, \cdots, A_n$

Approximation chains

$\boldsymbol{(\sigma^{(k)}_{A_1^k B})_{k=1}^n}$ **as an $\boldsymbol{\epsilon}$-approximation chain of $\boldsymbol{\rho_{A_1^n B}}$:** $\|\rho_{A_1^k B} - \sigma^{(k)}_{A_1^k B}\|_1 \leq \epsilon$ for every k.

Suppose, further that $H\left(A_k \middle| A_1^{k-1} B\right)_{\sigma^{(k)}} \geq c$ for some constant $c > 0$. Then, we have

$$H(A_1^n|B)_\rho = \sum_{k=1}^{n} H\left(A_k \middle| A_1^{k-1} B\right)_\rho$$

Approximation chains

$\boldsymbol{(\sigma^{(k)}_{A_1^k B})_{k=1}^n}$ **as an $\boldsymbol{\epsilon}$-approximation chain of $\boldsymbol{\rho_{A_1^n B}}$:** $\|\rho_{A_1^k B} - \sigma^{(k)}_{A_1^k B}\|_1 \leq \epsilon$ for every k.

Suppose, further that $H\left(A_k \middle| A_1^{k-1} B\right)_{\sigma^{(k)}} \geq c$ for some constant $c > 0$. Then, we have

$$\begin{aligned} H(A_1^n|B)_\rho &= \sum_{k=1}^n H\left(A_k \middle| A_1^{k-1} B\right)_\rho \\ &\geq \sum_{k=1}^n H\left(A_k \middle| A_1^{k-1} B\right)_{\sigma^{(k)}} - g(\epsilon, |A|) \end{aligned}$$

Approximation chains

$\boldsymbol{(\sigma^{(k)}_{A_1^k B})_{k=1}^{n}}$ **as an $\boldsymbol{\epsilon}$-approximation chain of $\boldsymbol{\rho_{A_1^n B}}$:** $\|\rho_{A_1^k B} - \sigma^{(k)}_{A_1^k B}\|_1 \leq \epsilon$ for every k.

Suppose, further that $H\left(A_k \middle| A_1^{k-1} B\right)_{\sigma^{(k)}} \geq c$ for some constant $c > 0$. Then, we have

$$
\begin{aligned}
H(A_1^n|B)_\rho &= \sum_{k=1}^{n} H\left(A_k \middle| A_1^{k-1} B\right)_\rho \\
&\geq \sum_{k=1}^{n} H\left(A_k \middle| A_1^{k-1} B\right)_{\sigma^{(k)}} - g(\epsilon, |A|) \\
&\geq n(c - g(\epsilon, |A|))
\end{aligned}
$$

Approximation chains

$(\boldsymbol{\sigma}^{(\boldsymbol{k})}_{\boldsymbol{A_1^k B}})_{\boldsymbol{k=1}}^{\boldsymbol{n}}$ **as an $\boldsymbol{\epsilon}$-approximation chain of $\boldsymbol{\rho_{A_1^n B}}$:** $\|\rho_{A_1^k B} - \sigma^{(k)}_{A_1^k B}\|_1 \leq \epsilon$ for every k, then

$$H(A_1^n|B)_\rho \geq \sum_{k=1}^{n} H\left(A_k \middle| A_1^{k-1} B\right)_{\sigma^{(k)}} - ng(\epsilon, |A|).$$

A similar argument cannot be true for smooth min-entropy:

$$H^{\epsilon}_{min}(A_1^n|B)_\rho \gtrsim \sum_{k=1}^{n} H^{\epsilon'}_{min}\left(A_k \middle| A_1^{k-1} B\right)_{\sigma^{(k)}} - n\,\mathrm{small}(\epsilon, |A|)$$

can be shown to be **false.**

Approximate independence

The state $\rho_{A_1^n B}$ is such that for every $1 \leq k \leq n$,

$$\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$$

Note that these ϵ are the same. The smoothing parameter depends on ϵ.

for some $\epsilon > 0$. For simplicity assume $\rho_{A_k} = \rho_{A_1}$ for all k.

Problem: To prove that the smooth min-entropy of A_1^n given B is *large*, or specifically,

$$H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho.$$

Need the smoothing parameter to be independent of n. Particularly the results should work in the regime $n \gg 1/\epsilon$.

Approximate independence: triangle inequality

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$. Need to prove that $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

If we were to try to bound the trace distance between $\rho_{A_1^n B}$ and $\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B$, then the best we can do is:

$$\|\rho_{A_1^n B} - \rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B\|_1$$
$$\leq \sum_{k=1}^{n} \|\rho_{A_n} \otimes \rho_{A_{n-1}} \otimes \cdots \otimes \rho_{A_{k+1}} (\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B})\|_1$$
$$\leq n\epsilon$$

and if $n \gg 1/\epsilon$ then this bound is trivial.

Entropic triangle inequality

Though, $n\epsilon$ trace distance yields a trivial bound, $n\epsilon$ is small as "information" distance.

<u>Idea</u>: Instead of a metric based triangle inequality, use an entropy based triangle inequality:

Suppose, we want to bound $H_{min}^{\delta}(A|B)_{\rho}$ of ρ_{AB} in terms of $H_{min}(A|B)_{\eta}$ of another state η_{AB}.

Say $D_{max}^{\delta}(\rho_{AB}||\eta_{AB}) = d$. Then, there exists $\tilde{\rho}_{AB} \approx_{\delta} \rho_{AB}$ such that:

$$\tilde{\rho}_{AB} \leq 2^{d}\eta_{AB}$$

Entropic triangle inequality

Though, $n\epsilon$ trace distance yields a trivial bound, $n\epsilon$ is small as "information" distance.

<u>Idea</u>: Instead of a metric based triangle inequality, use an entropy based triangle inequality:

Suppose, we want to bound $H^{\delta}_{min}(A|B)_{\rho}$ of ρ_{AB} in terms of $H_{min}(A|B)_{\eta}$ of another state η_{AB}.

Say $D^{\delta}_{max}(\rho_{AB}||\eta_{AB}) = d$. Then, there exists $\tilde{\rho}_{AB} \approx_{\delta} \rho_{AB}$ such that:

$$\begin{aligned} \tilde{\rho}_{AB} &\leq 2^{d}\eta_{AB} \\ &\leq 2^{d}\, 2^{-H_{min}(A|B)_{\eta}}\, I_A \otimes \sigma_B \end{aligned}$$

$$\Rightarrow H^{\delta}_{min}(A|B)_{\rho} \geq H_{min}(A|B)_{\eta} - D^{\delta}_{max}(\rho_{AB}||\eta_{AB})$$

Entropic triangle inequality

H_{min}^{δ} triangle inequality:

$$H_{min}^{\delta}(A|B)_{\rho} \geq H_{min}(A|B)_{\eta} - D_{max}^{\delta}(\rho_{AB}||\eta_{AB})$$

Lemma: Can be improved to:

$$H_{min}^{\epsilon+\delta}(A|B)_{\rho} \geq H_{\alpha}(A|B)_{\eta} - \frac{\alpha}{\alpha-1} D_{max}^{\delta}(\rho_{AB}||\eta_{AB}) - \frac{g(\epsilon,\delta)}{\alpha-1}$$

for $0 < \epsilon, \delta < 1/2$ and $\alpha \in (1,2]$.

This is implied by the triangle inequality:

$$\widetilde{D}_{\alpha}(\rho||\sigma) \leq \widetilde{D}_{\alpha}(\eta||\sigma) + \frac{\alpha}{\alpha-1} \mathrm{D}_{max}(\rho||\eta)$$

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$. Need to prove that $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

How can we bound D_{max}^{δ} distance between $\rho_{A_1^n B}$ and $\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B$?

If instead we had to bound relative entropy distance, then we have:

$$D(\rho_{A_1^n B} || \rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B) = I(A_1 : A_2 : \cdots : A_n : B)_\rho$$

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$. Need to prove that $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

How can we bound D_{max}^{δ} distance between $\rho_{A_1^n B}$ and $\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B$?

If instead we had to bound relative entropy distance, then we have:

$$
\begin{aligned}
D(\rho_{A_1^n B} || \, \rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B) &= I(A_1 : A_2 : \cdots : A_n : B)_\rho \\
&= \sum_{k=1}^{n} I\left(A_k : A_1^{k-1} B\right)_\rho
\end{aligned}
$$

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$. Need to prove that $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

How can we bound D_{max}^{δ} distance between $\rho_{A_1^n B}$ and $\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B$?

If instead we had to bound relative entropy distance, then we have:

$$\begin{aligned} D(\rho_{A_1^n B} || \rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B) &= I(A_1 : A_2 : \cdots : A_n : B)_\rho \\ &= \sum_{k=1}^{n} I\left(A_k : A_1^{k-1} B\right)_\rho \\ &\leq \sum_{k=1}^{n} I\left(A_k : A_1^{k-1} B\right)_{\rho_{A_k} \otimes \rho_{A_1^{k-1} B}} + f(\epsilon, |A|) \end{aligned}$$

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$. Need to prove that $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

How can we bound D_{max}^{δ} distance between $\rho_{A_1^n B}$ and $\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B$?

If instead we had to bound relative entropy distance, then we have:

$$
\begin{aligned}
D(\rho_{A_1^n B} || \rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B) &= I(A_1: A_2: \cdots : A_n: B)_\rho \\
&= \sum_{k=1}^{n} I\left(A_k: A_1^{k-1} B\right)_\rho \\
&\leq nf(\epsilon, |A|)
\end{aligned}
$$

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$. Need to prove that: $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

For $\rho_{A_1^n B}$, we have: $D(\rho_{A_1^n B}|| \ \rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B) \leq nf(\epsilon, |A|)$.

<u>**Substate theorem**</u> **[JRS02]:** For two state ρ and σ and $\delta \in (0,1)$, we have

$$D_{max}^{\delta}(\rho||\sigma) \leq \frac{D(\rho||\sigma) + 1}{\delta^2} + [\text{small term}].$$

This implies for $\delta = f(\epsilon, |A|)^{1/4} = O\left(\epsilon \log \frac{|A|}{\epsilon}\right)^{1/4}$

$$D_{max}^{\delta}(\rho_{A_1^n B}|| \ \rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B) \leq n\delta^2 + O\left(\frac{1}{\delta^2}\right)$$

[JRS02]: R. Jain, J. Radhakrishnan, and P. Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$.

Need to prove that: $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

For $\delta = O\left(\epsilon \log \frac{|A|}{\epsilon}\right)^{1/4}$: $D_{max}^{\delta}(\rho_{A_1^n B} || \underbrace{\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B}_{=: \eta_{A_1^n B}}) \leq n\delta^2 + O\left(\frac{1}{\delta^2}\right)$

Using the entropic triangle inequality,

$$H_{min}^{2\delta}(A_1^n|B)_\rho \geq H_\alpha(A_1^n|B)_\eta - \frac{\alpha}{\alpha - 1} D_{max}^{\delta}(\rho_{A_1^n B} || \eta_{A_1^n B}) - \frac{g(\delta, \delta)}{\alpha - 1}$$

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$.

Need to prove that: $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

For $\delta = O\left(\epsilon \log \frac{|A|}{\epsilon}\right)^{1/4}$: $D_{max}^{\delta}(\rho_{A_1^n B} || \underbrace{\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B}_{=:\eta_{A_1^n B}}) \leq n\delta^2 + O\left(\frac{1}{\delta^2}\right)$

Using the entropic triangle inequality,

$$
\begin{aligned}
H_{min}^{2\delta}(A_1^n|B)_\rho &\geq H_\alpha(A_1^n|B)_\eta - \frac{\alpha}{\alpha-1} D_{max}^{\delta}(\rho_{A_1^n B}||\eta_{A_1^n B}) - \frac{g(\delta,\delta)}{\alpha-1} \\
&\geq nH_\alpha(A_1)_\rho - \frac{\alpha}{\alpha-1} n\delta^2 - \frac{1}{\alpha-1} O\left(\frac{1}{\delta^2}\right)
\end{aligned}
$$

Approximate independence

$\rho_{A_1^n B}$ is such that for every k: $\|\rho_{A_1^k B} - \rho_{A_k} \otimes \rho_{A_1^{k-1} B}\|_1 \leq \epsilon$.

Need to prove that: $H_{min}^{f(\epsilon)}(A_1^n|B)_\rho \gtrsim nH(A_1)_\rho$.

For $\delta = O\left(\epsilon \log \frac{|A|}{\epsilon}\right)^{1/4}$: $D_{max}^{\delta}(\rho_{A_1^n B} || \underbrace{\rho_{A_1} \otimes \rho_{A_2} \otimes \cdots \otimes \rho_B}_{=: \eta_{A_1^n B}}) \leq n\delta^2 + O\left(\frac{1}{\delta^2}\right)$

Using the entropic triangle inequality,

$$
\begin{aligned}
H_{min}^{2\delta}(A_1^n|B)_\rho &\geq H_\alpha(A_1^n|B)_\eta - \frac{\alpha}{\alpha - 1} D_{max}^{\delta}(\rho_{A_1^n B} || \eta_{A_1^n B}) - \frac{g(\delta,\delta)}{\alpha - 1} \\
&\geq nH_\alpha(A_1)_\rho - \frac{\alpha}{\alpha - 1} n\delta^2 - \frac{1}{\alpha - 1} O\left(\frac{1}{\delta^2}\right) \\
&\geq n\big(H(A_1)_\rho - 2\delta\big) - O\left(\frac{1}{\delta^3}\right)
\end{aligned}
$$

Choose $\alpha = 1 + \delta$ and use continuity of H_α:

Quick and dirty proofs of security

For CHSH based sequential device-independent quantum key distribution (DIQKD), it can easily be shown that there exists a winning threshold ω_0, such that if the protocol does not abort:

Here A_k is Alice's answer in the kth round

$$H\left(A_k \middle| A_1^{k-1}\left[\mathrm{Eve's\ info}\right]\right)_\rho \geq 1-\epsilon$$

Problem is that the winning threshold depends on the smoothing parameter (/security parameter).

for every k.
This implies that:

$$\|\rho_{A_1^k E} - \rho_{A_k} \otimes \rho_{A_1^{k-1}E}\|_1 \leq \mathrm{small}(\epsilon)$$

which in turn implies: $H_{min}^{f(\epsilon)}(A_1^n|E)_\rho \geq \Omega(n)$.

Source correlations

BB84 QKD protocol with perfect source:

In each round:

$x \in_R \{0,1\}$,
$\theta \in_R \{X, Z\}$ → Source → $|x\rangle_\theta$

State produced by Alice in every round:

$$\hat{\rho}_{X\Theta A} = \sum_{x,\theta} \frac{1}{4} |x,\theta\rangle\langle x,\theta| \otimes H^\theta |x\rangle\langle x| H^\theta$$

and in n rounds, Alice produces $\hat{\rho}_{X\Theta A}^{\otimes n}$.

Approximate independence: applications

Dealing with source correlations:

Suppose the source $\rho_{X_1^n \Theta_1^n A_1^n}$ satisfies the assumptions:

1. Local states are approximately correct: $\|\rho_{X_k \Theta_k A_k} - \hat{\rho}_{X\Theta A}\|_1 \leq \epsilon$.
2. Classical random variables are perfectly produced

Approximate independence: applications

Dealing with source correlations:

For $\epsilon_s = \left(g'(\epsilon)\right)^{1/4}$:

$$D_{max}^{\epsilon_s}\left(\rho_{X_1^n \Theta_1^n A_1^n} || \underbrace{\hat{\rho}_{X_1 \Theta_1 A_1}^{(\epsilon)} \otimes \cdots \otimes \hat{\rho}_{X_n \Theta_n A_n}^{(\epsilon)}}_{=:\eta}\right) \leq n\sqrt{g'(\epsilon)} + O_\epsilon(1)$$

Using the triangle inequality:

$$H_{min}^{\epsilon_s+\delta}\left(X_1^n | E \Theta_1^n \widehat{\Theta}_1^n\right)_{\underbrace{QKD(\rho)}_{\text{QKD protocol performed on the state produced by the source}}} \geq H_\alpha\left(X_1^n | E \Theta_1^n \widehat{\Theta}_1^n\right)_{\underbrace{QKD(\eta)}_{\text{QKD protocol performed on i.i.d depolarised perfect states}}} - \frac{\alpha}{\alpha - 1} D_{max}^{\epsilon_s}(\rho || \eta) - O(1)$$

Approximate independence: applications

Problem: the security parameter is lower bounded by the noise of the source
→ Can be made arbitrarily small by instead using quantum sampling [BF10]

Dealing with source correlations:

For $\epsilon_s = \left(g'(\epsilon)\right)^{1/4}$:

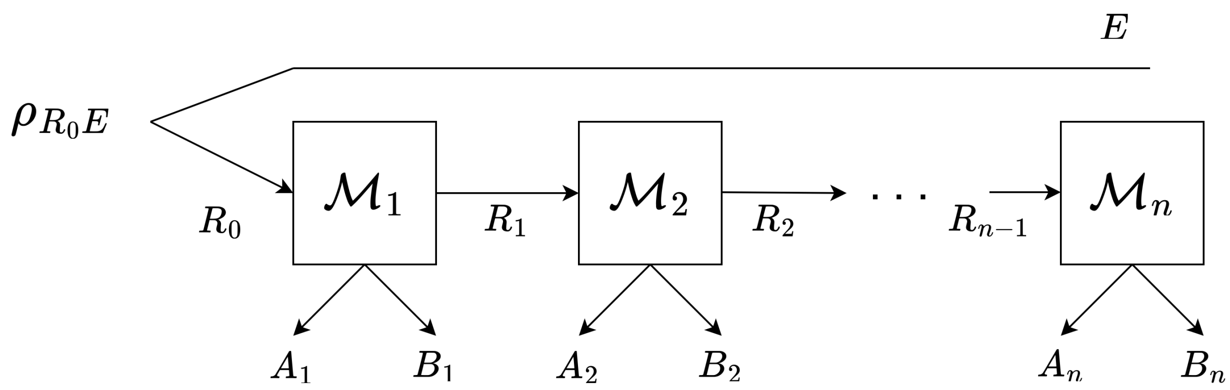
$$D_{max}^{\epsilon_s}\left(\rho_{X_1^n\Theta_1^nA_1^n}\,||\underbrace{\hat{\rho}^{(\epsilon)}_{X_1\Theta_1A_1}\otimes\cdots\otimes\hat{\rho}^{(\epsilon)}_{X_n\Theta_nA_n}}_{=:\eta}\right)\leq n\sqrt{g'(\epsilon)}+O_\epsilon(1)$$

Using the triangle inequality:

$$H_{min}^{\epsilon_s+\delta}\left(X_1^n|E\Theta_1^n\hat{\Theta}_1^n\right)_{QKD(\rho)}\geq H_\alpha\left(X_1^n|E\Theta_1^n\hat{\Theta}_1^n\right)_{QKD(\eta)}-\frac{\alpha}{\alpha-1}\underbrace{n\sqrt{g'(\epsilon)}}_{\text{Leads to }\left(g'(\epsilon)\right)^{1/4}\text{ entropy loss per round}}-O(1)$$

[BF10]: Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications.

Approximate entropy accumulation



Entropy accumulation [DFR20] states for $\rho_{A_1^n B_1^n E} \coloneqq \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0 E})$:

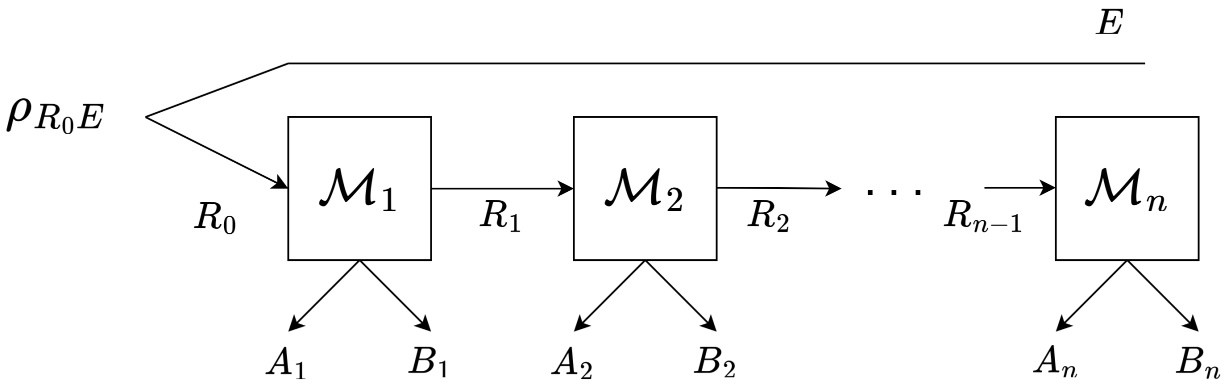
$$H_{min}^{\delta}(A_1^n|B_1^n E)_\rho \geq \sum_{k=1}^{n} \inf_{\omega_{RR_{k-1}}} H(A_k|B_k R)_{\mathcal{M}_k(\omega)} - O(\sqrt{n})$$

as long as for every $1 \leq k \leq n$:

$$B_k \leftrightarrow B_1^{k-1} E \leftrightarrow A_1^{k-1}$$

We wish to relax these assumptions

Approximate entropy accumulation



Suppose, instead we have $\|\mathcal{M}_k - \mathcal{N}_k\|_\diamond \leq \epsilon$ and $\mathcal{N}_k$ satisfy some nice Markov chain properties

It is sufficient to lower bound smooth min-entropy of $\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E})$ in terms of $\mathcal{N}_n \circ \cdots \circ \mathcal{N}_1(\rho_{R_0E})$.

Approximate entropy accumulation

In smooth max-relative entropy distance:

$$D_{max}^{\epsilon\prime}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right)||\mathcal{N}_n \circ \cdots \circ \mathcal{N}_1\left(\rho_{R_0E}\right)\right)$$
$$\leq \widetilde{D}_\alpha\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right)||\mathcal{N}_n \circ \cdots \circ \mathcal{N}_1\left(\rho_{R_0E}\right)\right) + \frac{O(1)}{\alpha - 1}$$

Approximate entropy accumulation

In smooth max-relative entropy distance:

$$
\begin{aligned}
&D_{max}^{\epsilon\prime}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E}) || \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1(\rho_{R_0E})\right) \\
&\leq \widetilde{D}_\alpha\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E}) || \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1(\rho_{R_0E})\right) + \frac{O(1)}{\alpha - 1} \\
&\leq \widetilde{D}_\alpha\left(\mathcal{M}_{n-1} \circ \cdots \circ \mathcal{M}_1(\rho_{R_0E}) || \mathcal{N}_{n-1} \circ \cdots \circ \mathcal{N}_1(\rho_{R_0E})\right) + \widetilde{D}_\alpha^{reg}(\mathcal{M}_n || \mathcal{N}_n) + \frac{O(1)}{\alpha - 1}
\end{aligned}
$$

Approximate entropy accumulation

In smooth max-relative entropy distance:

$$
\begin{aligned}
&D_{max}^{\epsilon'}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0 E}\right) || \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1\left(\rho_{R_0 E}\right)\right) \\
&\leq \widetilde{D}_\alpha\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0 E}\right) || \mathcal{N}_n \circ \cdots \circ \mathcal{N}_1\left(\rho_{R_0 E}\right)\right) + \frac{O(1)}{\alpha - 1} \\
&\leq \widetilde{D}_\alpha\left(\mathcal{M}_{n-1} \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0 E}\right) || \mathcal{N}_{n-1} \circ \cdots \circ \mathcal{N}_1\left(\rho_{R_0 E}\right)\right) + \widetilde{D}_\alpha^{reg}(\mathcal{M}_n || \mathcal{N}_n) + \frac{O(1)}{\alpha - 1} \\
&\leq \sum_{k=1}^{n} \widetilde{D}_\alpha^{reg}(\mathcal{M}_k || \mathcal{N}_k) + \frac{O(1)}{\alpha - 1}
\end{aligned}
$$

If each of these terms were small, we would be done

But $\|\mathcal{M}_k - \mathcal{N}_k\|_\diamond \leq \epsilon$ does not imply any kind of bound on $\widetilde{D}_\alpha^{reg}(\mathcal{M}_k || \mathcal{N}_k)$.

Approximate entropy accumulation

Same argument with mixed channels $\mathcal{N}_k^{\delta} \coloneqq (1-\delta)\mathcal{N}_k + \delta\mathcal{M}_k$:

$$
\begin{aligned}
&D_{max}^{\epsilon'}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right) || \mathcal{N}_n^{\delta} \circ \cdots \circ \mathcal{N}_1^{\delta}\left(\rho_{R_0E}\right)\right) \\
&\leq \widetilde{D}_{\alpha}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right) || \mathcal{N}_n^{\delta} \circ \cdots \circ \mathcal{N}_1^{\delta}\left(\rho_{R_0E}\right)\right) + \frac{O(1)}{\alpha-1} \\
&\leq \widetilde{D}_{\alpha}\left(\mathcal{M}_{n-1} \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right) || \mathcal{N}_{n-1}^{\delta} \circ \cdots \circ \mathcal{N}_1^{\delta}\left(\rho_{R_0E}\right)\right) + \widetilde{D}_{\alpha}^{reg}(\mathcal{M}_n || \mathcal{N}_n^{\delta}) + \frac{O(1)}{\alpha-1} \\
&\leq \sum_{k=1}^{n} \widetilde{D}_{\alpha}^{reg}(\mathcal{M}_k || \mathcal{N}_k^{\delta}) + \frac{O(1)}{\alpha-1}
\end{aligned}
$$

Approximate entropy accumulation

Same argument with mixed channels $\mathcal{N}_k^{\delta} := (1-\delta)\mathcal{N}_k + \delta\mathcal{M}_k$:

$$D_{max}^{\epsilon'}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right) || \mathcal{N}_n^{\delta} \circ \cdots \circ \mathcal{N}_1^{\delta}\left(\rho_{R_0E}\right)\right)$$

$$\leq \widetilde{D}_{\alpha}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right) || \mathcal{N}_n^{\delta} \circ \cdots \circ \mathcal{N}_1^{\delta}\left(\rho_{R_0E}\right)\right) + \frac{O(1)}{\alpha - 1}$$

$$\leq \widetilde{D}_{\alpha}\left(\mathcal{M}_{n-1} \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right) || \mathcal{N}_{n-1}^{\delta} \circ \cdots \circ \mathcal{N}_1^{\delta}\left(\rho_{R_0E}\right)\right) + \widetilde{D}_{\alpha}^{reg}(\mathcal{M}_n || \mathcal{N}_n^{\delta}) + \frac{O(1)}{\alpha - 1}$$

$$\leq \sum_{k=1}^{n} \widetilde{D}_{\alpha}^{reg}(\mathcal{M}_k || \mathcal{N}_k^{\delta}) + \frac{O(1)}{\alpha - 1}$$

$$\leq \sum_{k=1}^{n} D_{\alpha}^{\#}(\mathcal{M}_k || \mathcal{N}_k^{\delta}) + \frac{O(1)}{\alpha - 1}$$

Sharp Rényi divergence [FF21]

[FF21]: Hamza Fawzi and Omar Fawzi. Defining quantum divergences via convex optimization. Quantum.

Approximate entropy accumulation

Lemma: If $\frac{1}{2}\|\mathcal{N}-\mathcal{M}\|_\diamond \leq \epsilon$, then for $\mathcal{N}^\delta \coloneqq (1-\delta)\mathcal{N} + \delta\mathcal{M}$ and $\alpha > 1$, we have

$$D_\alpha^\#(\mathcal{M}||\mathcal{N}^\delta) \leq \frac{\alpha+1}{\alpha-1}\log\left((1+\sqrt{\epsilon})^{\frac{\alpha}{\alpha+1}} + \left(\frac{\sqrt{\epsilon}}{\delta^\alpha}\right)^{\frac{1}{\alpha+1}}\right).$$

This is small if, say $\delta = \epsilon^{\frac{1}{4\alpha}}$.

We get:

$$D_{max}^{\epsilon\prime}\left(\mathcal{M}_n \circ \cdots \circ \mathcal{M}_1\left(\rho_{R_0E}\right)||\mathcal{N}_n^\delta \circ \cdots \circ \mathcal{N}_1^\delta\left(\rho_{R_0E}\right)\right) \leq \sum_{k=1}^n D_\alpha^\#\left(\mathcal{M}_k||\mathcal{N}_k^\delta\right) + \frac{O(1)}{\alpha-1}$$
$$\leq n \cdot O(\epsilon^{\frac{1}{12}})$$

for $\alpha = 2$.

Approximate entropy accumulation

We have:

$$\rho_{A_1^n B_1^n E} = \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0 E})$$
$$\eta_{A_1^n B_1^n E} = \mathcal{N}_n^\delta \circ \cdots \circ \mathcal{N}_1^\delta\left(\rho_{R_0 E}\right)$$

Using the entropic triangle inequality:

$$H_{min}^{\epsilon\prime+\epsilon\prime\prime}(A_1^n|B_1^n E)_\rho \geq H_\alpha(A_1^n|B_1^n E)_\eta - \frac{\alpha}{\alpha-1}\underbrace{D_{max}^{\epsilon\prime}(\rho||\eta)}_{n \cdot O(\epsilon^{\frac{1}{12}})\ ✅} - \frac{g(\epsilon', \epsilon'')}{\alpha - 1}$$

Can't use EAT on this because $\mathcal{N}_k^\delta :=$ $(1-\delta)\mathcal{N}_k + \delta\mathcal{M}_k$, which mixes the nice channel with the bad channel $\mathcal{M}_k$- this could create correlations between B_k and the previous answers A_1^{i-1}

Approximate entropy accumulation

We have:

$$\rho_{A_1^n B_1^n E} = \mathcal{M}_n \circ \cdots \circ \mathcal{M}_1(\rho_{R_0 E})$$
$$\eta_{A_1^n B_1^n E} = \mathcal{N}_n^\delta \circ \cdots \circ \mathcal{N}_1^\delta(\rho_{R_0 E})$$

Using the entropic triangle inequality:

$$H_{min}^{\epsilon' + \epsilon''}(A_1^n | B_1^n E)_\rho \geq H_\alpha(A_1^n | B_1^n E)_\eta - \frac{\alpha}{\alpha - 1} \underbrace{D_{max}^{\epsilon'}(\rho || \eta)}_{n \cdot O(\epsilon^{\frac{1}{12}})} - \frac{g(\epsilon', \epsilon'')}{\alpha - 1}$$

✅

Still $\mathcal{N}_k^\delta := (1 - \delta)\mathcal{N}_k + \delta \mathcal{M}_k$ is good enough- like flipping a coin every round and choosing between the good and bad channel.

✅

Approximate entropy accumulation

Theorem:

Suppose $|A_k| = |A|$, $|B_k| = |B|$ and

Need the size of the side information to be bounded- is necessary

1. Approximation: $\frac{1}{2}\|\mathcal{M}_k - \mathcal{N}_k\|_\diamond \leq \epsilon$.
2. Markov conditions: for every $1 \leq i \leq k-1$ and for all choices of channels $\Phi_i \in \{\mathcal{M}_i, \mathcal{N}_i\}$, the state $\mathcal{N}_k \circ \Phi_{k-1} \circ \cdots \circ \Phi_1(\rho_{R_0E})$ satisfies $B_k \leftrightarrow B_1^{k-1}E \leftrightarrow A_1^{k-1}$,

then

$$H_{min}^{\epsilon\prime+\epsilon\prime\prime}(A_1^n|B_1^nE)_\rho \geq \sum_{k=1}^{n} \inf_{\omega_{RR_{k-1}}} H(A_k|B_kR)_{\mathcal{N}_k(\omega)} - nO\left(\epsilon^{1/24}\right) - O\left(\frac{1}{\epsilon^{1/24}}\right)$$

Smoothing error is arbitrary

Entropy loss per round is poor due to bad bound for channel divergence

tldr; triangle inequality:

$$d(\rho,\sigma) \leq d(\rho,\eta) + d(\eta,\sigma)$$

$$H_{min}^{\epsilon+\delta}(A|B)_\rho$$
$$\geq H_\alpha(A|B)_\eta - \frac{\alpha}{\alpha-1} D_{max}^{\delta}(\rho_{AB}||\eta_{AB}) - \frac{g(\epsilon,\delta)}{\alpha-1}$$

Summary

We used the entropic triangle inequality to:

1. create a smooth min-entropy lower bound for approximately independent registers
    - can also create a "weak" approximate AEP– can we do better?

2. provide a solution to the source correlation problem
    - is it practically good enough?
    - can we use different/ better assumptions?
    - better analysis?

3. create an approximate entropy accumulation theorem
    - improve the channel divergence bounds/ rate loss
    - can we relax assumptions further?

Thank you.