TUHH
Technische Universität Hamburg-Harburg

INSTITUT FÜR NACHRICHTENTECHNIK
PROF. DR.-ING. GERHARD BAUCH

Exam SS 2015

Information Theory and Coding

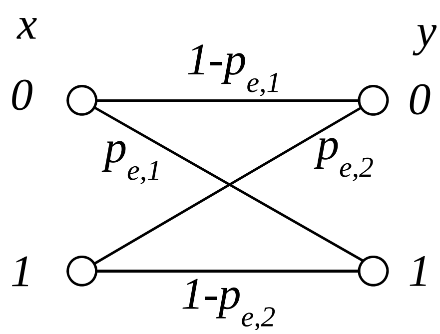
Name: …………………………………………………………..	Immatriculation number: ……………………………	
	Points	from
Problem 1		
Problem 2		
Total points		
Grade		

- The following aids are allowed in this exam:
  - 2 Din A4 sheets, handwritten on both sides (4 pages in total)
  - calculator (non-programmable)
  - Pens
- Other aids are not allowed.
- Please use a separate solution sheet for each task.
- Write your name and matriculation number on each solution sheet.
- An arrow next to a question means that this part of the task can be solved independently of the previous questions.
- Please do not write with pencils and do not use a red pen.
- The duration of the exam is 90 minutes.
- The exam consists of **4** pages (including this cover page).
- Switch off your cell phones!

Good luck!

Problem 1: Capacity of Asymmetric Binary Input Binary Output Channel

Consider a general binary input binary output channel with transmit symbols $x \in \{0, 1\}$, output symbols $y \in \{0, 1\}$ and error probabilities $p_{e,i}$, $i=1,2$:



A transmit symbol $x=0$ occurs with probability p_0, a transmit symbol $x=1$ occurs with probability $1\text{-}p_0$.

a) Determine the channel transition probabilities $p(y|x)$ for all possible possible x and y pair.

Answer:

x	y	$p(y\|x)$
0	0	$1 - p_{e1}$
0	1	p_{e1}
1	0	p_{e2}
1	1	$1 - p_{e2}$

b) Determine the probabilities $p(y=0)$ and $p(y=1)$.

Answer:

$$\begin{aligned} p(y=0) &= p(y=0|x=0)p(x=0) + p(y=0|x=1)p(x=1) \\ &= (1-p_{e1})p_0 + p_{e2}(1-p_0) \\ &= p_0(1-p_{e1}-p_{e2}) + p_{e2} \end{aligned}$$

$$\begin{aligned} p(y=1) &= p(y=1|x=0)p(x=0) + p(y=1|x=1)p(x=1) \\ &= (p_{e1})p_0 + (1-p_{e2})(1-p_0) \\ &= p_0(p_{e1}+p_{e2}-1) + 1 - p_{e2} \end{aligned}$$

Test: $p(y=0) + p(y=1) = 1$

c) Determine the joint probabilities $p(x,y)$ for every possible x and y pair.

Answer:

x	*y*	*p(x,y)*
0	0	$(1-p_{e1})p_0$
0	1	$p_{e1}p_0$
1	0	$p_{e2}(1-p_0)$
1	1	$(1-p_{e2})(1-p_0)$

d) Determine the entropy *H(Y)* of the channel output depending on p_0, $p_{e,1}$, $p_{e,2}$. Express your solution using the binary entropy function $H_b(p)$.

Answer:

$$H(Y) = \sum_y p(y)\log_2 \frac{1}{p(y)}$$

$$= [p_0(1-p_{e1}-p_{e2})+p_{e2}]\log_2 \frac{1}{p_0(1-p_{e1}-p_{e2})+p_{e2}}$$

$$+[p_0(p_{e1}+p_{e2}-1)+1-p_{e2}]\log_2 \frac{1}{p_0(p_{e1}+p_{e2}-1)+1-p_{e2}]}$$

$$= H_b(p_0(1-p_{e1}-p_{e2})+p_{e2})$$

e) Determine the conditional entropy *H(Y|X)* depending on p_0, $p_{e,1}$, $p_{e,2}$. Express your solution using binary entropy functions $H_b(p)$.

Answer:

$$H(Y) = \sum_x \sum_y p(x,y)\log_2 \frac{1}{p(y|x)}$$

$$= (1-p_{e1})p_0\log_2 \frac{1}{1-p_{e1}} + p_{e1}p_0\log_2 \frac{1}{p_{e1}}$$

$$p_{e2}(1-p_0)\log_2 \frac{1}{p_{e2}} + (1-p_{e2})(1-p_0)\log_2 \frac{1}{1-p_{e2}}$$

$$= p_0[(1-p_{e1})\log_2 \frac{1}{1-p_{e1}} + p_{e1}\log_2 \frac{1}{p_{e1}} - p_{e2}\log_2 \frac{1}{p_{e2}}$$

$$-(1-p_{e2})\log_2 \frac{1}{1-p_{e2}}] + p_{e2}\log_2 \frac{1}{p_{e2}} + (1-p_{e2})\log_2 \frac{1}{1-p_{e2}}$$

$$= p_0[H_b(p_{e1}) - H_b(p_{e2})] + H_b(p_{e2})$$

$$= p_0 H_b(p_{e1}) + (1-p_0)H_b(p_{e2})$$

f) Determine the mutual information *I(X,Y)* between channel input and channel output depending on p_0, $p_{e,1}$, $p_{e,2}$. Results of previous problems can be used. Express your solution using binary entropy functions $H_b(p)$.

Answer:

$$I(X,Y) = H(Y) - H(Y|X)$$

$$= H_b(p_0(1-p_{e1}-p_{e2})+p_{e2}) - p_0 H_b(p_{e1}) - (1 - p_0)H_b(p_{e2})$$

g) Determine the capacity achieving probability p_0 of a transmit symbol $x=0$ depending on $p_{e,1}$, $p_{e,2}$.

Help:
$$\frac{dH_b(p)}{dp} = \log_2\left(\frac{1}{p}-1\right)$$

Answer:

The capacity achieving probability p_0 of a transmit symbol x is the one which maximizes the mutual information $I(X,Y)$. It can be found by solving the following for p_0:

$$\frac{d}{dp_0} I(X,Y) = 0$$

Substituting $I(X,Y)$:

$$\frac{d}{dp_0}\{H_b(p_0(1-p_{e1}-p_{e2})+p_{e2}) - p_0 H_b(p_{e1}) - (1-p_0)H_b(p_{e2})\} = 0$$

Computing the derivative w.r.t p_0:

$$(1-p_{e1}-p_{e2})\log_2\left(\frac{1}{(1-p_{e1}-p_{e2})}-1\right) - H_b(p_{e1}) + H_b(p_{e2}) = 0$$

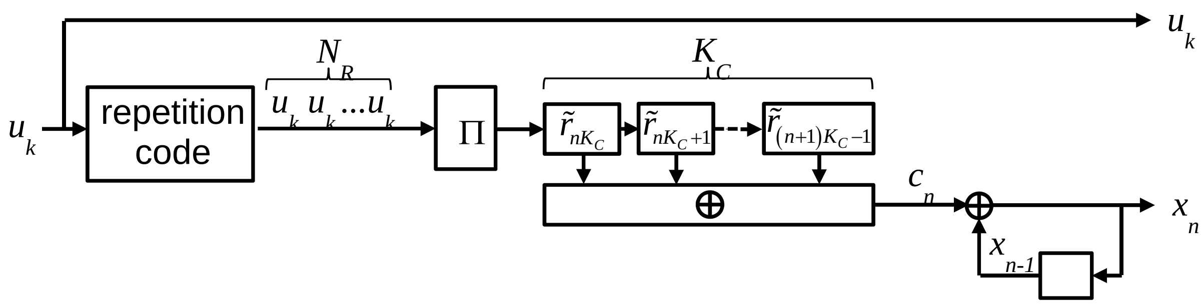
$$\frac{1}{p_0(1-p_{e1}-p_{e2})+p_{e2}} = 2^{\frac{H_b(p_{e1})-H_b(p_{e2})}{(1-p_{e1}-p_{e2})}} + 1$$

Rearranging:

$$p_0 = \left[\frac{1}{2^{\frac{H_b(p_{e1})-H_b(p_{e2})}{(1-p_{e1}-p_{e2})}}+1} - p_{e2}\right]\frac{1}{1-p_{e1}-p_{e2}}$$

Problem 2: Repeat Accumulate (RA) Code

The block diagram of a repeat accumulate (RA) code is depicted in the following figure:



The information bits and parity bits are denoted by $u_k \in \{0,1\}$ and $x_n \in \{0,1\}$, respectively.

A parity check matrix of the RA-code is given by

$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

⇨ a) Is the RA-code systematic ? Give reasons !

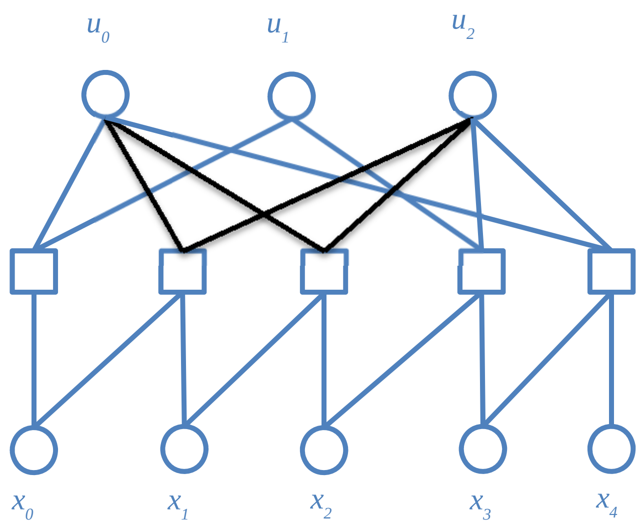
Answer: Yes, the information bits are an explicit part of the codewords.

⇨ b) Is the RA-code regular or irregular ? Give reasons !

Answer: The RA-code is irregular. The columns of $\mathbf{H}^T$ representing the repetition and combiner part have different weight e.g. first column has weight 4 but second column has weight 2.

c) Sketch the Tanner graph which represents the parity check matrix $\mathbf{H}^T$ above.

Answer:



d) Determine the girth of the Tanner graph.

Answer: girth of the graph is 4.

e) Explain precisely why a short girth is undesired for message passing decoding.

Answer: In message passing decoding, extrinsic information is exchanged along the edges of the Tanner graph. The nodes update the information based on all incoming information and the received channel information. The update rules assume that all incoming information and the channel information at a node are statistically independent. However, when the Tanner graph has cycles, the incoming information is not independent anymore after a few iterations resulting in a suboptimal decoding.

f) Mark a shortest cycle in the Tanner graph from c). Mark also the entries in the parity check matrix $\mathbf{H}^T$ which correspond to the marked cycle.

Answer: The shortest cycle is marked in black in the answer to task c. The corresponding entries are marked in the following parity check matrix:

$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

⇨ g) Determine the rate R_R of the repetition coding part within the RA-code.

Answer: The repetition code has unequal rate for various input bits:

$R_R = \frac{1}{4}$ for u_0 and u_2. $R_R = \frac{1}{2}$ for u_1.

⇨ h) Determine the rate R_C of the combiner part within the RA-code.

Answer: Rate of the combiner part is $R_C = 2$

⇨ i) Determine the rate R_A of the accumulator part within the RA-code.

Answer: Rate of the accumulator part is $R_A = 1$

⇨ j) Determine the overall code rate R of the RA-code.

Answer: The overall code rate R of the RA-code can be found from the parity check matrix or the Tanner graph as;

$$R = \frac{K}{N} = \frac{3}{3+5} = \frac{3}{8}$$

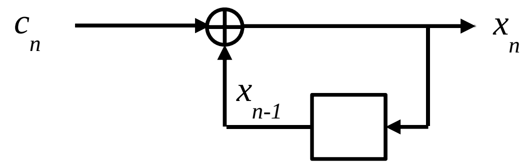
Or from the following formula:

$$R = \frac{K}{K(1 + \frac{\bar{N}_R}{R_C})}$$

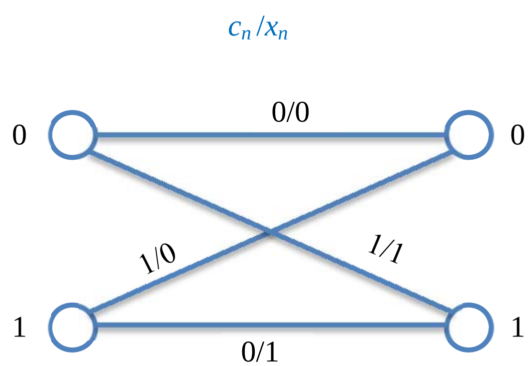
Using R_C from subtask (h) and average number of bits out of the repetition code $\bar{N}_R = \frac{4+2+4}{3} = \frac{10}{3}$ (where the average number of bits $\bar{N}_R$ is used instead of N_R due to the fact that the repetition code is irregular):

$$R = \frac{1}{1 + \frac{10}{3 \times 2}} = \frac{6}{16} = \frac{3}{8}$$

Now consider only the accumulator part of the RA-code as depicted in the following figure.



k) Sketch a trellis segment which describes the accumulator. Label the states and transitions completely.



l) Determine a generator polynomial *g(D)* which describes the accumulator as a convolutional encoder.

Answer: The generator polynomial describing the accumulator is:

$$g(D) = \frac{1}{1 + D}$$

m) Give the octal representation of the generator polynomial found in l).

Answer: Octal representation of the generator polynomial is:

$$g = \frac{(0\ 1\ 0)_2}{(0\ 1\ 1)_2} = \frac{2}{3}$$

n) The accumulator part of the RA-code can be decoded using the Viterbi algorithm.

(1) Determine the metric increment for hard decision decoding.

Answer: The metric increment for hard decision decoding of the *k*th symbol for transition from state *i* to state *j* will be:

$$\Delta\mu_k(s_i, s_j) = y_k \oplus x_k(s_i, s_j)$$

With the above metric increment, the path with smaller state metric will survive at state *i*. For a path with larger state metric to survive at any state, the above metric increment is preceded by a $-$, i.e.

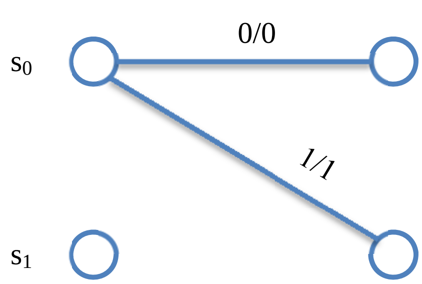
$$\Delta\mu_k(s_i, s_j) = -y_k \oplus x_k(s_i, s_j)$$

(2) Assume that the accumulator was initialized in the zero state at the beginning of encoding. The sequence

1, 1, 0

is observed at the output of a BSC channel. Perform Viterbi decoding for this sequence. Make sure that every single step is given and can be clearly understood in your solution. State also clearly the decoding result.

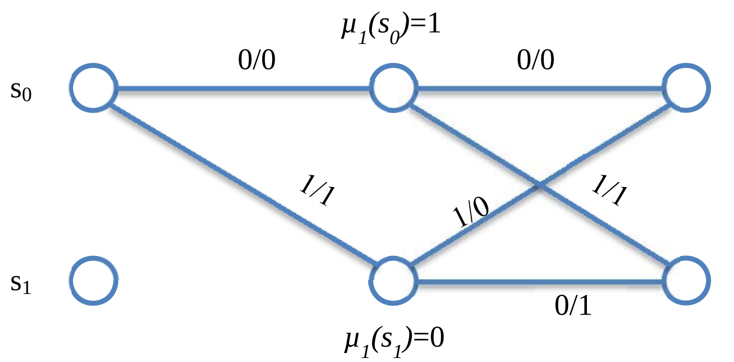
Answer: The received symbol sequence is given as $y_0, y_1, y_2 = 1{,}1{,}0$. Initialize the state metric for state s_0 as $\mu_0(s_0) = 0$. Starting with the first symbol $y_0 = 1$;



The state metric at both the states for *k*=1 are computed as:

$$\mu_1(s_0) = \mu_0(s_0) + [y_0 \oplus 0] = 0 + [1 \oplus 0] = 1$$

$$\mu_1(s_1) = \mu_0(s_0) + [y_0 \oplus 1] = 0 + [1 \oplus 1] = 0$$



For k =2 symbol i.e. $y_1 = 1$, the path metrics are calculated as following.
For state s_0:

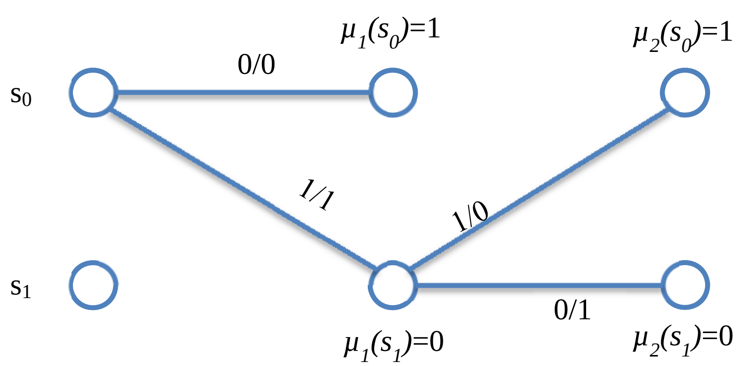
$$\mu_2(s_0) = \begin{cases} \mu_1(s_0) + [y_1 \oplus 0] = 1 + [1 \oplus 0] = 2 \\ \mu_1(s_1) + [y_1 \oplus 0] = 0 + [1 \oplus 0] = 1 \end{cases}$$

The upper path with larger path metric will be dropped and the state metric will be $\mu_2(s_0) = 1$.

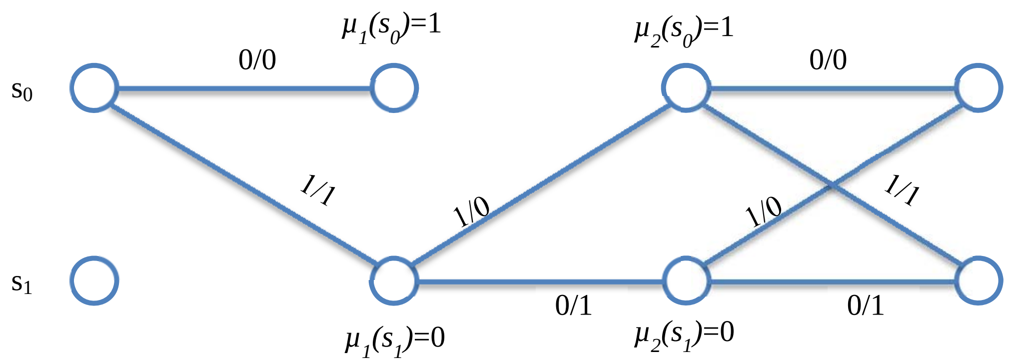
For state s_1:

$$\mu_2(s_1) = \begin{cases} \mu_1(s_0) + [y_1 \oplus 1] = 1 + [1 \oplus 1] = 1 \\ \mu_1(s_1) + [y_1 \oplus 1] = 0 + [1 \oplus 1] = 0 \end{cases}$$

The upper path entering state s_1 with larger path metric will be dropped and the state metric will be $\mu_2(s_0) = 0$. The trellis will look like:



Now for the last observed symbol i.e. $y_2 = 0$, the path metrics will be computed.



For state s_0:

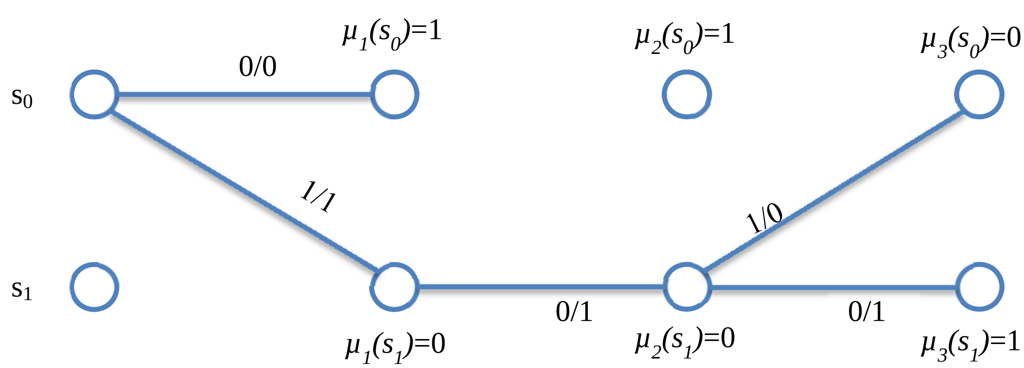
$$\mu_3(s_0) = \begin{cases} \mu_2(s_0) + [y_2 \oplus 0] = 1 + [0 \oplus 0] = 1 \\ \mu_2(s_1) + [y_2 \oplus 0] = 0 + [0 \oplus 0] = 0 \end{cases}$$

The upper path with larger path metric will be dropped and the state metric will be $\mu_3(s_0) = 1$.

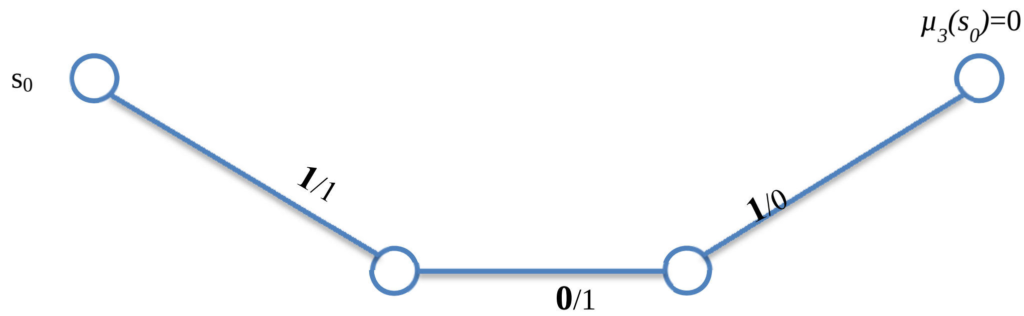
For state s_1:

$$\mu_2(s_1) = \begin{cases} \mu_2(s_0) + [y_2 \oplus 1] = 1 + [0 \oplus 1] = 2 \\ \mu_2(s_1) + [y_2 \oplus 1] = 0 + [0 \oplus 1] = 1 \end{cases}$$

The upper path entering state s_1 with larger path metric will be dropped and the state metric will be $\mu_3(s_0) = 1$. The trellis will look like:



The path terminating in the state s_0 has the minimum path metric and is thus maximum likely path. The trace back path is shown in the following figure.



So the decoding result will be $\underline{c} = [1,0,1]$