2025 IEEE European School of Information Theory (ESIT)

Minimum Rényi Entropy Couplings

Anuj Yadav   Yanina Shkel

Problem Statement

Given: m marginal distributions $\{P_i\}_{i=1}^m$.
Find: coupling $C^\star(X_1, X_2, \cdots, X_m) \in \mathscr{C}$.
Such that:

1. $X_i \sim P_i$ for every $i \in [m]$.
2. $H_\alpha(C^\star) = \min_{C\in\mathscr{C}} H_\alpha(C)$, $\forall \alpha \in [0,\infty)$.

It is a **NP-Hard** problem in the support size of the distributions.

Lower Bounds - Converse type results.

Upper Bounds - Achievability type results.

Applications:

- Minimum Entropy functional representation.
- Entropic Causal Inference.
- Perfectly secure Steganography.
- Secure data compression, etc…

Interlude

Majorization ($\preceq$)

Let $P = (p_1, p_2 \cdots)$ and $Q = (q_1, q_2, \cdots)$ be PMFs in the non-increasing order. Then, we say : $Q \preceq P$ if $\sum_{i=1}^k q_i \le \sum_{i=1}^k p_i$ for every $k \ge 1$.

Schur Concavity: $Q \preceq P \implies H_\alpha(Q) \ge H_\alpha(P)$.

Greatest lower bound for $\{P_i\}_{i=1}^m$: $Q \preceq \bigwedge_{j=1}^m P_j \preceq P_i$ for every Q, $i \in [m]$.

Information-Spectrum Majorization ($\preceq_\imath$)

We say $Q \preceq_\imath P$, if $\mathbb{F}_{\imath_Q}(t) \le \mathbb{F}_{\imath_P}(t)$ i.e., $\mathbb{P}\left[\imath_Q \le t\right] \le \mathbb{P}\left[\imath_P \le t\right]$, $\forall t \in [0,\infty)$.

Fact 1: $Q \preceq_\imath P \implies Q \preceq P$.

Fact 2: Let $\mathscr{F} = \{Q \colon Q \preceq_\imath P_i \quad \forall i \in [m]\}$. Then, $\exists Q^* \in \mathscr{F}$ such that $Q \preceq Q^*$, for every $Q \in \mathscr{F}$.

Lower Bounds

Trivial Lower Bound 1

$\forall\, C(X_1, \cdots, X_m) \in \mathscr{C}$, we see that $C(X_1, \cdots, X_m) \sqsubseteq P_i$, $\forall\, i \in [m]$.

Aggregation ($\sqsubseteq$) implies Majorization ($\preceq$).

Thus, $C^\star(X_1, \cdots, X_m) \preceq P_i$, $\forall\, i \in [m] \Longrightarrow H_\alpha(C^\star) \ge \max_{i\in[m]} H_\alpha(P_i)$

Existing Lower Bound 2 [Cicalese et al. '19]

($\preceq$) is a partial order and forms a compelete lattice.

Thus, $C^\star(X_1, \cdots, X_m) \preceq \bigwedge_{j=1}^m P_j \preceq P_i$, $\forall\, i \in [m]$.

Consequently, we have $H_\alpha(C^\star) \ge H_\alpha\left(\bigwedge_{j=1}^m P_j\right)$.

Main Result 1 [Yadav-Shkel '23]

Theorem: $\forall\, C(X_1, \cdots, X_m) \in \mathscr{C}$, $\mathbb{P}\left[\imath_C > t\right] \ge \max_{i\in[m]} \mathbb{P}\left[\imath_{P_i} > t\right]$, $\forall t \in [0,\infty)$.

i.e., $\mathbb{F}_{\imath_{C^\star}}(t) \le \mathbb{F}_{\imath_{P_i}}(t) \implies C^\star(X_1, \cdots, X_m) \preceq_\imath P_i$, $\forall\, i \in [m]$.

Therefore, we have

$$H(C^\star) = \mathbb{E}[\imath_{C^\star}] = \int_0^\infty \left(1 - \mathbb{F}_{\imath_{C^\star}}(t)\right) dt \ge \int_0^\infty \max_{i\in[m]} \left(1 - \mathbb{F}_{\imath_{P_i}}(t)\right) dt$$

Main Result 2 [Yadav-Shkel '23]

Theorem: Let $\mathscr{S} = \{Q \colon Q \preceq_\imath P_i, \forall i \in [m]\}$. Then, $\exists Q^* \in \mathscr{S}$ such that $Q \preceq Q^*, \forall Q \in \mathscr{S}$.

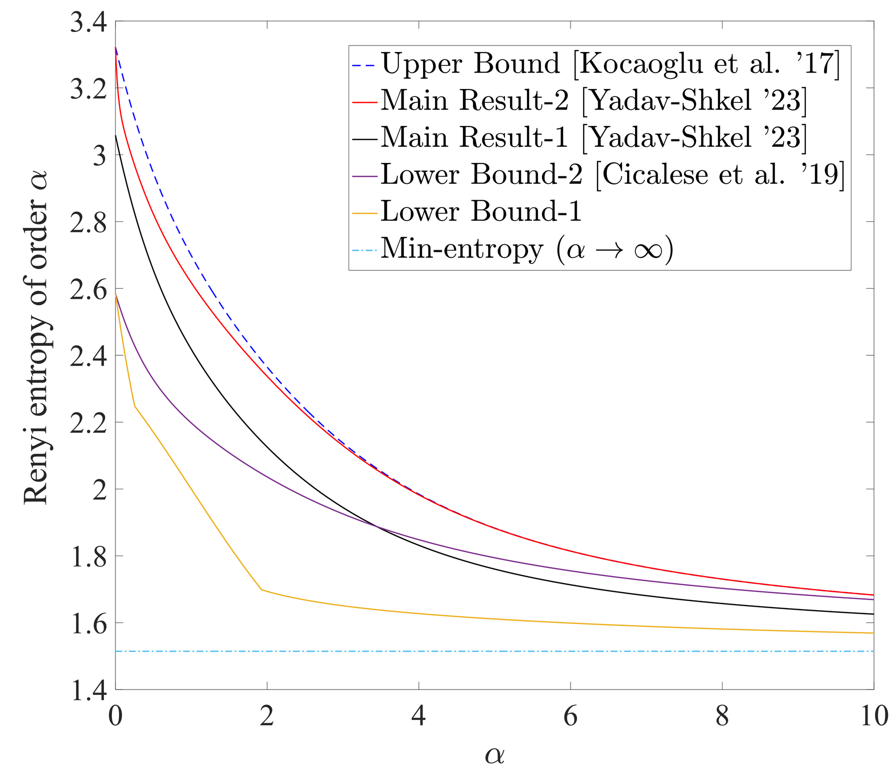
Note that $C^\star(X_1, \cdots, X_m) \in \mathscr{S}$. Thus, $C^\star \preceq Q^* \preceq_\imath P_i$, for every $i \in [m]$.

Therefore, we have $H_\alpha(C^\star) \ge H_\alpha(Q^*)$.

Greedy algo. to construct Q^* with linear complexity in support size of PMFs.

This result improves on all the existing lower bounds.

Scan for more details !



Upper Bounds

Greedy Coupling Algorithm [Kocaoglu et al.]

Input: m marginal distributions $\{P_i\}_{i=1}^m$.

Algo: Sort each PMF in the non-increasing order.
Find the min. of the max. of each PMF i.e., $q = \min_{i\in[m]} \{P_i(1)\}$.

While $q > 0$ **do**
 Append q as the next state of $\tilde{C}$.
 Update the max. state of each PMF i.e., $\forall i, P_i(1) := P_i(1) - q$.
 Sort each PMF in non-increasing order and compute q.
end while
Return Coupling $\tilde{C}$.

Tighter Approximation analysis [Yadav-Shkel '25]

Theorem: Let $\tilde{C}$ denote the output of the greedy coupling algorithm on the set of marginal PMFs $\{P_i\}_{i=1}^m$. Then,

$$H_\alpha(\tilde{C}) \le H_\alpha(C^\star) + F(\alpha, m)$$

where, $F(\alpha, m) = \frac{1}{\alpha - 1} \log\left[\max(0, 1 - \tilde{r}(\alpha, m))\right]$ such that

$$\tilde{r}(\alpha, m) := (-1)^{\mathbf{1}(\alpha>1)} \max_{\substack{w_1 = 0,\, w_{m+1} = 1 \\ w_1 < w_2 \le \ldots \le w_m < w_{m+1}}} \left[(-1)^{\mathbf{1}(\alpha>1)} \sum_{k=2}^m w_k \left(w_k^{\alpha-1} - w_{k+1}^{\alpha-1}\right)\right].$$

No closed form solution of $F(\alpha, m)$ for $m \ge 3$.

$F(\alpha, m)$ is non-decreasing in m, for every $\alpha \in [0,\infty)$. Thus,

$$H_\alpha(\tilde{C}) \le H_\alpha(C^\star) + \lim_{m\to\infty} F(\alpha, m) = H_\alpha(C^\star) + \frac{1}{\alpha - 1} \log\left[\max\left(0, \frac{2\alpha - 1}{\alpha}\right)\right].$$

Best known result - For high values of α i.e., $\alpha \ge \alpha^\star(m)$ where $\alpha^\star(m)$ is approximately between 0.36 and 0.78.