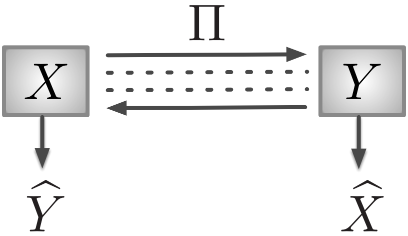
Interactive Communication for Data Exchange

Himanshu Tyagi
Indian Institute of Science, Bangalore

Joint work with Pramod Viswanath and Shun Watanabe

The Data Exchange Problem

[ElGamal-Orlitsky ‘84], [Csiszár-Narayan’04]



A protocol π constitutes an ϵ-data exchange (ϵ-DE) protocol if

$$\Pr\left(\hat{X} = X, \hat{Y} = Y\right) \geq 1 - \epsilon.$$

What is the minimum length $L_\epsilon(X, Y)$ of an ϵ-DE protocol?

The Slepian-Wolf Problem

Only X needs to be sent to an observer of Y.

- [Slepian-Wolf '73] Optimal rate for the case of IID observations:

$$R_\epsilon^* = H(X|Y), \quad 0 < \epsilon < 1.$$

- [Miyake-Kanaya '95] Single-shot bounds:

$$L_\epsilon(X|Y) \geq \lambda + \log\left[1 - \epsilon - \Pr\left(h(X|Y) \leq \lambda\right)\right] : \text{ lower bound}$$

$$L_\epsilon(X|Y) \leq \lambda - \log\left[\epsilon - \Pr\left(h(X|Y) \geq \lambda\right)\right] \quad : \text{ upper bound}$$

The Slepian-Wolf Problem

Only X needs to be sent to an observer of Y.

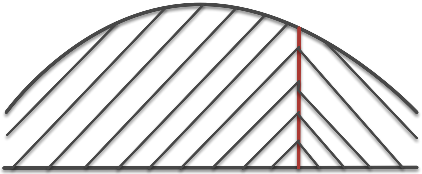
- [Slepian-Wolf '73] Optimal rate for the case of IID observations:

$$R_\epsilon^* = H(X|Y), \quad 0 < \epsilon < 1.$$

- [Miyake-Kanaya '95] Single-shot bounds:

$$L_\epsilon(X|Y) \geq \lambda + \log\left[1 - \epsilon - \Pr\left(h(X|Y) \leq \lambda\right)\right] : \text{ lower bound}$$

$$L_\epsilon(X|Y) \leq \lambda - \log\left[\epsilon - \Pr\left(h(X|Y) \geq \lambda\right)\right] \quad : \text{ upper bound}$$



Spectrum of $h(X|Y) = -\log P_{X|Y}(X|Y)$

Can Interaction Help?

"Asymptotically", interaction does not help in the SW problem.

Can Interaction Help?

"Asymptotically", interaction does not help in the SW problem.

Instances where interaction is known to help:

- [Orlitsky '90] Single-shot, worst-case length:

  One round of interaction is almost optimal without error

- [Feder-Shulman'02] Universal version, adaptive rate:

  An interactive protocol accomplishes this task

- [Yang-He '10] Single-shot, average length

  An interactive protocol attains roughly $H(X|Y)$

Can Interaction Help?

"Asymptotically", interaction does not help in the SW problem.

Instances where interaction is known to help:

- [Orlitsky '90] Single-shot, worst-case length:

  One round of interaction is almost optimal without error

- [Feder-Shulman'02] Universal version, adaptive rate:

  An interactive protocol accomplishes this task

- [Yang-He '10] Single-shot, average length

  An interactive protocol attains roughly $H(X|Y)$

Can interaction help in the data exchange problem?

Using Slepian-Wolf scheme for Data Exchange

The following rate is achievable for the IID case:

$$H(X \triangle Y) \stackrel{\text{def}}{=} H(X|Y) + H(Y|X).$$

Using Slepian-Wolf scheme for Data Exchange

The following rate is achievable for the IID case:

$$H(X \triangle Y) \stackrel{\text{def}}{=} H(X|Y) + H(Y|X).$$

[Csiszár-Narayan '04]

This rate is the least possible.

The proof relies on a property of interactive communication:

$$H(\Pi) \geq H(\Pi|X, U) + H(\Pi|Y, V).$$

Implication: Noninteractive communication can attain the optimal rate

Using Slepian-Wolf scheme for Data Exchange

The following rate is achievable for the IID case:

$$H(X \triangle Y) \stackrel{\text{def}}{=} H(X|Y) + H(Y|X).$$

[Csiszár-Narayan '04]

This rate is the least possible.

The proof relies on a property of interactive communication:

$$H(\Pi) \geq H(\Pi|X, U) + H(\Pi|Y, V).$$

Implication: Noninteractive communication can attain the optimal rate

Is interaction of any use for data exchange?

Main Result: Bounds on $L_\epsilon(X, Y)$

We show that interaction is indeed helpful.

We characterize the min. length of interactive communication needed,

thereby characterizing the gain due to interaction.

Main Result: Bounds on $L_\epsilon(X,Y)$

We show that interaction is indeed helpful.

We characterize the min. length of interactive communication needed, thereby characterizing the gain due to interaction.

Define *sum conditional entropy* $h(X \triangle Y) \stackrel{\text{def}}{=} h(X|Y) + h(Y|X)$

Theorem (Single-shot)

For every $0 < \epsilon < 1$, *we have*

$$L_\epsilon(X,Y) \lesssim \lambda - \log\left[\epsilon - \Pr\left(h(X \triangle Y) \geq \lambda\right)\right], \quad \forall\, \lambda > 0,$$

$$L_\epsilon(X,Y) \gtrsim \lambda + \log\left[1 - \epsilon - \Pr\left(h(X \triangle Y) \leq \lambda\right)\right], \quad \forall\, \lambda > 0.$$

Corollary 1: Second-Order Asymptotics for IID Sources

Let $(X^n, Y^n) = (X_i, Y_i)_{i=1}^n$ be IID realizations of (X, Y).

Theorem

For every $0 < \epsilon < 1$, we have

$$L_\epsilon(X^n, Y^n) = nH(X \triangle Y) + \sqrt{n\mathrm{Var}[h(X \triangle Y)]}Q^{-1}(\epsilon) + o(\sqrt{n}).$$

Corollary 1: Second-Order Asymptotics for IID Sources

Let $(X^n, Y^n) = (X_i, Y_i)_{i=1}^n$ be IID realizations of (X, Y).

Theorem

For every $0 < \epsilon < 1$, we have

$$L_\epsilon(X^n, Y^n) = nH(X \triangle Y) + \sqrt{n\mathrm{Var}[h(X \triangle Y)]}Q^{-1}(\epsilon) + o(\sqrt{n}).$$

This length is strictly smaller than that attained by noninteractive protocols.

Corollary 2: Minimum Rate for General Sources

Let $(\mathbf{X}, \mathbf{Y}) = (X_n, Y_n)_{n=1}^{\infty}$ be a general source sequence.

Define the minimum rate of communication for data exchange as

$$R^*(\mathbf{X}, \mathbf{Y}) \stackrel{\text{def}}{=} \inf_{\{\epsilon_n\}} \limsup_n \frac{1}{n} L_{\epsilon_n}(X_n, Y_n),$$

where the infimum is over all sequences $\epsilon_n \to 0$.

Theorem

For a general source sequence $(\mathbf{X}, \mathbf{Y})$*,*

$$R^*(\mathbf{X}, \mathbf{Y}) = \overline{H}(\mathbf{X} \triangle \mathbf{Y}),$$

where $\overline{H}(\mathbf{X} \triangle \mathbf{Y})$ *denotes the* $\limsup$ *in probability of* $h(X_n \triangle Y_n)$*.*

Corollary 2: Minimum Rate for General Sources

Let $(\mathbf{X}, \mathbf{Y}) = (X_n, Y_n)_{n=1}^{\infty}$ be a general source sequence.

Define the minimum rate of communication for data exchange as

$$R^*(\mathbf{X}, \mathbf{Y}) \stackrel{\text{def}}{=} \inf_{\{\epsilon_n\}} \limsup_n \frac{1}{n} L_{\epsilon_n}(X_n, Y_n),$$

where the infimum is over all sequences $\epsilon_n \to 0$.

Theorem

For a general source sequence $(\mathbf{X}, \mathbf{Y})$*,*

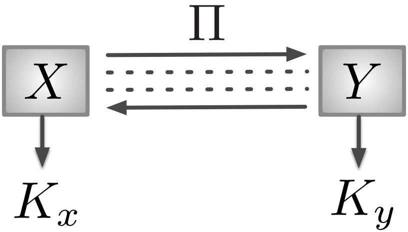
$$R^*(\mathbf{X}, \mathbf{Y}) = \overline{H}(\mathbf{X} \triangle \mathbf{Y}),$$

where $\overline{H}(\mathbf{X} \triangle \mathbf{Y})$ *denotes the* $\limsup$ *in probability of* $h(X_n \triangle Y_n)$*.*

This rate is strictly smaller than that attained by noninteractive protocols.

Proof Sketch for the Converse

Digression: Secret Key Agreement



K constitutes an ϵ-secret key of length $\log \mathcal{K}$ if

$$\frac{1}{2}\|\mathrm{P}_{K_x K_y \mathbf{F}} - \mathrm{P}^{(2)}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}}\|_1 \le \epsilon,$$

where

$$\mathrm{P}^{(2)}_{\mathtt{unif}}(k_x, k_y) = \frac{1}{|\mathcal{K}|}\mathbb{1}(k_x = k_y).$$

The maximum length of an ϵ-SK is denoted by $S_\epsilon(X, Y)$.

Main Heuristic

Parties with correlated observations share more bits

than what they communicate.

The extra bits shared can be extracted as a secret key.

Thus, if the parties share $R_{\texttt{shared}}$ bits and communicate R bits,

$$R_{\texttt{shared}} - R \lesssim S(X, Y)$$
$$\Updownarrow$$
$$R_{\texttt{shared}} - S(X, Y) \lesssim R$$

- [Csisár-Narayan '04] First formalized this duality to obtain SK capacity
- [T-Narayan-Gupta '10, T '12] characterization of secure computability

Warm-up: Optimal Rate for Data Exchange

Csiszár-Narayan approach flipped around:

Consider a rate R protocol for data exchange.

- Both parties share roughly $nH(XY)$ bits at the end.
- Using an "extractor lemma" we can generate a SK of rate

$$H(XY) - R,$$

  which must be less than the SK capacity $I(X \wedge Y)$.

Thus,

$$\begin{aligned} R &\geq H(XY) - I(X \wedge Y) \\ &= H(X|Y) + H(Y|X). \end{aligned}$$

Warm-up: Optimal Rate for Data Exchange

Csiszár-Narayan approach flipped around:

Consider a rate R protocol for data exchange.

- Both parties share roughly $nH(XY)$ bits at the end.
- Using an "extractor lemma" we can generate a SK of rate

$$H(XY) - R,$$

which must be less than the SK capacity $I(X \wedge Y)$.

Thus,

$$\begin{aligned} R &\geq H(XY) - I(X \wedge Y) \\ &= H(X|Y) + H(Y|X). \end{aligned}$$

We seek to extend this argument to a single-shot setup.

Upper Bound for Secret Key Length

[T-Watanabe '14]

Theorem

For every $0 < \epsilon, \eta < 1$ *with* $\eta < 1 - \epsilon$*, we have*

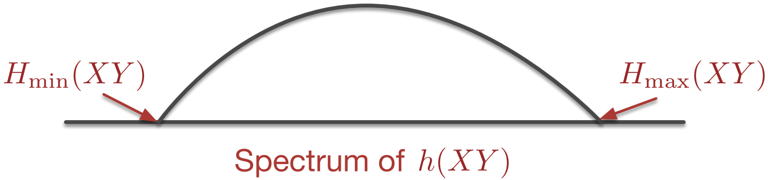
$$S_\epsilon(X, Y) \le \lambda - \log\left(\mathrm{P}_\lambda - \epsilon - \eta\right) + 2\log 1/\eta, \quad \forall\, \lambda > 0,$$

where

$$\mathrm{P}_\lambda = \mathrm{P}_{XY}\left(\left\{(x, y) : \log\frac{\mathrm{P}_{XY}(x, y)}{\mathrm{Q}_X(x)\,\mathrm{Q}_Y(y)} < \lambda\right\}\right).$$

Converse for Almost Uniform Sources

Consider a data exchange protocol of length l.

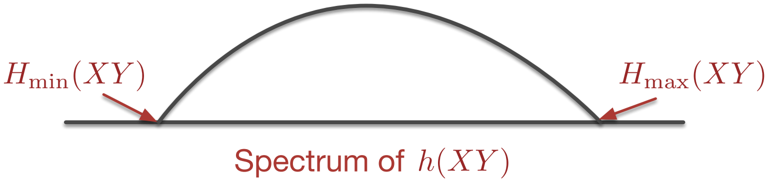


- Using the *Leftover Hash Lemma*, we can extract a SK of length

$$\approx H_{\min}(XY) - l.$$

Converse for Almost Uniform Sources

Consider a data exchange protocol of length l.

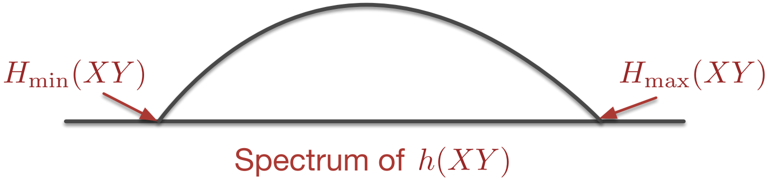


- Using the upper bound for $S_\epsilon(X,Y)$,

$$\begin{aligned} H_{\min}(XY) - l &\lesssim \lambda - \log\left(\mathrm{P}_{XY}\left(i(X \wedge Y) < \lambda\right) - \epsilon\right) \\ &= \lambda - \log\left(\mathrm{P}_{XY}\left(h(XY) - h(X \triangle Y) < \lambda\right) - \epsilon\right) \\ &\leq H_{\max}(XY) - \gamma - \log\left(\mathrm{P}_{XY}\left(h(X \triangle Y) > \gamma\right) - \epsilon\right) \end{aligned}$$

Converse for Almost Uniform Sources

Consider a data exchange protocol of length l.



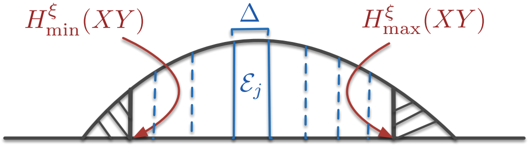
Thus,

$$l \gtrsim H_{\max}(XY) - H_{\min}(XY) + \gamma + \log\left(\mathrm{P}_{XY}\left(h(X \triangle Y) > \gamma\right) - \epsilon\right),$$

which gives the converse bound if $H_{\max}(XY) \approx H_{\min}(XY)$.

General Converse via Spectrum Slicing

Slice the spectrum into N slices of width Δ each.



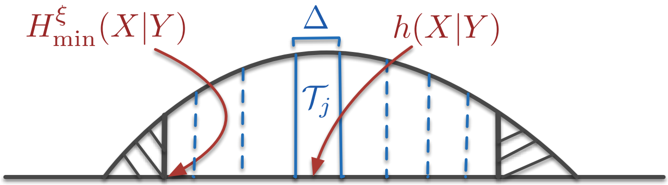
- There exists a slice $\mathcal{E}_j$ with $\mathrm{P}_{XY}(\mathcal{E}_j) \geq N^{-2}$, and so

$$\mathrm{P}_{XY} \leq \mathrm{P}_{XY|\mathcal{E}_j} \leq N^2 \mathrm{P}_{XY}.$$

The proof is completed by applying the previous bound to $\mathrm{P}_{XY|\mathcal{E}_j}$.

Our Achievability Scheme

Rough Sketch of Our Scheme



$$h_i \equiv \begin{cases} \text{random binning of } X \text{ into } H_{\min}^{\xi}(X|Y) \text{ values}, & i = 1, \\ \text{random binning of } X \text{ into } \Delta \text{ values}, & 2 \le i \le N. \end{cases}$$

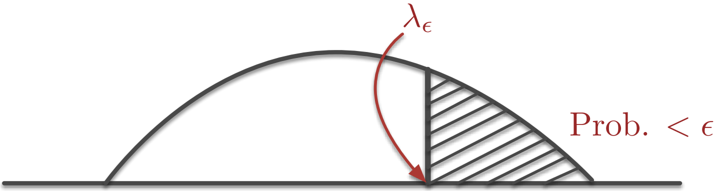
First party sends bin indices $\Pi_i = h_i(x)$ successively until

it receives an ACK or $i = N$

Second party sends an ACK when it finds an $\hat{x}$ s.t.

$$(\hat{x}, y) \in \mathcal{T}_i \quad \text{and} \quad h_j(\hat{x}) = \Pi_j, \quad 1 \le j \le i.$$

In Closing ...



Spectrum of $h(X \triangle Y)$

The minimum length of communication for ϵ-data exchange

is equal to roughly the ϵ-tail λ_ϵ of $h(X \triangle Y)$.

Interaction is necessary to attain this rate.