

# Universal Multiparty Data Exchange

Himanshu Tyagi

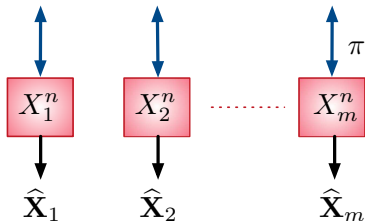
Indian Institute of Science, Bangalore

Shun Watanabe

Tokyo University of Agriculture and Technology

# Multiparty Data Exchange

# Source model for data exchange



Set of parties,  $\mathcal{M} = \{1, \dots, m\}$

Observations  $X_{\mathcal{M}}^n = \{X_{\mathcal{M}t}\}_{t=1}^n$  are iid with common pmf  $P_{X_{\mathcal{M}}}$

$\pi$  constitutes an omniscience protocol if  $\mathbb{P}(\hat{X}_1 = \dots = \hat{X}_m = X_{\mathcal{M}}^n) \approx 1$

$R_{\text{CO}}(P_{X_{\mathcal{M}}}) \equiv$  Minimum rate of communication for omniscience

# Characterization of min. comm. for omniscience

[Csiszár-Narayan 04]

$$R_{\text{co}}(P_{X_{\mathcal{M}}}) = \min_{(R_1, \dots, R_m) \in \mathcal{R}_{\text{co}}} \sum_{i=1}^m R_i,$$

where

$$\mathcal{R}_{\text{co}} = \{(R_1, \dots, R_m) : \sum_{i \in B} R_i \geq H(X_B | X_{B^c}), \quad \forall B \subsetneq \mathcal{M}\}$$

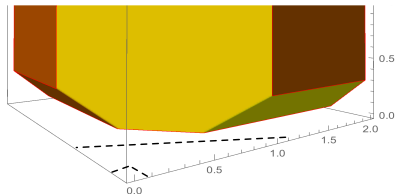
# Characterization of min. comm. for omniscience

[Csiszár-Narayan 04]

$$R_{\text{CO}}(P_{X_{\mathcal{M}}}) = \min_{(R_1, \dots, R_m) \in \mathcal{R}_{\text{CO}}} \sum_{i=1}^m R_i,$$

where

$$\mathcal{R}_{\text{CO}} = \{(R_1, \dots, R_m) : \sum_{i \in B} R_i \geq H(X_B | X_{B^c}), \quad \forall B \subsetneq \mathcal{M}\}$$



# Characterization of min. comm. for omniscience

[Csiszár-Narayan 04]

$$R_{\text{co}}(P_{X_{\mathcal{M}}}) = \min_{(R_1, \dots, R_m) \in \mathcal{R}_{\text{co}}} \sum_{i=1}^m R_i,$$

where

$$\mathcal{R}_{\text{co}} = \{(R_1, \dots, R_m) : \sum_{i \in B} R_i \geq H(X_B | X_{B^c}), \quad \forall B \subsetneq \mathcal{M}\}$$

[Chan-Zheng 10]

$$\min_{(R_1, \dots, R_m) \in \mathcal{R}_{\text{co}}} \sum_{i=1}^m R_i = \max_{\sigma \in \Sigma(\mathcal{M})} \frac{1}{|\sigma| - 1} \mathbb{H}_{\sigma},$$

where

$$\mathbb{H}_{\sigma} = \sum_{i=1}^{|\sigma|} H(X_{\mathcal{M}} | X_{\sigma_i})$$

## Our work: A universal protocol

Given  $(\mathbf{x}_1, \dots, \mathbf{x}_m)$ , enable data exchange using  
roughly  $nR_{\text{CO}}(\mathbb{P}_{\mathbf{x}_{\mathcal{M}}})$  bits of communication

# Building a Universal Protocol



# A basic building block

How should we send  $x$  to  $y$ ?

[Shulman-Feder 02, Yang-He 10, Braverman-Rao 11]

- ▶ Incrementally send  $n\Delta$  bits of random hash of  $x$
- ▶ Use a variant of “minimum conditional entropy” decoder:

Find the type  $P_{\bar{X}\bar{Y}}$  s.t.

1.  $P_{\bar{Y}} = P_Y$  and  $R \geq H(\bar{X}\bar{Y}) - H(\bar{Y})$
2.  $\exists$  unique  $x$  of conditional type  $P_{\bar{X}|\bar{Y}}$  given  $y$   
and consistent with hash values

# A basic building block

How should we send  $x$  to  $y$ ?

[Shulman-Feder 02, Yang-He 10, Braverman-Rao 11]

- ▶ Incrementally send  $n\Delta$  bits of random hash of  $x$
- ▶ Use a variant of “minimum conditional entropy” decoder:

Find the type  $P_{\bar{X}\bar{Y}}$  s.t.

1.  $P_{\bar{Y}} = P_Y$  and  $R \geq H(\bar{X}\bar{Y}) - H(\bar{Y})$
2.  $\exists$  unique  $x$  of conditional type  $P_{\bar{X}|\bar{Y}}$  given  $y$   
and consistent with hash values

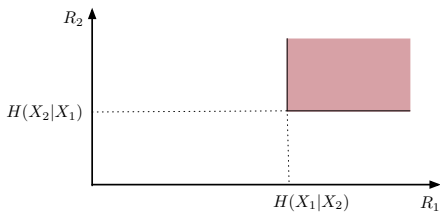
Shall use this to send  $x_{A \setminus \{i\}}$  to  $x_i$

## Ideal assumptions: Oracle model

- ▶ *Continuous rate*: Rate can be increased continuously
- ▶ *Ideal decoder*: An ideal decoder with following features is available
  1. Returns correct  $\mathbf{x}_A$ ,  $A \subset \mathcal{M}$ , as soon as  $(R_i, i \in A) \in \mathcal{R}_{\text{co}}(A)$
  2. If the condition above does not hold for any  $A$ , returns a NACK

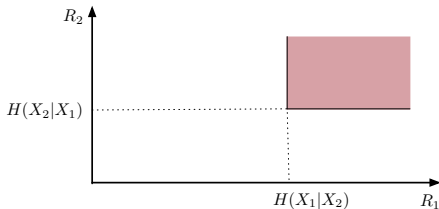
# Protocol for two parties

$$\mathcal{R}_{\text{co}}(\mathbb{P}_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



# Protocol for two parties

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$

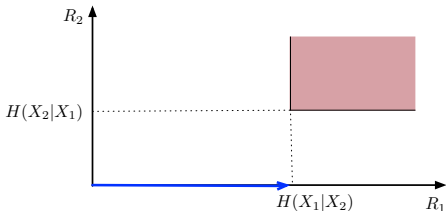


*Universal Protocol 1:*

1. Party 1 increases the rate until party 2 can decode

# Protocol for two parties

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$

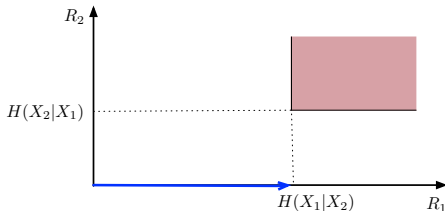


*Universal Protocol 1:*

1. Party 1 increases the rate until party 2 can decode

# Protocol for two parties

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$

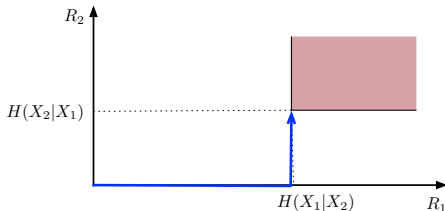


*Universal Protocol 1:*

1. Party 1 increases the rate until party 2 can decode
2. Party 2 increases the rate until Party 1 can decode

# Protocol for two parties

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



*Universal Protocol 1:*

1. Party 1 increases the rate until party 2 can decode
2. Party 2 increases the rate until Party 1 can decode



## What should we handle the case of $m > 2$ parties?

- ▶ Who should start communicating?
- ▶ When to start communicating?
- ▶ How to increase the rates?

# What should we handle the case of $m > 2$ parties?

- ▶ Who should start communicating?

Principle 1: Least compressible first

- ▶ When to start communicating?

- ▶ How to increase the rates?

# What should we handle the case of $m > 2$ parties?

- ▶ Who should start communicating?

Principle 1: Least compressible first

The party with the least value of  $H(P_{x_i})$  starts first

- ▶ When to start communicating?

- ▶ How to increase the rates?

# What should we handle the case of $m > 2$ parties?

- ▶ Who should start communicating?

Principle 1: Least compressible first

The party with the least value of  $H(P_{x_i})$  starts first

- ▶ When to start communicating?

Principle 2: Conservation of entropy difference

- ▶ How to increase the rates?

# What should we handle the case of $m > 2$ parties?

- ▶ Who should start communicating?

Principle 1: Least compressible first

The party with the least value of  $H(P_{\mathbf{x}_i})$  starts first

- ▶ When to start communicating?

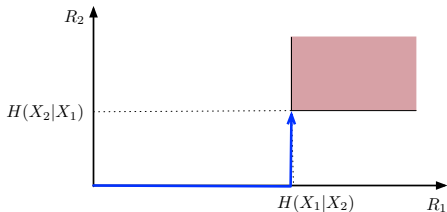
Principle 2: Conservation of entropy difference

Maintain  $H(\mathbf{x}_i) - H(\mathbf{x}_j)$  for all communicating parties  $i, j$

- ▶ How to increase the rates?

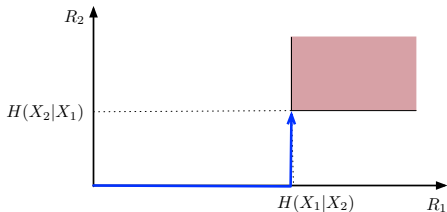
# Example 1 ( $m = 2$ )

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



## Example 1 ( $m = 2$ )

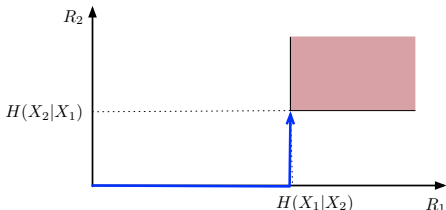
$$\mathcal{R}_{\text{co}}(\mathbb{P}_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



Observation 1:  $R_1^* - R_2^* = H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)$

## Example 1 ( $m = 2$ )

$$\mathcal{R}_{\text{co}}(\mathbb{P}_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



Observation 1:  $R_1^* - R_2^* = H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)$

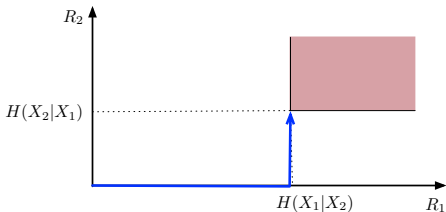
*Universal Protocol 2:*

1. Parties compute their types (empirical distributions)  $\mathbb{P}_{\mathbf{x}_i}$  and share



## Example 1 ( $m = 2$ )

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



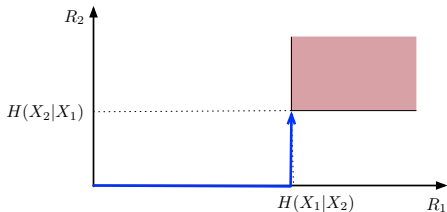
Observation 1:  $R_1^* - R_2^* = H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)$

*Universal Protocol 2:*

1. Party with higher value of  $H(P_{x_i})$  initializes communication

## Example 1 ( $m = 2$ )

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



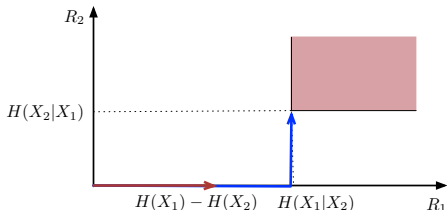
Observation 1:  $R_1^* - R_2^* = H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)$

*Universal Protocol 2:*

1. Party with higher value of  $H(P_{x_i})$  initializes communication
2. Party 2 starts communicating when  $R_1 = H(P_{x_1}) - H(P_{x_2})$

## Example 1 ( $m = 2$ )

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



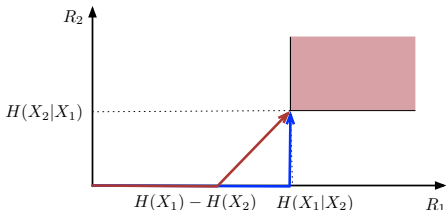
Observation 1:  $R_1^* - R_2^* = H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)$

*Universal Protocol 2:*

1. Party with higher value of  $H(P_{x_i})$  initializes communication
2. Party 2 starts communicating when  $R_1 = H(P_{x_1}) - H(P_{x_2})$
3. Parties increase the rates until they recover each other

## Example 1 ( $m = 2$ )

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



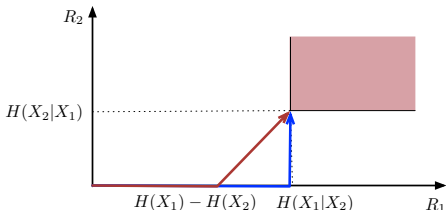
Observation 1:  $R_1^* - R_2^* = H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)$

*Universal Protocol 2:*

1. Party with higher value of  $H(P_{x_i})$  initializes communication
2. Party 2 starts communicating when  $R_1 = H(P_{x_1}) - H(P_{x_2})$
3. Parties increase the rates until they recover each other

## Example 1 ( $m = 2$ )

$$\mathcal{R}_{\text{co}}(P_{X_1 X_2}) = \{(R_1, R_2) : R_i \geq H(X_1, X_2 | X_i), i \in \{1, 2\}\}$$



Observation 1:  $R_1^* - R_2^* = H(X_1|X_2) - H(X_2|X_1) = H(X_1) - H(X_2)$

Observation 2: Both parties will simultaneously decode each other

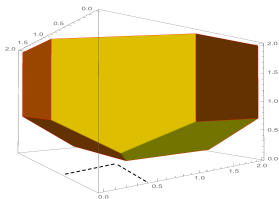
*Universal Protocol 2:*

1. Party with higher value of  $H(P_{x_i})$  initializes communication
2. Party 2 starts communicating when  $R_1 = H(P_{x_1}) - H(P_{x_2})$
3. Parties increase the rates until they recover each other

## Example 2 ( $m = 3$ )

$$X_1 \sim \text{Ber}(1/2), \quad X_3 \sim \text{Ber}(q), \quad X_2 = X_1 \oplus X_3, \quad h(q) > 1/2$$

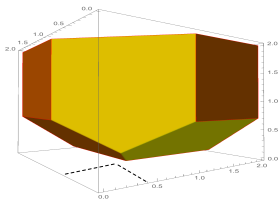
- Finest partition is dominant
- The unique optimal rate assignment is given by  $\mathbf{R}^* = (1/2, 1/2, h(q) - 1/2)$



## Example 2 ( $m = 3$ )

$$X_1 \sim \text{Ber}(1/2), \quad X_3 \sim \text{Ber}(q), \quad X_2 = X_1 \oplus X_3, \quad h(q) > 1/2$$

- Finest partition is dominant
- The unique optimal rate assignment is given by  $\mathbf{R}^* = (1/2, 1/2, h(q) - 1/2)$

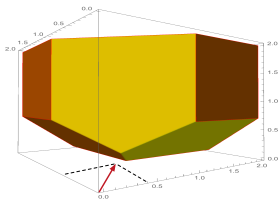


1.  $H(X_1) = H(X_2) = 1 > H(X_3) \Rightarrow$  Parties 1 and 2 start at slope 1

## Example 2 ( $m = 3$ )

$$X_1 \sim \text{Ber}(1/2), \quad X_3 \sim \text{Ber}(q), \quad X_2 = X_1 \oplus X_3, \quad h(q) > 1/2$$

- Finest partition is dominant
- The unique optimal rate assignment is given by  $\mathbf{R}^* = (1/2, 1/2, h(q) - 1/2)$



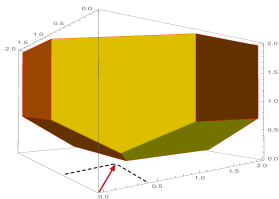
1.  $H(X_1) = H(X_2) = 1 > H(X_3) \Rightarrow$  Parties 1 and 2 start at slope 1



## Example 2 ( $m = 3$ )

$$X_1 \sim \text{Ber}(1/2), \quad X_3 \sim \text{Ber}(q), \quad X_2 = X_1 \oplus X_3, \quad h(q) > 1/2$$

- Finest partition is dominant
- The unique optimal rate assignment is given by  $\mathbf{R}^* = (1/2, 1/2, h(q) - 1/2)$

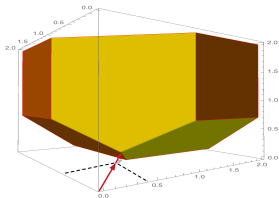


1.  $H(X_1) = H(X_2) = 1 > H(X_3) \Rightarrow$  Parties 1 and 2 start at slope 1
2. Party 3 starts when  $R_1 = R_2 = H(X_1) - H(X_3) = 1 - h(q)$

## Example 2 ( $m = 3$ )

$$X_1 \sim \text{Ber}(1/2), \quad X_3 \sim \text{Ber}(q), \quad X_2 = X_1 \oplus X_3, \quad h(q) > 1/2$$

- Finest partition is dominant
- The unique optimal rate assignment is given by  $\mathbf{R}^* = (1/2, 1/2, h(q) - 1/2)$



1.  $H(X_1) = H(X_2) = 1 > H(X_3) \Rightarrow$  Parties 1 and 2 start at slope 1
2. Party 3 starts when  $R_1 = R_2 = H(X_1) - H(X_3) = 1 - h(q)$

# What needs to be done for $m > 2$ parties?

- ▶ Who starts communicating?

Principle 1: Least compressible first

- ▶ When to start communicating?

Principle 2: Conservation of entropy difference

- ▶ How to increase the rates?

# What needs to be done for $m > 2$ parties?

- ▶ Who starts communicating?

Principle 1: Least compressible first

- ▶ When to start communicating?

Principle 2: Conservation of entropy difference

- ▶ How to increase the rates?

Principle 3: Combine and share the rate

## What needs to be done for $m > 2$ parties?

- ▶ Who starts communicating?

Principle 1: Least compressible first

- ▶ When to start communicating?

Principle 2: Conservation of entropy difference

- ▶ How to increase the rates?

Principle 3: Combine and share the rate

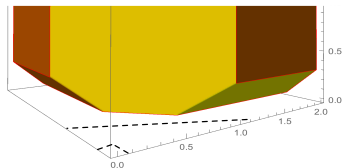
If parties in  $A$  attain “local omniscience,” they start behaving as one and increment the rates at slope  $1/|A|$

## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant

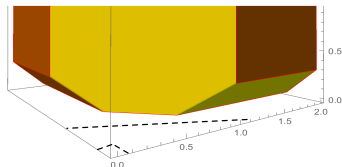


## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant



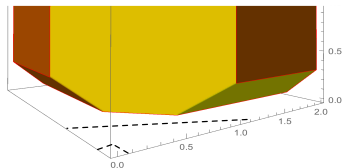
1. Parties 1 and 2 start at slope 1

## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant



1. Parties 1 and 2 start at slope 1
2. They attain local omniscience when  $R_1 = h(q) = R_2$

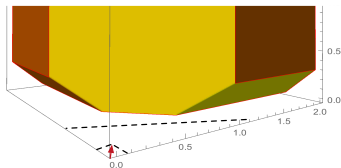


## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant



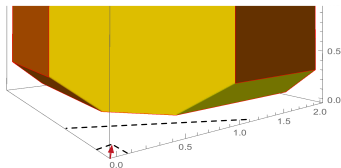
1. Parties 1 and 2 start at slope 1
2. They attain local omniscience when  $R_1 = h(q) = R_2$

## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant



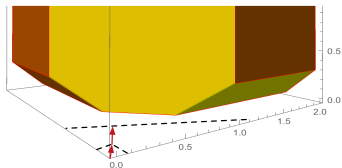
1. Parties 1 and 2 start at slope 1
2. They attain local omniscience when  $R_1 = h(q) = R_2$
3. Parties 1 and 2 increase rates at slope 1/2

## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant



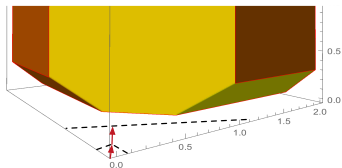
1. Parties 1 and 2 start at slope 1
2. They attain local omniscience when  $R_1 = h(q) = R_2$
3. Parties 1 and 2 increase rates at slope 1/2

## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant



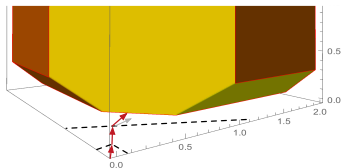
1. Parties 1 and 2 start at slope 1
2. They attain local omniscience when  $R_1 = h(q) = R_2$
3. Parties 1 and 2 increase rates at slope  $1/2$
4. Parties 3 starts when  $R_1 + R_2 - R_3 = H(X_1, X_2) - H(X_3) = 1 + h(q)$

## Example 3 ( $m = 3$ )

$$W_1, W_2 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2$$

- Partition  $\{12|3\}$  is dominant



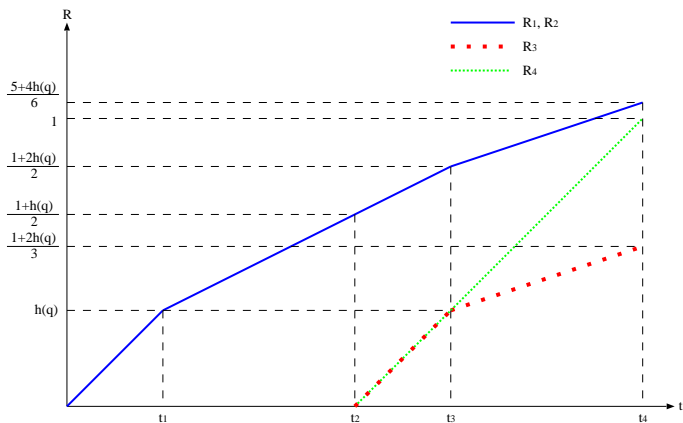
1. Parties 1 and 2 start at slope 1
2. They attain local omniscience when  $R_1 = h(q) = R_2$
3. Parties 1 and 2 increase rates at slope  $1/2$
4. Parties 3 starts when  $R_1 + R_2 - R_3 = H(X_1, X_2) - H(X_3) = 1 + h(q)$

## Example 4 ( $m = 4$ )

$$W_1, W_2, W_3 \sim \text{Ber}(1/2), \quad V_1, V_2 \sim \text{Ber}(q), \quad q < 1/2$$

$$X_1 = (W_1, W_2), \quad X_2 = (W_1 \oplus V_1, W_2), \quad X_3 = W_2 \oplus V_2, \quad X_4 = W_3$$

- Partition  $\{123|4\}$  is dominant



# A Universal Protocol for Multiparty Data Exchange

# The OMN subroutine

$\text{OMN}(\sigma, \mathbf{H}, \mathbf{R})$

## Inputs

$\mathbf{H} = (H_{\sigma_1}, \dots, H_{\sigma_k})$  is a decreasing sequence

$\mathbf{R} = (R_1, \dots, R_m)$

## Outputs

$\mathcal{O}$  : the set of subsets that attain omniscience

$\mathbf{R}^{\text{out}}$  : rates of communication when OMN terminates

## Execution

**While** all decoders output NACK

1. All parties with  $R_i > 0$ ,  $i \in \sigma_l$ , increase their rates at “slope”  $1/|\sigma_l|$
2. A new party  $j \equiv \sigma_j$  starts communicating if

$$R_{\sigma_1} - R_{\sigma_j} = H_{\sigma_1} - H_{\sigma_j}$$

3. Each party is running the ideal decoder



## Main observation: The recursive structure of OMN

If OMN is called with a valid rate vector  $\mathbf{R}$

If a new subset  $A$  attains local omniscience:

(i)  $A$  is of the form  $\{\sigma_{i_1}, \dots, \sigma_{i_l}\}$ ;

(ii)  $\mathbf{R}^{\text{out}}$  is as if the parties in  $A$  were together from the start

## Main observation: The recursive structure of OMN

If OMN is called with a valid rate vector  $\mathbf{R}$

If a new subset  $A$  attains local omniscience:

(i)  $A$  is of the form  $\{\sigma_{i_1}, \dots, \sigma_{i_l}\}$ ;

(ii)  $\mathbf{R}^{\text{out}}$  is as if the parties in  $A$  were together from the start

The sum rate  $R_A$  is given by

$$R_A = \mathbb{H}_{\sigma_f(A)}(A) = \frac{1}{l-1} \sum_{j=1}^l H(X_A | X_{\sigma_{i_j}})$$

# Protocol under ideal assumptions

## Initialization

$$\mathbf{R} = (0, -1, -1, \dots, -1)$$

$$\mathbf{H} = (H(P_{\mathbf{x}_1}), \dots, H(P_{\mathbf{x}_m}))$$

$$\sigma = \sigma_f(\mathcal{M})$$

## Execution

**While** omniscience is not attained

1. Call  $\text{OMN}(\sigma, \mathbf{H}, \mathbf{R})$ ; let output be  $\mathcal{O}$  and  $\mathbf{R}^{\text{out}}$

2. **Update:**

$$\mathbf{R} = \mathbf{R}^{\text{out}}$$

$\sigma =$  parts consist of subsets that have attained local omniscience

$$\mathbf{H} = (H_{\sigma_1}, \dots, H_{\sigma_k})$$

3. Go to step 1

The Fact of the Matter

# Individual sequence performance

## Theorem

*For every  $\Delta > 0$  and every sequence  $\mathbf{x}_{\mathcal{M}}$ , the probability of error for our protocol is bounded above by*

$$C_1 \left( \frac{\log |\mathcal{X}_{\mathcal{M}}|}{\Delta} + m \right) p(n) 2^{-n\Delta}.$$

*Furthermore, if an error does not occur, the number of bits communicated by the protocol for input  $\mathbf{x}_{\mathcal{M}}$  is bounded above by*

$$nR_{\text{CO}}(\mathcal{M}|\mathbf{P}_{\mathbf{x}_{\mathcal{M}}}) + nC_2\Delta + C_3 \left( \frac{\log |\mathcal{X}_{\mathcal{M}}|}{\Delta} + m \right) + C_4 \log n.$$