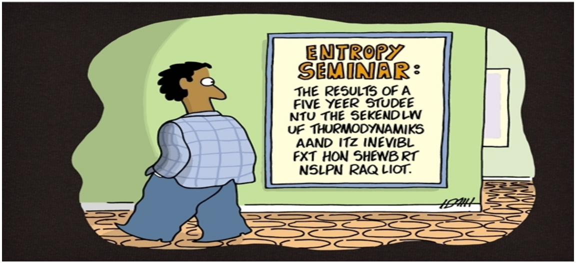
Codes, entropies and groups

Terence Chan[†]

[†] ITR, University of South Australia



Entropies (Physical meanings)

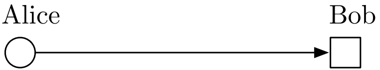
Given random variables X and Y,

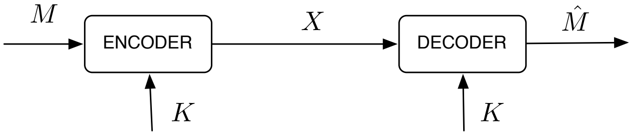
- Entropy measures the amount of uncertainty in a random variable:

$$H(X) \triangleq -\sum_{x} p(x) \log p(x)$$
$$H(X,Y) \triangleq -\sum_{x,y} p(x,y) \log p(x,y)$$

- $H(X) \geq 0$. Equality holds iff X is deterministic
- $H(X,Y) - H(Y) \geq 0$ (or simply $H(X|Y) \geq 0$). Equality holds iff X is a function of Y
- $H(X,Y) \leq H(X) + H(Y)$. Equality holds iff X and Y are independent

Secure communications (single link)





- Secrecy: $I(M; X) = 0$
- Encoding: $H(X|M, K) = 0$ (i.e., X is a function of M and K)
- Decoding: $H(M|K, X) = 0$ (i.e., M is a function of X and K)

Applying information inequalities, one can prove that

$$H(K) \geq H(M)$$

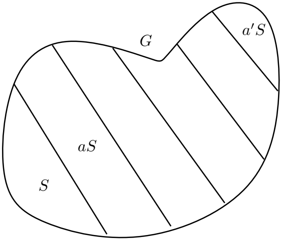
Groups and Inequalities

Brief introduction on groups

- A group $(G, \circ)$ consists of a set G and a binary group operator $\circ$ such that
  - $\circ$ is *associative* (i.e., $(a \circ b) \circ c = a \circ (b \circ c)$)
  - Existence of *identity* element $\mathbf{1}$ such that $\mathbf{1} \circ a = a \circ \mathbf{1} = a$
  - Existence of *inverse* a^{-1} such that $a^{-1} \circ a = a \circ a^{-1} = \mathbf{1}$
- *Example:* G is the set of nonzero real numbers and $\circ$ is multiplication

Constructing a random variable from a subgroup

- U – random variable, uniform over finite group G.
- S – subgroup of G
- S induces a random variable X – the random left (or right) coset of S in G containing U



- (By Lagrange's Theorem) $\Pr(x) = |S|/|G|$. Then $H(X) = \log |G|/|S|$.

Example

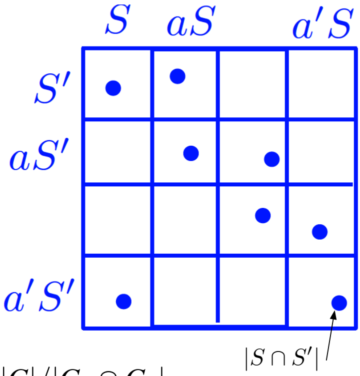
- Let $G = \{0, 1, 2, 3\}$ and $G_1 = \{0, 2\}$. The group operation is the $\mod 4$ addition.
- G_1 partitions G into two cosets $\{0, 2\}$ and $\{1, 3\}$.
- Each coset of size the same as G_1.
- Let U be a random variable which takes values "uniformly" over G.
- G_1 induces a random variable X_1 such that X_1 takes two "values"

$$X_1 = \begin{cases} \{0, 2\} & \text{if } U = 0 \text{ or } 2 \\ \{1, 3\} & \text{if } U = 1 \text{ or } 3. \end{cases}$$

- $H(X_1) = \log 4/2$

Another example - Two variables

- Example: Two group induced random variables



- $H(X_1, X_2) = \log |G|/|G_1 \cap G_2|$.
- Quasi-uniform (i.e., uniform over its supports)

Implication: Group-theoretic inequalities

Theorem (Chan, Yeung 2002)

Let $\sum_{\alpha \subseteq \mathcal{N}} c_\alpha H(X_\alpha) \geq 0$ be a valid information inequality. Then for any finite group G and its subgroups $\{G_i, i \in \mathcal{N}\}$,

$$\sum_{\alpha \subseteq \mathcal{N}} c_\alpha \log \frac{|G|}{|\cap_{i \in \alpha} G_i|} \geq 0,$$

or equivalently, $|G|^{\sum_{\alpha \subseteq \mathcal{N}} c_\alpha} \geq \prod_{\alpha \subseteq \mathcal{N}} |\cap_{i \in \alpha} G_i|^{c_\alpha}$.

Proof: Let X_i be constructed from subgroup G_i.

Converse also holds !!

Implication: Group-theoretic inequalities

Theorem (Chan, Yeung 2002)

Let $\sum_{\alpha \subseteq \mathcal{N}} c_\alpha H(X_\alpha) \geq 0$ be a valid information inequality. Then for any finite group G and its subgroups $\{G_i, i \in \mathcal{N}\}$,

$$\sum_{\alpha \subseteq \mathcal{N}} c_\alpha \log \frac{|G|}{|\cap_{i \in \alpha} G_i|} \geq 0,$$

or equivalently, $|G|^{\sum_{\alpha \subseteq \mathcal{N}} c_\alpha} \geq \prod_{\alpha \subseteq \mathcal{N}} |\cap_{i \in \alpha} G_i|^{c_\alpha}$.

Proof: Let X_i be constructed from subgroup G_i.

Converse also holds !!

Non-Shannon inequality

The non-Shannon inequality

$$\begin{aligned} & H(X_1) + H(X_2) + 2H(X_1, X_2) + 4H(X_3) + 4H(X_4) \\ & +5H(X_1, X_3, X_4) + 5H(X_2, X_3, X_4) \\ & \quad \leq \quad 6H(X_3, X_4) + 4H(X_1, X_3) + 4H(X_1, X_4) \\ & \qquad\quad +4H(X_2, X_3) + 4H(X_2, X_4), \end{aligned}$$

implies

$$\begin{aligned} & |G_{34}|^6 |G_{13}|^4 |G_{14}|^4 |G_{23}|^4 |G_{24}|^4 \\ & \qquad \leq |G_1||G_2||G_3|^4 |G_4|^4 |G_{12}|^2 |G_{134}|^5 |G_{234}|^5. \end{aligned}$$

Group theoretic proof

Prove: $I(X_1; X_2) \geq 0$

- Step 1: Transform into group theoretic inequality:

$$
\begin{aligned}
& I(X_1; X_2) \geq 0 \\
& \Leftrightarrow H(X_1) + H(X_2) - H(X_1, X_2) \geq 0 \\
& \Leftrightarrow \log |G|/|G_1| + \log |G|/|G_2| - \log |G|/|G_1 \cap G_2| \geq 0 \\
& \Leftrightarrow |G||G_1 \cap G_2| \geq |G_1|G_2|
\end{aligned}
$$

Group theoretic proof

Step 2: Proving the group inequality:

Let $G_1 \circ G_2 = \{a \circ b : a \in G_1, b \in G_2\}$.

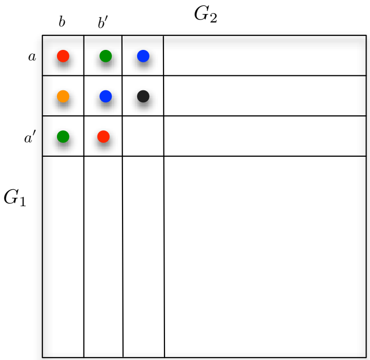
- $|G_1 \circ G_2| \leq |G|$
- $|G_1 \circ G_2| \leq |G_1||G_2|$
- $|G_1 \cap G_2| < |G_1||G_2|$ if there are duplications:

  $$a \circ b = (a \circ k) \circ (k^{-1} \circ b)$$

  where $k \in G_1 \cap G_2$
- Hence,

  $$|G_1 \circ G_2| = |G_1||G_2| / |G_1 \cap G_2|$$

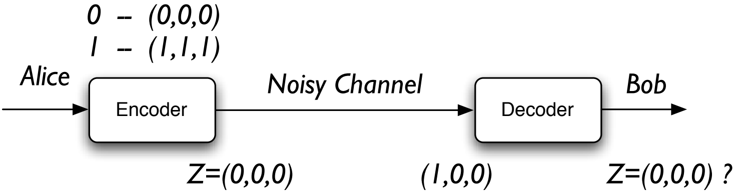
- As a result, $|G| \geq |G_1||G_2| / |G_1 \cap G_2|$



Codes and Random Variables

What are codes?

- (Error control) coding is a technique to protect transmitted data against errors



- Codebook size vs. Error correcting capability

$$\text{Error probability} = \Pr(\text{more than one symbol error})$$

- Code – a set of random variables $(Z_1, \ldots, Z_n)$
  - Z_i – the i^{th} codeword symbol.

From codes to random variables

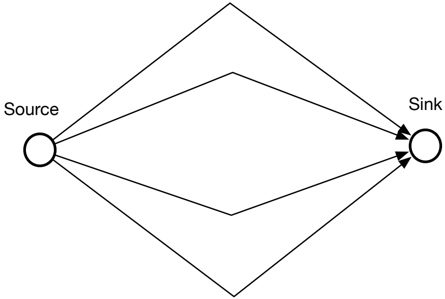
- Let $\mathcal{C} \subseteq \prod_{i=1}^{n} \mathcal{Z}_i$ be a code. It induces n random variables $(Z_1, \ldots, Z_n)$ such that

$$\Pr(z_1, \ldots, z_n) = \begin{cases} 1/|\mathcal{C}| & \text{if } (z_1, \ldots, z_n) \in \mathcal{C} \\ 0 & \text{otherwise.} \end{cases}$$

- $Z_1, \ldots, Z_n$ are called the *codeword symbol random variables* induced by the code C.
- Use language involved random variables
- Can consider a larger class of codes (where the underlying distribution is arbitrarily)

Tamper-proof transmission

- Transmitter and receiver connected via n parallel links
- Adversary – obstruct data transmission
  - Replacing the messages transmitted on the attacked links with any other messages.
  - Message transmitted on untampered link received without error.
- The same concept as in classical error correcting codes



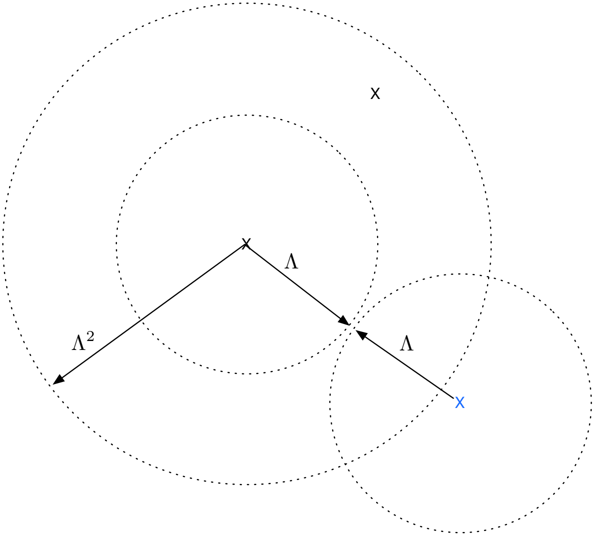
Tamper-proof transmission

Find the highest rate code that resilient to attacks:

- Adversary's *tampering pattern* Λ – the possible link subsets that an adversary can attack.
- If the adversary can attack up to any t links, then Λ contains all subsets of sizes up to t.
- Codebook size - $H(Z_1, \ldots, Z_n)$

Tamper-proof transmission

Code is resilient if $H(Z_1, \ldots, Z_n | Z_i, i \in \alpha^c) = 0$ for all $\alpha \subseteq \Lambda^2$ where $\Lambda^2 \triangleq \{\mathcal{B} \cup \mathcal{C} \,:\, \mathcal{B}, \mathcal{C} \in \Lambda\}$.



Distributed Storage

- Data encoded into n pieces $Z_1, \ldots, Z_n$,
- each stored in a data centre (DC)
- In case of data centre failures, the stored data can be restored from other DC
- Ξ – failure pattern,
- Design a storage code such that data can be restored if a set $\mathcal{A} \in \Xi$ of data centres fail.

Distributed Storage

Find the most efficient storage code (resilient to failures)

- Code size – $H(Z_1, \ldots, Z_n)$
- Robustness if

$$H(Z_1, \ldots, Z_n | Z_j, j \in \alpha^c) = 0$$

  for all $\alpha \in \Xi$
- Extension to subset recovery

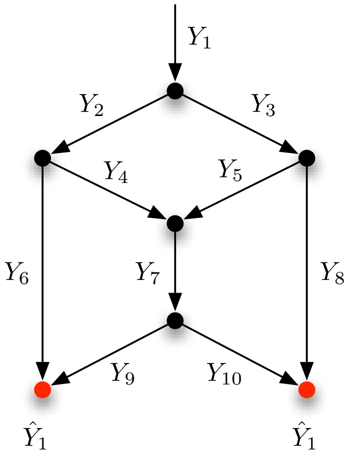
Network Coding

- Network code - specified by a set of random variables
- Source variables
- Link variables
- Topological constraint:

$$H(Y_7|Y_4, Y_5) = 0$$

- Decoding constraint:

$$H(Y_1|Y_6, Y_9) = 0$$



Secret Sharing

- Dealer share a secret with $n-1$ participants, indexed by the set $\{2,\dots,n\}$. (Dealer is player 1)
- only specified legitimate groups of participants can reconstruct the secret data
- Ω – *access structure*, only participants indexed by $\mathcal{A} \in \Omega$ can access the secret.
- A secret sharing scheme is a random vector $(Z_1,\dots,Z_n)$ such that
  1. Z_1 is the secret;
  2. Z_j is the share held by participant j;
  3. $H(Z_1|Z_j, j \in \mathcal{A}) = 0$ if $\mathcal{A} \in \Omega$;
  4. Z_1 and $(Z_j\ :\ j \in \mathcal{A})$ are independent whenever $\mathcal{A} \notin \Omega$.

Fundamental questions ...

These are codes

- specified by random variables
- satisfied functional dependency constraint

The basic questions are ...

- How to find an efficient code?
- Bounds on the rate of codes?
- Necessary condition for the existence of a code?
- In particular, assume a finite regime – alphabet sizes are fixed

Characterising Codes and Random Variables

- Codes are random variables
- Hence, information inequalities also govern codes
- Examples - Linear Programming Bound in Network Coding and Secret Sharing
- “Asymptotic” in nature – Singleton Bound is tight for sufficiently large alphabet

Finite Codes

- Let $\mathcal{Z}_1, \ldots, \mathcal{Z}_n$ be a set of non-empty sets, of sizes $N_1, \ldots, N_n$
- Assume WLOG $\mathcal{Z}_i = \{0, \ldots, N_i - 1\}$
- A code $\mathcal{C}$ is a non-empty subset of $\prod_{i=1}^{n} \mathcal{Z}_i$ (or simply $\mathcal{Z}^{\mathcal{N}}$).
- For any codewords, $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathcal{Z}^{\mathcal{N}}$, their
  - *difference* – $(\mathbf{a} - \mathbf{b}) \triangleq (a_1 - b_1, \ldots, a_n - b_n)$
  - *support* – $S(\mathbf{a}, \mathbf{b}) \triangleq \{j \in \{1, \ldots, n\} : a_j - b_j \neq 0\}$.
  - *distance* – $|S(\mathbf{a}, \mathbf{b})|$
- The minimum distance of a code $\mathcal{C}$ is defined as

$$\min_{\mathbf{a},\mathbf{b} \in \mathcal{C} : \mathbf{a} \neq \mathbf{b}} |S(\mathbf{a}, \mathbf{b})|.$$

Example

- Suppose $\mathcal{C} = \{(0,1,1),(0,2,1),(1,2,1)\}$ where $N_i = \{0,1,2\}$
- Consider the pair of codewords $(0,1,1)$ and $(0,2,1)$
  - Difference is $(0,2,0)$
  - Support is the subset $\{1\}$ and the distance is 1.
- Consider the pair of codewords $(0,1,1)$ and $(1,2,1)$
  - Difference is $(2,2,0)$
  - Support is the subset $\{1,2\}$ and the distance is 2.
- Denote the support be a *binary vector* of length n
- E.g., $(0,1,0)$ and $(1,1,0)$ (i.e., a subset is a binary vector)

Enumerators

Given a code $\mathcal{C}$,

- *Difference enumerator (FE)*

$$Diff(\mathbf{a}) = |\{(\mathbf{b},\mathbf{c}) :\ \mathbf{b},\mathbf{c} \in \mathcal{C} \text{ and } \mathbf{b}-\mathbf{c} = \mathbf{a}\}|.$$

- *Support enumerator (SE)*

$$\begin{aligned} Supp(\mathbf{r}) &= |\{(\mathbf{b},\mathbf{c}) :\ \mathbf{b},\mathbf{c} \in \mathcal{C} \text{ and } S(\mathbf{b},\mathbf{c}) = \mathbf{r}\}| \\ &= \sum_{\mathbf{a}:a_i \neq 0 \text{ iff } i \in \mathbf{r}} Diff(\mathbf{a}). \end{aligned}$$

- *Distance enumerator (DE)*

$$\begin{aligned} Dist(i) &= |\{(\mathbf{b},\mathbf{c}) :\ \mathbf{b},\mathbf{c} \in \mathcal{C} \text{ and } |S(\mathbf{b},\mathbf{c})| = i\}| \\ &= \sum_{\mathbf{r}:|\mathbf{r}|=i} Supp(\mathbf{r}). \end{aligned}$$

- Sometimes, normalised with the factor $1/|\mathcal{C}|^2$

Necessary condition

Think of $Supp(\mathbf{r})$ as a vector of size 2^n:

Theorem (Necessary condition)

Support enumerator will satisfy the following conditions:

$$Supp(\mathbf{r}) \geq 0$$

$$\sum_{\mathbf{r}} Supp(\mathbf{r}) \prod_{j=1}^{n} \kappa_{N_j}(r_j, s_j) \geq 0$$

where $\mathbf{r} = (r_1, \ldots, r_n), \mathbf{s} = (s_1, \ldots, s_n) \subseteq \mathcal{N}$, *and*

$$\kappa_{N_j}(r_j, s_j) = \begin{cases} 1 & \textit{if } r_j = 0 \\ N_j - 1 & \textit{if } s_j = 0 \textit{ and } r_j = 1 \\ -1 & \textit{otherwise,} \end{cases}$$

Proof

- For each code $\mathcal{C}$, it is associated with an "indicator function" J defined as follows

$$J(z_1, \ldots, z_n) = \begin{cases} 1 & \text{if } (z_1, \ldots, z_n) \in \mathcal{C} \\ 0 & \text{otherwise.} \end{cases}$$

- The indication function is a "scaled" probability distribution
- Then $Supp(\mathbf{a}) = \sum_{\mathbf{b}} J(\mathbf{b})J(\mathbf{b}+\mathbf{a})$.

Theorem (Nonnegativity)

- $Diff(\mathbf{a}) = \sum_{\mathbf{b}} J(\mathbf{b})J(\mathbf{b}+\mathbf{a}) \geq 0.$
- $\widehat{Diff}(k_1, \ldots, k_n) \triangleq \sum_{a_1,\ldots,a_n} Diff(a_1, \ldots, a_n) \prod_{j=1}^{n} e^{-2\pi a_j k_j / N_j} \geq 0$

Proof

- Let
$$\delta_{N_j}(a_j, r_j) = \begin{cases} 1 & \text{if } a_j = r_j = 0 \\ 1 & \text{if } a_j, r_j \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

- $$Supp(\mathbf{r}) = \sum_{a_1,\ldots,a_n} \mathit{Diff}(a_1, \ldots, a_n) \prod_{j=1}^{n} \delta_{N_j}(a_j, r_j)$$

- Let
$$\kappa_{N_j}(r_j, s_j) = \begin{cases} 1 & \text{if } r_j = 0 \\ N_j - 1 & \text{if } s_j = 0 \text{ and } r_j = 1 \\ -1 & \text{otherwise,} \end{cases}$$

  Then
$$\sum_{k_1,\ldots,k_n} \prod_{j=1}^{n} e^{-2\pi a_j k_j / N_j} \delta_{N_j}(k_j, s_j) = \sum_{r_1,\ldots,r_n} \prod_{j=1}^{n} \delta_{N_j}(a_j, r_j) \kappa_{N_j}(r_j, s_j)$$

Proof

- $\sum_{a_1,\ldots,a_n} \mathit{Diff}(a_1,\ldots,a_n) \prod_{j=1}^{n} e^{-2\pi a_j k_j / N_j} \geq 0$
- Notice that

$$\sum_{k_1,\ldots,k_n} \left(\sum_{a_1,\ldots,a_n} \mathit{Diff}(a_1,\ldots,a_n) \prod_{j=1}^{n} e^{-2\pi a_j k_j / N_j} \right) \delta_{N_j}(k_j, s_j) \geq 0$$

$$\sum_{a_1,\ldots,a_n} \mathit{Diff}(a_1,\ldots,a_n) \left(\sum_{k_1,\ldots,k_n} \prod_{j=1}^{n} e^{-2\pi a_j k_j / N_j} \delta_{N_j}(k_j, s_j) \right) \geq 0$$

$$\sum_{a_1,\ldots,a_n} \mathit{Diff}(a_1,\ldots,a_n) \left(\sum_{r_1,\ldots,r_n} \prod_{j=1}^{n} \delta_{N_j}(a_j, r_j) \kappa_{N_j}(r_j, s_j) \right) \geq 0$$

$$\sum_{r_1,\ldots,r_n} \left(\sum_{a_1,\ldots,a_n} \mathit{Diff}(a_1,\ldots,a_n) \prod_{j=1}^{n} \delta_{N_j}(a_j, r_j) \right) \kappa_{N_j}(r_j, s_j) \geq 0$$

$$\sum_{r_1,\ldots,r_n} \mathit{Supp}(\mathbf{r}) \prod_{j=1}^{n} \kappa_{N_j}(r_j, s_j) \geq 0$$

Delsarte's LP bound

Theorem (Delsarte's LP bound)

Let $\mathcal{C}$ be a code such that the minimum Hamming distance of $\mathcal{C}$ is at least d. Then $|\mathcal{C}|^2$ is upper bounded by the maximum of the following optimisation problem:

$$
\begin{array}{lll}
\textbf{maximize} & \sum_{\mathbf{r}} Supp(\mathbf{r}) & \\
\textbf{subject to} & Supp(\mathbf{r}) \geq 0 & \forall \mathbf{r} \\
 & \displaystyle\sum_{\mathbf{s}} Supp(\mathbf{s}) \prod_{j=1}^{n} \kappa_{N_j}(s_j, r_j) \geq 0 & \forall \mathbf{r} \\
 & |Supp(\mathbf{r})| = 0 & \forall \mathbf{r} : \ 1 \leq |\mathbf{r}| \leq d-1 \,.
\end{array}
$$

Renyi entropy and codes

Renyi entropy

Definition

Let Z be a random variable with probability distribution $f(z)$. Then its Renyi entropy of order α for $\alpha \geq 0$ and $\alpha \neq 1$ is defined as

$$H_\alpha(Z) \triangleq \frac{1}{1-\alpha} \log \left(\sum_{z:f(z)>0} f(z)^\alpha \right).$$

When $\alpha = 1$, $H_1(Z) \triangleq \lim_{\alpha \to 1} H_\alpha(Z)$.

Examples

$$H_2(Z) = -\log \left(\sum_z f(z)^2 \right)$$

$$H_1(Z) = -\sum_z f(z) \log f(z)$$

$$H_0(Z) = \log \left| \{z : f(z) > 0\} \right|.$$

Renyi Entropy - Interpretation

- Let X and Y be two independent random variables, identically distributed as Z.
- Then $H_2(Z) = -\log \Pr(X = Y)$.
- Let $\mathbf{X} = (X_1, \ldots, X_n)$ and $\mathbf{Y} = (Y_1, \ldots, Y_n)$ be two independent sets of random variables with the same probability distribution f. Then for any $\mathbf{s} \subseteq \mathcal{N}$,

$$\psi_f(\mathbf{s}) \triangleq \Pr(S(\mathbf{X}, \mathbf{Y}) \subseteq \mathbf{s}) = 2^{-H_2(X_{\bar{\mathbf{s}}})}.$$

Extension

- Let f be a probability mass function for random variables $(Z_1, \ldots, Z_n)$.
- Let

$$F(\mathbf{a}) = \sum_{\mathbf{b}} f(\mathbf{b}) f(\mathbf{b} + \mathbf{a})$$

$$\phi(\mathbf{r}) = \sum_{\mathbf{a}} F(\mathbf{a}) \prod_{j=1}^{n} \delta_{N_j}(a_j, r_j)$$

(Compare: $Supp(\mathbf{r}) = \sum_{\mathbf{a}} F(\mathbf{a}) \prod_{j=1}^{n} \delta_{N_j}(a_j, r_j)$ when $f = J$)

- Let $\mathbf{X} = (X_1, \ldots, X_n)$ and $\mathbf{Y} = (Y_1, \ldots, Y_n)$ be two independent sets of random variables with the same probability distribution f.
- Then for any $\mathbf{r} \subseteq \mathcal{N}$,

$$\phi(\mathbf{r}) = \Pr(S(\mathbf{X}, \mathbf{Y}) = \mathbf{r}).$$

Extension

Theorem (Support Enumerator)

$$\phi_f(\mathbf{r}) \geq 0$$

$$\sum_{\mathbf{r}} \phi_f(\mathbf{r}) \prod_{j=1}^{n} \kappa_{N_j}(r_j, s_j) \geq 0$$

for all $\mathbf{r} = (r_1, \ldots, r_n), \mathbf{s} = (s_1, \ldots, s_n) \subseteq \mathcal{N}$.

For f induced by a code $\mathcal{C}$, then

$$\phi_f(\mathbf{r}) = \frac{1}{|\mathcal{C}|^2} Supp(\mathbf{r}).$$

Mobius Transform

Recall

$$\psi_f(\mathbf{s}) = \Pr(S(\mathbf{X}, \mathbf{Y}) \subseteq \mathbf{s}) = 2^{-H_2(X_{\bar{\mathbf{s}}})}$$
$$\phi_f(\mathbf{s}) = \Pr(S(\mathbf{X}, \mathbf{Y}) = \mathbf{s})$$

Theorem (Relation to Renyi entropy)

$$\sum_{\mathbf{r}:\mathbf{r}\subseteq\mathbf{s}} \phi_f(\mathbf{r}) = \psi_f(\mathbf{s}),$$
$$\sum_{\mathbf{s}:\mathbf{s}\subseteq\mathbf{v}} (-1)^{|\mathbf{v}\setminus\mathbf{s}|}\psi_f(\mathbf{s}) = \phi_f(\mathbf{v})$$

for all $\mathbf{r}, \mathbf{s}, \mathbf{v} \subseteq \mathcal{N}$

Renyi information inequalities

Theorem

Let f be a probability distribution of a set of discrete random variables $(Z_1, \ldots, Z_n)$. Then for all $\mathbf{r} \subseteq \mathcal{N}$,

$$\phi_f(\mathbf{r}) = \sum_{\mathbf{s}:\mathbf{s}\subseteq\mathbf{r}} (-1)^{|\mathbf{r}\setminus\mathbf{s}|} 2^{-H_2(Z_{\bar{\mathbf{s}}})} \geq 0,$$

$$\sum_{\mathbf{r}} \phi_f(\mathbf{r}) \prod_{j=1}^{n} \kappa_{N_j}(r_j, s_j) = \sum_{\mathbf{u}:\mathbf{u}\subseteq\mathbf{r}} (-1)^{|\mathbf{u}|} 2^{-H_2(Z_{\bar{\mathbf{u}}\cap\mathbf{r}})} \prod_{j:j\in\mathbf{r}\setminus\mathbf{u}} 2^{H_0(Z_j)} \geq 0.$$

Corollary

Theorem

Let $\{Z_1, \ldots, Z_n\}$ *be a set of marginally uniform random variables. Then for all* $\mathbf{r} \subseteq \mathcal{N}$*,*

$$\sum_{\mathbf{s}:\mathbf{s}\subseteq\mathbf{r}} (-1)^{|\mathbf{r}\setminus\mathbf{s}|} 2^{-H_2(Z_{\bar{\mathbf{s}}})} \geq 0,$$

$$\sum_{\mathbf{u}:\mathbf{u}\subseteq\mathbf{r}} (-1)^{|\mathbf{u}|} 2^{-H_2(Z_{\mathbf{r}\setminus\mathbf{u}})+\sum_{j:j\in\mathbf{r}\setminus\mathbf{u}} H_2(Z_j)} \geq 0.$$

Dualities

Theorem (Dualities)

- *Let f be a probability distribution of a set of marginally uniform discrete random variables $(Z_1, \ldots, Z_n)$.*
- *Let $\rho(\mathbf{r}) \triangleq H_2(Z_j, j \in \mathbf{r})$ be the collision (or extension) entropy function*
- *Let $\mu(\mathbf{r}) \triangleq \sum_{i \in \mathbf{r}} \rho(i) + \rho(\bar{\mathbf{r}}) - \rho(\mathcal{N})$ be its induced dual.*
- *Then for all $\mathbf{r} \subseteq \mathcal{N}$,*

$$\sum_{\mathbf{s}:\mathbf{s} \subseteq \mathbf{r}} (-1)^{|\mathbf{r} \setminus \mathbf{s}|} 2^{\rho(\mathcal{N}) - \rho(\bar{\mathbf{s}})} \geq 0$$

$$\sum_{\mathbf{s}:\mathbf{s} \subseteq \mathbf{r}} (-1)^{|\mathbf{r} \setminus \mathbf{s}|} 2^{\mu(\mathcal{N}) - \mu(\bar{\mathbf{s}})} \geq 0$$

Group induced random variables

Theorem

Let G be a finite group and $G_1, \ldots, G_n$ be its subgroups. There exists random variables $U_1, \ldots, U_n$ such that

$$H_0(U_i, i \in \alpha) = H_2(U_i, i \in \alpha) = \log|G| - \log|\cap_{i\in\alpha} G_i|.$$

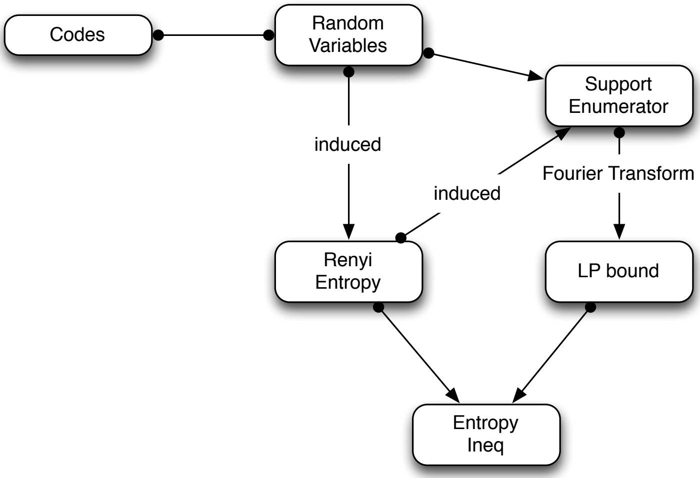
Corollary

$$\sum_{\mathbf{s}:\mathbf{s}\supseteq\bar{\mathbf{r}}} (-1)^{|\mathbf{s}-\mathbf{r}|} |\cap_{i\in\mathbf{s}} G_i| \geq 0$$

$$\sum_{\mathbf{s}:\mathbf{s}\subseteq\mathbf{r}} \left(\frac{-1}{|G|}\right)^{|\mathbf{s}|} \frac{|\cap_{i\in\mathbf{r}\setminus\mathbf{s}} G_i|}{\prod_{j:j\in\mathbf{r}\setminus\mathbf{s}} |G_j|} \geq 0$$

for all $\mathbf{r} \subseteq \mathcal{N}$.

Conclusion



Codes
Random Variables
Support Enumerator
induced
Fourier Transform
induced
Renyi Entropy
LP bound
Entropy Ineq

What about applications?

Coding constraint

Suppose $\mathcal{C} \subseteq \mathcal{Z}^{\mathcal{N}}$ is a code. Let

$$Shorten(\mathbf{s}) = \sum_{\mathbf{r}:\mathbf{r}\subseteq\mathbf{s}} Supp(\mathbf{r})$$

- $Shorten(\mathbf{s})$ – *number of codeword pairs such that the two codewords agree at "positions" not in $\mathbf{s}$*.
- Compare $\psi_f(\mathbf{s}) = \sum_{\mathbf{r}:\mathbf{r}\subseteq\mathbf{s}} \phi_f(\mathbf{r})$

$$\phi_f(\mathbf{s}) \Leftrightarrow \frac{1}{|\mathcal{C}|^2} Supp(\mathbf{s})$$

$$2^{-H_2(\mathbf{Z}_{\bar{\mathbf{s}}})} = \psi_f(\mathbf{s}) \Leftrightarrow \frac{1}{|\mathcal{C}|^2} Shorten(\mathbf{s})$$

- If $\mathbf{Z}_{\mathcal{B}}$ is a function of $\mathbf{Z}_{\mathcal{A}}$, then

$$Shorten(\mathcal{N} - (\mathcal{A} \cup \mathcal{B})) = Shorten(\mathcal{N} - \mathcal{A})$$

- If $\mathbf{Z}_{\mathcal{A}}$ and $\mathbf{Z}_{\mathcal{B}}$ are independent, then

$$Shorten(\mathcal{N} - (\mathcal{A} \cup \mathcal{B})) Shorten(\mathcal{N}) = Shorten(\mathcal{N} - \mathcal{A}) Shorten(\mathcal{N} - \mathcal{B})$$

Delsarte's LP bound

Theorem (Delsarte's LP bound)

Let $\mathcal{C}$ be a code such that the minimum Hamming distance of $\mathcal{C}$ is at least d. Then $|\mathcal{C}|^2$ is upper bounded by the maximum of the following optimisation problem:

$$
\begin{array}{lll}
\textbf{\textit{maximize}} & \sum_{\mathbf{r}} Supp(\mathbf{r}) & \\
\textbf{\textit{subject to}} & Supp(\mathbf{r}) \geq 0 & \forall \mathbf{r} \\
 & \displaystyle\sum_{\mathbf{s}} Supp(\mathbf{s}) \prod_{j=1}^{n} \kappa_{N_j}(s_j, r_j) \geq 0 & \forall \mathbf{r} \\
 & |Supp(\mathbf{r})| = 0 & \forall \mathbf{r} :\ 1 \leq |\mathbf{r}| \leq d-1 \,.
\end{array}
$$

Bounds - Tamper proof communications

$|\mathcal{C}|^2$ is upper-bounded by the optimum of the following linear programming problem:

$$
\begin{array}{lll}
\textbf{maximize} & \sum_{\mathbf{r}} Supp(\mathbf{r}) & \\
\textbf{subject to} & Supp(\mathbf{r}) \geq 0 & \forall \mathbf{r} \\
& \displaystyle\sum_{\mathbf{s}} Supp(\mathbf{s}) \prod_{j=1}^{n} \kappa_{N_j}(s_j, r_j) \geq 0 & \forall \mathbf{r} \\
& \displaystyle Shorten(\mathbf{r}) = \sum_{\mathbf{s} \subseteq \mathbf{r}} Supp(\mathbf{s}) & \forall \mathbf{r} \\
& Shorten(\mathcal{A}) = 1 & \forall \mathcal{A} \in \Lambda^2 .
\end{array}
$$

Bounds - Secret Sharing

The optimum efficiency is upper-bounded by the optimum of the following optimisation:

maximize $\min_{j \in \mathcal{N} - \{1\}} \frac{\log Shorten(\mathcal{N}) - \log Shorten(\mathcal{N} - \{1\})}{\log Shorten(\mathcal{N}) - \log Shorten(\mathcal{N} - \{j\})}$

subject to

$$Supp(\mathbf{r}) \geq 0$$

$$\sum_{\mathbf{s}} Supp(\mathbf{s}) \prod_{j=1}^{n} \kappa_{N_j}(s_j, r_j) \geq 0$$

$$Shorten(\mathbf{r}) = \sum_{\mathbf{s} \subseteq \mathbf{r}} Supp(\mathbf{s})$$

$$Shorten(\mathcal{N} - (\mathcal{A} \cup \{1\})) = Shorten(\mathcal{N} - \mathcal{A}), \quad \forall \mathcal{A} \in \Omega$$

$$Shorten(\mathcal{N} - (\mathcal{A} \cup \{1\}))Shorten(\mathcal{N}) = Shorten(\mathcal{N} - \mathcal{A})Shorten(\mathcal{N} - \{1\}), \quad \forall \mathcal{A} \notin \Omega$$

Thank You !!