Entropic Vector and Network Coding

Michael Wu

November 9, 2011

1 Motivation

The max-flow bound for the throughput of a network can be violated using network coding. The two classic examples are transmission through an intermediate node, or the butterfly network. (The graph for two examples are omitted here). To understand the limitation of arbitrary network codes, we study entropic vectors.

2 Entropic Vectors and Network Codes

Definition 1. *(Entropic Vectors) Let $X_1, X_2, \ldots, X_n$ to be random variables, and $N = \{1, 2, \ldots, n\}$, and entropic vector is a map $2^N \to \mathbb{R}$ such that $\alpha \mapsto H(X_\alpha)$ where H is the entropy function and X_α is a subset of $X_1, \ldots, X_n$ whose indicies are in α.*

Denote the region of entropic vectors with n random variables to be Γ_n^*. Loosely define the idea of achievable rate R, which is set of tuples $\omega = (\omega_s : s \in S)$ where S is the sources, and ω_s refers to the source output bitrate. The definition requires the target have arbitrar fidelity and each channel does exceed their capacity.

Definition 2. *The strongly typical set $T^n_{[X]\delta}$ with respect to $p(x)$ is the set of sequences $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in X^n$ such that $N(x; \mathbf{x}) = 0$ for $x \notin S_x$ and*

$$\sum_x |\frac{1}{n} N(x; \mathbf{x}) - p(x)| \leq \delta$$

where $N(x; \mathbf{x})$ is the number of occurrences of x in the seqence $\mathbf{x}$, and δ is the arbitrarily small positive real number. The sequene in $T^n_{[X]\delta}$ are called strongly $\delta-$typical sequences.

Theorem 1. *(AEP: asymptotic equiparition property) If $\mathbf{x} \in T^n_{[X]\delta}$, then*

$$2^{-n(H(X)+\eta)} \leq p(\mathbf{x}) \leq 2^{-n(H(X)-\eta)}$$

and $Pr\{\mathbf{X} \in T^n_{[X]\delta}\} > 1-\delta$, *for* n *sufficiently large* $(1-\delta)2^{n(H(X)-\eta)} \leq |T^n_{[X]\delta}| \leq 2^{n(H(x)+\eta)}$.

Definition 3. *Let* R' *be the set of all information rate ruples* ω *such that there exist auxiliary random variables* $Y_s, s \in S$ *and* $U_e, e \in E$ *where satisfy the following conditions:*

$$
\begin{aligned}
H(Y_s) =& \sum_{s \in S} H(Y_s) && (1)\\
H(Y_s) >& \omega_s, s \in S && (2)\\
H(U_{Out(s)|Y_s}) =& 0, s \in S && (3)\\
H(U_{Out(i)}|U_{In(i)}) =& 0, \forall i \in V \setminus S && (4)\\
H(U_e) <& R_e, e \in E && (5)\\
H(Y_{\beta(i)}|U_{In(i)}) =& 0, \forall i \in T && (6)
\end{aligned}
$$

Theorem 2. $R' \subset R$

We can recast R' into the following equations. Let $N = \{Y_s : s \in S; U_e : e \in E\}$, we can define entropic vector $h \in \Gamma^*_N$, and choose R' to be all the possible tuple ω such that

$$
\begin{aligned}
h_{Y_s} =& \sum_{s \in S} h_{Y_s} && (7)\\
h_{Y_s} >& \omega_s, s \in S && (8)\\
h_{U_{out(s)}}|Y_s =& 0, s \in S && (9)\\
h_{U_{Out(i)}|U_{In(i)}} =& 0, i \in V \setminus S && (10)\\
h_{U_e} <& R_e, e \in E && (11)\\
h_{Y_{\beta(i)}|U_{In(i)}} =& 0, i \in T && (12)
\end{aligned}
$$

We call $R_{in} = \overline{con}(R')$, if instead we choose $h \in \bar{\Gamma}^*_N$, and change the inequality in to $\leq$, and $\geq$, then take the convex closure, we get R_{out}. We have the theorem

Theorem 3. $R_{in} \subseteq R \subseteq R_{out}$

The proof is omitted, but the general idea is to use AEP to generate near optimal code. The outer bound is the other direction of inequality of the AEP theorem.

3 Characterizing Γ^*_n

3.1 Convexity

Theorem 4. $\bar{\Gamma_n}^*$ *is a convex cone*

Proof. First if $h, h' \in \Gamma_n^*$, then $h+h' \in \Gamma_n^*$, since we just let $Y_i = (X_i, X_i')$, where the two are independent. From therewe show for any $k \in \mathbb{Z}, k > 0$, $kh \in \Gamma_n^*$. Now let $Y_1, \ldots, Y_n$ describes h and $Z_1, \ldots, Z_n$ describes h', to obtain $bh+(1-b)h'$ we create a ternary random variable U, such that

$$Pr(U = 0) = 1 - \delta - \mu, Pr(U = 1) = \delta, Pr(U = 2) = \mu$$

Let $\mathbf{Y}_i$ be k independent copies of Y_i, and $\mathbf{Z}_i$ be k independent copies of Z_i Then we construct $X_1, \ldots, X_n$ to be

$$X_i = \begin{cases} 0 & \text{if } U = 0 \\ \mathbf{Y}_i & \text{if } U = 1 \\ \mathbf{Z}_i & \text{if } U = 2 \end{cases}$$

Note when $\delta, \mu \to 0$, $H(U) \to 0$, so

$$\begin{aligned} H(X_\alpha) \leq & H(X_\alpha, U) \\ = & H(U) + H(X_\alpha|U) \\ = & H(U) + \delta k H(Y_\alpha) + \mu k H(Z_\alpha) \end{aligned}$$

Meanwhile

$$H(X_\alpha) \geq H(X_\alpha|U) = \delta k H(Y_\alpha) + \mu k H(Z_\alpha)$$

Thus

$$0 \leq H(X_\alpha) - (\delta k H(Y_\alpha) + \mu k H(Z_\alpha)) \leq H(U)$$

By letting $\delta = b/k, \mu = (1-b)/k$ and let k sufficiently large, we made $H(X_\alpha)$ to be sufficiently close to $bh + (1-b)h'$. $\square$

3.2 Shannon Inequaltiy and Γ_n

Shannon inequality is $H(X_\alpha) + H(X_\beta) \geq H(X_{\alpha\cap\beta}) + H(X_{\alpha\cap\beta})$. The entropy vector that satisfies the linear combination of this region is called Γ_n.

Theorem 5. $\Gamma_n^* \subset \Gamma_n$

Proof is omitted. This means that this polytope a lose upper bound of the entropic space.

3.3 Group charactizable vectors and Quasi-Uniform Distribution

One way to charactize Γ_n^* is by looking at some special distributions.

Definition 4. *A group characterizable vector h is also defined to be $2^N \to \mathbb{R}$ such that there exists a group G and subgroups $G_1, G_2, \ldots, G_n$, and for $\alpha \subseteq N$, $h(\alpha) = \log \frac{|G|}{|G_\alpha|}$ if $G_\alpha \neq \emptyset$, and 0 otherwise. Here $G_\alpha = \cap_{i\in\alpha} G_i$.*

The set of all group charactizable vectors is Υ_n, Now we have the following theorem

Theorem 6. $\Upsilon_n \subseteq \Gamma_n^*$.

Proof. Let Λ be a discrete random variable defined on the sample space GA with uniform distribution. For $i \in N$, let X_i be a function of Λ such that $X_i = aG_i$ if $\Lambda = a$. Then

$$Pr(X_i = a_i G_i : i \in \alpha) = \frac{|\cap_{i\in\alpha} a_i G_i}{|G|}$$

$\square$

Theorem 7. $\overline{con}(\Upsilon_n) = \bar{\Gamma}_n^*$.

Proof. We show that $\forall h \in \Gamma_n^*$, $\exists$ a sequence $\{f^{(r)}\}$ such that $\lim_{r\to\infty} f^{(r)} = h$. Let h be defined with random variables $X_1, X_2, \ldots, X_n$. further assume $p(x_1, \ldots, x_n)$ are all rational values, since we are dealing with closure here. Denote $Q_\alpha(\mathbf{x})$ to be $p_\alpha(a)$ where p_α is the marginal probability calculated from $p(\mathbf{x})$ Also here we assume $|X| < \infty, \forall X_i$. Assume q is the common denomenator of all of the probabilities. Let $r = q, 2q, 3q, \ldots,$ and consider the $n \times r$ matrix $\mathbf{x}$ where each column is a possible choice of value $X_1, \ldots, X_n$ and the number of the appearance is exactly $rQ_N(a)$. Denote $\mathbf{x}_\alpha$ the submatrix that are rows of $\mathbf{x}$ corresponding to $\alpha \subseteq N$. Then the number of occurance of a particular column a_α is exactly $rQ_\alpha(a)$ in $\mathbf{x}_\alpha$.
Let G be the permutatino group of $\{1, 2, \ldots, r\}$. Let G_i to be the subgroup such that $\sigma[\mathbf{x}_i] = [x_{i,\sigma(1)}, x_{i,\sigma(2)}, \ldots, x_{i,\sigma(r)}] = x_i$, so we have if $\sigma \in G_\alpha$, then $\sigma[\mathbf{x}_\alpha] = \mathbf{x}_\alpha$. Whence we conclude $|G_\alpha| = \prod_{a\in X_\alpha}(rQ_\alpha(a))!$. Using the lemma that

$$\lim_{r\to\infty} \frac{1}{r} \log \frac{r!}{\prod_x (rp(x))!} = H(X)$$

we have shown that $\lim_{r\to\infty} \frac{1}{r}\mathbf{f}^{(r)} = \mathbf{h}$. $\square$