Performance of Codes over Convex Combinations of BSCs

Hesam and Raj

I. Basic Setup

Assuming that the all zero codeword was transmitted, the LLR of a BSC with crossover probability p is given by

$$\phi_p = p\Delta_{\log \frac{p}{1-p}} + (1-p)\Delta_{-\log \frac{p}{1-p}},$$

where Δ_x denotes a Delta function at the value x. Define $\mathbf{p} = (p_1, \ldots, p_N)$ and $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_N)$. Let $\sum_{i=1}^{N} \lambda_i = 1$. We define a new channel CBSC$(\mathbf{p}, \boldsymbol{\lambda})$ to be the channel whose LLR ϕ corresponds to the convex combination of the BSC LLRs:

$$\phi = \sum_{i=1}^{N} \lambda_i \phi_{p_i}.$$

Consider the binary input, $2N-$ary output channel with the particular transition probabilities show in Fig. 1. Let the outputs of the channel be denoted by $\{0_i, 1_i\}_{i=1}^{N}$. It can be verified that the channel shown in Fig. 1 gives rise to the above mentioned LLR ϕ.

II. Entropy of the output of CBSC$(\mathbf{p}, \boldsymbol{\lambda})$

We now compute the entropy of the output Z of the channel in Fig. 1. Let the input probability distribution $P(X=0) = \alpha, P(X=1) = 1-\alpha$. For every $i = 1, \ldots, N$, we have that

$$\begin{aligned} P(Z = 0_i) &= \alpha\lambda_i(1-p_i) + (1-\alpha)\lambda_i p_i \\ &= \alpha\lambda_i(1-2p_i) + \lambda_i p_i \\ &\triangleq c_i\alpha + d_i, \end{aligned}$$

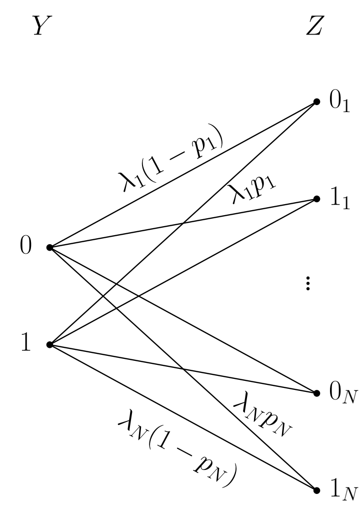

Fig. 1. Convex combination of BSCs

where $c_i = \lambda_i(1-2p_i)$ and $d_i = \lambda_i p_i$. Also,

$$\begin{aligned} P(Z=1_i) &= \alpha\lambda_i p_i + (1-\alpha)\lambda_i(1-p_i) \\ &= \alpha\lambda_i(2p_i-1) + \lambda_i(1-p_i) \\ &\triangleq e_i\alpha + f_i, \end{aligned}$$

where $e_i = \lambda_i(2p_i-1)$ and $d_i = \lambda_i(1-p_i)$.

Hence the output entropy

$$H(Z) = -\sum_{i=1}^{N}\left[(c_i\alpha+d_i)\log(c_i\alpha+d_i) + (e_i\alpha+f_i)\log(e_i\alpha+f_i)\right] \tag{1}$$

Define $c_i' \triangleq c_i/\lambda_i$, $d_i' \triangleq d_i/\lambda_i$, $e_i' \triangleq e_i/\lambda_i$ and $f_i' \triangleq f_i/\lambda_i$. We may rewrite the output entropy as

$$\begin{aligned} H(Z) = -\sum_{i=1}^{N}\lambda_i \Big[&(c_i'\alpha+d_i')\log(c_i'\alpha+d_i') + (e_i'\alpha+f_i')\log(e_i'\alpha+f_i') \\ &+(c_i'\alpha+d_i')\log\lambda_i + (e_i'\alpha+f_i')\log\lambda_i\Big] \end{aligned}$$

Notice that $c_i'\alpha + d_i' = \alpha(1-2p_i)+p_i$ and $e_i'\alpha+f_i' = \alpha(2p_i-1)+(1-p_i)$ are exactly equal to the output probabilities of the channel BSC(p_i), when the input probabilities are α and $1-\alpha$. Defining the random variable Z_i as the output of a BSC with transition probability p_i, we obtain the entropy of the output of the channel CBSC$(\mathbf{p},\boldsymbol{\lambda})$ in terms of the constituent BSCs as

$$H(Z) = H(\boldsymbol{\lambda}) + \sum_{i=1}^{N} \lambda_i H(Z_i). \tag{2}$$

From the above expression, it is also clear that uniform inputs achieve the capacity of CBSC$(\mathbf{p},\boldsymbol{\lambda})$, owing to them being optimal for the BSC.

Further, we may compute the conditional entropy of the output of CBSC$(\mathbf{p},\boldsymbol{\lambda})$ given the input as

$$\begin{aligned}
H(Z|X) &= H(Z|X=0) \\
&= -\sum_{i=1}^{N} [\lambda_i(1-p_i)\log\lambda_i(1-p_i) + \lambda_i p_i \log \lambda_i p_i] \\
&= -\sum_{i=1}^{N} [(1-p_i)\log(1-p_i) + (1-p_i)\log\lambda_i + p_i\log\lambda_i + p_i \log p_i] \\
&= H(\boldsymbol{\lambda}) + \sum_{i=1}^{N} \lambda_i h(p_i),
\end{aligned}$$

where $h(\cdot)$ denotes the binary entropy function.

III. Equivalence Between the CBSC and Compound BSCs

Consider the compound channel shown in Fig. 2. The channel is a BSC, whose crossover probability is determined by the random variable Λ. More specifically, let Λ be an $N-$ary random variable taking on the value i with probability λ_i, for all $i = 1, 2, \ldots, N$. Each time the compound channel is used, a realization i of Λ is chosen i.i.d., and according to this value i, the compound channel behaves as BSC(p_i). Let Z' denote the output of the BSC with transition probability p_i. We consider both Λ and

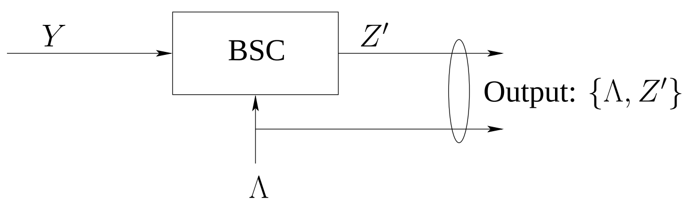

Fig. 2. Equivalent Channel

Z' to be the output of the compound channel. The output entropy of the compound channel is given by

$$\begin{aligned} H(\Lambda, Z') &= H(\Lambda) + H(Z'|\Lambda) \\ &= H(\boldsymbol{\lambda}) + \sum_{i=1}^{N} \lambda_i H(Z_i), \end{aligned}$$

where Z_i is the corresponding output of BSC(p_i) as defined in the previous section. From (2), it is clear that the channel CBSC$(\mathbf{p}, \boldsymbol{\lambda})$ with output Z is indistinguishable in terms of output entropy from the compound channel in Fig. 2 with output (Z', Λ). We will hence focus on the compound channel, in order to compute the entropy of the output of CBSC$(\mathbf{p}, \boldsymbol{\lambda})$.

Also note that while we have shown the equivalence of the output entropies for a single use of the channel, it follows that the joint output entropies of $n-$length symbols of these two channels are also equal to each other. We will work with the vector channel in the sequel.

A. *Output entropy of the Compound BSC channel*

Let $[N]$ denote the set $\{1, 2, \ldots, N\}$. We simplify the output entropy of $n-$uses of the compound channel as

$$\begin{aligned} H(\Lambda, Z') &= H(\Lambda) + H(Z'|\Lambda) \\ &= nH(\boldsymbol{\lambda}) + \sum_{\mathbf{s} \in [N]^n} p(\mathbf{s}) H(Z'|\Lambda = \mathbf{s}). \end{aligned}$$

From Corollary 1 in [1], we bound the above as

$$\begin{aligned} H(\Lambda, Z') &\geq nH(\boldsymbol{\lambda}) + \sum_{\mathbf{s} \in [N]^n} \left(\prod_{i=1}^{n} \lambda_{s_i} \right) \left[n - \log_2 \left(\sum_{c \in C^\perp} \prod_{\{i | c_i = 1\}} (1 - 2p_{s_i})^2 \right) \right] \\ &= n(1 + H(\boldsymbol{\lambda})) - \sum_{\mathbf{s} \in [N]^n} \left(\prod_{i=1}^{n} \lambda_{s_i} \right) \log_2 \left(\sum_{c \in C^\perp} \prod_{\{i | c_i = 1\}} (1 - 2p_{s_i})^2 \right), \end{aligned}$$

since $\sum_{\mathbf{s} \in [N]^n} \left(\prod_{i=1}^{n} \lambda_{s_i} \right) = \left(\sum_{i=1}^{N} \lambda_i \right)^n = 1$. Using Jensen's inequality, we obtain

$$\begin{aligned} H(\Lambda, Z') &\geq n(1 + H(\boldsymbol{\lambda})) - \log_2 \left[\sum_{\mathbf{s} \in [N]^n} \left(\prod_{i=1}^{n} \lambda_{s_i} \right) \sum_{c \in C^\perp} \prod_{\{i | c_i = 1\}} (1 - 2p_{s_i})^2 \right] \\ &= n(1 + H(\boldsymbol{\lambda})) - \log_2 \left[\sum_{c \in C^\perp} \sum_{\mathbf{s} \in [N]^n} \left(\prod_{i=1}^{n} \lambda_{s_i} \right) \prod_{\{i | c_i = 1\}} (1 - 2p_{s_i})^2 \right]. \end{aligned}$$

We define the notation $\mathbf{s}_{\mathcal{I}} \triangleq \{s_i | i \in \mathcal{I}\}$, and $\mathcal{I}_{\mathbf{c}} = \{i | c_i = 1\}$. Notice that $|\mathcal{I}_{\mathbf{c}}| = w_H(\mathbf{c})$. Continuing,

$$\begin{aligned} H(\Lambda, Z') &\geq n(1+H(\boldsymbol{\lambda})) - \log_2 \left[\sum_{c \in C^\perp} \sum_{\mathbf{s}_{[N]\setminus\mathcal{I}_{\mathbf{c}}} \in [N]^{n-w_H(\mathbf{c})}} \left(\prod_{i \in [N]\setminus\mathcal{I}_{\mathbf{c}}} \lambda_{s_i} \right) \cdot \sum_{\mathbf{s}_{\mathcal{I}_{\mathbf{c}}} \in [N]^{w_H(\mathbf{c})}} \left(\prod_{i \in \mathcal{I}_{\mathbf{c}}} \lambda_i (1-2p_{s_i})^2 \right) \right] \\ &= n(1+H(\boldsymbol{\lambda})) - \log_2 \left[\sum_{c \in C^\perp} \left[\sum_{i=1}^{N} \lambda_i (1-2p_i)^2 \right]^{w_H(\mathbf{c})} \underbrace{\sum_{\mathbf{s}_{[N]\setminus\mathcal{I}_{\mathbf{c}}} \in [N]^{|\mathbf{s}_{[N]\setminus\mathcal{I}_{\mathbf{c}}}|}} \left(\prod_{i \in [N]\setminus\mathcal{I}_{\mathbf{c}}} \lambda_{s_i} \right)}_{= \left[\sum_{i=1}^{N} \lambda_i\right]^{n-w_H(\mathbf{c})} = 1} \right]. \end{aligned}$$

Defining $\mathcal{P} \triangleq \sum_{i=1}^{N} \lambda_{s_i} (1-2p_{s_i})^2$, we obtain that

$$H(\Lambda, Z') \geq n(1+H(\boldsymbol{\lambda})) - \log_2 \left[\sum_{w=0}^{n} B_w \mathcal{P}^w \right]. \tag{3}$$

When we set $N = 1$, we recover our earlier bound for the BSC.

IV. Thresholds of the MI for CBSC$(\mathbf{p}, \boldsymbol{\lambda})$

Set $\mathcal{C} = \text{CBSC}(\mathbf{p}, \boldsymbol{\lambda})$. From Lemma 4 in [Pakzad-Shokrollahi], we have that (using the same notation as in [Pakzad-Shokrollahi])

$$\begin{aligned} P\{I(X;Z) < n\text{Cap}(\mathcal{C})\} &\leq n\text{Cap}(\mathcal{C}) - \mathbb{E}\left[I(X;Z)\right] \\ &= n[1+H(\boldsymbol{\lambda})] - H(Z|Y) - \mathbb{E}[H(Z)] + H(Z|Y) \\ &= n[1+H(\boldsymbol{\lambda})] - \mathbb{E}[H(Z)] \end{aligned}$$

From (3) and the equivalence between the channels that we established, we obtain

$$\begin{aligned} P\{I(X;Z) < n\text{Cap}(\mathcal{C})\} &\leq \mathbb{E}\left\{ \log_2 \left[\sum_{w=0}^{n} B_w \mathcal{P}^w \right] \right\} \\ &\leq \log_2 \left[\sum_{w=0}^{n} \mathbb{E}[B_w] \mathcal{P}^w \right] \end{aligned}$$

We now replicate the BSC theorem, replacing "p" with "$\mathcal{P}$".

References

[1] K. Raj Kumar, Payam Pakzad, Amir Hesam Salavati and Amin Shokrollahi, "Phase Transitions for Mutual Information," Submitted to the 6^{th} *Intl. Symp. on Turbo Codes & Iterative Information Processing (ISTC 2010)*, Apr. 2010.