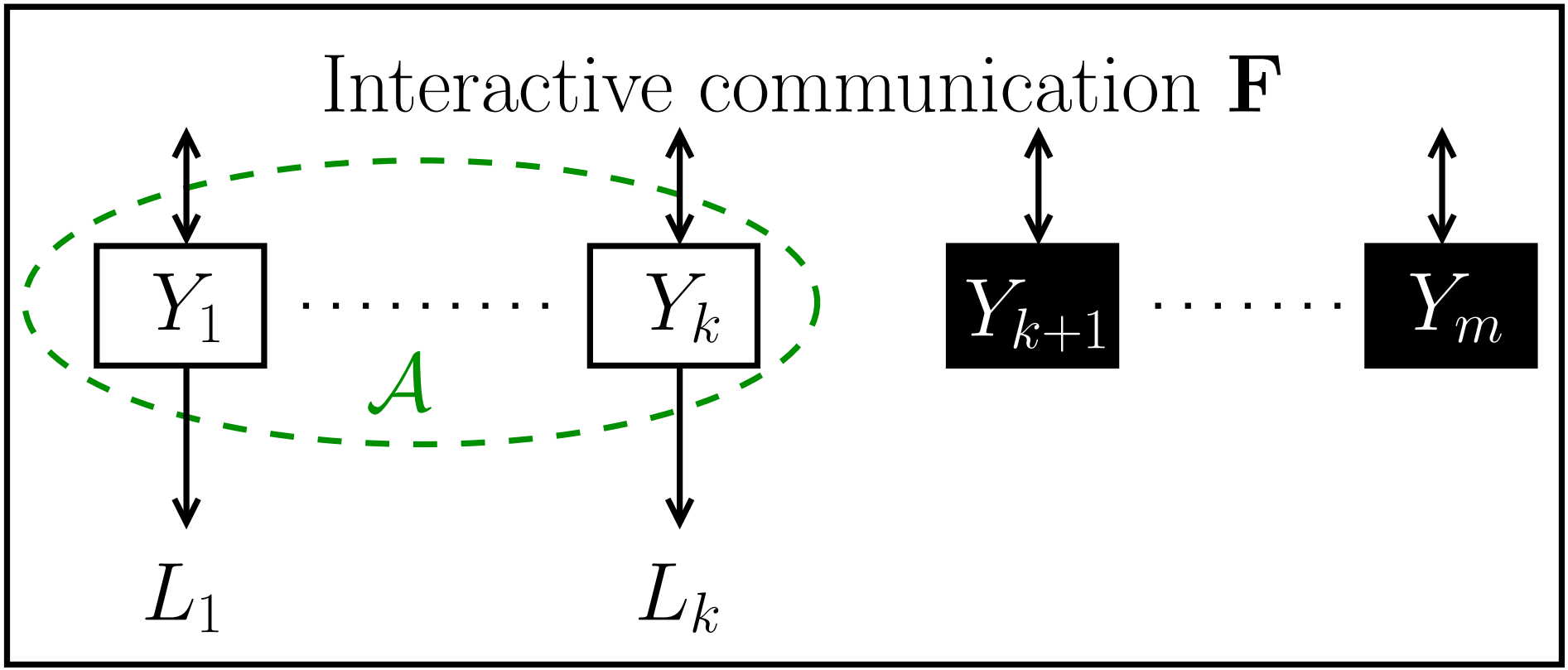
How Many Queries Will Resolve Common Randomness?

Himanshu Tyagi and Prakash Narayan

Department of Electrical and Computer Engineering
and Institute of System Research
University of Maryland, College Park, USA

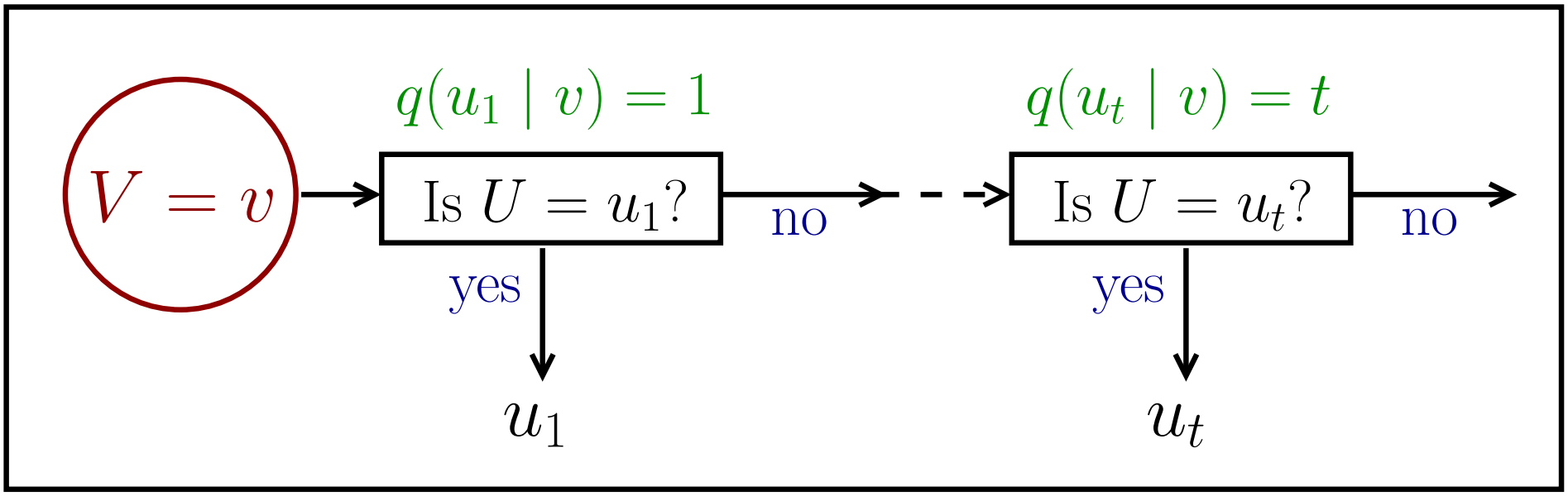
Common Randomness



Definition. L is an ϵ-common randomness for $\mathcal{A}$ from $\mathbf{F}$ if

$$\mathrm{P}\left(L = L_i(Y_i, \mathbf{F}),\ i \in \mathcal{A}\right) \geq 1 - \epsilon$$

Query Strategy



Query strategy for U given V

Massey '94, Arikan '96, Arikan-Merhav '99, Hanawal-Sundaresan '11

Query Strategy

Given rvs U, V with values in the sets $\mathcal{U}, \mathcal{V}$.

Definition. A *query strategy* q for U given $V = v$ is a bijection

$$q(\cdot|v) : \mathcal{U} \to \{1, ..., |\mathcal{U}|\},$$

where the querier, upon observing $V = v$, asks the question

$$\text{“Is } U = u\text{?”}$$

in the $q(u|v)^{\text{th}}$ query.

$q(U|V)$: random query number for U upon observing V

Query Strategy

Given rvs U, V with values in the sets $\mathcal{U}, \mathcal{V}$.

Definition. A *query strategy* q for U given $V = v$ is a bijection

$$q(\cdot|v) : \mathcal{U} \to \{1, ..., |\mathcal{U}|\},$$

where the querier, upon observing $V = v$, asks the question

$$\text{“Is } U = u\text{?”}$$

in the $q(u|v)^{\text{th}}$ query.

$q(U|V)$: random query number for U upon observing V

$$|\{u : q(u \mid v) < \gamma\}| < \gamma$$

Optimum Query Exponent

$Y_i = (X_{i1}, ..., X_{in}) = X_i^n, \quad 1 \le i \le m$: i.i.d. observations

Definition. $E \ge 0$ is an ϵ-achievable *query exponent* if there exists ϵ-CR L_n for $\mathcal{A}$ from $\mathbf{F}_n$ such that

$$\sup_q \mathrm{P}\left(q(L_n \mid \mathbf{F}_n) < 2^{nE}\right) \to 0 \quad \text{as} \quad n \to \infty,$$

where the sup is over every query strategy for L_n given $\mathbf{F}_n$.

Optimum Query Exponent

$Y_i = (X_{i1}, ..., X_{in}) = X_i^n, \quad 1 \le i \le m$: i.i.d. observations

Definition. $E \ge 0$ is an ϵ-achievable *query exponent* if there exists ϵ-CR L_n for $\mathcal{A}$ from $\mathbf{F}_n$ such that

$$\sup_q \mathrm{P}\left(q(L_n \mid \mathbf{F}_n) < 2^{nE}\right) \to 0 \quad \text{as} \quad n \to \infty,$$

where the sup is over every query strategy for L_n given $\mathbf{F}_n$.

$$E^*(\epsilon) \triangleq \sup\{E : E \text{ is an } \epsilon\text{-achievable query exponent}\}$$

$$E^* \triangleq \inf_{0<\epsilon<1} E^*(\epsilon) : \text{ optimum query exponent}$$

Main Result

Theorem

For $0 < \epsilon < 1$, *the optimum query exponent* E^* *equals*

$$E^* = E^*(\epsilon) = H\left(X_{\mathcal{M}}\right) - \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right).$$

$$\mathcal{B} = \{B \subsetneq \mathcal{M} : B \neq \emptyset, \mathcal{A} \nsubseteq B\}$$

$$\Lambda(\mathcal{A}) = \text{set of all } \{\lambda_B \in [0,1] : B \in \mathcal{B}\} \text{ such that}$$

$$\sum_{B \in \mathcal{B}: B \ni i} \lambda_B = 1, \quad i \in \mathcal{M}$$

$\lambda \in \Lambda(\mathcal{A})$ is a *fractional partition* of $\mathcal{M}$

Main Result

Theorem

For $0 < \epsilon < 1$, *the optimum query exponent* E^* *equals*

$$E^* = E^*(\epsilon) = H\left(X_{\mathcal{M}}\right) - \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right).$$

For $m = 2$: The expression on the right $= I\left(X_1 \wedge X_2\right)$

Strong Converse for Secret Key Capacity

Secret Key Capacity

Definition. $C(\epsilon)$ is the supremum over rates of rv $K \in \mathcal{K}$ s.t.

(i) K is an ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$

(ii) K is almost independent of $\mathbf{F}$:

$$n\, \mathrm{s}_{\mathrm{var}}(K; \mathbf{F}) = n \left\| \mathrm{P}_{K,\mathbf{F}} - \mathrm{U}_{\mathcal{K}} \times \mathrm{P}_{\mathbf{F}} \right\|_1 \to 0$$

Secret key capacity C is defined as $\inf_{0<\epsilon<1} C(\epsilon)$

Secret Key Capacity

Definition. $C(\epsilon)$ is the supremum over rates of rv $K \in \mathcal{K}$ s.t.

(i) K is an ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$

(ii) K is almost independent of $\mathbf{F}$:

$$n \, \mathrm{s}_{\mathrm{var}}(K; \mathbf{F}) = n \left\| \mathrm{P}_{K,\mathbf{F}} - \mathrm{U}_{\mathcal{K}} \times \mathrm{P}_{\mathbf{F}} \right\|_1 \to 0$$

Secret key capacity C is defined as $\inf_{0<\epsilon<1} C(\epsilon)$

$$C = H\left(X_{\mathcal{M}}\right) - \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right)$$

I. Csiszár and P. Narayan, Secret key capacity for multiple terminals, IEEE Trans. Inform. Theory, 2004.

Optimum Query Exponent and SK Capacity

Theorem

For $0 < \epsilon < 1$, *the optimum query exponent* E^* *equals*

$$E^* = E^*(\epsilon) = C.$$

Optimum Query Exponent and SK Capacity

Theorem

For $0 < \epsilon < 1$, the optimum query exponent E^* equals

$$E^* = E^*(\epsilon) = C.$$

Proof.

Achievability: $E^*(\epsilon) \geq C(\epsilon)$ - Easy

Converse: $E^*(\epsilon) \leq C$ - Main contribution

Optimum Query Exponent and SK Capacity

Theorem

For $0 < \epsilon < 1$, the optimum query exponent E^* equals

$$E^* = E^*(\epsilon) = C.$$

Proof.

Achievability: $E^*(\epsilon) \geq C(\epsilon)$ - Easy

Converse: $E^*(\epsilon) \leq C$ - Main contribution

Theorem (Strong converse for SK capacity)

For $0 < \epsilon < 1$, the ϵ-SK capacity is given by

$$C(\epsilon) = E^* = C.$$

Proof of Achievability

Query Strategies and Conditional Probabilities

Lemma. The rvs U, V, satisfy

$$\mathrm{P}\left(\left\{(u,v) : \mathrm{P}_{U|V}\left(u|v\right) \leq \frac{1}{\gamma}\right\}\right) \approx 1. \quad (*)$$

Then for every query strategy q for U given V,

$$\mathrm{P}\left(q(U|V) \geq \gamma\right) \approx 1.$$

Query Strategies and Conditional Probabilities

Lemma. The rvs U, V, satisfy

$$\mathrm{P}\left(\left\{(u,v) : \mathrm{P}_{U|V}\left(u|v\right) \leq \frac{1}{\gamma}\right\}\right) \approx 1. \quad (*)$$

Then for every query strategy q for U given V,

$$\mathrm{P}\left(q(U|V) \geq \gamma\right) \approx 1.$$

Also, the converse holds.

Query Strategies and Conditional Probabilities

Lemma. The rvs U, V, satisfy

$$\mathrm{P}\left(\left\{(u,v) : \mathrm{P}_{U|V}\left(u|v\right) \leq \frac{1}{\gamma}\right\}\right) \approx 1. \quad (*)$$

Then for every query strategy q for U given V,

$$\mathrm{P}\left(q(U|V) \geq \gamma\right) \approx 1.$$

Also, the converse holds.

- Proof of $C(\epsilon) \leq E^*(\epsilon)$

  $U =$ SK of rate R, $V = \mathbf{F} \Rightarrow (*)$ holds with $\gamma \approx 2^{nR}$

Proof of Converse

Proof of Converse for $\mathcal{A} = \mathcal{M}$

Alternative Expression for C when $\mathcal{A} = \mathcal{M}$

[Csiszár-Narayan '04] observed that for $\mathcal{A} = \mathcal{M}$

$$C \leq \frac{1}{k-1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{k} \mathrm{P}_{X_{\pi_i}} \right),$$

for every partition $\pi = \{\pi_1, ..., \pi_k\}$ of $\mathcal{M}$.

Alternative Expression for C when $\mathcal{A} = \mathcal{M}$

[Chan-Zheng '10] showed that for $\mathcal{A} = \mathcal{M}$

$$C = \min_{\pi} \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}} \right).$$

Alternative Expression for C when $\mathcal{A} = \mathcal{M}$

[Chan-Zheng '10] showed that for $\mathcal{A} = \mathcal{M}$

$$C = \min_{\pi} \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}} \right).$$

We shall show

$$E^*(\epsilon) \leq E_\pi = \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}} \right), \quad \text{for every } \pi.$$

Alternative Expression for C when $\mathcal{A} = \mathcal{M}$

[Chan-Zheng '10] showed that for $\mathcal{A} = \mathcal{M}$

$$C = \min_{\pi} \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}} \right).$$

We shall show

$$E^*(\epsilon) \leq E_\pi = \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}} \right), \quad \text{for every } \pi.$$

Roughly: For an ϵ-CR L for $\mathcal{M}$ from $\mathbf{F}$, there exists q_0 s.t.

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \leq 2^{nE_\pi} \right) > 0, \quad \text{for every } \pi$$

A General Converse

For rvs $Y_1, ..., Y_k$, let L be an ϵ-CR for $\{1, ..., k\}$ from $\mathbf{F}$.

Theorem

Let θ be such that

$$\mathrm{P}\left(\left\{(y_1, ..., y_k) : \frac{\mathrm{P}_{Y_1,...,Y_k}(y_1, ..., y_k)}{\prod_{i=1}^{k} \mathrm{P}_{Y_i}(y_i)} \leq \theta\right\}\right) \approx 1.$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \lesssim \theta^{\frac{1}{k-1}}\right) \geq (1 - \sqrt{\epsilon})^2 > 0.$$

A General Converse

For rvs $Y_1, ..., Y_k$, let L be an ϵ-CR for $\{1, ..., k\}$ from $\mathbf{F}$.

Theorem

Let θ be such that

$$\mathrm{P}\left(\left\{(y_1, ..., y_k) : \frac{\mathrm{P}_{Y_1,...,Y_k}(y_1, ..., y_k)}{\prod_{i=1}^{k} \mathrm{P}_{Y_i}(y_i)} \leq \theta\right\}\right) \approx 1.$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \lesssim \theta^{\frac{1}{k-1}}\right) \geq (1 - \sqrt{\epsilon})^2 > 0.$$

- Proof of $E^*(\epsilon) \leq E_\pi$

  Choose $Y_i = X^n_{\pi_i}$ for $i \in \{1, ..., k = |\pi|\}$.

Proof Outline for the General Converse

We show: $\exists$ a subset $\mathcal{I}_0$ of values of $\mathbf{F}$ and sets $\mathcal{L}(\mathbf{i}) \subseteq \mathcal{L}$ s.t.

$$|\mathcal{L}(\mathbf{i})| \lesssim \theta^{\frac{1}{k-1}} \quad \text{and} \quad \mathrm{P}_{L|\mathbf{F}}\left(\mathcal{L}(\mathbf{i}) \mid \mathbf{i}\right) > 0, \quad \mathbf{i} \in \mathcal{I}_0$$

$$\mathrm{P}_{\mathbf{F}}\left(\mathcal{I}_0\right) > 0$$

Lossless Data Compression:

Find small cardinality sets with large $\mathrm{P}_{L|\mathbf{F}}$ probabilities

Small Cardinality Sets with Large Probabilities

Rényi entropy of order α of a probability measure μ on $\mathcal{U}$:

$$H_\alpha(\mu) \triangleq \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha, \quad 0 \leq \alpha \neq 1$$

Lemma. There exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu(\mathcal{U}_\delta) \geq 1 - \delta$ s.t.

$$|\mathcal{U}_\delta| \lesssim \exp\left(H_\alpha(\mu)\right), \qquad 0 \leq \alpha < 1.$$

Small Cardinality Sets with Large Probabilities

Rényi entropy of order α of a probability measure μ on $\mathcal{U}$:

$$H_\alpha(\mu) \triangleq \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha, \quad 0 \leq \alpha \neq 1$$

Lemma. There exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu(\mathcal{U}_\delta) \geq 1 - \delta$ s.t.

$$|\mathcal{U}_\delta| \lesssim \exp\left(H_\alpha(\mu)\right), \qquad 0 \leq \alpha < 1.$$

Conversely, for any set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu(\mathcal{U}_\delta) \geq 1 - \delta$,

$$|\mathcal{U}_\delta| \gtrsim \exp\left(H_\alpha(\mu)\right), \qquad \alpha > 1.$$

Small Cardinality Sets with Large Probabilities

Rényi entropy of order α of a probability measure μ on $\mathcal{U}$:

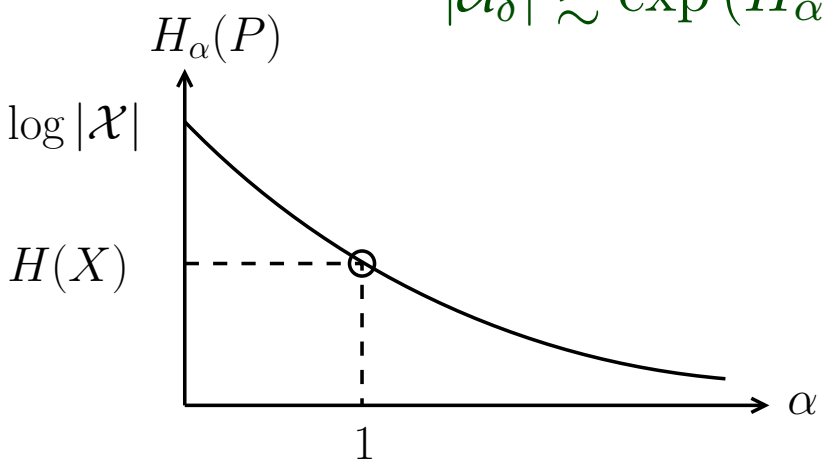
$$H_\alpha(\mu) \triangleq \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha, \quad 0 \leq \alpha \neq 1$$

Lemma. There exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu(\mathcal{U}_\delta) \geq 1 - \delta$ s.t.

$$|\mathcal{U}_\delta| \lesssim \exp\left(H_\alpha(\mu)\right), \qquad 0 \leq \alpha < 1.$$

Conversely, for any set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu(\mathcal{U}_\delta) \geq 1 - \delta$,

$$|\mathcal{U}_\delta| \gtrsim \exp\left(H_\alpha(\mu)\right), \qquad \alpha > 1.$$



Digression: Lossless Source Coding

Given probability measures μ_n on finite sets $\mathcal{U}_n$, $n \geq 1$.

$$R^*(\delta) \triangleq \inf\{R : \ \mu_n(\mathcal{V}_n) \geq 1-\delta, \ \limsup(1/n)\log|\mathcal{V}_n| \leq R\}$$

Proposition. For each $0 < \delta < 1$,

$$\lim_{\alpha\downarrow 1} \limsup_n \frac{1}{n} H_\alpha(\mu_n) \ \leq \ R^*(\delta) \ \leq \ \lim_{\alpha\uparrow 1} \limsup_n \frac{1}{n} H_\alpha(\mu_n).$$

If μ_n is an i.i.d. probability measure on $\mathcal{U}_n = \mathcal{U}^n$, then

$$R^*(\delta) = H(\mu_1), \qquad 0 < \delta < 1.$$

Abstract Alphabet and Communication

Let θ be such that

$$\mathrm{P}\left(\left\{y^k : \frac{d\,\mathrm{P}_{Y_1,\ldots,Y_k}}{d\prod_{i=1}^{k}\mathrm{P}_{Y_i}}(y^k) \leq \theta\right\}\right) \approx 1.$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \lesssim \theta^{\frac{1}{k-1}}\right) > 0.$$

- Upper bound on $E^*(\epsilon)$ for jointly Gaussian rvs
- Strong converse for Gaussian secret key capacity

Summary

Main Result: $E^* = E^*(\epsilon) = C(\epsilon) = C$

- Largest rate SK makes the task of querying eavesdropper the most onerous.
- We proved a strong converse for the SK capacity,
- And a converse for general alphabet and communication.
- Rényi entropy can be interpreted as an answer to a lossless source coding problem.