

Entropic Relations for Communication Protocols

Sankeerth Rao

January 7, 2015

Guides : Vinod Prabhakaran(TIFR,IITB), Sibi Raj Pillai(IITB)
Part of Master's Project done at IIT Bombay



An Example to begin with

We start with an example from Deepesh [1]

Lemma

Alice, Bob and Charlie start with independent randomness and start talking to each other over the telephone lines.

$$I(M_1; M_2) \geq I(M_1; M_2 | M_3)$$

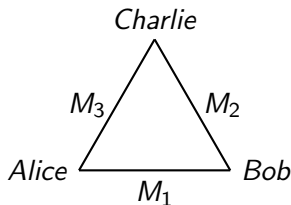


Figure: 3-cycle - the edges represent the communication links

Proof Idea

- Not generally true for arbitrary random variables - If M_1 and M_2 were two independent coin tosses and M_3 is the indicator of the event $\{M_1 = M_2\}$, then the inequality does not hold, but such random variables cannot arise from communication protocols.



The inequality can be rewritten as

$$\begin{aligned}
 &H(M_1) + H(M_2) + H(M_3) - H(M_1, M_2) \\
 &\quad - H(M_2, M_3) - H(M_3, M_1) + H(M_1, M_2, M_3) \geq 0
 \end{aligned}$$

Induction

We induct on the number of rounds(t) of the protocol,

- **Initialization:** $t = 1$ Trivially true
- **Induction Hypothesis:** After t rounds

$$\begin{aligned} H(M_1) &+ H(M_2) + H(M_3) - H(M_1, M_2) \\ &- H(M_2, M_3) - H(M_3, M_1) + H(M_1, M_2, M_3) \geq 0 \end{aligned}$$

- **Increment:** $\Delta M - (M_1, M_3) - M_2$
- **Induction Step:**

$$\begin{aligned} H(M_1 \Delta M) &+ H(M_2) + H(M_3) - H(M_1 M_2 \Delta M) \\ &- H(M_2 M_3) - H(M_3 M_1 \Delta M) + H(M_1 M_2 M_3 \Delta M) \geq 0 \end{aligned}$$

Induction Step

- It is sufficient to prove that

$$H(\Delta M|M_1) - H(\Delta M|M_1, M_2) - H(\Delta M|M_1, M_3) + H(\Delta M|M_1, M_2, M_3) \geq 0$$

- Which is equivalent to showing that

$$I(\Delta M; M_2|M_1) - \overbrace{I(\Delta M; M_2|M_1, M_3)}^{=0} \geq 0$$

Question

Given a graph as input, characterise all such inequalities which hold for communication protocols over a network of n people which can be proved using Shannon type inequalities.

Entropic Equalities

Question

Characterise the subspace in which all these communication protocol entropic vectors lie ?

- Let M_e denote all the messages sent over the edge "e" during the protocol.
- let M_T denote the collection of random variables $\{M_e : e \in T\}$.
- We are trying to characterise equalities of the form

$$\sum_{T \subset \mathcal{E}} \alpha_T H(M_T) = 0 \quad (1)$$

Question

Characterise $\{\alpha_T : T \subset \mathcal{E}\}$ such that the equality (1) holds for all communication protocols.

Cutset Conditions

Lemma

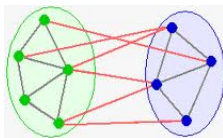
Let $\{A, B, C\}$ be a partition of \mathcal{E} such that when the edges of C are removed the collections of edges A and B don't share a vertex. Then

$$I(M_A; M_B | M_C) = 0 \quad (2)$$

- The proof follows from a similar induction step.

Lemma

Let $\{A, B, C\}$ be a partition of \mathcal{E} such that $I(M_A; M_B | M_C) = 0$ then on removal of the edges of C , A and B don't share a vertex.



5-cycle

5-cycle	13	14	24	25	35	123	124	125	134	135	145	234	235	245	345	1234	1235	1245	1345	2345	12345
13	-1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	-1
14	0	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	-1
24	0	0	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	-1
25	0	0	0	-1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	-1
35	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	-1
124	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	-1
134	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	1	0	0	1	0	-1
135	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	1	0	1	0	-1
235	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	1	0	0	0	1	-1
245	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	1	0	1	0	-1

$$\begin{aligned}
 I(M_A; M_B | M_C) &= H(M_A, M_C) + H(M_B, M_C) - H(M_C) - H(M_A, M_B, M_C) \\
 &= H(M_{AUC}) + H(M_{BUC}) - H(M_C) - H(M_{\mathcal{E}})
 \end{aligned}$$

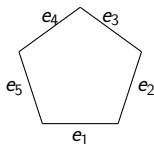


Figure: 5-cycle - the edges represent the communication links

Signalling

Lemma

The cut matrix M_1 just defined is of full row rank

- The entropic vector obtained from any protocol will be orthogonal to all the rows of the matrix M_1 .
- We are done if we find a collection of protocols whose entropic vectors span the orthogonal complementary space of the row space of M_1 .

Lemma

The number of connected subgraphs of a graph + the number of subsets (cut-subsets) of edges which when removed disconnect the graph = $2^m - 1$, where m is the number of edges in the graph

Signalling Strategies

- Let us look at the following signalling strategies
- A node tosses a fair coin and circulates the outcome among the edges of a connected subgraph



Lemma

These entropic vectors are linearly independent and account for the dimension of the orthogonal complementary space of the cut space.

4-cycle

4-cycle	1	2	3	4	12	13	14	23	24	34	123	124	134	234	1234
1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1
2	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1
3	0	0	1	0	0	1	0	1	0	1	1	0	1	1	1
4	0	0	0	1	0	0	1	0	1	1	0	1	1	1	1
12	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1
14	1	0	0	1	1	1	1	0	1	1	1	1	1	1	1
23	0	1	1	0	1	1	0	1	1	1	1	1	1	1	1
34	0	0	1	1	0	1	0	1	1	1	1	1	1	1	1
123	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
124	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
134	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
234	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1234	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

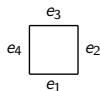
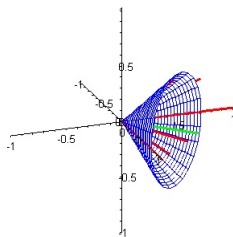


Figure: 4-cycle

Work yet to be done!



Question

Thus we have characterized the minimal subspace in which all the communication protocol entropic vectors lie in. The natural question to ask would be to characterize the minimal cone containing all the entropic vectors ?

Bibliography



D. Data, V.M. Prabhakaran, and M.M. Prabhakaran, "On the communication complexity of secure computation", <http://arxiv.org/abs/1311.7584v2/>, 2014