Graph entropy

Maximilien Gadouleau
Durham University

Work done by Søren Riis

Nice, November 10 2015

Oultline

Fixed points of FDSs

Network coding

Entropy of random variables

Graph entropy

Shannon entropy of graphs

Outline

Finite Dynamical Systems

A Finite Dynamical System (FDS) is a function $f:[q]^n \to [q]^n$, where $[q] = \{0, 1, \ldots, q-1\}$.

We denote $f = (f_1, \ldots, f_n)$ where $f_v : [q]^n \to [q]$.

We refer to $x = (x_1, \ldots, x_n) \in [q]^n$ as a state where $x_v \in [q]$.

A fixed point of f is a state x s.t.

$$f(x) = x.$$

The guessing number of f:

$$g(f) = \log_q |\mathrm{Fix}(f)|.$$

Interaction graph

The function f can be represented by its interaction graph $\mathrm{IG}(f)$, with n vertices and where (u,v) is an arc iff f_v depends on x_u.

For any digraph D, the guessing number of D:

$$g(D,q) := \max\{g(f) : f \in F(D,q)\},$$
$$F(D,q) = \{f : [q]^n \to [q]^n : \mathrm{IG}(f) \subseteq D\},$$
$$g(f) = \log_q |\mathrm{Fix}(f)|.$$

The guessing number was introduced by Riis (Riis 06, Riis 07) in his study of Network Coding.

The feedback bound

Let $\tau(D)$ denote the size of a minimum feedback vertex set (complement of a maximum induced acyclic subgraph).

Theorem. For all D and q,

$$g(D,q) \leq \tau(D).$$

Proof. Let I a MFVS and $J = V \setminus I$ in topological order. Let $x, y \in \mathrm{Fix}(f)$ with $x_I = y_I$. Then

$$\begin{aligned} x_{j_1} &= y_{j_1} = f_{j_1}(x_I) \\ x_{j_2} &= y_{j_2} = f_{j_2}(x_I, x_{j_1}), \\ &\vdots \\ x_{j_k} &= y_{j_k} = f_{j_k}(x_I, x_{J-j_k}), \end{aligned}$$

and hence $x = y$.

Outline

The butterfly network

The same message (bit) is sent on all outgoing links

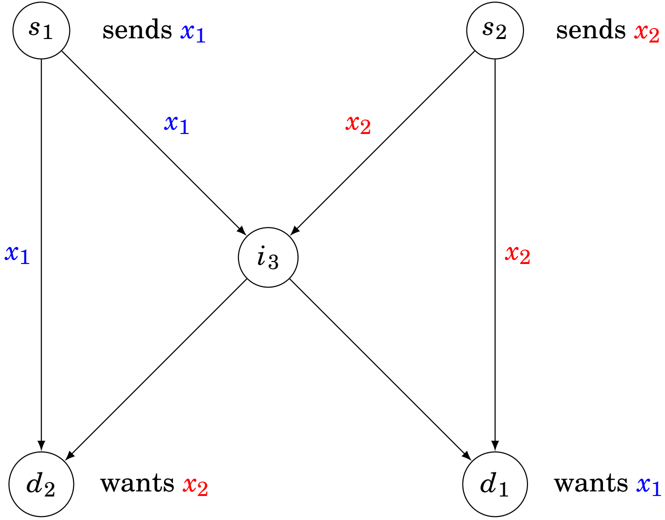


Figure : Butterfly network

The butterfly network

The same message (bit) is sent on all outgoing links

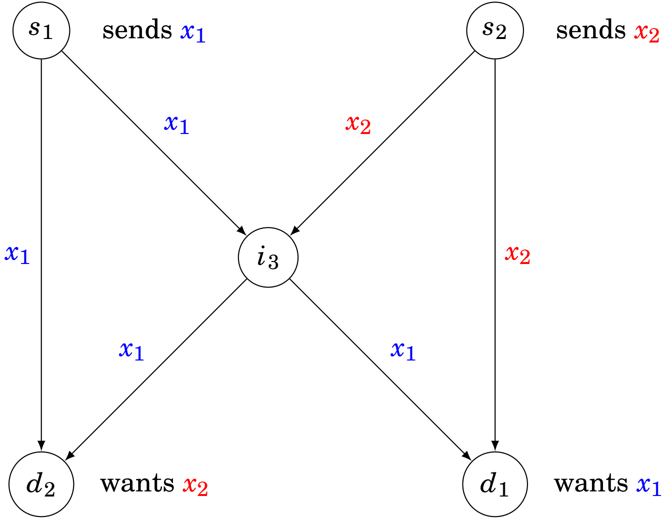


Figure : Butterfly network: Routing

The butterfly network

The same message (bit) is sent on all outgoing links

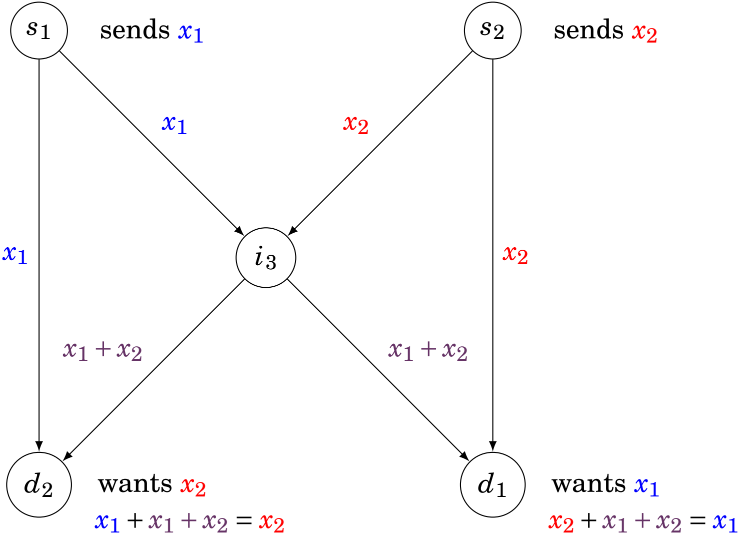


Figure : Butterfly network: Network coding

Network coding and guessing number

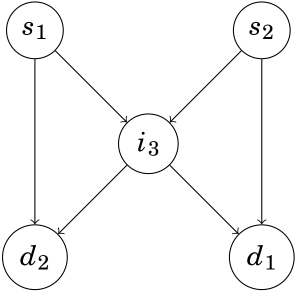
Network coding solvability: can all messages be transmitted at the same time?

Riis converts this problem in terms of guessing number.

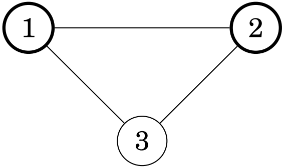
The question becomes: for a digraph D associated to the original Network coding instance,

$$g(D, q) = \tau(D)?$$

Butterfly network and guessing number



(a) Butterfly network



(b) Guessing number of K_3

In general, $g(K_n, q) = n - 1$ and hence

$$g(D, q) \geq n - \pi(D),$$

the clique cover number of D.

Outline

Entropy of random variables

Let X be a discrete random variable with support $\mathscr{X}$ and distribution $p_X(x)$ for all $x \in \mathscr{X}$.

The q-ary entropy of X:

$$H_q(X) = -\sum_{x \in \mathscr{X}} p_X(x) \log_q p_X(x),$$

The entropy is the information (uncertainty) content of X. We have

$$0 \leq H_q(X) \leq \log_q |\mathscr{X}|,$$

where $H(X) = 0$ iff X is deterministic and $H(X) = \log_q |\mathscr{X}|$ iff X is uniform.

Definitions

The joint entropy of a pair of variables (X, Y):

$$H(X,Y) := -\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} p_{X,Y}(x,y)\log p_{X,Y}(x,y).$$

We have

$$H(X,Y) = H(Y,X) \geq \max\{H(X), H(Y)\}.$$

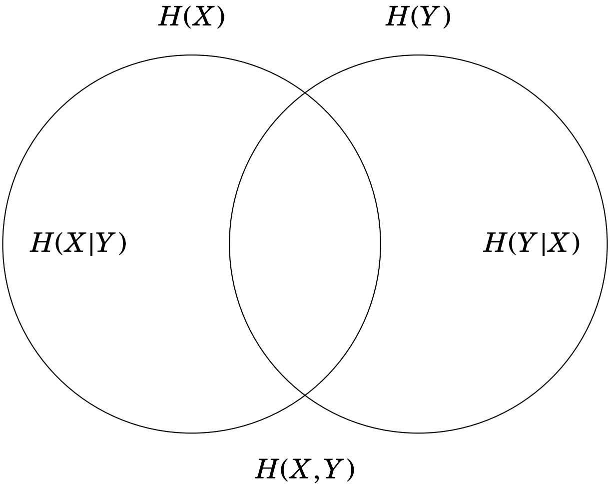
The conditional entropy of Y given X:

$$H(Y|X) := \sum_{x\in\mathcal{X}} p_X(x) H(Y|X=x).$$

We have

$$H(X,Y) = H(X) + H(Y|X) \leq H(X) + H(Y).$$

Venn diagram of entropy



Sub-additivity of entropy

Let $X_1, \ldots, X_n$ a collection of n variables. Build 2^n variables, one for each $S = \{s_1, \ldots, s_k\} \subseteq V$:

$$X_S = (X_{s_1}, \ldots, X_{s_k}).$$

($X_\emptyset$ has entropy 0.)

Denote $H(S) := H(X_S)$ for all $S \subseteq V$.

Theorem. The entropy is sub-additive, i.e. for all $S, T \subseteq V$

$$H(S \cup T) \leq H(S) + H(T).$$

Proof. $H(S \cup T) = H(X_S, X_T) \leq H(X_S) + H(X_T) = H(S) + H(T).$

Outline

Fixed points of FDSs

Network coding

Entropy of random variables

Graph entropy

Shannon entropy of graphs

Definition

The idea is to study a uniformly chosen fixed point of f:

$$X^f \sim p_{X^f}(x) = \frac{1}{|\mathrm{Fix}(f)|} \quad \forall x \in \mathrm{Fix}(f).$$

Then $H(X^f) = g(f)$.

Let $x \in \mathrm{Fix}(f)$. If we know $x_{N_{\mathrm{in}}(v)}$, then we know $x_v = f_v(x_{N_{\mathrm{in}}(v)})$.

Hence $H(X^f_v | X^f_{N_{\mathrm{in}}(v)}) = 0$ and

$$H(X^f_{N_{\mathrm{in}}(v)\cup v}) = H(X^f_{N_{\mathrm{in}}(v)}) + H(X^f_v | X^f_{N_{\mathrm{in}}(v)}) = H(X^f_{N_{\mathrm{in}}(v)}).$$

The q-ary entropy of D is

$$H(D,q) := \sup H_q(V),$$

sup taken over all families of variables $\{X_v : v \in V\}$, each over $[q]$, s.t.

$$H(N_{\mathrm{in}}(v) \cup v) = H(N_{\mathrm{in}}(v)) \quad \forall v \in V.$$

Using entropy: First attempt

The naive entropy of D is $\epsilon(D) := \sup h(V)$, supremum taken over all $h : 2^V \to \mathbb{R}$ s.t.

$$
\begin{aligned}
h(v) &\leq 1 && \forall v \in V, \\
h(S) &\leq h(T) && \forall S \subseteq T \subseteq V, \\
h(S \cup T) &\leq h(S) + h(T) && \forall S, T \subseteq V, \\
h(N_{\text{in}}(v) \cup v) &= h(N_{\text{in}}(v)) && \forall v \in V.
\end{aligned}
$$

Theorem (Riis 06, G 14).

$$g(D,q) = H(D,q) \leq \epsilon(D) = \tau(D).$$

Outline

Mutual information

Mutual information between X and Y:

$$I(X;Y) := H(X) + H(Y) - H(X,Y).$$

It is the amount of information that X and Y have in common.

Shannon inequality:

$$I(X;Y) \geq 0.$$

Venn diagram

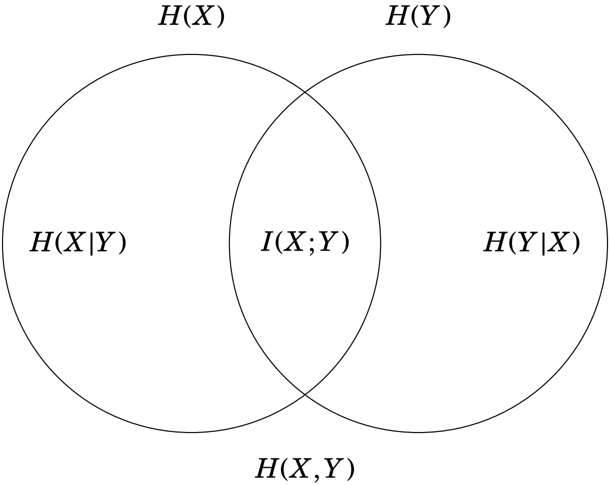


Figure : Venn diagram of entropy

Submodularity of entropy

Theorem. Entropy is submodular, i.e. for all $S, T \subseteq V$,

$$H(S \cup T) + H(S \cap T) \leq H(S) + H(T).$$

Intuition. $X_{S \cap T}$ is common to X_S and X_T, thus

$$\begin{aligned} H(S \cap T) &\leq I(X_S; X_T) \\ &= H(X_S) + H(X_T) - H(X_S, X_T) \\ &= H(S) + H(T) - H(S \cup T). \end{aligned}$$

Shannon entropy of graphs

The Shannon entropy of D is

$$\eta(D) := \sup h(V),$$

sup taken over all functions $h : 2^V \to \mathbb{R}$ s.t.

$$\begin{aligned}
h(v) &\leq 1 && \forall v \in V, \\
h(S) &\leq h(T) && \forall S \subseteq T \subseteq V, \\
h(S \cup T) + h(S \cap T) &\leq h(S) + h(T) && \forall S, T \subseteq V, \\
h(N_{\text{in}}(v) \cup v) &= h(N_{\text{in}}(v)) && \forall v \in V.
\end{aligned}$$

The pentagon

For the pentagon,

$$\tau(C_5) = 3, \quad n - \pi(C_5) = 2, \quad n - \pi^*(C_5) = 2.5.$$

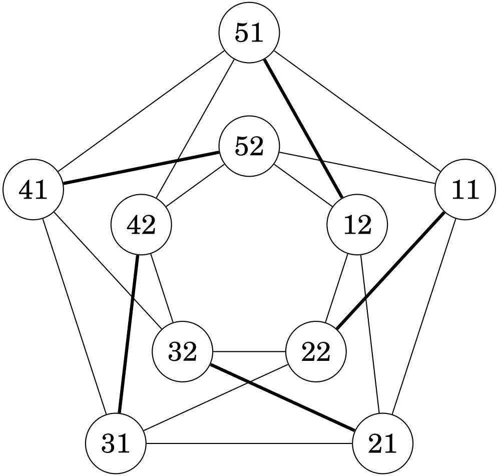


Figure : Optimal fractional clique cover of C_5

Shannon entropy of the pentagon

Let h satisfy the constraints for C_5, then

$$\begin{aligned}
h(V) &= h(2,3,4,5) && \{2,3,4,5\} \text{ is a feedback vertex set,}\\
h(V) &= h(1,3,4) && \{1,3,4\} \text{ is a feedback vertex set,}\\
&\le h(1) + h(3,4) && \text{sub-additivity,}\\
2h(V) &\le h(1) + h(3,4) + h(2,3,4,5) && \text{summation,}\\
&\le h(1) + h(2,3,4) + h(3,4,5) && \text{submodularity,}\\
&= h(1) + h(2,4) + h(3,5) && \{2,4\} = N_{\text{in}}(3) \text{ and } \{3,5\} = N_{\text{in}}(4),\\
&\le 5 && h(v) \le 1 \text{ for all } v \in V.
\end{aligned}$$

Thus $h(V) \le 2.5$.

Further results based on graph entropy

Two extensions in (Christofides and Markström 11).

For odd cycles C_{2k+1} $(k \geq 2)$,

$$\sup_{q\geq 2} g(C_{2k+1}, q) = \eta(C_{2k+1}) = k + \frac{1}{2} < \tau(C_{2k+1}) = k+1.$$

For their complements,

$$\sup_{q\geq 2} g(\overline{C_{2k+1}}, q) = \eta(\overline{C_{2k+1}}) = 2k - 1 - \frac{1}{k} < \tau(\overline{C_{2k+1}}) = 2k-1.$$

And that's it!

Other results on the guessing number

Using non-Shannon inequalities (Baber, Christofides, Dang, Riis, Vaughan 14)

Guessing graph (G + Riis 11): relation to coding theory, extension to signed interaction graphs in (G + Richard + Riis 15)

Approach based on closure solvability: links with matroid theory and secret sharing (G 13, G 14)

System reduction and linear network coding solvability (G + Richard + Fanchon, 15+)