LINKÖPINGS UNIVERSITET

Exam in TSDT16 Error-correcting codes

Date: 2015-10-30 **Time:** 14.00-18.00

Teacher: Danyo Danev, tel: 013-281335

Place: TER1

Allowed aids: No aids allowed except pocket calculators.

Language: Solutions in both english and swedish are accepted.

Grading: Each correctly answered question yields 3 points. For grade 3 you need 6 points, for grade 4 you need 9 points, for grade 5 you need 12 points. The ECTS levels are as follows: E − > 6, D − > 7, C − > 9, B − > 10, A − > 12. Sloppy solutions and solutions that are hard to read are subject to hard judgement, as are unreasonable answers.

Solutions: Will be published after the exam at http://www.commsys.isy.liu.se/en/student/kurser/tentor?TSDT16

Grading list: A preliminary grading list will be send to all registered for the exam no later than 2015-11-10. Others can get information about the results from the course leader or at the exam return.

Exam return: 2015-11-13, kl. 12.15-12.45 in Hammingrummet, house B, entrance 27-29, 2nd floor, corr. A.

Complaints: No later than 2015-11-13.

Good luck!

1 Determine the generator polynomials of all binary primitive BCH codes of length 31. Use the fact that the polynomial $\mathbf{p}(X) = X^5 + X^2 + 1$ is primitive over $\mathbf{GF}(2)$.

2 The double error-correcting RS code C of length 15 over $\mathbf{GF}(16)$ is is defined by the generator polynomial

$$\mathbf{g}(X) = (X + \alpha)(X + \alpha^2)(X + \alpha^3)(X + \alpha^4),$$

where $\alpha \in \mathbf{GF}(16)$ is a primitive element and a root of the polynomial $1 + X^3 + X^4$. Create a table utilizing easy computations in $\mathbf{GF}(16)$ based on α and find the codeword in C which is closest, in terms of Hamming distance, to the received vector

$$\mathbf{r} = (0, 0, \alpha^{10}, 0, \alpha^4, \alpha^7, 1, 0, 0, 0, \alpha^5, 0, 0, 0, 0).$$

3 Let C be a binary cyclic code of length n with generator polynomial $\mathbf{g}(X)$ and weight enumerator $A(z)$. Show that if there is a codeword in C of odd weight, then the weight enumerator $A_1(z)$ of the cyclic code C_1 of length n with generator polynomial $\mathbf{g_1}(X) = (1 + X)\mathbf{g}(X)$ can be calculated as follows

$$A_1(z) = \frac{A(z) + A(-z)}{2}.$$

4 The cyclic binary code C has length 21 and the parity-check polynomial

$$\mathbf{h}(X) = X^9 + X^8 + X^7 + X^5 + X^4 + X + 1.$$

Devise a syndrome computation and encoding circuits for this cyclic code and compute the syndrome of the received polynomial $\mathbf{r}(X) = X^{17} + X^{10} + X^7 + X^3 + X + 1$. Show the contents of the syndrome register after each shift of the received word $\mathbf{r}$ into the syndrome computation circuit.

5 The convolutional code of rate $R = 2/3$ with a generator matrix

$$\mathbf{G}(D) = \begin{bmatrix} D & 1+D & 1+D \\ 1 & D & 1+D \end{bmatrix}.$$

has been used to decrease the BER when transmitting binary information over a discrete memoryless channel (DMC). The demodulator provides two versions of the transmitted binary symbols. The integer metric table that can be obtained based on the corresponding probabilities is

	$\mathbf{0_1}$	$\mathbf{0_2}$	$\mathbf{1_2}$	$\mathbf{1_1}$
0	10	5	1	0
1	0	1	5	10

After passing the DMC the result from the demodulator is the following vector

$$\mathbf{r} = (1_1 1_2 0_2, 1_1 0_1 0_1, 1_1 0_2 1_2, 0_1 0_2 0_1, 1_2 1_1 1_2).$$

Determine the message $\mathbf{m}$ that has been sent if a maximum-likelihood decoding algorithm is used. Assume that the encoder is put into the initial all-zero state after the encoding of the message.

Some useful equations

$$d_\mu = S_{\mu+1} + \sigma_1^{(\mu)} S_\mu + \sigma_2^{(\mu)} S_{\mu-1} + \cdots + \sigma_{l_\mu}^{(\mu)} S_{\mu+1-l_\mu}$$

$$\sigma^{(\mu+1)}(X) = \sigma^{(\mu)}(X) - d_\mu d_\rho^{-1} X^{\mu-\rho} \sigma^{(\rho)}(X)$$