

Channel Coding Theory: Exercises

Laura Cottatellucci

I. BLOCK CODES

Exercise 1

Given a BSC $p(y/x)$ with error probability $p = 0.1$, we consider a transmission through the concatenation channel $p_c(y'/x)$ shown in Figure 1. The information bits are encoded by the following randomly generated codebook (7,3):

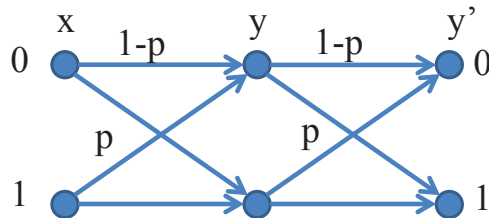


Fig. 1. Concatenated Binary Symmetric Channels

$$\mathcal{C} = \{0010000, 1001011, 0010101, 0001110, 1011001, 1000001, 0001111, 1000100\}.$$

We refer to the first, second, etc, codeword as codeword with index 1, 2, etc, respectively.

The Hamming distances between pairs of codewords are shown in the following table.

Institute Eurecom, Mobile Communications, Sophia Antipolis, France (email: laura.cottatellucci@ftw.at)

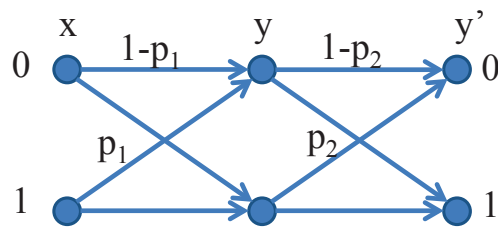


Fig. 2. Concatenated Binary Symmetric Channel

<i>index</i>	1	2	3	4	5	6	7	8
1	0	5	2	4	3	3	5	3
2	5	0	5	3	2	2	2	4
3	2	5	0	4	3	3	3	3
4	4	3	4	0	5	5	1	3
5	3	2	3	5	0	2	4	4
6	3	2	3	5	2	0	4	2
7	5	2	3	1	4	4	0	4
8	3	4	3	3	4	2	4	0

- 1) Determine $p_c(y'|x)$, the BSC equivalent to the concatenation of the two identical BSCs $p(y|x)$.
- 2) What is the minimum distance of the code?
- 3) Under the assumption that the transmitted information messages are equally distributed determine the probability of undetected errors.
- 4) Provide an example of an error pattern with weight 1 that determines an undetected error.

Exercise 2

Consider a BSC in Figure 2 obtained by the concatenation of two BSCs, with error probability p_1 and p_2 .

- 1) Determine the error probability of the equivalent concatenated BSC channel.
- 2) Provide the expression of the capacity of the concatenated BSC.
- 3) Assume $p_1 = 10^{-1}$ and $p_2 = 2 * 10^{-1}$. Does the capacity of the concatenated BSC is higher, equal, or lower than the capacity of a BSC with error probability $p = 3 * 10^{-1}$?

Exercise 3 An $(8,1)$ code consists of the all 0s word and the all 1s word.

What is the weight distribution of the dual code?

Exercise 4

- Consider the following codebooks

$$\mathcal{C}_1 = \{(00000), (11001), (01100), (11111)\}$$

$$\mathcal{C}_2 = \{(00000), (11001), (00110), (11111)\}$$

$$\mathcal{C}_3 = \{(00000), (10101), (01010), (11111)\}$$

which of them is a linear block code? Explain why, eventually, they are not linear block code.

- Provide the generator matrix of a linear block code in the previous item (if there are more than one, you choose one and indicate the codebook for which you provided the generator matrix).
- Given the codebook $\mathcal{C}^* = \{101101, 111111\}$ add one or more codewords such that the resulting codebook is linear.

Exercise 5

Consider a systematic $(8, 4)$ code whose parity-check equations are

$$v_0 = u_1 + u_2 + u_3$$

$$v_1 = u_0 + u_1 + u_2$$

$$v_2 = u_0 + u_1 + u_3$$

$$v_3 = u_0 + u_2 + u_3$$

where u_0, u_1, u_2 , and u_3 , are message digits, and v_0, v_1, v_2 , and v_3 are parity check digit. Find the generator and the parity check matrix of this code. Show analytically that the minimum distance of this code is 4.

Exercise 6

Construct an encoder for the code given in the previous exercise.

Exercise 7

Construct a syndrome circuit for the code given in Exercise 5.

Exercise 8

Consider a systematic $(8, 4)$ code given in exercise 5. Suppose that the code is used for BSC with $\varepsilon = 10^{-2}$.

- Provide the probability of undetected errors of the code. Is the code performing better or worse than the average of the $(8, 4)$ linear codes?

- This code is capable of correcting 16 error patterns. Device a decoder for this code based on the look up decoding scheme. The decoder is designed to correct the 16 most probable error patterns.
- Provide the error probability of the error correcting decoder.
- Write the dual code and provide the undetected error probability of the dual code.

Exercise 9

Let \mathbf{H} be the parity check matrix of an (n, k) code C that has both odd- and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix:

$$\mathbf{H}_1 = \left(\begin{array}{c|cccc} 0 & & & & \\ 0 & & & & \\ \vdots & & \mathbf{H} & & \\ 0 & & & & \\ \hline 1 & 1 & 1 & \dots & 1 \end{array} \right)$$

(Note that the last row of \mathbf{H}_1 consists of all 1's)

- Show that C_1 is an $(n+1, k)$ linear code. C_1 is called the extension of C .
- Show that every codeword of C_1 has even weight.
- Show that C_1 can be obtained from C by adding an extra parity-check digit, denoted by v_∞ , between the systematic part and the parity check part of each codeword \mathbf{v} , as follows: (1) if \mathbf{v} has odd weight, then $v_\infty = 1$, and (2) if \mathbf{v} has even weight, then $v_\infty = 0$. The parity-check digit v_∞ is called an overall parity-check digit.

Exercise 10

Let C be a linear code with both even- and odd-weight codewords. Shows that the number of even-weight codewords is equal to the number of odd-weight codewords.

Exercise 11 Let C be an $(16, 8, 4)$ code over a binary field \mathbb{F} . A codeword of C is transmitted over a BSC with crossover probability $p = 10^{-2}$.

- 1) Compute the rate of C .
- 2) Given a word $\mathbf{r} \in \mathbb{F}^{16}$, show that if there is a codeword $\mathbf{c} \in C$ such that $d(\mathbf{c}, \mathbf{r}) \leq 1$ then every other codeword $\mathbf{c}' \in C \setminus \{\mathbf{c}\}$ must satisfy $d(\mathbf{r}, \mathbf{c}') \geq 3$.
- 3) Compute the probability of having exactly two errors in the received word.

- 4) Compute the probability of having exactly three or more errors in the received word.
- 5) The following decoder $\mathcal{D} : \mathbb{F}^{16} \rightarrow \mathcal{C} \cup \{“e”\}$ is applied to the received word:

$$\mathcal{D}(\mathbf{r}) = \begin{cases} \mathbf{c}, & \text{if there is } \mathbf{c} \in \mathcal{C} \text{ such that } d(\mathbf{r}, \mathbf{c}) \leq 1; \\ “e”, & \text{otherwise.} \end{cases} \quad (1)$$

Compute the decoding error probability of \mathcal{D} ; namely, compute the probability that \mathcal{D} produces either “e” or a wrong codeword.

- 6) Show that the value computed in item 4 bounds from above the probability that the decoder \mathcal{D} in item 5 produces a wrong codeword.

Exercise 12

Let \mathcal{C}_1 and \mathcal{C}_2 be linear codes of the same length n over $F = GF(2)$ and let \mathbf{G}_1 and \mathbf{G}_2 be generator matrices of \mathcal{C}_1 and \mathcal{C}_2 , respectively. Define the following codes

- $\mathcal{C}_3 = \mathcal{C}_1 \cup \mathcal{C}_2$
- $\mathcal{C}_4 = \mathcal{C}_1 \cap \mathcal{C}_2$
- $\mathcal{C}_5 = \mathcal{C}_1 + \mathcal{C}_2 = \{\mathbf{v}_1 + \mathbf{v}_2 : \mathbf{v}_1 \in \mathcal{C}_1 \text{ and } \mathbf{v}_2 \in \mathcal{C}_2\}$
- $\mathcal{C}_6 = \{(\mathbf{v}_1 | \mathbf{v}_2) : \mathbf{v}_1 \in \mathcal{C}_1 \text{ and } \mathbf{v}_2 \in \mathcal{C}_2\}$ (here $(\cdot | \cdot)$ stands for concatenation of words).

For $i = 1, 2, \dots, 6$, denote by k_i the dimension $\log_2 |\mathcal{C}_i|$. Assume that both k_1 and k_2 are greater than zero.

- 1) Show that \mathcal{C}_3 is linear if and only if either $\mathcal{C}_1 \subseteq \mathcal{C}_2$ or $\mathcal{C}_2 \subseteq \mathcal{C}_1$.
- 2) Show that the codes \mathcal{C}_4 , \mathcal{C}_5 , and \mathcal{C}_6 are linear.
- 3) Show that if $k_4 > 0$ then $d_4 \geq \max\{d_1, d_2\}$.
- 4) Show that $k_5 \leq k_1 + k_2$ and that equality holds if and only if $k_4 = 0$.
- 5) Show that $d_5 \leq \min\{d_1, d_2\}$.
- 6) Show that

$$\begin{pmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{pmatrix}$$

is a generator matrix of \mathcal{C}_6 and so $k_6 = k_1 + k_2$.

- 7) Show that $d_6 = \min\{d_1, d_2\}$.

Exercise 13

Let S denote the memoryless binary erasure channel with input alphabet $F = \{0, 1\}$ and output alphabet $\Phi = F \cup \{\Delta\}$, and erasure probability $p = 0.1$. A codeword of the binary $(4, 3)$ parity check code \mathcal{C} is transmitted through S and the following decoder $\mathcal{D} : \Phi^4 \rightarrow \mathcal{C} \cup \{\Delta\}$ is applied to the received word

$$\mathcal{D}(\mathbf{y}) = \begin{cases} \mathbf{c}, & \text{if } \mathbf{y} \text{ agrees with exactly one } \mathbf{c} \in \mathcal{C} \text{ on the entries in } F; \\ \Delta, & \text{otherwise.} \end{cases}$$

- 1) Compute the probability that \mathcal{D} produces Δ .
- 2) Does this probability depend on which codeword is transmitted?
- 3) Compute the probability that \mathcal{D} produces Δ when instead of using the parity check code the code $\mathcal{C} = \{0000, 0111, 1011, 1101\}$ is adopted. Does this probability depend on which codeword is transmitted?

Hints: (1) For the first two items you may make use of the properties of the parity check code that we studied. (2) For the third item, observe that the code is not linear and you need to make specific observations on the structure of the codewords.

Exercise 14 with numerical simulations

Consider the communication system shown in Figure 3.

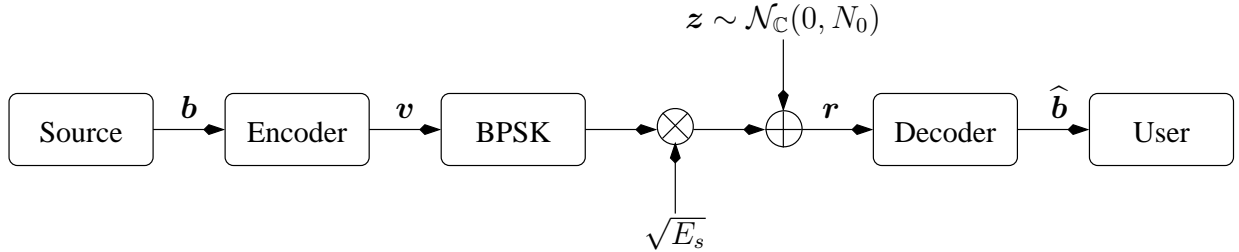


Fig. 3. Communication system

A source generates sequences of $K = 4$ information bits $\mathbf{b}[i]$ which are encoded with a binary linear code in exercise 1.

The encoded output sequence $\mathbf{v}[i]$, is sent to a BPSK modulator with mapping rule $\mu : \{0, 1\} \rightarrow \{-1, +1\}$ and then transmitted through an AWGN channel with power spectral density N_0 . Let $\mathbf{r}[i] = \sqrt{E_s}\mu(\mathbf{v}[i]) + \mathbf{z}[i]$ be the received sequence where $\mathbf{z}[i] = [z_1[i], z_2[i], \dots, z_n[i]]$ is the noise with $z_j[i], j = 1, \dots, n$, i.i.d. and $z_j[i] \sim \mathcal{N}(0, N_0)$. The received sequence \mathbf{r} is the input of a decoder. The decoder provides the user with the decoded information sequence $\hat{\mathbf{b}}$.

- Plot the undetected error probability of an error detection decoder versus¹ $\frac{E_b}{N_0}$ (expressed in dB) in the range $\frac{E_b}{N_0}|_{dB} \in [-2, 12]$.
- Plot the error correction probability of the decoder designed in Exercise 8 versus $\frac{E_b}{N_0}$ (expressed in dB) in the range $\frac{E_b}{N_0}|_{dB} \in [-2, 12]$.

Exercise 15

A $(5, 3)$ block code is defined through the correspondence given in the following table

u_1	u_2	u_3	v_1	v_2	v_3	v_4	v_5
1	1	0	1	0	1	0	1
1	0	1	0	1	0	1	0
0	1	0	0	1	1	0	0

Determine the generator matrix.

Exercise 16

A $(6, 2)$ block code has the following parity check matrix

$$\mathbf{H} = \begin{pmatrix} h_1 & 1 & 0 & 0 & 0 & 1 \\ h_2 & 0 & 0 & 0 & 1 & 1 \\ h_3 & 0 & 0 & 1 & 0 & 1 \\ h_4 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

- 1) Choose the h 's in such a way that $d_{\text{MIN}} \geq 3$.
- 2) Obtain the generator matrix of the equivalent systematic code and list the 4 code words.

Exercise 17

A systematic $(10, 3)$ linear block code is defined by the following parity check equations:

¹Not $\frac{E_s}{N_0}$!

$$v_1 + v_3 + v_4 = 0$$

$$v_5 + v_3 = 0$$

$$v_6 + v_1 + v_3 = 0$$

$$v_7 + v_2 + v_3 = 0$$

$$v_8 + v_1 + v_2 = 0$$

$$v_9 + v_2 = 0$$

$$v_{10} + v_1 + v_2 = 0$$

- 1) Determine the weight distribution of this code.
- 2) Find the percentage of error patterns with 1, 2, 3, 4, 5, 6, 7, 8, 9 error patterns that can be detected by the decoder.
- 3) Compute the probability of an undetected error.
- 4) Device the encoder.
- 5) Device the syndrome circuit.

Exercise 18

Consider the (8,4) linear systematic code with generator matrix

$$C = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Determine the Weight Enumerating Function (WEF), the minimum distance, and the error detection probability. Write the standard array and devise the corresponding error correcting decoder detailing the look-up table.

Exercise 19

A (5, 2) linear block code is defined by the following table

u_1	u_2	v_1	v_2	v_3	v_4	v_5
0	0	0	0	0	0	0
0	1	0	1	1	0	1
1	0	1	0	1	1	1
1	1	1	1	0	1	0

- 1) Find the generator matrix and the parity check matrix of the code.
- 2) Build the standard array and the decoding table to be used on a BSC.
- 3) What is the probability of making errors in decoding a codeword assuming an error detection strategy of the decoder?
- 4) What if we assume error correction capability?

Exercise 20

Given the linear $(15, 4)$ linear encoder defined by the following table

u_1	u_2	u_3	u_4	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}	v_{15}
0	0	0	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
1	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0	0
0	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1
0	0	1	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1

- 1) Find the generator matrix of such an encoder.
- 2) Write the equivalent code with systematic generator matrix.
- 3) write the parity check equations of the equivalent code.
- 4) What is the probability of making errors in decoding a codeword assuming an error detection strategy of the decoder and transmission over a BSC with error probability $\varepsilon = 10^{-2}$?
- 5) Provide an upper bound of making errors when adopt an error correction decoder and transmission over an BSC with error probability $\varepsilon = 10^{-2}$?

II. CYCLIC CODES

Exercise 21

Consider the generator polynomial

$$g(X) = X + 1$$

- 1) Show that it generates a cyclic code of any length.
- 2) Obtain the parity check polynomial $h(X)$, the parity check matrix \mathbf{H} , and the generator matrix \mathbf{G} .

Exercise 22

Given the $(7, 4)$ Hamming code generated by the polynomial

$$g(X) = X^3 + X + 1$$

obtain the code generated by

$$g(X) = (X + 1)(X^3 + X + 1).$$

- 1) How it is related to the original $(7, 4)$ code?
- 2) What is its minimum distance?
- 3) Show that the new code can correct all single errors and simultaneously detect all double errors.

Exercise 23

A cyclic code is generated by

$$g(X) = X^8 + X^7 + X^6 + X^4 + 1.$$

- 1) Find the length n of the code.
- 2) Sketch the encoding circuit with k and $n - k$ shift register.

Exercise 24

Show that the $(7, 4)$ code generated by the polynomial

$$g^{(d)}(X) = X^3 + X + 1$$

is the dual of the $(7, 3)$ code generated by

$$g(X) = X^4 + X^3 + X^2 + 1.$$

Exercise 25

Consider the $(15, 11)$ cyclic Hamming code generated by the polynomial

$$g(X) = X^4 + X + 1.$$

- 1) Determine the parity polynomial $h(X)$ of this code.
- 2) Determine the generator polynomial of its dual code.
- 3) Find the generator and the parity check matrix in systematic form of this code.

Exercise 26

Devise an encoder and a decoder for the $(15, 11)$ cyclic Hamming code generated by

$$g(X) = X^4 + X + 1.$$

Exercise 27

Show that

$$g(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$$

generates a $(21, 11)$ cyclic code. Devise a syndrome circuit for this code. Let $r(X) = 1 + X^2 + X^{17}$ be a received polynomial. Compute the syndrome of $r(X)$. Display the content of the syndrome circuit after each digit of r has been shifted into the syndrome computation circuit.

Exercise 28

Let $g(X)$ be the generator polynomial of a binary cyclic code of length n .

- 1) Show that if $g(X)$ has $X + 1$ as a factor the code contains no codeword of odd weight.
- 2) If n is odd and $X + 1$ is not a factor of $g(X)$ show that the code contains a codeword consisting of all 1's.

Exercise 29

The polynomial $X^{15} + 1$ when factored yields

$$X^{15} + 1 = (X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 + X + 1)(X^2 + X + 1)(X + 1).$$

Consider the generator polynomial

$$g(X) = (X^4 + X^3 + X^2 + X + 1)(X^4 + X + 1)(X^2 + X + 1).$$

- 1) Write the generator matrix of a systematic (15,5) code with generator polynomial $g(X)$.
- 2) Is the polynomial $X^{13} + X^{12} + X^9 + X^8 + X^7 + X^4 + X^2 + 1$ a code polynomial? What is its syndrome?
- 3) Determine the weight distribution of the code. What is the minimum distance of the code?
- 4) Assume that the code is used for transmission over a binary symmetric channel with error probability p . Determine the probability that transmission errors are not detected.
- 5) Assume that the code is used for transmission over a BIAWGN channel. The symbols are transmitted with energy E and the additive white Gaussian noise channel has variance σ^2 . Provide an upper bound of the error correction probability.
- 6) Consider the burst correction capabilities of the code. How many error bursts of length ℓ , with $\ell = 1, \dots, 15$ can be detected?

Hints: (1) For item 3, it is not required to list all the codewords. Properties of the cyclic codes can be efficiently applied to determine the weight distribution of the code.

Exercise 30

Given the cyclic code with generator polynomial $(6, 5)_8$ (octal notation) determine:

- 1) The weight enumerating function (WEF).
- 2) The minimum distance.
- 3) The probability of undetected errors assuming a binary symmetric channel (BSC) with $\varepsilon = 10^{-2}$.
- 4) Find the percentage of error patterns with 3 and 4 errors that cannot be detected by the code (assume an error detection strategy).
- 5) Find the fraction of undetectable bursts of length 12 and motivate the result.

Note: the code parameters (n, k) are not given but you can determine them.

Hints: In order to determine the WEF work on the dual code. Take into account the fundamental properties of linear cyclic codes. Take into account that if the codeword length n is odd and $X + 1$ is not a factor of $g(X)$ the code contains a codeword consisting of all 1's.

Recall: $(a + b)^n = \sum_{j=0}^n \binom{n}{j} a^{n-j} b^j.$

Exercise 31

Given the cyclic code in the previous exercise draw the corresponding Meggitt decoder. Describe in detail how to determine the error pattern detection circuit.

Exercise 32

Given the $(21,16)$ cyclic code \mathcal{C} with generator polynomial $g(x) = x^5 + x^4 + 1$ determine:

- 1) The generator polynomial of the dual code.
- 2) The WEF of the dual code.
- 3) The WEF of the original code.
- 4) Find the fraction of undetectable bursts of length 10 in \mathcal{C} and motivate the result.

Hints: In order to determine the WEF work on the WEF of the dual code. Take into account the fundamental properties of linear cyclic codes. Take into account that the data words in polynomial notation $a_1(x) = 1$, $a_2(x) = 1 + x + x^2$, and $a_3(x) = 1 + x^2 + x^3$ are encoded by the dual code into 3 codewords that are **not** one the cyclic shifted version of the others.

Recall: $(a + b)^n = \sum_{j=0}^n \binom{n}{j} a^{n-j} b^j$.

Exercise 33

Given the cyclic code \mathcal{C} in the previous exercise draw an implementation of the encoder with $n - k = 5$ shift registers. Explain how to construct an encoder with $k = 16$ shift registers.

III. FACTOR GRAPHS**Exercise 34**

Draw the FSFG for the Markov chain

$$p_{XYZ}(x, y, z) = p_X(x)p_{Y|X}(y|x)p_{Z|Y}(z|y).$$

Compute the messages at each node to compute all marginals.

Exercise 35

Assume that the two binary symbols x and y are mapped by a function m into one 4-AM symbol, call it z , as in the following table

x	y	$z = m(x, y)$
0	0	1
1	0	2
0	1	3
1	1	4

In more detail, $m : X \times Y \rightarrow Z$. Draw the corresponding FSFG. Starting from the general message passing rule and assuming that the incoming messages are $\mu_{x,m}(x)$, $\mu_{y,m}(y)$, and $\mu_{z,m}(z)$ respectively, what are the outgoing messages $\mu_{m,x}(x)$, $\mu_{m,y}(y)$, and $\mu_{m,z}(z)$?

Exercise 36

Consider a quantizer. Let \mathcal{X} be the finite input alphabet and \mathcal{Y} be the finite output alphabet. Let q be the quantization function $q : \mathcal{X} \rightarrow \mathcal{Y}$. Draw the corresponding FSFG. Starting from the general message passing rule and assuming that the incoming messages are $\mu_{xq}(x)$ and $\mu_{yq}(y)$, respectively what are the outgoing messages $\mu_{qx}(x)$ and $\mu_{qy}(y)$?

Exercise 37

Consider the classical linear state space model

$$X[k] = AX[k-1] + BU[k]$$

$$Y[k] = CX[k-1] + W[k]$$

being $U[k]$ and $V[k]$ white Gaussian processes with mean m_U and m_W and variances σ_U^2 and σ_W^2 , respectively ($U[k] \sim \mathcal{N}(m_U, \sigma_U^2)$ and $W[k] \sim \mathcal{N}(m_W, \sigma_W^2)$).

Draw the FSFG for such a system. Consider that the message passing forwards Gaussian distributions and the Gaussian distributions are completely defined by their means and their variances. Write the message passing rules for the Gaussian distributions as functions of their means and variances.

Assume that the process $Y[0], Y[1], \dots, Y[k]$ is given. The a posteriori probability of $X[k]$ is provided by the Kalman filter given the process $Y[0], Y[1], \dots, Y[k]$. Write the Kalman filter as a sum product algorithm over the factor graph of the classical linear state space model. Show that the sum product algorithm is equivalent to a max product algorithm.

Hint: Look at the provided article: Loeliger, "Introduction to factor graph"

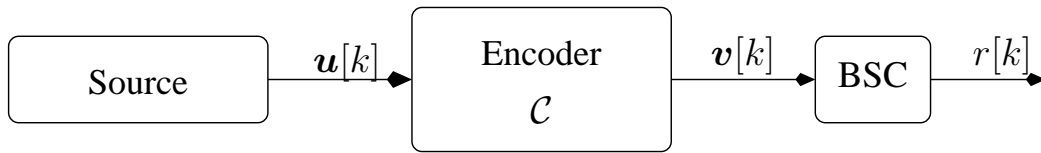


Fig. 4. Point to point system.

Exercise 38

Consider the point to point system in Figure 4 where a source generating i.i.d. equiprobable binary stream transmits through a binary symmetric channel with error probability ε . The datawords \mathbf{u} are encoded by a cyclic codes $\mathcal{C}(15, 5)$ defined by the generator polynomial $g(X) = X^{10} + X^8 + X^5 + X^4 + X^2 + X^1 + 1$. Its generator matrix is given by:

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Let us denote by \mathbf{r} the received signal.

- 1) Write the generator matrix of the code in a systematic form.
- 2) Draw the Tanner graph of the code.
- 3) Write the conditional probability function of the parity check variables $\mathbf{v}_c = (v_0, v_1, \dots, v_9)$ conditioned to the message $\mathbf{u} = (u_0, u_1, u_2, u_3, u_4)$, i.e. $p(\mathbf{v}_c | \mathbf{u})$.
- 4) Write the joint probability $p(\mathbf{v}_c, \mathbf{u})$.
- 5) For the received symbols r_0 and r_{10} write the multivariate probability mass function $f_i(r_i, \mathbf{u}, \mathbf{v})$. Does it factorize?
- 6) Draw the factor graph of $f_i(r_i, \mathbf{u}, \mathbf{v})$.
- 7) Write the expressions for the functions at the factor nodes and label the variable nodes. What is the size of the messages?

Exercise 39

Consider a theoretical multiple access system in Figure 5 with three active users impaired by additive white noise with equiprobable random values $w[k] \in \{\pm 1\}$ (obtained by binary quantization of an additive white

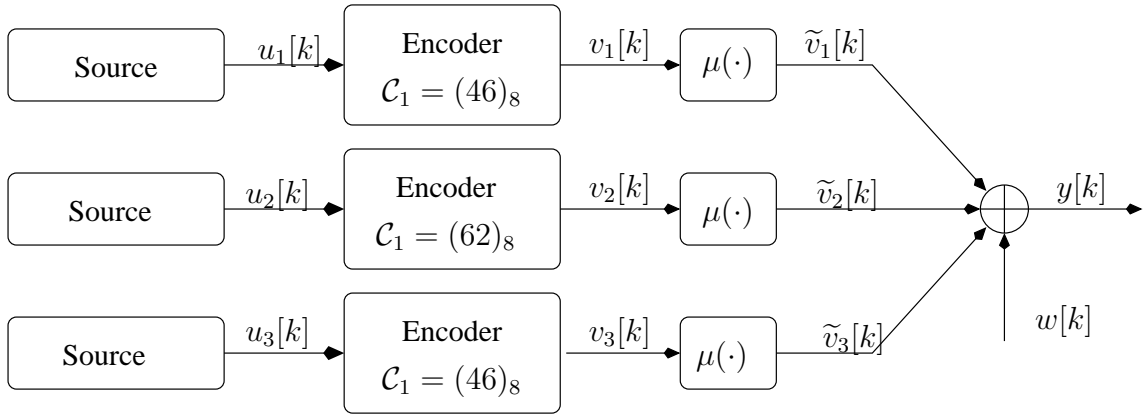


Fig. 5. Multiple access channel

Gaussian channel). The datawords \mathbf{u}_1 , \mathbf{u}_2 , \mathbf{u}_3 are encoded by cyclic codes \mathcal{C}_1 , \mathcal{C}_2 , \mathcal{C}_3 . \mathcal{C}_1 , \mathcal{C}_2 , \mathcal{C}_3 are defined in octal notation by the factors of $(z + 1)^{15}$ $(46)_8$, $(62)_8$ and (46) , respectively. The binary symbols of the codewords \mathbf{v}_1 , \mathbf{v}_2 , \mathbf{v}_3 are mapped by the function $\mu : 0, 1 \rightarrow \{\pm 1\}$ with $\mu(0) = -1$ and $\mu(1) = +1$ and then transmitted synchronously through the multiple access channel.

The k -th received symbol $y[k]$ is given by

$$y[k] = \mu\{v_1[k]\} + \mu\{v_2[k]\} + \mu\{v_3[k]\} + w[k]$$

with $\mathbf{v}_1 = \mathbf{G}_1 \mathbf{u}_1$, $\mathbf{v}_2 = \mathbf{G}_2 \mathbf{u}_2$, $\mathbf{v}_3 = \mathbf{G}_3 \mathbf{u}_3$ and \mathbf{G}_1 , \mathbf{G}_2 , \mathbf{G}_3 the generating matrices.

Draw the joint code/channel factor graph. Write the expressions for the functions at the factor nodes and label the variable nodes. What is the size of the messages?

Exercise 40 Consider a theoretical multiple access system in figure 6 with 3 active users impaired by additive white noise with equiprobable random values $w[k] \in \{\pm 1\}$ (obtained by binary quantization of an additive white Gaussian channel). The datawords u_1 , u_2 , u_3 are encoded by convolutional codes \mathcal{C}_1 , \mathcal{C}_2 , \mathcal{C}_3 defined by:

- $\mathcal{C}_1 \rightarrow (1, 1 + D, 1 + D^2)$
- $\mathcal{C}_2 \rightarrow (1, 1 + D + D^2)$
- $\mathcal{C}_3 \rightarrow (1, 1 + D)$.

The binary symbols of the codewords \mathbf{v}_1 , \mathbf{v}_2 , \mathbf{v}_3 are mapped by the function $\mu : 0, 1 \rightarrow \{\pm 1\}$ with $\mu(0) = -1$ and $\mu(1) = +1$ and then transmitted synchronously through the multiple access channel.

The k -th received symbol $y[k]$ is given by

$$y[k] = \mu\{\mathbf{v}_1[k]\} + \mu\{\mathbf{v}_2[k]\} + \mu\{\mathbf{v}_3[k]\} + w[k]$$

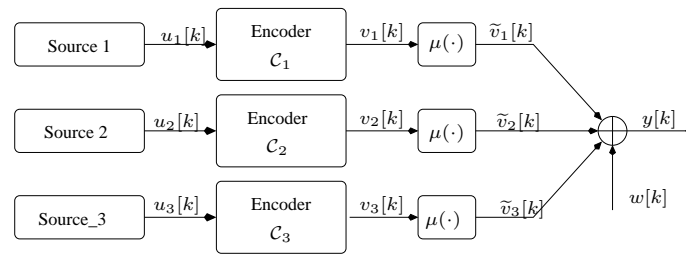


Fig. 6. Multiple access channel

where $+$ is the ordinary sum on the field of integers, and $v_i[k]$ is the k -th bit of the codeword v_i .

- 1) Write the state diagram of the convolutional code C_1 .
- 2) Write a set of equations that describes the encoder C_1 as a finite state machine.
- 3) Determine the linear block codes corresponding to sequences of two bits for C_1 , four bits for C_2 , and five bits for C_3 , (do not forget to append the zero sequence). What is the codeword length?
- 4) Let us assume the use of the linear block codes obtained at the previous item by trellis termination. Draw the joint code/channel factor graph.
- 5) Write the expressions for the kernel functions at the factor nodes and label the variable nodes (Please, be careful in the definition of kernel function at the factor node corresponding to the multiple access channel).
- 6) What is the size of the messages?

Exercise 41 Consider a system consisting of two independent subsystems \mathcal{S}_i , $i = 1, 2$. Subsystem \mathcal{S}_1 has as input a discrete random variable A_1 and as output a binary random variable C_1 . C_1 and A_1 are related by a random function $f_{C_1|A_1}(c_1|a_1)$. Subsystem \mathcal{S}_2 consists of source of i.i.d. binary random variables. The variables c_1, c_2 are combined by the exor function

c_1	c_2	output
0	0	0
0	1	1
1	0	1
1	1	0

and coded by the linear block code defined by the generator matrix

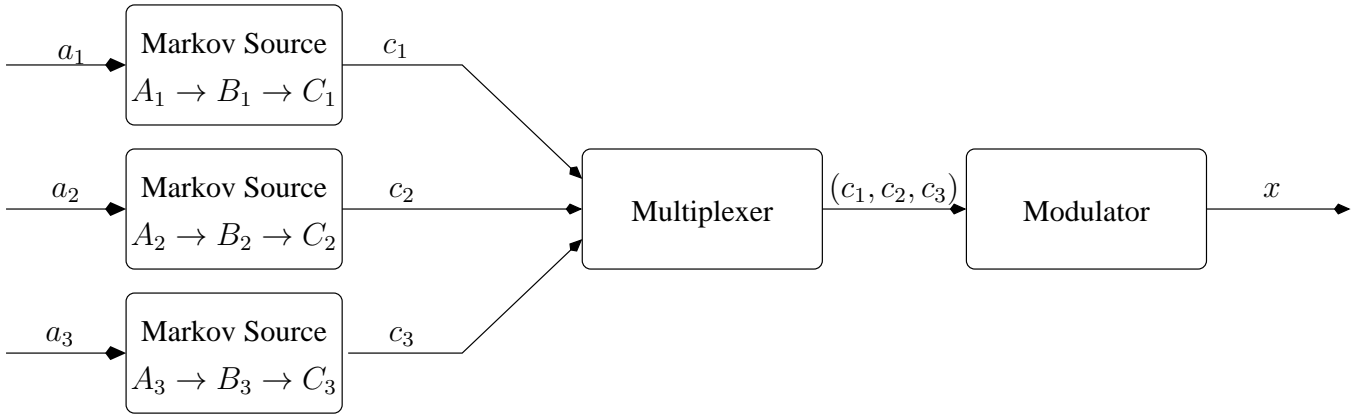


Fig. 7. Modulator of multiplexed Markov sources.

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The outputs of the linear block code are mapped by the function $f(c_{2\ell}, c_{2\ell+1})$, $\ell = 0, \dots, 4$ into an alphabet \mathcal{X} with cardinality $|\mathcal{X}| = 4$. The function $f(c_{2\ell}, c_{2\ell+1})$ is presented in the following table

$c_{2\ell}$	$c_{2\ell+1}$	$x = f(c_{2\ell}, c_{2\ell+1})$
0	0	1
0	1	2
1	0	3
1	1	4.

Draw the factor graph to compute all marginals providing the function at each factor node.

Exercise 42

Consider the system shown in Figure 7.

It consists of three independent subsystems \mathcal{S}_i , $i = 1, \dots, 3$. Subsystem \mathcal{S}_i has as input a discrete random variable A_i and as output a binary random variable C_i . C_i and A_i , $i = 1, \dots, 3$, are related by the Markov chain

$$A_i \rightarrow B_i \rightarrow C_i \quad (2)$$

with joint probability density function $p_{A_i B_i C_i}(a_i b_i c_i) = p_{A_i}(a_i) p_{B_i|A_i}(b_i|a_i) p_{C_i|B_i}(c_i|b_i)$. The variables c_1, c_2, c_3 are multiplexed and mapped by the function $f(c_1, c_2, c_3)$ into an alphabet \mathcal{X} with cardinality $|\mathcal{X}| = 8$. The function $f(c_1, c_2, c_3)$ is presented in the following table

c_1	c_2	c_3	$x = f(c_1, c_2, c_3)$
0	0	0	1
0	1	0	2
0	0	1	3
0	1	1	4
1	0	0	5
1	1	0	6
1	0	1	7
1	1	1	8.

Draw the factor graph to compute all marginals providing the function at each factor node.

Exercise 43 Consider a system consisting of 2 independent subsystems \mathcal{S}_i , $i = 1, 2$. Subsystem \mathcal{S}_1 has as input a discrete random variable A_1 and as output a binary random variable C_1 related by the Markov chain

$$A_1 \rightarrow B_1 \rightarrow C_1 \quad (3)$$

with joint probability density function $p_{A_1 B_1 C_1}(a_1 b_1 c_1) = p_{A_1}(a_1) p_{B_1|A_1}(b_1|a_1) p_{C_1|B_1}(c_1|b_1)$. Subsystems \mathcal{S}_2 consists of a source of i.i.d. binary random variables. The variables c_1, c_2 are combined by the exor function

c_1	c_2	output
0	0	0
0	1	1
1	0	1
1	1	0

and coded by the $R = 2/3$ convolutional code defined by

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & (1+D^2) & (1+D+D^2) \end{array} \right)$$

The outputs of the convolutional code are mapped by the function $f(c_{2\ell}, c_{2\ell+1})$, $\ell = 0, \dots, 6$ into an alphabet \mathcal{X} with cardinality $|\mathcal{X}| = 4$. The function $f(c_{2\ell}, c_{2\ell+1})$ is presented in the following table

$c_{2\ell}$	$c_{2\ell+1}$	$x = f(c_{2\ell}, c_{2\ell+1})$
0	0	1
0	1	2
1	0	3
1	1	4.

Draw the factor graph to compute all marginals providing the function at each factor node.

Hint: To model the convolutional code consider the equivalent $(12, 4)$ linear block code including the zero padding for trellis termination.

Exercise 44

Hansel and Gretel together with all their classmates take a field trip. The forest in which they are walking is so dark that each kid can only see its immediate neighbors. Assume that communication is limited to the nearest neighbors as well and that the whole group of schoolchildren forms a tree (in the graph sense) with respect to this neighborhood structure.

Construct a message passing algorithm which allow them to count to ensure that none of the children was eaten by the wolf. What is the initialization and what are the message passing rules? How do you modify them to count only girls?

Exercise 45

A party elects its leader among two candidates $\{A, B\}$ according to the following mechanism. The party is divided into four groups $\{1, 2, 3, 4\}$, grouped in two sections: Left (groups 1 and 2), and Right (3 and 4). Each of the groups chooses its favorites candidate according to popular vote: we call him $x_i \in \{A, B\}$, with $i \in \{1, 2, 3, 4\}$. Then, the Left candidate y_L , and the Right candidate y_R are decided according to the following rule. If the preferences x_1 and x_2 in groups 1 and 2 agree, then y_L takes the commune value. In they do not agree y_L is decided according to a fair coin trial (randomly assigning to each candidate probability $1/2$ to be selected). The same procedure is adopted for the choice of y_D , given x_3, x_4 . Finally, the leader $z \in A, B$ is decided on the basis of the choices y_L and y_D in the two sections using the same rule as inside each section. A polling institute has obtained fairly good estimates of the probabilities $p_i(x_i)$ for the popular vote in each group i to favor the candidate x_i . You are requested to calculate the probability of

each candidate to become the party leader by using a factor graph. It is clear that the electoral procedure yields a probability distribution that can be factorized as:

$$P(x_1, x_2, x_3, x_4, y_L, y_D, z) = f(z|y_L, y_D)f(y_L|x_1, x_2)f(y_D|x_3, x_4) \prod_{i=1}^4 p_i(x_i).$$

- 1) Write explicit forms for the function f .
- 2) Draw the corresponding factor graph.
- 3) Describe the messages at the output of each node as function of the input messages.
- 4) Compute the probability the candidate A is elected if $p_1(A) = 0.3$, $p_2(A) = 0.8$, $p_3(A) = 0.45$, and $p_4(A) = 0.6$.

Exercise 46

Fred lives in Los Angeles and commute 60 miles to work. Whilst at work, he receives a phone-call from his neighbor saying that the Fred's burglar alarm is ringing. What is the probability that there was a burglar in his house today? While driving back home to investigate, Fred hears on the radio that there was a small earthquake that set off the alarm. What is the probability that there was a burglar in his house? (After Pearl, 1988). Express the joint probability distribution for this problem as a factor graph, and find the marginal probabilities of all the variables as each piece of information comes to Fred's attention using the sum-product algorithm.

Exercise 47 Consider a systematic convolutional code with rate $1/2$. At each time instant, its output consists of a single information bit u_ℓ and a parity check bit v_ℓ . Let us denote with \mathbf{r}^s the received symbols corresponding to transmitted information bit and by \mathbf{r}^p the received symbols corresponding to transmitted parity check bits. Then, the maximum a posteriori (MAP) decoder for the transmitted information bit u_ℓ can

be written in terms of an auxiliary vector variable \mathbf{s} with components s_j as

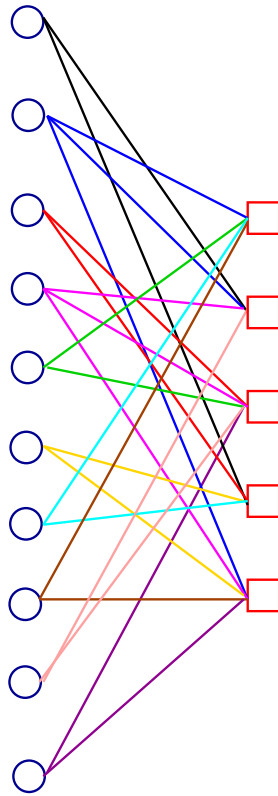
$$\begin{aligned}
 \hat{u}_\ell &= \operatorname{argmax}_{u_\ell \in \{0,1\}} p(u_\ell | \mathbf{r}^s, \mathbf{r}^p) \\
 &= \operatorname{argmax}_{u_\ell \in \{0,1\}} \sum_{\sim u_\ell} p(\mathbf{u}, \mathbf{v}^p, \mathbf{s} | \mathbf{r}^s, \mathbf{r}^p) \\
 &= \operatorname{argmax}_{u_\ell \in \{0,1\}} \sum_{\sim u_\ell} p(\mathbf{r}^s, \mathbf{r}^p | \mathbf{u}, \mathbf{v}^p, \mathbf{s}) p(\mathbf{u}, \mathbf{v}^p, \mathbf{s}) \\
 &= \operatorname{argmax}_{u_\ell \in \{0,1\}} \sum_{\sim u_\ell} p(s_0) \prod_{j=1}^{K+\nu_{MAX}} p(r_j^s | u_j) p(r_j^p | v_j^p) \\
 &\quad \times p(u_j) p(v_j^p, s_j | u_j, s_{j-1})
 \end{aligned}$$

- 1) Draw the corresponding factor graph;
- 2) Does the message passing algorithm applied to the factor graph drawn in the previous item provides exact marginals?
- 3) Describe a scheduling algorithm that enables to determine all the marginals step by step showing the activated nodes.

IV. LDPC CODES

Exercise 48

Consider the Tanner graph in the following figure:



- 1) Write the generator matrix \mathbf{G} .
- 2) Write the variable and check degree distributions $\Lambda(x)$ and $P(x)$ from a node perspective.
- 3) Write the variable and check degree distribution from an edge perspective.
- 4) Find the design rate.
- 5) Draw the directed neighborhood of the edge that connects the first variable node and the second check node of depth 5. Does it contain cycles?
- 6) Determine the density evolution function.
- 7) Give an approximation of the average probability that a message output of a variable node at the 4th decoder iteration is an erasure for $\varepsilon = 0.3$. Under which assumptions is this approximation realistic?
- 8) Determine the threshold ε^{BP} .
- 9) Assume that the vector $\mathbf{r} = (0, \Delta, 0, \Delta, \Delta, 0, 0, 0, 0, 0)$ has been received. Determine the transmitted codeword by applying the message passing algorithm.
- 10) Find a blocking set.
- 11) Assume that the vector $\mathbf{r} = (0, 0, 0, \Delta, \Delta, 0, \Delta, \Delta, 0, 0)$ has been received. Determine the transmitted codeword by applying the message passing algorithm.

Exercise 49

Consider the LDPC code defined by the parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(This is only an academic example...). The code is used for transmission over a BEC.

1) Determine the density evolution function.

2) For the received word

$$\mathbf{y} = [1, \Delta, \Delta, \Delta, \Delta, 1, 0, 0, 0, 1, \Delta, 1, \Delta, \Delta, \Delta, 1]$$

provide the values of the variable nodes for the **first two rounds** of the message passing algorithm (If you prefer, you can avoid to write all the messages passed at each step and just compute them from a factor graph representation in your mind and the parity check matrix. In this case, please provide information about the parity check nodes that provide interesting information at each iteration.)

Exercise 50

- 1) Write a reasonable parity check matrix with 5 rows and 10 columns for an LDPC code such that the design rate surely differs from the rate of the code. Explain the criteria you adopted to build it.
- 2) Why the design rate may differ from the actual rate of the code? When do they differ? Which of them is greater?

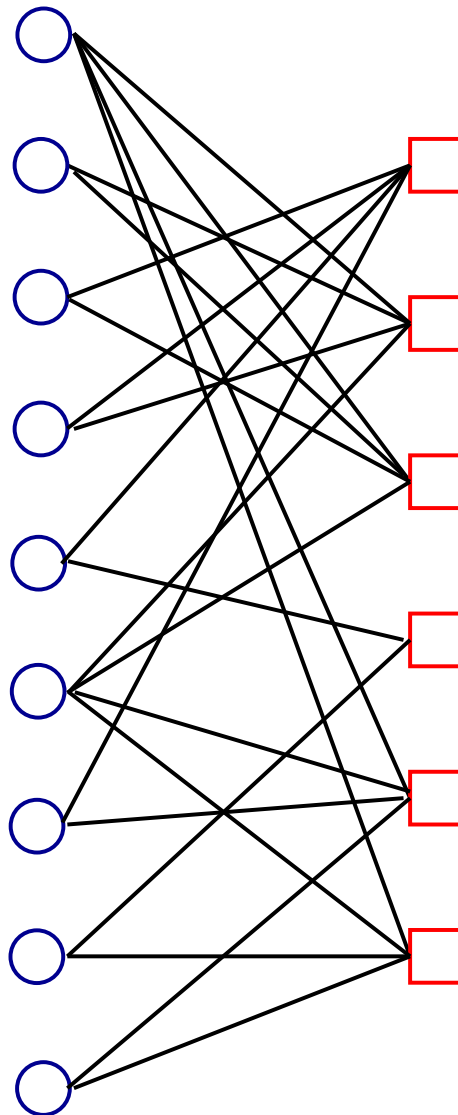
Exercise 51

- A. Given the LDPC ensemble $(\Lambda(x) = 9x^4, P(x) = 6x^6)$ determine the **design rate**.
- B. Consider the realization of the previous LDPC ensemble corresponding to the permutation $\sigma = (9, 13, 25, 36, 7, 8, 10, 14, 1, 15, 16, 17, 2, 3, 4, 11, 5, 19, 20, 21, 12, 18, 26, 32, 6, 27, 28, 29, 22, 23, 24, 33, 30, 34, 35, 31)$ and draw the Tanner graph.
- C. Determine the parity check matrix \mathbf{H} and the **rate** of the corresponding code.
- D. Consider the Tanner graph associated to the parity check matrix \mathbf{H} (Tanner graph without parallel edges) and determine the variable and node distribution from an edge perspective $\lambda(x)$ and $\rho(x)$.
- D. Determine a stopping set with 2 or 3 variable nodes if there is one.
- E. Given the LDPC ensemble $(\lambda(x), \rho(x), n)$ determine the **design rate** and the **rate** as $n \rightarrow +\infty$ (assume that the conditions on the asymptotic relation between rate and design rate are satisfied).
- F. Determine the density evolution function.
- G. Apply the message passing algorithm for the received signal $\mathbf{r} = (0, 0, 0, \Delta, 0, 0, 0, \Delta, \Delta)$.

Exercise 52

Given the Tanner graph in the following figure

Variable Nodes Check Nodes

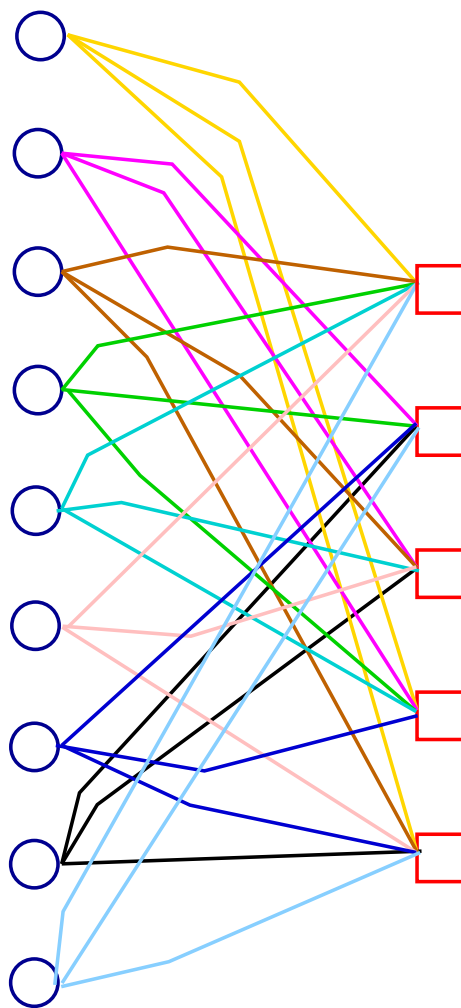


- 1) Describe the corresponding LDPC ensemble in terms of the variable and node distributions from an edge perspective $\lambda(x)$ and $\rho(x)$.
- 2) Determine a stopping set with 2 or 3 variable nodes if there is one.
- 3) Determine the density evolution function.
- 4) Apply the message passing algorithm for the received signal $\mathbf{r} = (0, 0, 0, \Delta, 0, 0, 0, \Delta, \Delta)$.

Exercise 53

Consider the bipartite graph given in the following figure.

Variable Nodes Check Nodes



- A. Identify at least one stopping set with three variable nodes.
- C. Consider the standard ensemble whom the code belongs to. For such standard ensemble and assuming that the codeword length tends to infinity, write the equations of density evolution for a BEC with erasure probability ε .
- D. Determine the equations of the EXIT chart.

Exercise 54 with numerical simulations

Given the irregular LDPC code with the variable-nodes specified in Table I and the check-nodes specified in Table II:

- Provide the variable and check degree distributions from an edge perspective (λ, ρ) .
- Assume that the code is utilized for transmission through a BEC with erasure probability ε . Provide

Degree of variable nodes	Number of variable nodes
2	4448
3	2969
5	676
6	100
7	913
8	99
10	100
12	99
18	100
19	99
30	397

TABLE I

SPECIFICATION OF THE VARIABLE NODES

Degree of check nodes	Number of check nodes
9	1345
10	3464

TABLE II

SPECIFICATION OF THE CHECK NODES

a recursive expression of the erasure probability after k iterations averaged over the standard LDPC ensemble and all possible outputs.

- *Plot the density evolution for $\varepsilon = 0.3; 0.57; 0.9$.*
- *Is it possible to determine all the erasures as $\varepsilon = 0.5$?*

Exercise 55 with numerical simulations

Given the check degree distribution from an edge perspective $\rho(z) = \frac{z^4}{4} + \frac{z^5}{4} + \frac{z^6}{2}$ find a variable degree distribution from an edge perspective which maximizes the transmission rate and enables decoding of all the

transmitted bits over all the erasure channels with erasure probabilities not greater than $\varepsilon^* = 0.6$.

- Compute the design rate of the LDPC ensemble for the variable degree distribution from an edge perspective $\lambda(z)$ determined by linear programming. How it is related to the capacity of a binary erasure channel with erasure probability $\varepsilon^* = 0.6$?
- Plot the density evolution function of the LDPC ensemble for $\varepsilon = 0.4, 0.6, 0.8$.
- Provide some qualitative comment on the convergence rate of a message passing algorithm for such a code and $\varepsilon = 0.4, 0.6, 0.8$. Do you expect it converges? Does it converges quickly?
- Play with your code:
 - What does it change when you increase the number of constraints?
 - What does it change when you keep all parameters fixed and you increase the degree of $\lambda(z)$? How does the design rate of the LDPC ensemble (λ, ρ) vary?

Include your program in the exercise solution.

Hints: increase the number of samples of the density evolution on which you enforce the constraints if your density evolution has a threshold lower than $\varepsilon^* = 0.6$.

You can choose to sample the points to enforce the constraints equally spaced.

Already for $\lambda(z)$ with degree 3, you should be able find an optimum ensemble which satisfies the requirements.

V. CONVOLUTIONAL CODES

Exercise 56

- 1) Consider a 4-PSK-constrained AWGN channel. What is the capacity of the channel in high SNR regime, i.e. for $\frac{E_b}{N_0} \rightarrow +\infty$? And the capacity of a 64-PAM-constrained AWGN channel?
- 2) Given any kind of decoder for a linear (N, K) code, is the bit error rate probability (BER) greater, equal, or lower than the word error rate probability (WER)? Provide an upper bound for the WER as a function of the BER.
- 3) Does a Viterbi algorithm minimize the WER, the BER, or both? Eventually, specify under which conditions it minimizes both BER and WER.

Exercise 57

1) Describe the main differences between the Viterbi algorithm (VA) and the BCJR algorithm (do not describe and detail the algorithms themselves but focus on their properties, features, and peculiarities). When is it convenient to use the VA and when is a BCJR needed?

2) Consider the trellis of a convolutional code at time instant ℓ and denote by \mathbf{s}_ℓ and $\mathbf{s}_{\ell+1}$ the initial and final states. Let $\mathbf{s}_\ell = \mathbf{s}'$ and $\mathbf{s}_{\ell+1} = \mathbf{s}$ be the initial and final state corresponding to a given input and let $\sigma_{\ell-1}$ be the set of all final states $\mathbf{s}_{\ell+1}$. Denote by $\alpha_\ell(\mathbf{s}')$, $\beta_{\ell+1}(\mathbf{s})$, and $\gamma_\ell(\mathbf{s}', \mathbf{s})$ the forward metric, the backward metric, and the branch metric, respectively. Show that the backward recursion is given by

$$\beta_\ell(\mathbf{s}') = \sum_{\mathbf{s} \in \sigma_{\ell+1}} \gamma_\ell(\mathbf{s}', \mathbf{s}) \beta_{\ell+1}(\mathbf{s})$$

and it is initialized by

$$\beta_K(\mathbf{s}') = \begin{cases} 1 & , \mathbf{s} = \mathbf{0} \\ 0 & \text{otherwise.} \end{cases}$$

Hint: A possible proof can follow the same line as the proof for the expression of the forward metric studied during the channel coding course.

Exercise 58

Consider the convolutional code of rate $R = \frac{2}{3}$ defined by

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1+D & ; & 0 & 1+D & D \end{array} \right)$$

- Is the convolutional code systematic?
- Draw the state diagram and the trellis of the code;
- Determine the weight enumerating function.
- Assume a transmission over a memoryless Laplacian channel

$$P_{Y|X}(y|x) = \frac{1}{2} e^{-|y - (-1)^x|}.$$

with $x \in \{0, 1\}$ and determine the branch metric of a Viterbi decoder for such a channel?

- What is the objective function maximized by the Viterbi algorithm?

Exercise 59

Determine the free distance of the rate $R = \frac{1}{2}$ convolutional code $(37, 21)_8$ (octal notation) applying the transfer function method.

Note: Example of a generator polynomial provided in octal notation with the highest-degree term on the left: $(3, 5) \rightarrow X^4 + X^3 + X^2 + 1$.

Exercise 60

Consider the convolutional code with rate $\frac{1}{2}$ and memory $\nu = 2$ with polynomial generators in octal notation $(5, 7)$.

- Write the state diagram of the convolutional code.
- Write a set of equations that describes the encoder as a finite state machine.
- Determine the linear block code corresponding to sequences of three symbols (do not forget to append the zero sequence!)
- Determine the the input output weighting enumerating function (IO-WEF) using the method of the transfer function.
- Describe how to determine a bound on the bit error probability using the IO-WEF.

Exercise 61

Consider the convolutional code defined by the following parameters

Memory	$\nu_\nu = 2$
Rate	$1/n = 1/4$
Generators (octal notation)	$(5, 5, 7, 7)$.

- Write the state diagram of the convolutional code.
- Draw the corresponding encoder.
- Determine the output to the following input sequence 101101100.
- Compute the Input Output Weight Enumerating Function (IO-WEF) making use of the transfer function method.
- Determine the free distance d_{free} .

Exercise 62 with numerical simulations

Consider the communication system shown in Figure 3. A source generates sequences of information bits

Memory	Rate	Generators
ν_ν	$1/n$	(octal notation)
2	1/3	(1,5,7)

TABLE III
CODE PARAMETERS

$b[i]$ which are encoded with a binary convolutional code. The parameters of the convolutional codes are defined in Table III.

The encoded output sequence $\mathbf{v}[i]$, is sent to a BPSK modulator with mapping rule $\mu : \{0, 1\} \rightarrow \{-1, +1\}$ and then transmitted through an AWGN channel with power spectral density N_0 . Let $\mathbf{r}[i] = \sqrt{E_s}\mu(\mathbf{v}[i]) + \mathbf{z}[i]$ be the received sequence where $\mathbf{z}[i] = [z_1[i], z_2[i], \dots, z_n[i]]$ is the noise with $z_j[i], j = 1, \dots, n$, i.i.d. and $z_j[i] \sim \mathcal{N}(0, N_0)$. The received sequence \mathbf{r} is decoded by a Viterbi algorithm. The decoder provides the user with the decoded information sequence $\hat{\mathbf{b}}$.

- Write the state diagram of the convolutional code.
- Consider the transmission of the $K = 3$ bits (101) and assume that $E_s = 1$, $N_0 = 1$, and the received sequence is $\mathbf{r} = (0.5674, -0.6656, 1.1253, -0.7123, -2.1465, 2.1909, 2.1892, 0.9624, -0.6727, -0.8254, -1.1867, 1.7258, -1.5883, 3.1832, 0.8636)$. Draw the trellis of the code. At each stage and for each state determine the survivor path and the corresponding metric. The Viterbi decoder decodes correctly the transmitted codeword?
- Compute the bounds on the BER via the symbolic transfer function method described below.

Numerical Computation of the Bit Error Probability Bound

In order to compute the upper bound on the bit error probability $P_b(E)$ it is necessary to determine the IOWEF $A(W, D)$. Let us adopt the same approach as in the course handouts. Let $\mathbf{x}(W, D)$ be the vector of the nonzero states and $\mathbf{x}_0(W, D)$ be the vector of the inputs. As shown in the handout it is possible to write the linear system

$$\mathbf{x}(W, D) = \mathbf{T}(W, D)\mathbf{x}(W, D) + \mathbf{x}_0(W, D)$$

and determine the nonzero states as solution of the system. The output-zero state can be reached from the nonzero states through the relation $\mathbf{C}(W, D)\mathbf{x}(W, D)$ where $\mathbf{C}(W, D)$ is row vector whose j -th element is

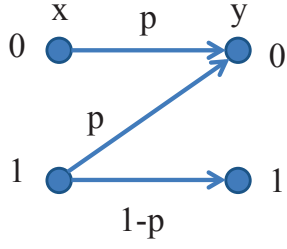


Fig. 8. Transition probability of a binary Z channel

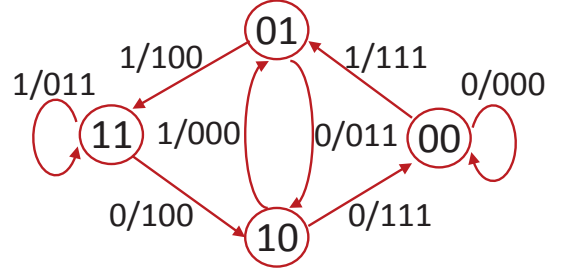


Fig. 9. State diagram of a convolutional code

the label of the transition in the modified graph that brings from the j -th nonzero state to the output zero state. Then,

$$A(W, D) = \mathbf{C}(W, D)(\mathbf{I} - \mathbf{T}(W, D))^{-1} \mathbf{x}_0.$$

The bit error probabilities $P_b(E)$ is bounded by

$$P_b(E) \leq \frac{1}{k} \frac{\partial}{\partial D} A(D, W) \Big|_{D=e^{-\frac{RE_b}{N_0}}, W=1}$$

In order to calculate the union bound avoiding the symbolic inversion of the matrix $(\mathbf{I} - \mathbf{T}(W, D))$ we can approximate the derivative of $A(D, W)$ with respect to D in $D = 1$ by the incremental ratio

$$\frac{\partial}{\partial W} A(W, D) \Big|_{W=1, D=e^{-\frac{RE_b}{N_0}}} \approx \frac{1}{\epsilon} \left(A(1 + \epsilon, e^{-\frac{RE_b}{N_0}}) - A(1, e^{-\frac{RE_b}{N_0}}) \right)$$

where ϵ is a small number (e.g. $\epsilon = 0.01$).

In any case, either if $\frac{\partial}{\partial W} A(W, D) \Big|_{W=e^{-\frac{RE_b}{N_0}}, D=1}$ is evaluated in a symbolic form or by the above numerical method, since $A(W, D)$ is a power-series, it is meaningful only when it is evaluated inside the region of convergence. It turns out that for $\frac{E_b}{N_0}$ smaller than a certain threshold the bound on $P_b(E)$ assumes values which may be greater than 1 or negative. In these case we are outside the convergence domain and we shall replace the bound on the BER by the value $\frac{1}{2}$ which is the trivial bound obtained by deciding randomly on every information bit by disregarding the decoder outcome.

Exercise 63

In some binary channels one of the input symbols is much more likely to be in error than the other (see e.g. optical fibers). This kind of binary channels are called Z-channels and their transition probability is given in Figure 8.

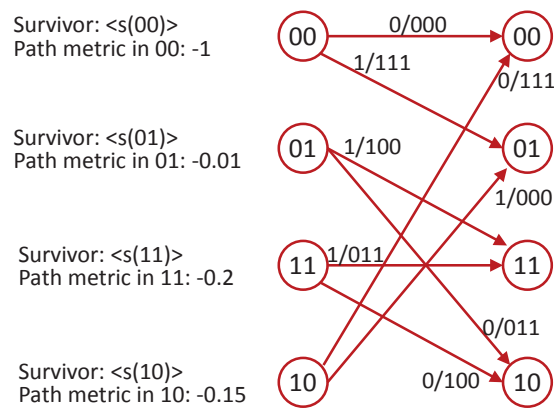


Fig. 10. Stage ℓ of the trellis for the convolutional code in Figure 9.

Assume that a convolutional code with the state diagram in Figure 9 is utilized for transmission through a Z-channel with $p = 0.1$.

- 1) Describe how to compute the bit and branch metrics of a Viterbi algorithm for such a system (convolutional encoder and Z-channel);
- 2) Consider the stage ℓ of the trellis as given in Figure 10 with the partial path metrics of the survivors up to stage $\ell - 1$ indicated on the left of each node. Assume that at stage ℓ the received vector is $\mathbf{r}_\ell = (010)$ and the error probability of the channel is $p = 10^{-1}$. Determine the survivors and their path metrics at the output of stage ℓ .

Remarks: To describe the bit metric function you can define it in each point, i.e. provide the values $M(r|v)$.

To describe a survivor at state wz you can adopt the notation $\langle s(wz) \rangle = \langle s(xy) \rangle \cup \langle xy, wz \rangle$ where the pair $\langle xy, wz \rangle$ denotes the edge between node xy and wz .

You can use the approximations $\ln 10^{-1} \approx -2.3$ and $\ln(1 - 10^{-1}) \approx -0.1$

Exercise 64

Consider the expression of the MAP of a single bit for a convolutional code and express the a posteriori probability as a function of the state as for the BCJR algorithm. Refer to the expression of the branch, forward, and backward metrics to provide the factor graph of the BCJR algorithm.

Exercise 65 with numerical simulations

Consider the communication system shown in Figure 3.

Memory	Rate	Generators
ν_ν	$1/n$	(octal notation)
3	1/2	(13,17)

TABLE IV

CODE PARAMETERS

A source generates sequences of $K = 128$ information bits $b[i]$ which are encoded with a binary convolutional code. The parameters of the convolutional codes are defined in Table I.

The encoded output sequence $\mathbf{v}[i]$, with² $i = 0, 1, \dots, (K + \nu_{\text{MAX}} - 1)$, is sent to a BPSK modulator with mapping rule $\mu : \{0, 1\} \rightarrow \{-1, +1\}$ and then transmitted through an AWGN channel with power spectral density N_0 . Let $\mathbf{r}[i] = \sqrt{E_s}\mu(\mathbf{v}[i]) + \mathbf{z}[i]$ be the received sequence where $\mathbf{z}[i] = [z_1[i], z_2[i], \dots, z_n[i]]$ is the noise with $z_j[i], j = 1, \dots, n$, i.i.d. and $z_j[i] \sim \mathcal{N}(0, N_0)$. The received sequence \mathbf{r} is decoded by a Viterbi algorithm. The decoder provides the user with the decoded information sequence $\hat{\mathbf{b}}$.

- Write the state diagram of the convolutional code.
- Write a system simulator.
- Implement the ML decoder based on the Viterbi algorithm.
- Plot the simulated BER and WER versus³ $\frac{E_b}{N_0}$ (expressed in dB). The WER must be computed for code-words corresponding to $K = 128$ plus the ν_{MAX} zero bits for trellis termination.

Hints: The simulator

If you use C, part of the simulator is provided in the package included to this project description. Copy the package in your local working directory and uncompress it with the following command:

```
unzip tpcc-2007.zip
```

The package consists of a set of .c files:

- `tp_random.c` contains libraries for random number generation.
- `tp_alloc.c` contains a useful function for handling memory allocation.
- `tp_convolutional.c` contains the functions concerning convolutional codes. Some of the functions contained in this file with their interfaces have been declared but they are empty. Your work

² n and ν_{MAX} depend on the specific code. ν_{MAX} is due to the trellis termination by transmission of additional ν_{MAX} information bits $b[i] = 0, i = K - 1, \dots, (K + \nu_{\text{MAX}} - 1)$

³Not $\frac{E_s}{N_0}$!

consists in filling each function with the required C code.

- `tp_main.c` is the simulator main file. It contains the `main()` and some other functions (e.g. the BPSK modulator and the error counter). In some of these files small piece of C code must be added.

Additional information concerning the simulator and the data structure are provided as comments in the source code.

Hints: Convolutional Codes

A convolutional code is characterized by the parameters $(n, k, \mathbf{G}(D))$ where $\frac{k}{n}$ is the code rate and \mathbf{G} is the generator matrix.

In order to simplify the simulator we only consider codes with $k = 1$, i.e., one information bit enters in the encoder for each trellis step. Therefore the generator matrix consists of a single row of impulse responses (generators) $(g_1(D), g_2(D), \dots, g_n(D))$. The code generator matrix expressed in octal format is assigned in Table 1.

If you work in C, the function `Initialize_convolutional_code()` converts the generators into the more useful binary format (code provided).

The generators fully determine the structure of the convolutional code, the trellis structure, and the trellis transition labels. However, it is more convenient to represent the trellis by using the Forward and Backward matrix data structures (If you work in C, it is already declared in the provided C code). These matrices are filled by a function contained in the source code according to the following convention (refer to Figure 2)

- The state of the convolutional code is the content of its memory, e.g. a code with memory 2 has 4 states that can be represented either by the binary labels $\{00, 01, 10, 11\}$ or by the decimal labels $\{0, 1, 2, 3\}$. In the simulator use the decimal representation to indicate a certain state s .
- When a bit enter in the encoder, it generates a transition and a set of n output bits, one bit per generator. Write the output bits using the notation (v_n, \dots, v_1) where v_i is the output generated by the generator $g_i(D)$. Refer to the output using labels in decimal format. This will be useful when indexing a matrix (e.g. if $n = 3$ and the output is $(v_3, v_2, v_1) = (1, 0, 1)$ then the decimal index of the transition output is $v = 5$.)
- After the transition the encoder reaches the state s' .

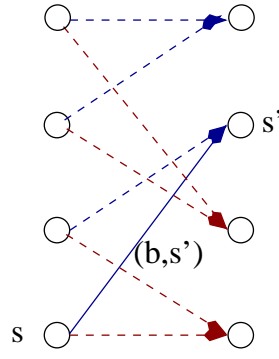


Fig. 11. Trellis

Forward Matrix: Let S denote the number of states. The forward matrix \mathbf{F} is a $S \times 2 \times 2$ matrix of integers. It describes the trellis when moving from the left to the right. Its contents is described as follows:

$$\mathbf{F}(s, b, 0) = s'$$

$$\mathbf{F}(s, b, 1) = v$$

for $b \in (0, 1)$ and $s \in \{0, 1, \dots, S - 1\}$.

Backward Matrix: The Backward matrix \mathbf{B} is a $S \times 2 \times 3$ matrix of integers. It describes the trellis when moving from the right to the left. Its contents is described as follows:

$$\mathbf{B}(s', t, 0) = s$$

$$\mathbf{B}(s', t, 1) = v$$

$$\mathbf{B}(s', t, 2) = b$$

where $t \in (0, 1)$ is the transition index (information bit that determine the transition (s, s')) and $s' \in \{0, 1, \dots, S - 1\}$.

Encoder: The encoder processes blocks (or frames) of length K sources per bit time. By default the initial state of the encoder is 0. Remember to append a frame of ν_{MAX} bits equal to zero to the block of K bits, so that the whole frame has length $K + \nu_{\text{MAX}}$. This will terminate the trellis in the state 0.

Decoder: Implement the Viterbi decoder. As a hint you can use the following data structures:

- Two vectors \mathbf{a}^0 and \mathbf{a}^1 of S elements, in which the path metrics are stored.
- Two arrays $\mathbf{Z}^0, \mathbf{Z}^1$ of size $S \times (K + \nu_{\text{MAX}})$ needed for the trace-back recursion.

Implement the Viterbi Algorithm according to the following pseudo code: let $\mathbf{r} = (r_0, r_1, \dots, r_{n(K+\nu_{\text{MAX}}-1)})$ denote the received signal sequence from the AWGN channel.

Path metric recursion

Let $a^0[0] = 0, a^0[s] = -\infty, \forall s = 1, \dots, S-1$, where ∞ denotes a very large number (e.g. 10^{10}).

For $i = 0, \dots, K + \nu_{\text{MAX}} - 1$

Compute the values of the i -th branch metric, given by

$$\omega_i(v) = \sum_{\ell=0}^{n-1} r_{ni+\ell} \mu(v_\ell)$$

for $v = 0, \dots, 2^n - 1$ ($(v_{n-1}, v_{n-2}, \dots, v_0)$ is the binary representation of the integer v and $\mu : \{0, 1\} \rightarrow \{+1, -1\}$ is the usual binary antipodal modulation mapping).

let $a = -\infty$

for $s' = 0, \dots, S-1$

let $\hat{t} = \operatorname{argmax}_{t=0,1} \{\omega_i(\mathbf{B}(s', t, 1)) + \mathbf{a}^0[\mathbf{B}(s', t, 0)]\}$

let $\mathbf{a}^1[s'] = \omega_i(\mathbf{B}(s', \hat{t}, 1)) + \mathbf{a}^0[\mathbf{B}(s', \hat{t}, 0)]$

let $\mathbf{Z}^0[s', i] = \mathbf{B}(s', \hat{t}, 0)$

let $\mathbf{Z}^1[s', i] = \mathbf{B}(s', \hat{t}, 1)$

let $a = \max\{a, \mathbf{a}^1[s']\}$

end loop

for $s' = 0, \dots, S-1$

let $\mathbf{a}^0[s'] = \mathbf{a}^1[s'] - a$

end loop

end loop

Trace-back recursion

let $s = 0$

for $i = K + \nu - 1, \dots, 0$

let $\hat{b}(i) = \mathbf{Z}^1[s, i]$

let $s = \mathbf{Z}^0[s, i]$

end loop

The ML decoded information bit sequence is given by $(\hat{b}_0, \hat{b}_1, \dots, \hat{b}_{K+\nu_{\text{MAX}}-1})$ where the last ν_{MAX} must be equal to zero (since we have forced the encoder to terminate all paths in the state zero) and have to be discarded from the total error count (i.e., only the first K information bits have to be considered in the computation of the BER for each simulated block of information).

Other Hints

- If you work in C, read the parameters of the convolutional code in Table I, then set the corresponding variables in the C code.
- Write the Viterbi decoder and check its performance first of all without adding noise. The number of error after decoding must be zero.
- Plot your curves versus $\frac{E_b}{N_0}$ in dB scale. The noise is generated with variance $N_0 = 1$. Then, in order to vary $\frac{E_b}{N_0}$ you must vary the symbol energy E_s , i.e. the transmitted symbols are $\pm\sqrt{E_s}$. Recall the relation between E_b and E_s (that depends on the coding rate) in order to map the desired value of $\frac{E_b}{N_0}$ into the value of SNR $\frac{E_s}{N_0}$ that will be used to scale the transmitted symbols.
- BER and WER can be determined at the same time, by generating many frames of $K = 128$ information bits (plus the trellis termination bits). For every value of $\frac{E_b}{N_0}$ many frames need to be transmitted in the simulation. Bits error and word errors are counted. A frame is in error if one or more information bits are in error after decoding.
- When running simulations, consider as reliable results only results obtained with a sufficient number of errors. A good value is between 100 and 200 bit errors. If the actual BER of the system is 10^{-4} it is necessary to transmit at least 10^6 information bits, that is, roughly 10000 frames of length 128 information bits. In order to save time simulation a loop exit condition is needed. Set the maximum number of transmitted frames to a very large number (e.g. 10^7). After decoding each frame, test the number of counted bit errors and word error accumulated at that point. If both are larger than a threshold, e.g. 100, the condition to exit from the simulation loop is satisfied and the the BER and WER can be determined.

Exercise 66

Consider the $R = 2/3$ convolutional code defined by

$$\left(\begin{array}{ccc|ccc} 1 & 0 & (1+D) & ; & 0 & 1 & (1+D+D^2) \end{array} \right)$$

- 1) Consider the equivalent $(12, 4)$ linear block code. Draw the corresponding Tanner graph, the complete factor graph of a decoder and the message passing rules.
- 2) Draw the factor graph for a BCJR decoder for the same code. Specify the message passing rules at each node.

3) Do the two message passing algorithms have the same performance. Why? Eventually, which one performs better?

(Hint: Do not forget to do zero padding for proper trellis termination.)

VI. TURBO CODES

Exercise 67

Given the convolutional code C_1 having generator polynomials $g_1^{(1)} = 1 + D + D^3$ and $g_2^{(1)} = 1 + D + D^2 + D^4$ draw the corresponding feedforward encoder and the feedback systematic encoder. Discuss briefly differences and similarities of the two encoders in terms of WER and BER.

Given the convolutional code C_2 defined by the polynomials $g_1^{(2)} = 1 + D^3 + D^4$ and $g_2^{(2)} = 1 + D + D^2 + D^3 + D^4$ draw the parallel concatenated encoder with interleaving based on C_1 and C_2 and rate $R = 1/3$. How to get from the previous code a code of rate $R = 1/2$?

Describe the impact of the implementation of the convolutional encoders (feedforward encoders versus systematic feedback encoders) and the interleaver on the performance of turbo codes. Provide an intuitive explanation.

Provide also an explanation for the error floor of turbo codes and how to modify it.

Exercise 68

- Consider two serially concatenated convolutional encoders (SCCC) with interleaving based on the same convolutional code. One is implemented by a non-systematic feed-forward convolutional encoder and the other is implemented by a systematic feedback convolutional encoder. Do they have the same performance?
- Explain the thinning effect.
- Does the interleaver length have an impact on the turbo cliff effect and on the $\frac{E_b}{N_0}|_{\text{cliff}}$ threshold?

Exercise 69

A systematic feedback convolutional encoder uses a parity generator $G(D) = \frac{1}{1+D+D^2}$. The length of the input sequence is 10. The sequence $\mathbf{u} = (1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$ is input to the turbo encoder.

- 1) Draw the encoder and state diagram of the convolutional code $(1, G(D))$;
- 2) Is $(1, G(D))$ a feedback or a feedforward convolutional encoder? Describe the differences in terms of performance between $(G^{-1}(D), 1)$ and $(1, G(D))$?
- 3) Draw the block diagram for the parallel concatenated encoder with interleaver with rate $R = \frac{1}{3}$ based on the parity generator $G(D)$;
- 4) Draw the block diagram for the serially concatenated encoder with interleaver with rate $R = \frac{1}{2}$ based on the parity generator $G(D)$;
- 5) Assume that the interleaver for the serially concatenated encoder is described by the sequence

$$\Pi = \{9, 15, 4, 19, 2, 11, 7, 17, 0, 10, 6, 18, 1, 12, 8, 14, 3, 13, 5, 16\}.$$

Determine the sequence v at the output of the turbo code.

- 6) Discuss the differences in terms of performance between parallel and serially concatenated encoders with interleavers.
- 7) What is the thinning effect? What are the key ingredients of a turbo code that determine the thinning effect?

Exercise 70

Consider the systematic recursive (feedback) convolutional code with generator $(23, 35)$ (octal form).

- Draw a serial concatenated code with interleaver (turbo code) base on such a convolutional code with rate $\frac{1}{2}$.
- Draw a parallel concatenated code with interleaver (turbo code) base on such a convolutional code with rate $\frac{1}{3}$.
- How to obtain a PCCC with rate $\frac{1}{2}$?
- How to obtain a PCCC with rate $\frac{1}{4}$?
- Draw the decoder for the SCCC with interleaver obtained in the first item of the exercise.

Exercise 71

Consider the feedback generator encoder $(1, \frac{1}{1+D+D^2})$. Assume that the length of the transmitted sequence is 10 (we do not perform zero padding in this case). The interleaver is described by the sequence

$\Pi = \{9, 4, 2, 7, 0, 6, 1, 8, 3, 5\}$, i.e. the information sequence $(u_0, u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9)$ is shuffled into $\{u_9, u_4, u_2, u_7, u_0, u_6, u_1, u_8, u_3, u_5\}$.

- 1) Draw a single generic stage of the trellis of the convolutional code;
- 2) Draw the block diagram of a parallel concatenated encoder with interleaver (turbo encoder) based on the above described convolutional encoder.
- 3) Given the sequence $(1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$ as input of the turbo encoder, determine the output sequences of all the branches of the turbo encoder $\mathbf{v}^{(0)}$ (systematic part), $\mathbf{v}^{(1)}$ (parity check part without interleaving), $\mathbf{v}^{(2)}$ (parity check part with interleaving), and the output of the turbo encoder \mathbf{v} .
- 4) The sequence is punctured to obtain a code with rate $R = 1/2$ by taking the even bit of $\mathbf{v}^{(1)}$ and the odd bit of $\mathbf{v}^{(2)}$. Determine the output sequence \mathbf{v} now.
- 5) Draw the factor graph of the corresponding decoder detailing the interleaver block according to the assigned interleaver.
- 6) Instead of using the parity check generator $\frac{1}{1+D+D^2}$ we use the polynomial $(1 + D + D^2)$. How does the Word Error Rate (WER) of the convolutional code change? And the BER? What about the performance of the turbo code?