EXIT Charts and the EXIT Area Theorem

Supplemental Material for Advanced Channel Coding
Henry D. Pfister

April 16th, 2015

1 Introduction

EXtrinsic Information Transfer (EXIT) charts were introduced by ten Brink in 1999 as a useful tool to understand the convergence of Turbo decoding for different component codes [1]. His work led to the EXIT area theorem and this was put on rigorous mathematical footing by Ashikhmin, Kramer, and ten Brink in 2004 [2]. A little later, Measson et al. showed that the area theorem also allows one to upper bound the MAP decoding threshold using information gleaned from iterative decoding [3]. Together these ideas highlight the fundamental connections between iterative information processing and optimal information processing.

2 EXIT Functions

Let $\mathcal{C}$ be a length-n binary code and assume that a random codeword $\underline{X} = (X_1, \ldots, X_n)$ is chosen according to $P_{\underline{X}}(\underline{x})$. Suppose $Y_i \in \{0, 1, ?\}$ is an observation of X_i through a BEC with erasure probability ϵ_i and $\underline{Y} = (Y_1, \ldots, Y_n)$ is the channel output vector. The notation $\underline{Y}_{\sim i}$ will be used to denote the vector $(Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_n)$ and the notation $\underline{Y}(\underline{\epsilon}) = (Y_1(\epsilon_1), \ldots, Y_n(\epsilon_n))$ will be used to emphasize the dependence on $\underline{\epsilon} = (\epsilon_1, \ldots, \epsilon_n)$.

Definition 1. The **EXIT function for the i-th bit** of $\mathcal{C}$ is defined to be

$$h_i(\underline{\epsilon}) \triangleq H(X_i | \underline{Y}_{\sim i}(\underline{\epsilon}_{\sim i})).$$

If all $\epsilon_i = \epsilon$ for $i \in [n]$, then the simplified notation $h_i(\epsilon) \triangleq h_i((\epsilon, \ldots, \epsilon)) = H(X_i | \underline{Y}_{\sim i}(\epsilon))$ is used. Similarly, the **average EXIT function** of $\mathcal{C}$ is defined to be $h(\underline{\epsilon}) = \frac{1}{n} \sum_{i=1}^{n} h_i(\underline{\epsilon})$ in the first case and $h(\epsilon) = \frac{1}{n} \sum_{i=1}^{n} h_i(\epsilon)$ in the second.

Lemma 2. *Using the above setup, the EXIT function for the i-th bit of $\mathcal{C}$ satisfies*

$$h_i(\underline{\epsilon}) = \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} H(\underline{X} | \underline{Y}(\underline{\epsilon})).$$

Proof. Suppressing the explicit dependence on $\underline{\epsilon}$, this follows from

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}\epsilon_i} H(\underline{X}|\underline{Y}) &= \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} \left[H(X_i|\underline{Y}) + H(\underline{X}_{\sim i}|X_i, \underline{Y}) \right] && (H \text{ chain rule}) \\
&= \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} H(X_i|\underline{Y}) + \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} \underbrace{H(\underline{X}_{\sim i}|X_i, \underline{Y}_{\sim i})}_{\text{ind. of } \epsilon_i} && (\underline{X}_{\sim i} \to X_i \to Y_i \text{ Markov chain}) \\
&= \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} \left[\mathbb{P}(Y_i = ?) H(X_i|\underline{Y}, Y_i = ?) + \mathbb{P}(Y_i \neq ?) \underbrace{H(X_i|\underline{Y}, Y_i \neq ?)}_{Y_i \neq ? \Rightarrow Y_i = X_i \Rightarrow H = 0} \right] && (\text{Average over } Y_i) \\
&= \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} \epsilon_i H(X_i|\underline{Y}_{\sim i}) = H(X_i|\underline{Y}_{\sim i}). && (\mathbb{P}(Y_i = ?) = \epsilon_i)
\end{aligned}$$

□

Lemma 3. *Using the above setup, let $H(\underline{X}|\underline{Y}(\underline{\epsilon}(t)))$ denote the conditional entropy evaluated along the BEC path $\underline{\epsilon}(t) = (\epsilon_1(t), \ldots, \epsilon_n(t))$ for $t \in [0,1]$. Then,*

$$H(\underline{X}|\underline{Y}(\underline{\epsilon}(1)) - H(\underline{X}|\underline{Y}(\underline{\epsilon}(0))) = \int_0^1 \underline{h}(\epsilon(t)) \cdot \underline{\epsilon}'(t) \mathrm{d}t = \int_0^1 \left(\sum_{i=1}^n h_i(\underline{\epsilon}(t)) \epsilon_i'(t) \right) \mathrm{d}t,$$

where $\underline{h}(\underline{\epsilon}) = (h_1(\underline{\epsilon}), \ldots, h_n(\underline{\epsilon}))$. If the BEC path satisfies $\epsilon_i(t) = \epsilon(t)$ for $i \in [n]$, then we find that

$$H(\underline{X}|\underline{Y}(\epsilon(1)) - H(\underline{X}|\underline{Y}(\epsilon(0))) = \int_0^1 \left(\sum_{i=1}^n h_i(\epsilon(t)) \epsilon'(t) \right) \mathrm{d}t = n \int_0^1 h(\epsilon(t)) \epsilon'(t) \mathrm{d}t.$$

Proof. These results follow directly from Lemma 2 and vector calculus. □

Example 4. Consider the non-linear code $\mathcal{C} = \{00, 10, 11\}$ where codewords are chosen, respectively, with probabilities $\frac{1}{2}, \frac{1}{4}, \frac{1}{4}$. In this case, $H(\underline{X}) = \frac{3}{2}$ and it is easy to verify that

$$\begin{aligned} H(X_1|Y_2(\epsilon_2)) &= \epsilon_2 + \frac{3}{4}(1-\epsilon_2) h(\tfrac{1}{3}) \\ H(X_2|Y_1(\epsilon_1)) &= \epsilon_1 h(\tfrac{1}{4}) + \frac{1}{2}(1-\epsilon_1), \end{aligned}$$

where $h(x) = x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x}$ is the binary entropy function. Integrating gives

$$\begin{aligned} \int_0^1 \left[H(X_1|Y_2(\epsilon)) + H(X_2|Y_1(\epsilon_1)) \right] \mathrm{d}\epsilon &= \int_0^1 \left[\epsilon + \frac{3}{4}(1-\epsilon) h(\tfrac{1}{3}) + \epsilon h(\tfrac{1}{4}) + \frac{1}{2}(1-\epsilon) \right] \mathrm{d}\epsilon \\ &= \left(\frac{1}{2} + \frac{1}{4} \right) + \left(\frac{3}{8} h(\tfrac{1}{3}) + \frac{1}{2} h(\tfrac{1}{4}) \right) \\ &= \frac{3}{4} + \frac{3}{4} = \frac{3}{2}. \end{aligned}$$

One can also verify, either directly or via differentiation, that

$$H(\underline{X}|\underline{Y}(\underline{\epsilon})) = \epsilon_1 \epsilon_2 \frac{3}{2} + \frac{1}{2}(1-\epsilon_1)\epsilon_2 + \frac{3}{4}\epsilon_1 (1-\epsilon_2) h(\tfrac{1}{3}).$$

2.1 Uniform Codeword Distribution

Now, let $\mathcal{C}$ be an (n,k) binary linear code with generator matrix G and parity-check matrix H. Assume that a random codeword $\underline{X}$ is chosen uniformly and transmitted through BECs with output $\underline{Y} \in \{0,1,?\}^n$. Let $\mathcal{E}(\underline{y}) \triangleq \{i \in [n] \,|\, y_i = ?\}$ be set of indices where an erasure occurs. For a set $\mathcal{E} = (e_1, e_2, \ldots, e_{|\mathcal{E}|})$ with $e_1 < e_2 < \cdots < e_{|\mathcal{E}|}$ and an $m \times n$ matrix $A = (\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n)$ whose i-th column is $\underline{a}_i$, we let $A_{\mathcal{E}} = (\underline{a}_{e_1}, \underline{a}_{e_2}, \ldots, \underline{a}_{e_{|\mathcal{E}|}})$. The same rule can be applied to row vectors by choosing $m = 1$.

Using this notation, the a posteriori probability (APP) distribution for $\underline{X}$ given $\underline{Y}$ is

$$P_{\underline{X}}(\underline{x}|\underline{y}) = \begin{cases} \frac{1}{|V(\underline{y})|} & \text{if } \underline{x} \in V(\underline{y}) \\ 0 & \text{otherwise,} \end{cases}$$

where $V(\underline{y}) = \left\{ \underline{z} \in \mathcal{C} \,|\, \underline{z}_{\mathcal{E}^c(\underline{y})} = \underline{y}_{\mathcal{E}^c(\underline{y})} \right\}$ is set of codewords that are compatible with the observations. Since $\mathcal{C}$ is linear, the set $V(\underline{y})$ is the affine subspace of $\underline{x} \in \{0,1\}^n$ satisfying

$$H_{\mathcal{E}} \underline{x}_{\mathcal{E}}^T = H_{\mathcal{E}^c} \underline{y}_{\mathcal{E}^c}^T,$$

where $\mathcal{E}(\underline{y})$ is denoted by $\mathcal{E}$ for simplicity and $\underline{y}_{\mathcal{E}^c}$ is a binary vector known by the decoder. Thus, dimension of the solution space is given by $|\mathcal{E}| - \operatorname{rank}(H_{\mathcal{E}})$. Similarly, affine subspace of input vectors $\underline{u} \in \{0,1\}^k$ compatible with $\underline{y}$ is defined by

$$\underline{u} G_{\mathcal{E}^c} = \underline{y}_{\mathcal{E}^c}$$

and dimension of the solution space is $k - \text{rank}(G_{\mathcal{E}^c})$. Of course, the two spaces must have the same dimension and this implies that

$$k - \text{rank}(G_{\mathcal{E}^c}) = |\mathcal{E}| - \text{rank}(H_{\mathcal{E}}).$$

Since the input distribution is uniform over $\mathcal{C}$, then these unknown dimensions have full entropy and

$$H(\underline{X}|\underline{Y} = \underline{y}) = |\mathcal{E}| - \text{rank}(H_{\mathcal{E}}) = k - \text{rank}(G_{\mathcal{E}^c}).$$

Lemma 5. *Using the above setup, the conditional entropy $H(\underline{X}|\underline{Y}(\underline{\epsilon}))$ is given by*

$$\begin{aligned} H(\underline{X}|\underline{Y}(\underline{\epsilon})) &= k - \sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}^c}(1-\epsilon_i)\right)\text{rank}(G_{\mathcal{E}^c}) \\ &= \sum_{i=1}^{n} \epsilon_i - \sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}^c}(1-\epsilon_i)\right)\text{rank}(H_{\mathcal{E}}). \end{aligned}$$

Let $H^{\perp}(\underline{X}|\underline{Y}(\underline{\epsilon}))$ denote the conditional entropy when $\underline{X}$ is chosen uniformly from the dual code $\mathcal{C}^{\perp}$. Then,

$$H^{\perp}(\underline{X}|\underline{Y}(\underline{\epsilon})) = H(\underline{X}|\underline{Y}(\underline{1}-\underline{\epsilon})) - k + \sum_{i=1}^{n} \epsilon_i$$

and computing the derivative with respect to ϵ_i shows that

$$h_i^{\perp}(\underline{\epsilon}) = 1 - h_i(\underline{1}-\underline{\epsilon}).$$

Proof. The first formula follows from averaging $H(\underline{X}|\underline{Y} = \underline{y}) = k - \text{rank}(G_{\mathcal{E}^c})$ over all all possible erasure patterns because the formula depends only on the erasure pattern and not on the unerased values. The second formula follows from averaging $H(\underline{X}|\underline{Y} = \underline{y}) = |\mathcal{E}| - \text{rank}(H_{\mathcal{E}})$ over all all possible erasure patterns. In this case, the expectation of $|\mathcal{E}|$ is computed using

$$\begin{aligned} \sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}^c}(1-\epsilon_i)\right)|\mathcal{E}| &= \sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}^c}(1-\epsilon_i)\right)\sum_{j=1}^{n}\mathbf{1}_{\mathcal{E}}(j) \\ &= \sum_{j=1}^{n}\sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}^c}(1-\epsilon_i)\right)\mathbf{1}_{\mathcal{E}}(j) \\ &= \sum_{j=1}^{n} \epsilon_j. \end{aligned}$$

For the dual code, we note that

$$\begin{aligned} H^{\perp}(\underline{X}|\underline{Y}(\underline{\epsilon})) &= \sum_{i=1}^{n} \epsilon_i - \sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}^c}(1-\epsilon_i)\right)\text{rank}(H_{\mathcal{E}}^{\perp}) && (\text{Definition of } H^{\perp}(\underline{X}|\underline{Y}(\underline{\epsilon}))) \\ &= \sum_{i=1}^{n} \epsilon_i - \sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}^c}(1-\epsilon_i)\right)\text{rank}(G_{\mathcal{E}}) && (H^{\perp} = G) \\ &= \sum_{i=1}^{n} \epsilon_i - \sum_{\mathcal{E}\subseteq[n]} \left(\prod_{i\in\mathcal{E}^c} \epsilon_i\right)\left(\prod_{i\in\mathcal{E}}(1-\epsilon_i)\right)\text{rank}(G_{\mathcal{E}^c}) && (\mathcal{E}\text{-sum invariant: } \mathcal{E}\mapsto\mathcal{E}^c) \\ &= \left(\sum_{i=1}^{n} \epsilon_i\right) - k + H(\underline{X}|\underline{Y}(\underline{1}-\underline{\epsilon})). && (\text{Definition of } H(\underline{X}|\underline{Y}(\underline{1}-\underline{\epsilon}))) \end{aligned}$$

Taking the derivative with ϵ_i gives

$$
\begin{aligned}
h_i^{\perp}(\underline{\epsilon}) &= \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} H^{\perp}(\underline{X}|\underline{Y}(\underline{\epsilon})) \\
&= \frac{\mathrm{d}}{\mathrm{d}\epsilon_i}\left[\left(\sum_{i=1}^{n}\epsilon_i\right) - k + H(\underline{X}|\underline{Y}(\underline{1}-\underline{\epsilon}))\right] \\
&= 1 - \frac{\mathrm{d}}{\mathrm{d}\epsilon_i} H(\underline{X}|\underline{Y}(\underline{1}-\underline{\epsilon})) \\
&= 1 - h_i(\underline{1}-\underline{\epsilon}).
\end{aligned}
$$

This completes the proof. □

2.2 Random Codes

Let $\mathcal{C}^{(j)}$ be a sequence of random linear codes, each defined by a randomly chosen parity-check matrix $H^{(j)}$ of size $(n_j - k_j) \times n_j$, where $r \triangleq k_j/n_j$ is design rate of the sequence and $n_j \to \infty$. No assumptions are made about the distribution of $H^{(j)}$. Still, the true rate of the j-th code is given by $r(\mathcal{C}^{(j)}) = 1 - \frac{1}{n}\mathrm{rank}(H^{(j)})$ and basic coding theory shows that $r(\mathcal{C}^{(j)}) \geq r$ with equality iff $H^{(j)}$ is full rank. Thus, we find that

$$
r \leq r(\mathcal{C}^{(j)}).
$$

Now, let $h^{(j)}(\epsilon)$ be the random EXIT function of the j-th random code and observe that

$$
\begin{aligned}
r &\leq \limsup_{j\to\infty} \mathbb{E}\left[r(\mathcal{C}^{(j)})\right] && (\mathbb{E} \text{ then } \limsup) \\
&= \limsup_{j\to\infty} \mathbb{E}\left[\int_0^1 h^{(j)}(\epsilon)\mathrm{d}\epsilon\right] && (\text{EXIT Theorem}) \\
&= \limsup_{j\to\infty} \int_0^1 \underbrace{\mathbb{E}\left[h^{(j)}(\epsilon)\right]}_{\overline{h}^{(j)}(\epsilon)} \mathrm{d}\epsilon && (\mathbb{E} \text{ over finite set}) \\
&\leq \int_0^1 \underbrace{\limsup_{j\to\infty} \overline{h}^{(j)}(\epsilon)}_{\overline{h}^{(\infty)}(\epsilon)} \mathrm{d}\epsilon && (\text{Fatou's Lemma}) \\
&= \int_0^1 \overline{h}^{(\infty)}(\epsilon)\mathrm{d}\epsilon.
\end{aligned}
$$

2.3 BP EXIT Functions

Let $\mathcal{C}^{(j)}$ be a sequence of codes from the ensemble LDPC(λ, ρ), each defined by a randomly chosen parity-check matrix $H^{(j)}$ of size $(n_j - k_j) \times n_j$, where $r \triangleq k_j/n_j$ is design rate of the sequence and $n_j \to \infty$. Suppose the normalized bit and check degree distributions of each code in the sequence are given by $\lambda(x)$ and $\rho(x)$. In this case, one can use the BP estimate after ℓ_j iterations for each bit in the code. In the limit as $n_j \to \infty$ and $\ell_j \to \infty$, the erasure rate is concentrated around the density evolution estimate

$$
h^{(BP)}(\epsilon) = L(x(\epsilon)),
$$

where $x(\epsilon)$ is the limit of the decreasing sequence $x_{\ell+1} = \epsilon\lambda(1-\rho(1-x_\ell))$ starting from $x_0 = 1$.

Since $h^{(j)}(\epsilon)$ is the EXIT function associated with optimal APP detection of $\mathcal{C}^{(j)}$, it follows that the EXIT function associated with any other estimator cannot be smaller. Thus, one finds that

$$
\overline{h}^{(\infty)}(\epsilon) \triangleq \limsup_{j\to\infty} \overline{h}^{(j)}(\epsilon) \leq h^{(BP)}(\epsilon).
$$

Let us define the MAP noise threshold to be

$$\epsilon^{(MAP)} \triangleq \sup\left\{\epsilon \in [0,1] \,\middle|\, \overline{h}^{(\infty)}(\epsilon) = 0\right\}.$$

Then, one finds that

$$\int_0^1 \overline{h}^{(\infty)}(\epsilon)\mathrm{d}\epsilon = \int_{\epsilon^{(MAP)}}^1 \overline{h}^{(\infty)}(\epsilon)\mathrm{d}\epsilon \le \int_{\epsilon^{(MAP)}}^1 \overline{h}^{(BP)}(\epsilon)\mathrm{d}\epsilon.$$

This implies the following upper bound on the MAP noise threshold.

Theorem 6. *Let $\overline{\epsilon}$ be the largest value such that*

$$\int_{\overline{\epsilon}}^1 \overline{h}^{(BP)}(\epsilon)\mathrm{d}\epsilon = r.$$

Then, $\epsilon^{(MAP)} \le \overline{\epsilon}$.

Proof. If $\epsilon^{(MAP)} > \overline{\epsilon}$, then one gets the contradiction

$$\begin{aligned} r &\le \int_0^1 \overline{h}^{(\infty)}(\epsilon)\mathrm{d}\epsilon \\ &\le \int_{\epsilon^{(MAP)}}^1 \overline{h}^{(\infty)}(\epsilon)\mathrm{d}\epsilon \\ &\le \int_{\epsilon^{(MAP)}}^1 \overline{h}^{(BP)}(\epsilon)\mathrm{d}\epsilon \\ &\overset{(a)}{<} \int_{\overline{\epsilon}}^1 \overline{h}^{(BP)}(\epsilon)\mathrm{d}\epsilon \\ &= r, \end{aligned}$$

where (a) follows from the fact that $\overline{h}^{(BP)}(\epsilon) \ge \overline{h}^{(\infty)}(\epsilon) > 0$ for $\epsilon \in (\overline{\epsilon}, \epsilon^{(MAP)})$. □

References

[1] S. ten Brink, "Convergence of iterative decoding," *Electronic Letters*, vol. 35, pp. 806–808, May 1999.

[2] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: model and erasure channel properties," *IEEE Trans. Inform. Theory*, vol. 50, pp. 2657–2674, Nov. 2004.

[3] C. Méasson, A. Montanari, and R. L. Urbanke, "Maxwell construction: The hidden bridge between iterative and maximum a posteriori decoding," *IEEE Trans. Inform. Theory*, vol. 54, pp. 5277–5307, Dec. 2008.