Aalto University School of Electrical Engineering
Department of Communications and Networking

EXAM
16.2.2015

S-72-3410 Coding Methods

1. (6p.) Finite fields.

   The additive (+) and multiplicative (·) operations of the finite field of order 8 with elements from the set $\{0, 1, \sharp, \triangle, \clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ are given in Table 1. Answer the following questions (the variable in the equations is x). Motivate your answers.

   (a) Solve the equation $\sharp \cdot x + \triangle = \heartsuit$.

   (b) Solve the equation $x^2 = \sharp$.

   (c) Solve the equation $x^3 = \heartsuit$.

   (d) Find a primitive element in this field.

   (e) Does the field have a subfield of order 2? It the answer is yes, find the elements of such a subfield. Answer the same question for a subfield of order 4.

+	0	1	$\sharp$	$\triangle$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
0	0	1	$\sharp$	$\triangle$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
1	1	0	$\triangle$	$\sharp$	$\diamondsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$
$\sharp$	$\sharp$	$\triangle$	0	1	$\heartsuit$	$\spadesuit$	$\clubsuit$	$\diamondsuit$
$\triangle$	$\triangle$	$\sharp$	1	0	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$
$\clubsuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$	0	1	$\sharp$	$\triangle$
$\diamondsuit$	$\diamondsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$	1	0	$\triangle$	$\sharp$
$\heartsuit$	$\heartsuit$	$\spadesuit$	$\clubsuit$	$\diamondsuit$	$\sharp$	$\triangle$	0	1
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$	$\triangle$	$\sharp$	1	0

·	0	1	$\sharp$	$\triangle$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
0	0	0	0	0	0	0	0	0
1	0	1	$\sharp$	$\triangle$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
$\sharp$	0	$\sharp$	$\clubsuit$	$\heartsuit$	$\diamondsuit$	$\spadesuit$	1	$\triangle$
$\triangle$	0	$\triangle$	$\heartsuit$	$\diamondsuit$	1	$\sharp$	$\spadesuit$	$\clubsuit$
$\clubsuit$	0	$\clubsuit$	$\diamondsuit$	1	$\spadesuit$	$\triangle$	$\sharp$	$\heartsuit$
$\diamondsuit$	0	$\diamondsuit$	$\spadesuit$	$\sharp$	$\triangle$	$\heartsuit$	$\clubsuit$	1
$\heartsuit$	0	$\heartsuit$	1	$\spadesuit$	$\sharp$	$\clubsuit$	$\triangle$	$\diamondsuit$
$\spadesuit$	0	$\spadesuit$	$\triangle$	$\clubsuit$	$\heartsuit$	1	$\diamondsuit$	$\sharp$

Table 1: Finite field of order 8

2. (6p.) Block codes.

   (a) Find a generator matrix and a parity check matrix for the binary linear code with the codewords 00000, 00110, 01010, 01100, 10010, 10100, 11000, 11110. What is the minimum distance of this code?

   (b) Determine the possible dimensions of a cyclic binary linear code of length 27 (analytically, that is, it is not sufficient to pick the answer directly from some table that you may have in your material).

3. (6p.) Convolutional codes. Consider the convolutional encoder with the transfer function matrix

$$\mathbf{G}(D) = [1 + D^2 \quad 1 + D + D^2].$$

CONT.

(a) Is the code catastrophic? (Motivate your answer.)

(b) Draw the state diagram of this encoder.

(c) Assume that this encoder is used over a binary symmetric channel (BSC). Use Viterbi decoding to find the maximum-likelihood codeword corresponding to the received sequence

$$\mathbf{r} = (11, 10, 11, 00, 01, 11).$$

Hint: For the BSC and the maximization version of the Viterbi algorithm, we have

$M(r \mid y)$	$r = 0$	$r = 1$
$y = 0$	1	0
$y = 1$	0	1

4. (6p.) Modern coding methods.

(a) Why is the following parity check matrix not a good choice for an LDPC code?

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(b) A fountain code is used for transmitting the bits b_1, b_2,...,b_4. The receiver gets the following sums of bits (over GF(2)): $b_2 + b_3 = 0$, $b_1 + b_2 + b_4 = 1$, $b_1 + b_3 = 1$, $b_3 + b_4 = 1$, ... Is it possible to determine the values of the bits after the first four sums have arrived? If not, why? If yes, determine the values of the bits.

(c) Ben and Bill each tell Ann which color they prefer out of *red*, *blue*, and *green*. Ben does not know Bill's preference and vice versa. Next all three persons meet and Ann wants to inform both Ben and Bill about the choices made. Of course, this can be done by first telling Bill about Ben's choice and then telling Ben about Bill's choice. But can they agree on some faster protocol? (Ann is allowed to use only the words *red*, *blue*, *green* and she can direct her speech towards Ben, Bill, or both.)