Why Turbo Codes cannot achieve Capacity

Jossy Sayir

Vienna Telecommunications Research Centre (ftw.)
Donau-City-Str. 1, A-1220 Vienna, Austria
E-mail: sayir@ftw.at

Abstract: *For the binary erasure channel with erasure probability 1/2, it is shown that coding systems based on parallel concatenation can not achieve arbitrarily reliable transmission with interleaver block length going to infinity at rates approaching capacity. The same is shown for serial concatenation when the rate of the inner code is smaller than 1. While this effect was known from simulations, we show that it is a simple consequence of the data processing theorem. In addition, a lower bound for the rate loss with regard to capacity is given for parallel and for serial concatenation.*

Keywords: Data Processing Theorem, EXIT Charts, Serial Concatenation, Parallel Concatenation, Binary Erasure Channel

1. Introduction

It has recently been observed (see, for example, [1]) that the performance of iterative decoding of serially concatenated codes is good only if the inner code has rate one or more. While capacity-achieving families of serially concatenated codes with inner code rate at least 1 have been constructed, it has not been possible to construct capacity-achieving codes using parallel concatenation. This can be explained using an area property of extrinsic information transfer (EXIT) charts [2]. We argue that this is also a simple consequence of the data processing theorem [3, Theorem 4.3.3]. We further *quantify* how much rate is lost when finite-memory inner codes are used for a binary erasure channel (BEC) with erasure probability 1/2. Our approach is to bound the information rate between the channel input blocks and the channel output blocks as a function of the inner code's memory and rate for serial concatenation, and as a function of one of the component code's memory and rate for parallel concatenation. Our bound thus applies to both *a-posteriori probability* (APP) decoding and iterative (turbo) decoding.

2. Applying the Data Processing Theorem

A serially concatenated coding system is illustrated in Figure 1 and a parallel concatenated coding system is illustrated in Figure 2.

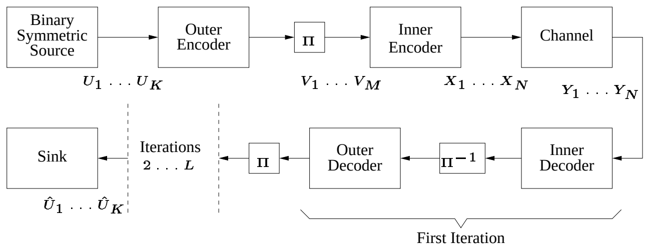

Figure 1: Serially Concatenated Coding

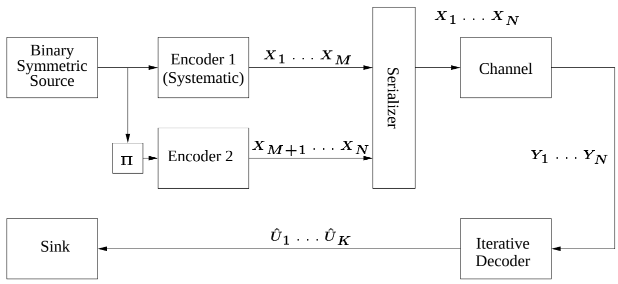

Figure 2: Parallel Concatenated Coding

The data processing theorem states in both cases that

$$I(U_1^K; \hat{U}_1^K) \leq I(X_1^N; Y_1^N), \qquad (1)$$

where U_1^K is used as a shorthand notation for $U_1 \dots U_K$. Let $R = K/N$ be the overall rate of the coding system. A necessary condition for arbitrarily reliable communication in the asymptotic case for a fixed rate R is that

$$\lim_{N\to\infty, K/N=R} \frac{1}{N} I(U_1^K; \hat{U}_1^K) = R. \qquad (2)$$

If we want the family of codes defined by our serial or parallel concatenation of encoders with interleaver size growing to infinity to be capacity-achieving, (2) must hold for a rate R equal to the capacity C of the channel.

For the special case of a binary erasure channel with erasure probability 1/2, we will show that there exists an upper bound on $I(U_1^K; \hat{U}_1^K)/N$ which is strictly less than the capacity of the channel for parallel concatenation of any encoders and for serial concatenation when the inner code is a finite-memory convolutional code of rate $R_{in} = M/N$ smaller than 1. Therefore, the condition (2) cannot be fulfilled for $R = C$ and these coding systems cannot approach capacity for this channel.

3. Markov Model Analysis for Serial Concatenation

We will start by treating the case of serial concatenation.

Let m be the memory (or maximum constraint length) of the rate $R_{in} = b/c$ inner convolutional encoder. We assume binary convolutional encoders throughout this paper. We define $\mu = km/R_{in}$. Let us consider the entropy of a block of L output symbols of the encoder when the initial state of the encoder is unknown. For this case, the following inequality holds

$$H(X_1^L) \leq \mu + (L-\mu)R_{in}. \tag{3}$$

To understand why this inequality holds, consider a feedforward systematic encoder: after observing the first μ symbols, we know the state of the encoder and our uncertainty about the remaining $L-\mu$ symbols is our uncertainty about the input sequence. For non-systematic encoders or recursive systematic encoders, the same inequality can be shown. In all cases, if the initial state is known, $H(X_1^L) = LR_{in} < \mu + (L-\mu)R_{in}$, so (3) still holds.

Let the channel be a binary erasure channel with erasure probability δ and let $E_1 \dots E_N$ be the erasure sequence of the channel, i.e., $E_i = 1$ if the i-th symbol is erased and $E_i = 0$ if it isn't. We can write

$$\begin{aligned} I(X_1^N; Y_1^N) &= H(Y_1^N) - H(Y_1^N|X_1^N) \\ &= H(Y_1^N|E_1^N) + H(E_1^N) - \\ &\quad H(E_1^N|Y_1^N) - Nh(\delta) \\ &= H(Y_1^N|E_1^N), \end{aligned} \tag{4}$$

where $h(.)$ denotes the binary entropy function and the last equation holds because $H(E_1^N) = Nh(\delta)$ and $H(E_1^N|Y_1^N) = 0$, since the channel output sequence determines the erasure sequence. We can develop $H(Y_1^N|E_1^N)$ to obtain

$$\begin{aligned} &I(X_1^N; Y_1^N) = (1-\delta)^N H(X_1^N) + \\ &\delta(1-\delta)^{N-1}[H(\neg X_1) + H(\neg X_2) + \ldots + H(\neg X_N)] \\ &+\delta^2(1-\delta)^{N-2}[H(\neg X_1 X_2) + H(\neg X_1 X_3) + \ldots \\ &\quad +H(\neg X_{N-1} X_N)] \\ &+\ldots \\ &+\delta^{N-2}(1-\delta)^2[H(X_1X_2) + H(X_1X_3) + \ldots \\ &\quad +H(X_{N-1}X_N)] + \\ &\delta^{N-1}(1-\delta)[H(X_1) + H(X_2) + \ldots H(X_N)], \end{aligned} \tag{5}$$

where the notation $H(\neg X_i X_j)$ is used to denote the entropy of the block X_1^N with the i-th and the j-th symbol missing.

We now restrict our attention to the binary erasure channel with erasure probability $\delta = 1/2$. All the factors $\delta^i(1-\delta)^{N-i}$ in (5) simplify to 2^{-N}. The first term in the sum can be upper bounded using (3). The difficulty in bounding the remaining terms lies in evaluating the entropies of blocks with gaps, such as $H(X_1^i X_j^N)$. If $i > \mu$ and $N - j > \mu$, we can write

$$\begin{aligned} H(X_1^i Y_j^N) &= H(X_1^i) + H(X_j^N|X_1^i) \\ &\leq H(X_1^i) + H(X_j^N) \\ &\leq 2\mu + (N-j+i-2\mu+1)R_{in} \end{aligned}$$

where we have used (3) twice in the last step. From this example, we learn that symbols that are at most μ positions from the beginning of the block or from the end of a gap contribute 1 bit to the upper bound, whereas symbols that are more than μ positions away from the beginning of the block and from the end of a gap contribute R_{in} bits to the upper bound.

If we now write out (5) as a sum of conditional entropies of single random variables, we obtain

$$\sum_{k=0}^{N} \binom{N}{k} k = N2^{N-1}$$

terms. Some of these terms, say $A(N)$ in total, contribute 1 bit to the expression in the sense described above, while the remaining terms, say $B(N)$ in total, contribute R_{in} bits to the expression. For $N = \mu$, we have $A(N) = N2^{N-1}$ and $B(N) = 0$. The following lemma allows us to compute $B(N)$ recursively:

Lemma 1

$$B(N+1) = 2B(N) + 2^{N-\mu},$$

for $N > \mu$.

The recursive equation in the lemma results in the equation

$$B(N) = (N-\mu)2^{N-\mu-1} \tag{6}$$

and, since $A(N) + B(N) = N2^{N-1}$,

$$A(N) = [\mu + N(2^\mu - 1)]2^{N-\mu-1}. \tag{7}$$

We can now write

$$\begin{aligned} I(X_1^N; Y_1^N) &\leq A(N) + R_{in}B(N) = \\ &= \frac{N2^\mu - N + \mu}{2^{\mu+1}} + R_{in}\frac{N-\mu}{2^{\mu+1}}. \end{aligned} \tag{8}$$

Equations 8 and 1 allow us to determine a lower bound on the gap to capacity, which is specified as follows

$$C - \frac{1}{N} I(U_1^K; \hat{U}_1^K) \geq \frac{N-\mu}{N} \frac{1-R_{in}}{2^{\mu+1}}. \tag{9}$$

Taking the limit, we obtain the following theorem:

Theorem 1 *For the binary erasure channel with erasure probability* $1/2$ *and capacity* $C = 1/2$,

$$C - \lim_{\substack{N\to\infty \\ K/N=R}} \frac{1}{N} I(U_1^K; \hat{U}_1^K) \geq \frac{1 - R_{in}}{2^{\mu+1}}. \quad (10)$$

In other words, it is not possible to achieve arbitrarily reliable transmission with serially concatenated encoders for rates above $C - (1 - R_{in})2^{-\mu-1}$, *even using ideal interleavers and interleaver blocklengths going to infinity.*

The gap to capacity vanishes when an inner encoder of rate $R_{in} = 1$ is chosen, confirming the experience of many researchers who observed this effect through simulation and convergence analysis of iterative decoders. It is interesting to notice that the gap also becomes smaller if the constraint length of the inner encoder is increased. Unfortunately, this is a "catch 22" situation: by increasing the constraint length, the performance can approach capacity using an ideal joint decoder; on the other hand, increasing the constraint length will increase the complexity of the decoder, which is precisely what iterative decoding is designed to avoid. In addition, unless the interleaver blocklength is chosen to be tremendously large, cycles will appear in the associated factor graph when the constraint length of a constituent encoder is increased and the convergence of iterative decoding will be impaired as a result.

4. The Data Processing Theorem for Parallel Concatenation

For parallel concatenation, the case represented in Figure 2 is of one (possibly punctured) systematic encoder with rate $R_1 = K/M$ in parallel with another (possibly punctured) encoder with rate $R_2 = K/(N - M)$. The overall rate of the encoder is $R = K/N$. Without loss of generality, we assume that $R_1 \leq 1$.

For a BEC with erasure probability δ, (4) holds. For parallel concatenation, we can write

$$\begin{aligned} H(Y_1^N|E_1^N) &= H(Y_1^M|E_1^N) + H(Y_{M+1}^N|E_1^N Y_1^M) \\ &\leq H(Y_1^M|E_1^M) + H(Y_{M+1}^N|E_{M+1}^N) \\ &\leq H(Y_1^M|E_1^M) + (N - M)(1 - \delta). \end{aligned}$$

Now we can use the analysis we applied for the inner encoder of serially concatenated codes to evaluate $H(Y_1^M|E_1^M)$. The only difference here is that the output of the convolutional Encoder 1 has been punctured to produce the codeword X_1^M. Equation 3 assumed no puncturing of the convolutional encoder outuput. Now if the encoder were a systematic direct-form encoder and no systematic bits had been punctured, then it is clear that (3) still holds. For a recursive systematic encoder with regular or random puncturing, it is possible to show that (3) also holds. It is not clear whether (3) holds for every puncturing strategy and there could be "malevolent" puncturing strategies where (3) does not hold. If we assume regular or random puncturing, we can apply the analysis used for the inner encoder for serially concatenated coding to yield, for $\delta = 1/2$,

$$H(Y_1^M|E_1^M) \leq \frac{M2^\mu - M + \mu}{2^{\mu+1}} + R_1 \frac{M - \mu}{2^{\mu+1}}. \quad (11)$$

Therefore, we conclude that

$$I(X_1^N; Y_1^N) \leq \frac{M2^\mu - M + \mu}{2^{\mu+1}} + R_1 \frac{M - \mu}{2^{\mu+1}} + \frac{N - M}{2}, \quad (12)$$

which in turn implies that

$$C - \frac{1}{N} I(U_1^K; \hat{U}_1^K) \geq \frac{M - \mu}{N} \frac{1 - R_1}{2^{\mu+1}}. \quad (13)$$

Taking the limit, we obtain the following theorem similar to the theorem we obtained for serially concatenated codes:

Theorem 2 *For the binary erasure channel with erasure probability* $1/2$ *and capacity* $C = 1/2$,

$$C - \lim_{\substack{N\to\infty \\ K/N=R}} \frac{1}{N} I(U_1^K; \hat{U}_1^K) \geq \frac{R}{R_1} \frac{1 - R_1}{2^{\mu+1}}. \quad (14)$$

In other words, it is not possible to achieve arbitrarily reliable transmission with parallel concatenated encoders for rates above $C - R/R_1\,(1 - R_1)2^{-\mu-1}$, *even using ideal interleavers and interleaver blocklengths going to infinity.*

We see that the rate loss in the case of parallel concatenated encoders is positive for all $R_1 \leq 1$, but since this is true by design, capacity can never be achieved using parallel concatenation for this particular channel. Again, capacity can be approached by increasing μ, but we run into the "catch 22" situation already described for serial concatenation: although the encoder is improved in principle by increasing μ, the complexity and performance of iterative decoding will suffer as a result.

5. Conclusion

We have shown that parallel concatenation and serial concatenation with inner codes of rate $R_{in} < 1$ have an inherent rate loss that prevents then from approaching capacity for the binary erasure channel with erasure probability 1/2. We hope to generalize this result to all binary erasure channels but we have not been able to evaluate the combinatorial expressions for $\delta \neq 1/2$ until now.

The bounds obtained can also be used to derive lower bounds on error probabilities for the encoders considered in the region of the gap below capacity. These error bounds can be derived using Fano's inequality. Furthermore, an alternative approach to the one presented here for bounding the mutual information consists in applying Viterbi's sphere-packing bound to obtain a lower bound on the error probability, and deriving an upper bound on the mutual information from this. This approach is currently under investigation.

Acknowledgements

The author wishes to thank Dr. Gerhard Kramer for his help and advice concerning the content and the formulation of this paper.

REFERENCES

[1] A. Ashikhmin, G. Kramer & S. ten Brink, "Code Rate and the Area under Extrinsic Information Transfer Curves," *2002 IEEE International Symposium on Information Theory,* June 30 -July 5, 2003, Lausanne, Switzerland.

[2] A. Ashikhmin, G. Kramer & S. ten Brink, "Extrinsic Information Transfer Functions: Model and Erasure Channel Properties," *Submitted to IEEE Trans. on Information Theory,* March 2003.

[3] Robert G. Gallager (1968), *Information Theory and Reliable Communications*, John Wiley and Sons, ISBN 0-471-29048-3.