Information Complexity Density
and
Simulation of Protocols

Himanshu Tyagi
Indian Institute of Science, Bangalore

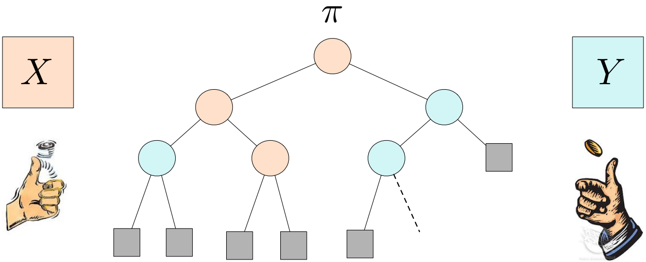
with Pramod Viswanath (UIUC), Shaileshh Venkatakrishnan (UIUC), and Shun Watanabe (TUAT)

Private Coin Interactive Protocols

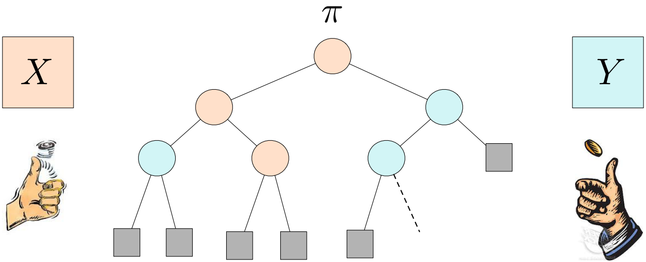
X

Y

Private Coin Interactive Protocols

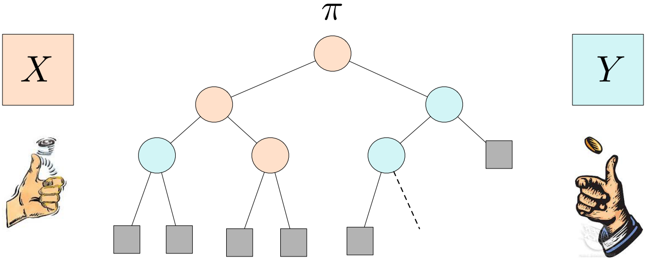


Private Coin Interactive Protocols



Denote by $\Pi = (\Pi_1, \Pi_2, \Pi_3, ...)$ the random transcript

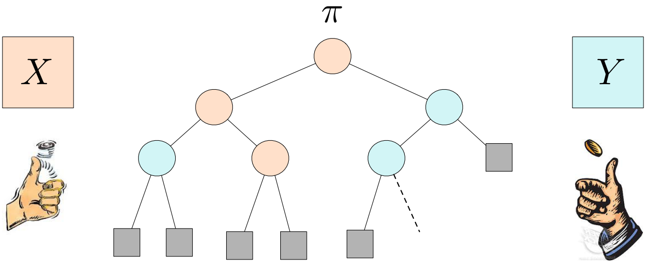
Private Coin Interactive Protocols



Denote by $\Pi = (\Pi_1, \Pi_2, \Pi_3, \ldots)$ the random transcript

$$\Pi_1 \text{---} X \text{---} Y$$
$$\Pi_2 \text{---} Y, \Pi_1 \text{---} X$$
$$\Pi_3 \text{---} X, \Pi_1, \Pi_2 \text{---} Y$$
$$\ldots$$

Private Coin Interactive Protocols

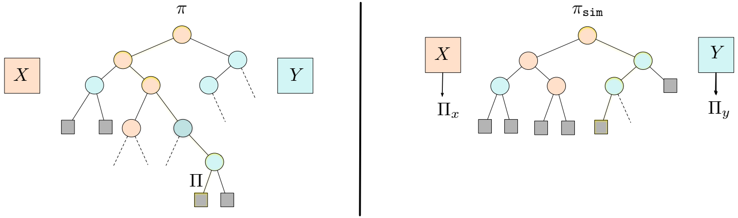


Denote by $\Pi = (\Pi_1, \Pi_2, \Pi_3, \ldots)$ the random transcript

$$\Pi_1 - X - Y$$
$$\Pi_2 - Y, \Pi_1 - X$$
$$\Pi_3 - X, \Pi_1, \Pi_2 - Y$$
$$\cdots$$

$|\pi|$ = depth of the protocol tree

ϵ-Simulation of a Protocol

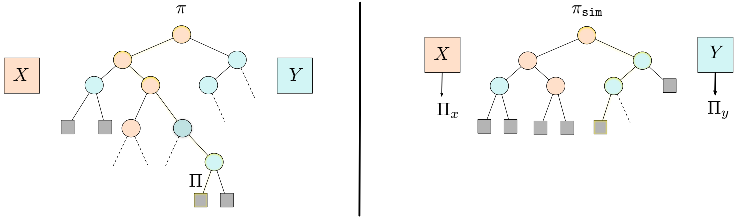


Definition

A protocol $\pi_{\mathtt{sim}}$ constitutes an ϵ-simulation of π if it can produce outputs Π_x and Π_y at X and Y, respectively, such that

$$\left\| \mathrm{P}_{XY\Pi\Pi} - \mathrm{P}_{XY\Pi_x\Pi_y} \right\|_{\mathtt{TV}} \leq \epsilon.$$

ϵ-Simulation of a Protocol



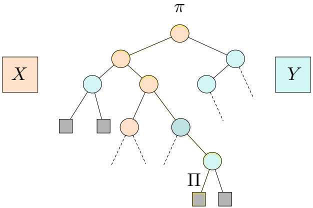
Definition

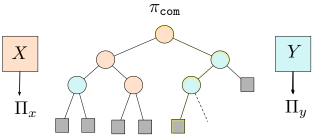
A protocol $\pi_{\mathtt{sim}}$ constitutes an ϵ-simulation of π if it can produce outputs Π_x and Π_y at X and Y, respectively, such that

$$\left\| \mathrm{P}_{XY\Pi\Pi} - \mathrm{P}_{XY\Pi_x\Pi_y} \right\|_{\mathtt{TV}} \leq \epsilon.$$

We seek to characterize $D_\epsilon(\pi|\mathrm{P}_{XY})$= min. length of an ϵ-simulation of π

ϵ-Compression of a Protocol



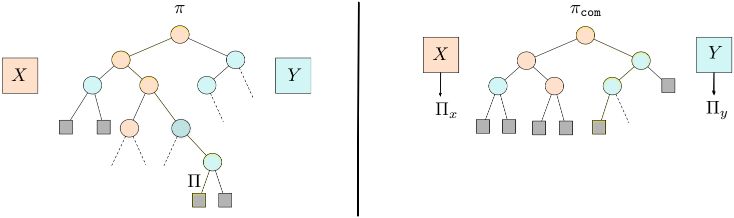


Definition

A protocol $\pi_{\texttt{com}}$ constitutes an ϵ-compression of π if it can produce outputs Π_x and Π_y at X and Y, respectively, such that

$$\Pr\left(\Pi = \Pi_x = \Pi_y\right) \geq 1 - \epsilon.$$

ϵ-Compression of a Protocol



Definition

A protocol $\pi_{\mathtt{com}}$ constitutes an ϵ-compression of π if it can produce outputs Π_x and Π_y at X and Y, respectively, such that

$$\Pr\left(\Pi = \Pi_x = \Pi_y\right) \geq 1 - \epsilon.$$

For deterministic protocols, compression $\equiv$ simulation.

Information Complexity of π

$$\mathtt{IC}(\pi) \stackrel{\text{def}}{=} I(\Pi \wedge X \mid Y) + I(\Pi \wedge Y \mid X)$$

Information Complexity of π

$$\texttt{IC}(\pi) \stackrel{\text{def}}{=} I(\Pi \wedge X \mid Y) + I(\Pi \wedge Y \mid X)$$

Examples

- $\Pi(x, y) = x$

$$IC(\pi) = H(X|Y)$$

- $\Pi(x, y) = (x, y)$

$$IC(\pi) = H(X|Y) + H(Y|X)$$

Information Complexity of π

$$\texttt{IC}(\pi) \stackrel{\text{def}}{=} I(\Pi \wedge X \mid Y) + I(\Pi \wedge Y \mid X)$$

Examples

- $\Pi(x, y) = x$

$$IC(\pi) = H(X|Y)$$

- $\Pi(x, y) = (x, y)$

$$IC(\pi) = H(X|Y) + H(Y|X)$$

Theorem (Amortized Communication Complexity [BR'10])

For coordinate-wise repetition π^n of π and i.i.d. (X^n, Y^n),

$$\lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} D_\epsilon\left(\pi^n | \mathrm{P}_{X^nY^n}\right) = IC(\pi).$$

Information Complexity of π

$$\mathtt{IC}(\pi) \overset{\text{def}}{=} I(\Pi \wedge X \mid Y) + I(\Pi \wedge Y \mid X)$$

Examples

- $\Pi(x,y) = x$ [Slepian-Wolf '74]

$$IC(\pi) = H(X|Y)$$

- $\Pi(x,y) = (x,y)$ [Csiszár-Narayan '04]

$$IC(\pi) = H(X|Y) + H(Y|X)$$

Theorem (Amortized Communication Complexity [BR'10])

For coordinate-wise repetition π^n of π and i.i.d. (X^n, Y^n),

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}D_\epsilon\left(\pi^n|\mathrm{P}_{X^nY^n}\right) = IC(\pi).$$

Questions

- *Strong converse.* Does $\lim_{n\to\infty} \frac{1}{n} D_\epsilon \left(\pi^n | \mathrm{P}_{X^nY^n}\right)$ depend on ϵ?

- *Mixed protocols.* What about a mixed protocol $\pi^{(n)}$ given by

$$\pi^{(n)} = \begin{cases} \pi_{\mathtt{h}}^n, & \text{w.p. } p, \\ \pi_{\mathtt{l}}^n, & \text{w.p. } 1-p. \end{cases}$$

  Note that $\mathtt{IC}(\pi^{(n)}) = n\big[p\mathtt{IC}(\pi_{\mathtt{h}}) + (1-p)\mathtt{IC}(\pi_{\mathtt{l}})\big]$

- ... General distributions? Second-order asymptotics? Single-shot?

Questions

- *Strong converse.* Does $\lim_{n\to\infty}\frac{1}{n}D_\epsilon\left(\pi^n|\mathrm{P}_{X^nY^n}\right)$ depend on ϵ?

- *Mixed protocols.* What about a mixed protocol $\pi^{(n)}$ given by

$$\pi^{(n)} = \begin{cases} \pi_{\mathtt{h}}^n, & \text{w.p. } p, \\ \pi_{\mathtt{l}}^n, & \text{w.p. } 1-p. \end{cases}$$

  Note that $\mathtt{IC}(\pi^{(n)}) = n\big[p\mathtt{IC}(\pi_{\mathtt{h}}) + (1-p)\mathtt{IC}(\pi_{\mathtt{l}})\big]$

- ... General distributions? Second-order asymptotics? Single-shot?

Why do we care?

Questions

- *Strong converse.* Does $\lim_{n\to\infty} \frac{1}{n} D_\epsilon\left(\pi^n | \mathrm{P}_{X^nY^n}\right)$ depend on ϵ?

- *Mixed protocols.* What about a mixed protocol $\pi^{(n)}$ given by

$$\pi^{(n)} = \begin{cases} \pi_{\mathtt{h}}^n, & \text{w.p. } p, \\ \pi_{\mathtt{l}}^n, & \text{w.p. } 1-p. \end{cases}$$

  Note that $\mathtt{IC}(\pi^{(n)}) = n\big[p\mathtt{IC}(\pi_{\mathtt{h}}) + (1-p)\mathtt{IC}(\pi_{\mathtt{l}})\big]$

- *...* General distributions? Second-order asymptotics? Single-shot?

Why do we care?

42.

The Tail of Information Complexity Density

Information Complexity Density

$$\mathtt{ic}(\tau; x, y) \stackrel{\text{def}}{=} \log \frac{\mathrm{P}_{\Pi|XY}(\tau|x, y)}{\mathrm{P}_{\Pi|X}(\tau|x)} + \log \frac{\mathrm{P}_{\Pi|XY}(\tau|x, y)}{\mathrm{P}_{\Pi|Y}(\tau|y)}$$

Note that $\mathbb{E}[\mathtt{ic}(\Pi; X, Y)] = \mathtt{IC}(\pi)$.

Information Complexity Density

$$\mathtt{ic}(\tau; x, y) \stackrel{\text{def}}{=} \log \frac{\mathrm{P}_{\Pi|XY}(\tau|x,y)}{\mathrm{P}_{\Pi|X}(\tau|x)} + \log \frac{\mathrm{P}_{\Pi|XY}(\tau|x,y)}{\mathrm{P}_{\Pi|Y}(\tau|y)}$$

Note that $\mathbb{E}[\mathtt{ic}(\Pi; X, Y)] = \mathtt{IC}(\pi)$.

ϵ-Tails of $\mathtt{ic}(\Pi; X, Y)$ are closely related to $D_\epsilon(\pi|\mathrm{P}_{XY})$

Illustration

Consider the Slepian-Wolf problem ($\Pi(x, y) = x$).

- $\texttt{ic}(\tau; x, y) = -\log \mathrm{P}_{X|Y}(x|y)$

Illustration

Consider the Slepian-Wolf problem ($\Pi(x, y) = x$).

- $\mathtt{ic}(\tau; x, y) = -\log \mathrm{P}_{X|Y}(x|y)$
- If $\Pr(\mathtt{ic}(\Pi; X, Y) \geq \lambda) \leq \epsilon$,

  - a random hash λ-bit hash of X constitutes an ϵ-compression.
- If $\Pr(\mathtt{ic}(\Pi; X, Y) \geq \lambda) > \epsilon$,

  - any subset with prob. $\geq 1 - \epsilon$ has cardinality less than λ

Illustration

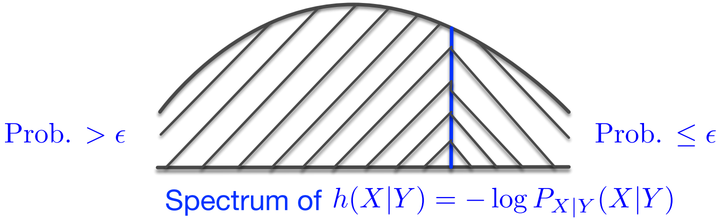
Consider the Slepian-Wolf problem ($\Pi(x, y) = x$).

- $\mathtt{ic}(\tau; x, y) = -\log \mathrm{P}_{X|Y}(x|y)$
- If $\Pr(\mathtt{ic}(\Pi; X, Y) \geq \lambda) \leq \epsilon$,

  - a random hash λ-bit hash of X constitutes an ϵ-compression.

- If $\Pr(\mathtt{ic}(\Pi; X, Y) \geq \lambda) > \epsilon$,

  - any subset with prob. $\geq 1 - \epsilon$ has cardinality less than λ



Main Results

Lower Bound

Theorem

Given $0 \leq \epsilon < 1$ *and a protocol* π*,*

$$D_\epsilon(\pi) \gtrsim \sup\{\lambda : \Pr\left(\mathtt{ic}(\Pi; X, Y) > \lambda\right) \geq \epsilon\}.$$

Lower Bound

Theorem

Given $0 \leq \epsilon < 1$ *and a protocol* π*,*

$$D_\epsilon(\pi) \gtrsim \sup\{\lambda : \Pr\left(\mathtt{ic}(\Pi; X, Y) > \lambda\right) \geq \epsilon\}.$$

Weaknesses.

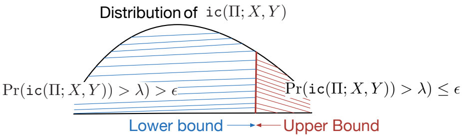
- The fudge parameters are of the order $\log($ spectrum width $)$.
- Uses only the joint pmf, not the structure of the protocol.

Upper bound

Theorem

Given $0 \leq \epsilon < 1$ *and a bounded rounds protocol* π*,*

$$D_\epsilon(\pi) \lesssim \sup\{\lambda : \Pr\left(\mathtt{ic}(\Pi; X, Y) > \lambda\right) \leq \epsilon\}.$$

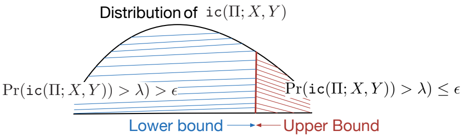


Upper bound

Theorem

Given $0 \leq \epsilon < 1$ *and a bounded rounds protocol* π*,*

$$D_\epsilon(\pi) \lesssim \sup\{\lambda : \Pr\left(\mathtt{ic}(\Pi; X, Y) > \lambda\right) \leq \epsilon\}.$$



Weaknesses.

- The fudge parameters depend on the number of rounds.
- Protocol based on round-by-round compression.

Questions

- *Strong converse.* Does $\lim_{n\to\infty} \frac{1}{n} D_\epsilon\left(\pi^n | \mathrm{P}_{X^n Y^n}\right)$ depend on ϵ?

- *Mixed protocols.* What about a mixed protocol $\pi^{(n)}$ given by

$$\pi^{(n)} = \begin{cases} \pi_{\mathtt{h}}^n, & \text{w.p. } p, \\ \pi_{\mathtt{l}}^n, & \text{w.p. } 1-p. \end{cases}$$

Note that $\mathtt{IC}(\pi^{(n)}) = n\big[p\mathtt{IC}(\pi_{\mathtt{h}}) + (1-p)\mathtt{IC}(\pi_{\mathtt{l}})\big]$

Questions

- *Strong converse.* Does $\lim_{n\to\infty}\frac{1}{n}D_\epsilon\left(\pi^n|\mathrm{P}_{X^nY^n}\right)$ depend on ϵ?
  Answer. No. In fact,

$$D_\epsilon(\pi^n) = n\mathtt{IC}(\pi) + \sqrt{n\mathbb{V}\left(\mathtt{ic}(\Pi;X,Y)\right)}Q^{-1}(\epsilon) + o(\sqrt{n})$$

- *Mixed protocols.* What about a mixed protocol $\pi^{(n)}$ given by

$$\pi^{(n)} = \begin{cases} \pi_{\mathtt{h}}^n, & \text{w.p. } p, \\ \pi_{\mathtt{l}}^n, & \text{w.p. } 1-p. \end{cases}$$

  Note that $\mathtt{IC}(\pi^{(n)}) = n\big[p\mathtt{IC}(\pi_{\mathtt{h}}) + (1-p)\mathtt{IC}(\pi_{\mathtt{l}})\big]$

Questions

- *Strong converse.* Does $\lim_{n\to\infty} \frac{1}{n} D_\epsilon\left(\pi^n | \mathrm{P}_{X^nY^n}\right)$ depend on ϵ?

  Answer. No. In fact,

$$D_\epsilon(\pi^n) = n\mathtt{IC}(\pi) + \sqrt{n\mathbb{V}\left(\mathtt{ic}(\Pi; X, Y)\right)}Q^{-1}(\epsilon) + o(\sqrt{n})$$

- *Mixed protocols.* What about a mixed protocol $\pi^{(n)}$ given by

$$\pi^{(n)} = \begin{cases} \pi_{\mathtt{h}}^n, & \text{w.p. } p, \\ \pi_{\mathtt{l}}^n, & \text{w.p. } 1-p. \end{cases}$$

  Note that $\mathtt{IC}(\pi^{(n)}) = n\big[p\mathtt{IC}(\pi_{\mathtt{h}}) + (1-p)\mathtt{IC}(\pi_{\mathtt{l}})\big]$

  Answer.

$$\lim_{\epsilon\to 0} \limsup_{n\to\infty} \frac{1}{n} D_\epsilon(\pi^{(n)}) = \mathtt{IC}(\pi_{\mathtt{h}})$$

Function Computation

[BR '10], [MI '10]:

$$\lim_{\epsilon \to 0} \lim_{n \to} \frac{1}{n} D_\epsilon(f^n) = \mathtt{IC}(f).$$

Function Computation

[BR '10], [MI '10]:

$$\lim_{\epsilon \to 0} \lim_{n \to} \frac{1}{n} D_\epsilon(f^n) = \mathtt{IC}(f).$$

- *Strong converse?* Our bound yields

$$\lim_{n \to} \frac{1}{n} D_\epsilon(f^n) \geq H(f(X,Y)|X) + H(f(X,Y)|Y)$$

Function Computation

[BR '10], [MI '10]:

$$\lim_{\epsilon\to 0}\lim_{n\to}\frac{1}{n}D_\epsilon(f^n) = \mathtt{IC}(f).$$

- *Strong converse?* Our bound yields

$$\lim_{n\to}\frac{1}{n}D_\epsilon(f^n) \geq H(f(X,Y)|X) + H(f(X,Y)|Y)$$

- *Direct product or Arimoto converse?*
  [BRWY '13], [BW'14]:

$$|\pi_n| < \frac{n\mathtt{IC}(f)}{\mathtt{poly}(\log n)} \Rightarrow \Pr\left(F = F_x = F_y\right) \leq e^{-nc}\,\forall n \text{ large}$$

Function Computation

[BR '10], [MI '10]:

$$\lim_{\epsilon \to 0} \lim_{n \to} \frac{1}{n} D_\epsilon(f^n) = \mathtt{IC}(f).$$

- *Strong converse?* Our bound yields

$$\lim_{n \to} \frac{1}{n} D_\epsilon(f^n) \geq H(f(X,Y)|X) + H(f(X,Y)|Y)$$

- *Direct product or Arimoto converse?*
  [BRWY '13], [BW'14]:

$$|\pi_n| < \frac{n\mathtt{IC}(f)}{\mathtt{poly}(\log n)} \Rightarrow \Pr\left(F = F_x = F_y\right) \leq e^{-nc} \forall n \text{ large}$$

Our bound yields a threshold of $n[H(F|X) + H(F|Y)]$.

42

Separation of $D_\epsilon(\pi)$ and $\mathtt{IC}(\pi)$

[BBCR '10]: $D_\epsilon(\pi) \leq \tilde{\mathcal{O}}(\sqrt{|\pi|\mathtt{IC}(\pi)})$

[B '12]: $D_\epsilon(\pi) \leq 2^{\mathcal{O}(\mathtt{IC}(\pi))}$

Separation of $D_\epsilon(\pi)$ and $\texttt{IC}(\pi)$

[BBCR '10]: $D_\epsilon(\pi) \leq \tilde{\mathcal{O}}(\sqrt{|\pi|\texttt{IC}(\pi)})$

[B '12]: $D_\epsilon(\pi) \leq 2^{\mathcal{O}(\texttt{IC}(\pi))}$

Arbitrary separation possible for vanishing ϵ

$$\pi(x,y) = \begin{cases} a & \text{if } x > \delta 2^n, y > \delta 2^n \\ b & \text{if } x > \delta 2^n, y \leq \delta 2^n \\ c & \text{if } x \leq \delta 2^n, y > \delta 2^n \\ (x,y) & \text{if } x \leq \delta 2^n, y \leq \delta 2^n \end{cases}$$

For (X,Y) random n-bit strings, $\delta = 1/n$, and $\epsilon = 1/n^2$

$$\texttt{IC}(\pi) = \mathcal{O}(n^{-2}) \ll D_\epsilon(\pi) = \Omega(2n).$$

Separation of $D_\epsilon(\pi)$ and $\mathtt{IC}(\pi)$

[BBCR '10]: $D_\epsilon(\pi) \leq \tilde{\mathcal{O}}(\sqrt{|\pi|\mathtt{IC}(\pi)})$

[B '12]: $D_\epsilon(\pi) \leq 2^{\mathcal{O}(\mathtt{IC}(\pi))}$

Arbitrary separation possible for vanishing ϵ

$$\pi(x,y) = \begin{cases} a & \text{if } x > \delta 2^n, y > \delta 2^n \\ b & \text{if } x > \delta 2^n, y \leq \delta 2^n \\ c & \text{if } x \leq \delta 2^n, y > \delta 2^n \\ (x,y) & \text{if } x \leq \delta 2^n, y \leq \delta 2^n \end{cases}$$

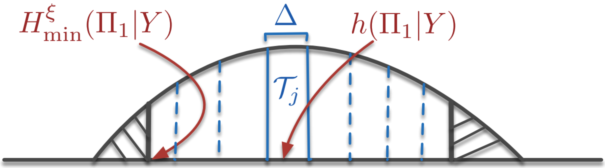
For (X, Y) random n-bit strings, $\delta = 1/n$, and $\epsilon = 1/n^2$

$$\mathtt{IC}(\pi) = \mathcal{O}(n^{-2}) \ll D_\epsilon(\pi) = \Omega(2n).$$

[GKR '13]: example with exponential separation even for ϵ fixed!

Proof Sketch

Simulaltion Scheme: The Compression Step



$$h_i \equiv \begin{cases} \text{Send } H_{\min}^{\xi}(\Pi_1|Y)\text{-bit random hash of } \Pi_1, & i = 1, \\ \text{Send } \Delta\text{-bit random hash of } \Pi_1, & 2 \le i \le N. \end{cases}$$

First party sends hash bits $h_i(t)$ successively until

it receives an ACK or $i = N$

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

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

Simulaltion Scheme: Compression to Simulation

- Generate Π_1 s.t. public coins can be treated as a hash of Π_1.

- Since this hash must be independent of (X, Y), can do this only for

$$H_{\min}(\Pi_1|XY) = H_{\min}(\Pi_1|X) \text{ bits .}$$

- Reduces the number of bits to be communicated from $h(\Pi_1|Y)$ to

$$h(\Pi_1|Y) - h(\Pi_1|X).$$

Lower Bound Proof: Super Sparse Version

- Based on reduction to secret key agreement with public discussion.
- We can compress since the parties agree on more bits L than the communicated bits R.
- $S \equiv$ max. length of a secret key that can be generated

$$L - R \leq S \Leftrightarrow L - S \leq R.$$

In closing ...

Information spectrum method is a promising approach for studying communication complexity

Open Problems:

- Strong converse and Arimoto converse for function computation
- Converse for [BBCR'10]
- Practical/universal versions of simulation algorithms
- Multiparty version