Partition-Symmetrical Entropy Functions

Qi Chen
joint work with Raymond W. Yeung

Institute of Network Coding
The Chinese University of Hong Kong

CAM 2016, HKU
August 24, 2016

Entropy region Γ_n^*

Entropy function

- $\mathcal{N} = \{1, 2, \cdots, n\}$

- $\mathcal{N} = \{1, 2, 3, 4\}$,

Entropy region Γ_n^*

Entropy function

- $\mathcal{N} = \{1, 2, \cdots, n\}$
- $\mathbf{X}_{\mathcal{N}} = (X_i : i \in \mathcal{N})$,
  $X_{\mathcal{A}} = (X_i, i \in \mathcal{A})$,
  $\mathcal{A} \subset \mathcal{N}$

- $\mathcal{N} = \{1, 2, 3, 4\}$,
- $\mathbf{X}_{\{1,2,3,4\}} = (X_1, X_2, X_3, X_4)$,
  $X_{23} = (X_2, X_3)$,

Entropy region Γ_n^*

Entropy function

- $\mathcal{N} = \{1, 2, \cdots, n\}$
- $\mathbf{X}_{\mathcal{N}} = (X_i : i \in \mathcal{N})$,
  $X_{\mathcal{A}} = (X_i, i \in \mathcal{A})$,
  $\mathcal{A} \subset \mathcal{N}$
- entropy function
  $\mathbf{h} : 2^{\mathcal{N}} \to \mathbb{R}$,
  $\mathbf{h}(\mathcal{A}) \triangleq H(X_{\mathcal{A}}),\ \forall \mathcal{A} \subset \mathcal{N}$ with $H(X_\emptyset) = 0$.

- $\mathcal{N} = \{1, 2, 3, 4\}$,
- $\mathbf{X}_{\{1,2,3,4\}} = (X_1, X_2, X_3, X_4)$,
  $X_{23} = (X_2, X_3)$,
- $\mathbf{h} = (0, H(X_1), \cdots, H(X_4), H(X_{12}), \cdots, H(X_{34}), \cdots, H(X_{1234}))$

Entropy region Γ_n^*

Entropy function

- $\mathcal{N} = \{1, 2, \cdots, n\}$
- $\mathbf{X}_\mathcal{N} = (X_i : i \in \mathcal{N})$,
  $X_\mathcal{A} = (X_i, i \in \mathcal{A})$,
  $\mathcal{A} \subset \mathcal{N}$
- entropy function
  $\mathbf{h} : 2^\mathcal{N} \to \mathbb{R}$,
  $\mathbf{h}(\mathcal{A}) \triangleq H(X_\mathcal{A})$, $\forall \mathcal{A} \subset \mathcal{N}$ with $H(X_\emptyset) = 0$.
- entropy space
  $\mathcal{H}_n \triangleq \mathbb{R}^{2^\mathcal{N}}$

- $\mathcal{N} = \{1, 2, 3, 4\}$,
- $\mathbf{X}_{\{1,2,3,4\}} = (X_1, X_2, X_3, X_4)$,
  $X_{23} = (X_2, X_3)$,
- $\mathbf{h} =$
  $(0, H(X_1), \cdots, H(X_4), H(X_{12}), \cdots, H(X_{34}), \cdots, H(X_{1234}))$
- $\mathcal{H}_4 \triangleq \mathbb{R}^{2^{\{1,2,3,4\}}}$

Entropy region Γ_n^*

Entropy function

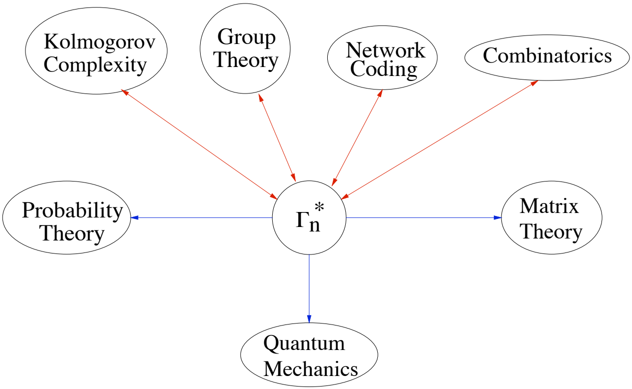
- $\mathcal{N} = \{1, 2, \cdots, n\}$
- $\mathbf{X}_{\mathcal{N}} = (X_i : i \in \mathcal{N})$, $X_{\mathcal{A}} = (X_i, i \in \mathcal{A})$, $\mathcal{A} \subset \mathcal{N}$
- entropy function $\mathbf{h} : 2^{\mathcal{N}} \to \mathbb{R}$, $\mathbf{h}(\mathcal{A}) \triangleq H(X_{\mathcal{A}})$, $\forall \mathcal{A} \subset \mathcal{N}$ with $H(X_{\emptyset}) = 0$.
- entropy space $\mathcal{H}_n \triangleq \mathbb{R}^{2^{\mathcal{N}}}$

- $\mathcal{N} = \{1, 2, 3, 4\}$,
- $\mathbf{X}_{\{1,2,3,4\}} = (X_1, X_2, X_3, X_4)$, $X_{23} = (X_2, X_3)$,
- $\mathbf{h} = (0, H(X_1), \cdots, H(X_4), H(X_{12}), \cdots, H(X_{34}), \cdots, H(X_{1234}))$
- $\mathcal{H}_4 \triangleq \mathbb{R}^{2^{\{1,2,3,4\}}}$

Entropy region:Γ_n^*

$$\Gamma_n^* \triangleq \{\mathbf{h} \in \mathcal{H}_n | \exists\ \mathbf{X}_{\mathcal{N}},\ \mathbf{h} \text{ is the entropy function of } \mathbf{X}_{\mathcal{N}}\}.$$

Subjects Related to Γ_n^*



Γ_n^* and Γ_n

Shannon-type inequalities

For any $\mathcal{A}, \mathcal{B} \subset \mathcal{N}$,

$$
\begin{aligned}
H(X_{\mathcal{A}}) &\geq 0, \\
H(X_{\mathcal{A}}) &\leq H(X_{\mathcal{B}}) \quad \text{if } \mathcal{A} \subset \mathcal{B}, \\
H(X_{\mathcal{A}}) + H(X_{\mathcal{B}}) &\geq H(X_{\mathcal{A}\cap\mathcal{B}}) + H(X_{\mathcal{A}\cup\mathcal{B}}).
\end{aligned}
$$

Γ_n^* and Γ_n

Shannon-type inequalities

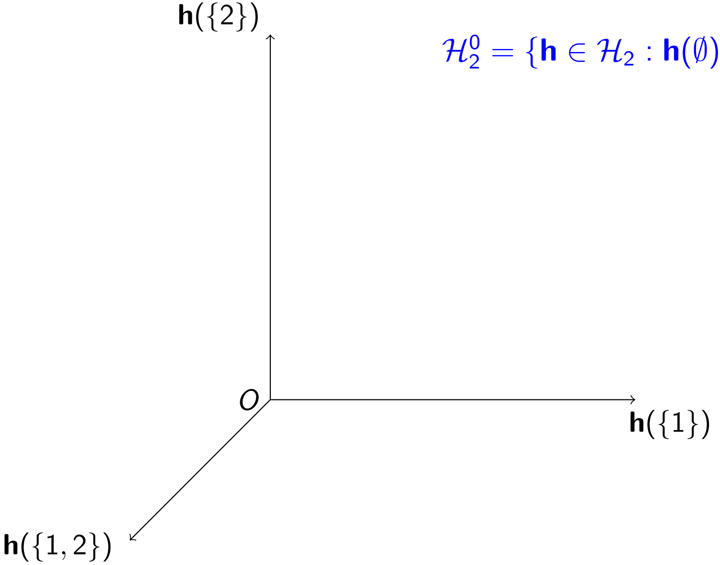
For any $\mathcal{A}, \mathcal{B} \subset \mathcal{N}$,

$$\begin{aligned} H(X_{\mathcal{A}}) &\geq 0, \\ H(X_{\mathcal{A}}) &\leq H(X_{\mathcal{B}}) \ \text{ if } \mathcal{A} \subset \mathcal{B}, \\ H(X_{\mathcal{A}}) + H(X_{\mathcal{B}}) &\geq H(X_{\mathcal{A}\cap\mathcal{B}}) + H(X_{\mathcal{A}\cup\mathcal{B}}). \end{aligned}$$

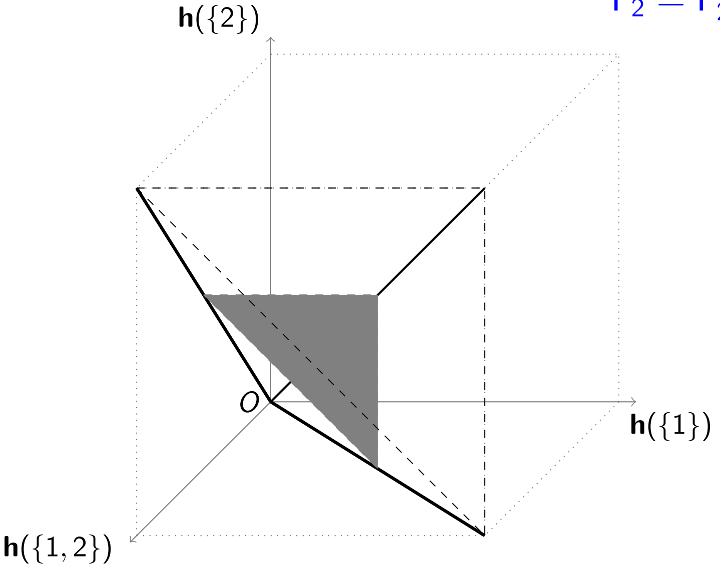
Polymatroidal region:Γ_n

$$\begin{aligned} \Gamma_n \triangleq \{\mathbf{h} \in \mathcal{H}_n : \ & \mathbf{h}(\mathcal{A}) \geq 0, \\ & \mathbf{h}(\mathcal{A}) \leq \mathbf{h}(\mathcal{B}), \quad \text{if } \mathcal{A} \subset \mathcal{B}, \\ & \mathbf{h}(\mathcal{A}) + \mathbf{h}(\mathcal{B}) \geq \mathbf{h}(\mathcal{A} \cap \mathcal{B}) + \mathbf{h}(\mathcal{A} \cup \mathcal{B})\}. \end{aligned}$$

$$\mathcal{H}_2^0 = \{\mathbf{h} \in \mathcal{H}_2 : \mathbf{h}(\emptyset) = 0\}$$



$\Gamma_2 = \Gamma_2^*$



Γ_n^* and Γ_n

Relations between Γ_n^* and Γ_n

- $\Gamma_n^* \subset \Gamma_n$,[Fujishige 78]
- $\Gamma_2^* = \Gamma_2$,
- $\Gamma_3^* \subsetneq \Gamma_3$, but $\overline{\Gamma_3^*} = \Gamma_3$,[Zhang and Yeung 97, Matúš 06, Chen and Yeung 12]
- $\overline{\Gamma_n^*} = \Gamma_n, \ \ n \leq 3$,
- $\overline{\Gamma_n^*} \subsetneq \Gamma_n, \ \ n \geq 4$, due to the existence of non-Shannon-type information inequalities.[Zhang and Yeung 98]

Γ_n^* and Γ_n

non-Shannon-type inequalities

- Z. Zhang and R. W. Yeung, On characterization of entropy function via information inequalities, IEEE Trans. Inform. Theory, vol. 44, pp. 1440-1452, Nov. 1998.

Γ_n^* and Γ_n

non-Shannon-type inequalities

- Z. Zhang and R. W. Yeung, On characterization of entropy function via information inequalities, IEEE Trans. Inform. Theory, vol. 44, pp. 1440-1452, Nov. 1998.
- X. Yan, R. W. Yeung and Z. Zhang, A class of non-Shannon type information inequalities and their applications, IEEE Int. Symp. Inf. Theory, Washington DC, June 2001.
- R. Dougherty, C. Freiling and K. Zeger, Six new non-Shannon information inequalities, IEEE Int. Symp. Inf. Theory, Seattle WA June 2006.
- ...

Γ_n^* and Γ_n

non-Shannon-type inequalities

- Z. Zhang and R. W. Yeung, On characterization of entropy function via information inequalities, IEEE Trans. Inform. Theory, vol. 44, pp. 1440-1452, Nov. 1998.
- X. Yan, R. W. Yeung and Z. Zhang, A class of non-Shannon type information inequalities and their applications, IEEE Int. Symp. Inf. Theory, Washington DC, June 2001.
- R. Dougherty, C. Freiling and K. Zeger, Six new non-Shannon information inequalities, IEEE Int. Symp. Inf. Theory, Seattle WA June 2006.
- ...
- F. Matúš, Infinitely many information inequalities, IEEE Int. Symp. Inf. Theory, Nice, France, June 2007.

Partition-symmetrical entropy functions and their applications to secrect-sharing[1]

[1] Q. Chen and R. W. Yeung, "Partition-Symmetrical Entropy functions," to appear in *IEEE Transactions on Information Theory*.

Permutation groups and partition groups

Permutation group

- Permutation σ: A bijection from $\mathcal{N} = \{1, \cdots, n\}$ to $\mathcal{N}$ itself
- Symmetric group S_n:The set of all permutations with composition being the binary operation
- Permutation group Σ: Any subgroup of the symmetric group.

Permutation groups and partition groups

Permutation group

- Permutation σ: A bijection from $\mathcal{N} = \{1, \cdots, n\}$ to $\mathcal{N}$ itself
- Symmetric group S_n:The set of all permutations with composition being the binary operation
- Permutation group Σ: Any subgroup of the symmetric group.

Partition group

- Partition p of $\mathcal{N}$: A set of disjoint subset $\{\mathcal{N}_1, \cdots, \mathcal{N}_t\}$ such that $\cup_{i=1}^{t} \mathcal{N}_i = \mathcal{N}$. Each $\mathcal{N}_i$ is called a block of p.
- Partition group Σ_p: A permutation group whose members are all permutations that permute the members of $\mathcal{N}$ within the same block of p, i.e.,

$$\Sigma_p = \{\sigma \in \Sigma_n : \sigma(j) \in \mathcal{N}_i,\ j \in \mathcal{N}_i,\ i = 1, \cdots, t\}.$$

Group actions

Definition (Group action)

For a set $\mathcal{S}$, a group Σ *acts* on $\mathcal{S}$ if there exist a function $\Sigma \times \mathcal{S} \to \mathcal{S}$, called an action, denoted by $(\sigma, s) \mapsto \sigma s$, such that

1. $(\sigma_1 \sigma_2)s = \sigma_1(\sigma_2 s)$ for all $\sigma_1, \sigma_2 \in \Sigma$ and $s \in \mathcal{S}$;
2. $1s = s$ for all $s \in \mathcal{S}$, where 1 is the identity of Σ.

Group actions

Definition (Group action)

For a set $\mathcal{S}$, a group Σ *acts* on $\mathcal{S}$ if there exist a function $\Sigma \times \mathcal{S} \to \mathcal{S}$, called an action, denoted by $(\sigma, s) \mapsto \sigma s$, such that

1. $(\sigma_1\sigma_2)s = \sigma_1(\sigma_2 s)$ for all $\sigma_1, \sigma_2 \in \Sigma$ and $s \in \mathcal{S}$;
2. $1s = s$ for all $s \in \mathcal{S}$, where 1 is the identity of Σ.

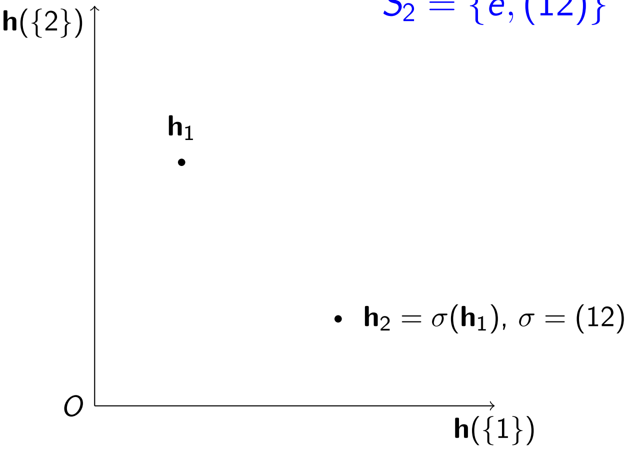
Group action $\Sigma \times \mathcal{H}_n \to \mathcal{H}_n$

For any $\sigma \in S_n$, define $\sigma : \mathcal{H}_n \to \mathcal{H}_n$ by

$$\sigma(\mathbf{h})(\mathcal{A}) = \mathbf{h}(\sigma(\mathcal{A})),\ \mathcal{A} \subset \mathcal{N}.$$

- $\sigma \times \mathbf{h} \mapsto \sigma(\mathbf{h})$ defines a group action S_n on $\mathcal{H}_n$
- Restricted the on a subgroup Σ, it becomes a group action Σ on $\mathcal{H}_n$.

$S_2 = \{e, (12)\}$


$\mathbf{h}(\{2\})$
$\mathbf{h}_1$
$\mathbf{h}_2 = \sigma(\mathbf{h}_1)$, $\sigma = (12)$
O
$\mathbf{h}(\{1\})$

Fixed set

Definition

If a group Σ acts on $\mathcal{S}$, the *fixed set* of the action is defined by

$$\operatorname{fix}_{\Sigma} = \{s \in \mathcal{S} : \sigma s = s, \forall \sigma \in \Sigma\}.$$

Fixed set

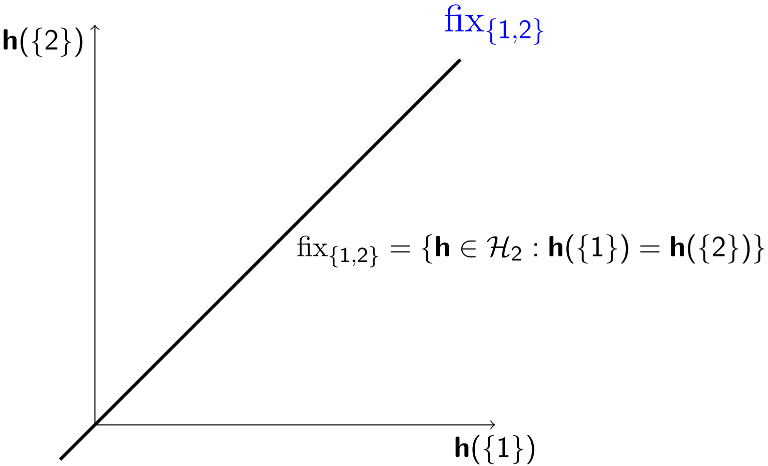
Definition

If a group Σ acts on $\mathcal{S}$, the *fixed set* of the action is defined by

$$\mathrm{fix}_{\Sigma} = \{s \in \mathcal{S} : \sigma s = s, \forall \sigma \in \Sigma\}.$$

Fix set of the partition group acting on $\mathcal{H}_n$

$$\begin{aligned}\mathrm{fix}_p = \mathrm{fix}_{\Sigma_p} = \{\mathbf{h} \in \mathcal{H}_n :\ & \mathbf{h}(\mathcal{A}) = \mathbf{h}(\mathcal{B}) \\ & \text{if } |\mathcal{A} \cap \mathcal{N}_i| = |\mathcal{B} \cap \mathcal{N}_i|,\ \forall i = 1, \cdots, t\}.\end{aligned}$$


$\mathrm{fix}_{\{1,2\}}$
$\mathbf{h}(\{2\})$
$\mathrm{fix}_{\{1,2\}} = \{\mathbf{h} \in \mathcal{H}_2 : \mathbf{h}(\{1\}) = \mathbf{h}(\{2\})\}$
$\mathbf{h}(\{1\})$

Main theorem

Constraining Γ_n^* and Γ_n by fix_p, we obtain the *p-symmetrical entropy region*

$$\Psi_p^* = \Gamma_n^* \cap \mathrm{fix}_p$$

and *p-symmetrical polymatroidal region*

$$\Psi_p = \Gamma_n \cap \mathrm{fix}_p,$$

respectively.

Main theorem

Constraining Γ_n^* and Γ_n by fix_p, we obtain the *p-symmetrical entropy region*

$$\Psi_p^* = \Gamma_n^* \cap \mathrm{fix}_p$$

and *p-symmetrical polymatroidal region*

$$\Psi_p = \Gamma_n \cap \mathrm{fix}_p,$$

respectively.

Theorem

For $n \geq 4$ and any $p \in \mathcal{P}_n$,

$$\overline{\Psi_p^*} = \Psi_p,$$

if and only if $p = \{\mathcal{N}\}$ or $p = \{\{i\}, \mathcal{N} \setminus \{i\}\}$.

Application to secret-sharing

Consider the secret be a random variable S on K, and each share be a random variable S_j on K_j, where $j \in \mathcal{P}$, the set of participants. Then the scheme $\mathbf{S} = (S, S_j)_{p_j \in \mathcal{P}}$ is a secret-sharing scheme realizing access structure $\mathcal{A}$, where $\mathcal{A} \subset 2^{\mathcal{P}}$ and $\mathcal{A}$ is monotone, if the following two conditions hold:

1. (**Correctness**) For any $B \in \mathcal{A}$,

$$H(S|S_B) = 0$$

2. (**Perfect Privacy**) For any $T \notin \mathcal{A}$,

$$H(S|S_T) = H(S)$$

Application to secret-sharing

Consider the secret be a random variable S on K, and each share be a random variable S_j on K_j, where $j \in \mathcal{P}$, the set of participants. Then the scheme $\mathbf{S} = (S, S_j)_{p_j \in \mathcal{P}}$ is a secret-sharing scheme realizing access structure $\mathcal{A}$, where $\mathcal{A} \subset 2^{\mathcal{P}}$ and $\mathcal{A}$ is monotone, if the following two conditions hold:

1. (**Correctness**) For any $B \in \mathcal{A}$,

$$H(S|S_B) = 0$$

2. (**Perfect Privacy**) For any $T \notin \mathcal{A}$,

$$H(S|S_T) = H(S)$$

Information ratio

$$\rho_{\mathbf{S}} \triangleq \frac{\max_{1 \leq j \leq n} H(S_j)}{H(S)}$$

The fundamental problem of secret sharing: optimal information ratio

Let $\mathcal{N} = \{s\} \cup \mathcal{P}$ and $\Gamma^*_{\mathcal{N}}$ be the entropy region on $\mathcal{N}$. Let $\mathcal{A}$ be an access structure on $\mathcal{P}$. Then the optimal information ratio on $\mathcal{A}$ is

$$\rho_{\mathcal{A}} \triangleq \inf_{\mathbf{h} \in \Gamma^*_{\mathcal{N}} \cap \Phi_{\mathcal{A}}} \frac{\max_{1 \leq j \leq n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where

$$\begin{aligned} \Phi_{\mathcal{A}} = \{\mathbf{h} : \mathbf{h}(\{s\} \cup B) &= \mathbf{h}(B) \quad \forall B \in \mathcal{A}, \\ \mathbf{h}(\{s\} \cup T) &= \mathbf{h}(\{s\}) + \mathbf{h}(T) \quad \forall T \notin \mathcal{A}\} \end{aligned}$$

Shamir's threshold scheme by entropy functions

For $1 \leq t \leq n$, let $\mathcal{A}_{t,n} = \{A \subset \mathcal{P} : |A| \geq t\}$. Then $\mathcal{A}_{t,n}$ is a access structure with threshold t.

For simplicity, let $\rho_{t,n} = \rho_{\mathcal{A}_{t,n}}$ and $\Phi_{t,n} = \Phi_{\mathcal{A}_{t,n}}$. Then

$$\rho_{t,n} = \inf_{\mathbf{h} \in \Gamma^*_{\mathcal{N}} \cap \Phi_{t,n}} \frac{\max_{1 \leq j \leq n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where

$$\begin{aligned} \Phi_{t,n} = \{\mathbf{h} : & \mathbf{h}(\{s\} \cup B) = \mathbf{h}(B) \quad \text{if } |B| \geq t, \\ & \mathbf{h}(\{s\} \cup B) = \mathbf{h}(\{s\}) + \mathbf{h}(B) \quad \text{if } |B| < t\} \end{aligned}$$

Shamir's threshold scheme by entropy functions

For $1 \leq t \leq n$, let $\mathcal{A}_{t,n} = \{A \subset \mathcal{P} : |A| \geq t\}$. Then $\mathcal{A}_{t,n}$ is a access structure with threshold t.
For simplicity, let $\rho_{t,n} = \rho_{\mathcal{A}_{t,n}}$ and $\Phi_{t,n} = \Phi_{\mathcal{A}_{t,n}}$. Then

$$\rho_{t,n} = \inf_{\mathbf{h} \in \Gamma^*_{\mathcal{N}} \cap \Phi_{t,n}} \frac{\max_{1 \leq j \leq n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where

$$\begin{aligned} \Phi_{t,n} = \{\mathbf{h} : & \mathbf{h}(\{s\} \cup B) = \mathbf{h}(B) \quad \text{if } |B| \geq t, \\ & \mathbf{h}(\{s\} \cup B) = \mathbf{h}(\{s\}) + \mathbf{h}(B) \quad \text{if } |B| < t\} \end{aligned}$$

Theorem

$$\rho_{t,n} = \inf_{\mathbf{h} \in \Psi^*_p \cap \Phi_{t,n}} \frac{\max_{1 \leq j \leq n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where $p = \{\{s\}, \mathcal{P}\}$

Shamir's threshold scheme by entropy functions

Theorem

$$\rho_{t,n} = \min_{\mathbf{h} \in \Psi_p \cap \Phi_{t,n}} \frac{\max_{1 \leq j \leq n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

and the solution is

$$\rho_{t,n} = 1$$

and

$$\arg\min \rho_{t,n} = \{\mathbf{h} : aU_{t,n+1}, a > 0\}$$

Further research: group-symmetrical entropy functions and their applications to other areas

From partition-symmetrical entropy functions to group-symmetrical entropy functions

Fix set induced by a partition-group Σ_p

$$\mathrm{fix}_p = \{\mathbf{h} \in \mathcal{H}_n : \ \mathbf{h}(\mathcal{A}) = \mathbf{h}(\mathcal{B}) \\ \text{if } |\mathcal{A} \cap \mathcal{N}_i| = |\mathcal{B} \cap \mathcal{N}_i|, \ \forall i = 1, \cdots, t\}.$$

Note that $\mathcal{A}$ and $\mathcal{B}$ such that $|\mathcal{A} \cap \mathcal{N}_i| = |\mathcal{B} \cap \mathcal{N}_i|, \ \forall i = 1, \cdots, t$ are in the same orbit of the action Σ_p on $2^{\mathcal{N}}$ for Σ_p.

From partition-symmetrical entropy functions to group-symmetrical entropy functions

Fix set induced by a partition-group Σ_p

$$\mathrm{fix}_p = \{\mathbf{h} \in \mathcal{H}_n : \ \mathbf{h}(\mathcal{A}) = \mathbf{h}(\mathcal{B}) \\ \text{if } |\mathcal{A} \cap \mathcal{N}_i| = |\mathcal{B} \cap \mathcal{N}_i|, \ \forall i = 1, \cdots, t\}.$$

Note that $\mathcal{A}$ and $\mathcal{B}$ such that $|\mathcal{A} \cap \mathcal{N}_i| = |\mathcal{B} \cap \mathcal{N}_i|, \ \forall i = 1, \cdots, t$ are in the same orbit of the action Σ_p on $2^{\mathcal{N}}$ for Σ_p.

Fix set induced by an arbitary permutation group $\Sigma \leq S_n$

Let $\mathfrak{O}_\Sigma$ be the set of all orbits of the action Σ on $2^{\mathcal{N}}$.

$$\mathrm{fix}_\Sigma = \{\mathbf{h} \in \mathcal{H}_n : \ \mathbf{h}(\mathcal{A}) = \mathbf{h}(\mathcal{B}) \text{ if } \mathcal{A}, \mathcal{B} \in \mathcal{O}, \mathcal{O} \in \mathfrak{O}_\Sigma\}.$$

Thank you!