Title: Approximate entropy accumulation

Speakers: Frédéric Dupuis

Collection/Series: Quantum Information

Subject: Quantum Information

Date: May 28, 2025 - 11:00 AM

URL: https://pirsa.org/25050048

Abstract:

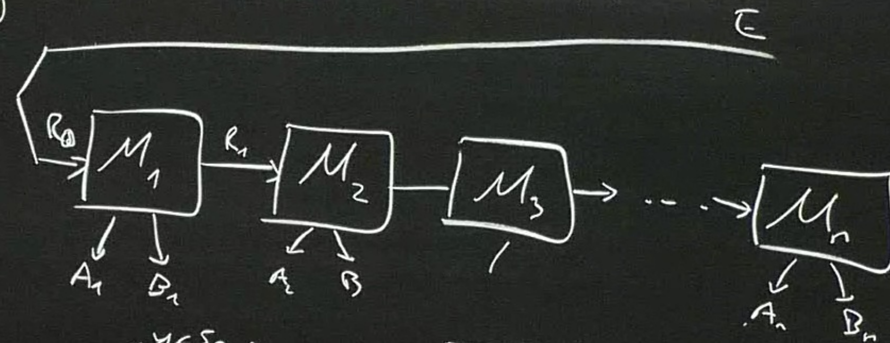
The entropy accumulation theorem (EAT) allows us to lower bound the min-entropy of a state that can be generated by a chain of quantum channels satisfying a Markov chain condition, and can be used to prove the security of QKD protocols, including device-independent ones. However, one of its drawbacks is that it only applies to states with a fairly rigid structure; in particular, the Markov chain condition must be satisfied exactly. What happens when we relax this assumption by allowing the required structure to be satisfies only approximately? Does doing so lead to interesting applications? We answer both questions by the affirmative: we present two flavours of approximate EAT, and show that it can be used to prove the security of parallel device-independent QKD, and to analyze QKD protocols under source correlations. Along the way, we will introduce the concept of "approximation chain" which underpins the new results.

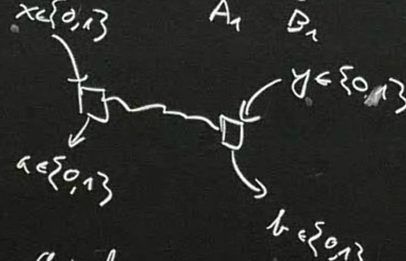
This is joint work with Ashutosh Marwah; the talk will cover material from 2412.06723, 2402.12346, and 2308.11736.

Approximate entropy accumulation

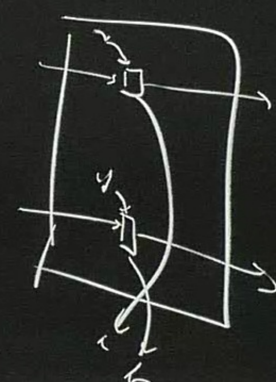
j.w.w. Ashutosh Marwah

- 2412.06723
- 2402.12346
- 2308.11736





$a + b = xy \pmod 2$



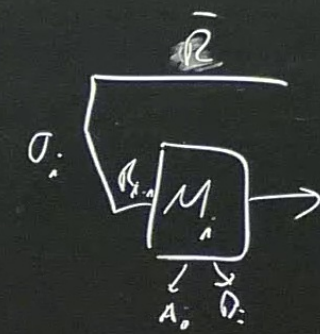
$$H(A_1^n | B_1^n E) \geq nh - o(n)$$

ρ_{XB}: $H_{min}(X|B)_\rho := -\log \Pr[\text{guessing } X \text{ by measuring } B]$.

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

$$H_{min}(A|B)_\rho = -\inf_{\sigma_B} D_{max}(\rho_{AB} \| \mathbb{1}_A \otimes \sigma_B).$$

$$H^\varepsilon_{min}(A|B)_\rho = \max_{\sigma : P(\rho,\sigma) \leq \varepsilon} H_{min}(A|B)_\sigma .$$



EAT: $H^\varepsilon_{min}(A_1^n | B_1^n E)_\rho \geq \sum \min_{\sigma_i} H(A_i | B_i \bar{R})_{\mathcal{M}_i(\sigma_i)} - O(\sqrt{n})$.

if $\forall i$: $A_1^{i-1} \leftrightarrow B_1^{i-1} E \leftrightarrow B_i$.

① Relax the EAT to channels that approx satisfy Markov :

$\exists \mathcal{N}_i \quad \frac{1}{2}\|\mathcal{M}_i - \mathcal{N}_i\|_\diamond \leq \varepsilon , \quad \mathcal{M}_i \circ \mathcal{N}_{i-1} \circ \cdots \circ \mathcal{N}_1$ satisfies Markov.

$$\rightarrow H_{min}^{\varepsilon}(A_1^n|B_1^n E)_\rho \geq \sum \inf_\sigma H(A_i|B_i \bar{R})_{\mathcal{N}_i(\sigma)} - O(\sqrt{n}).$$

$\hookrightarrow \sim \varepsilon^{1/24}.$

② Sps we have a state $\rho_{A_1^n B_1^n E}$ s.t. $\exists \begin{cases} \text{channel } \mathcal{M}_i \\ \text{states } \tilde{\rho}^{(i)} \end{cases}$

s.t. $\forall i: \frac{1}{2}\left\|\rho_{A_1^i B_1^i E} - \mathcal{M}_i\left(\tilde{\rho}^{(i)}_{A_1^{i-1} B_1^{i-1} R_{i-1} E}\right)\right\|_1 \leq \varepsilon.$

$$\Rightarrow H_{min}^{f(\varepsilon)}(A_1^n|B_1^n E) \geq \sum \inf_\sigma H(A_i|B_i \bar{R})_{\mathcal{M}_i(\sigma)} - O(\sqrt{n}).$$

Approximation chain: $\rho_{A_1^n B_1^n E}$, $\sigma^{(i)}_{A_1^i B_1^i E}$ is an approx chain for ρ if.

$\forall i$: $\| \rho_{A_1^i B_1^i E} - \sigma^{(i)}_{A_1^i B_1^i E} \|_1 \leq \varepsilon$. & satisfies Markov:

$$H(A_1^n | B_1^n E)_\rho = \sum_i H(A_i | A_1^{i-1} B_1^n E)_\rho$$

$$\leq \sum_i H(A_i | A_1^{i-1} B_1^i E)_\rho$$

$$\geq \sum_i \left(H(A_i | A_1^{i-1} B_1^i E)_{\sigma^{(i)}} - f(\varepsilon) \right).$$

Entropic triangle inequality:

ρ_{AB}, η_{AB}:

$$H_{\min}^{\delta_1+\delta_2}(A|B)_\rho \geq \underbrace{H_\alpha(A|B)_\eta}_{\alpha \in \mathbb{R},} - \frac{\alpha}{\alpha-1} D_{\max}^{\delta_2}(\rho\|\eta) - \frac{g(\delta_1,\delta_2)}{\alpha-1}.$$

$\alpha > 1$	$\sim H_{\min}$
$\alpha = 1$	$\sim H$
$\alpha < 1$	$\sim H_{\max}.$

$$H_{min}(A|B)_\rho \geq H_\alpha(A|B)_\eta - \frac{\alpha}{\alpha-1} D_{max}(\rho\|\eta) - \frac{1}{\alpha-1}$$

ρ_{AB} η_{AB}

$\alpha \in \mathbb{R}$, $\alpha > 1 \sim H_{min}$

$\alpha = 1 \sim H$

$\alpha < 1 \sim H_{max}$

$$H_{min}^{\delta_1+\delta_2}(A_1^n|B_1^n E)_\rho \geq \underbrace{H_\alpha(A_1^n|B_1^n E)_\eta}_{EAT} - \frac{\alpha}{\alpha-1} \underbrace{D_{max}^{\delta_2}(\rho\|\eta)} - \frac{g(\delta_1,\delta_2)}{\alpha-1}.$$

Substitute thm: $D_{max}^{\delta_2}(\rho\|\eta) \leq \frac{D_m(\rho\|\eta)+1}{\delta_2^2} + \log\frac{1}{1-\delta_2^2}$

Application to parallel DIQKD

$w(G)^{\Theta(n)}$

Sequential: $w(G)^n$

n-fold parallel rep

Parallel: $w(G^n) = \Pr\left[\bigwedge_{i=1}^{n} W_i\right] = \prod_{i=1}^{n} \Pr\left[W_i \,\middle|\, \bigwedge_{j=1}^{i-1} W_j\right]$

event that win i-th game

Raz: Find a set $C \subseteq \{1,\dots,n\}$ s.t. $|C| \in \Theta(n)$

$C = \{i_1, \dots, i_m\}$, $|C| = m$

Quantum: BVY

$w(G^n) \leq \Pr\left[\bigwedge_{j \in C} W_j\right] = \prod_{j=1}^{m} \Pr\left[W_{i_j} \,\middle|\, \bigwedge_{k=1}^{j-1} W_{i_k}\right] \approx \prod \Pr\left[W_{i_j}\right] \leq w(G)^m.$