Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam:
Kristian Gjøsteen 73 55 02 42

EXAM IN TMA4185 CODING THEORY

English
Saturday, May 29 2010
Time: 0900-1300
Sensurdato: June 19 2010
Any printed or hand-written material is allowed during the exam.
An approved, simple calculator is allowed.

All subproblems have equal weight. Show your work.

Problem 1 Let $\mathcal{C}$ be the code generated by the rows of the matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

a) Find a generator matrix G' on standard form. What is the dimension of the code? Use G' to encode $(1, 1, 1, 0)$.

b) Find a parity check matrix for the code. What is the code's minimum distance?

c) The sender used G' to encode. We received $y = (1, 1, 0, 1, 0, 1, 0, 1)$. Find the nearest code word, any error vector and the message.

Problem 2 Let $\mathcal{C}$ be a cyclic code of length 15 over $\mathbb{F}_2$. Let α be a primitive element in $\mathbb{F}_{2^4}$ that satisfies $\alpha^4 + \alpha + 1 = 0$.

a) Describe all such cyclic codes (e.g. by giving generating polynomials).

Let $\mathcal{C}$ be the code with generating polynomial $g(x) = x^8 + x^7 + x^6 + x^4 + 1$.

b) What is the dimension of the code? Show that the code's minimum distance is at least 5. Describe the code's dual.

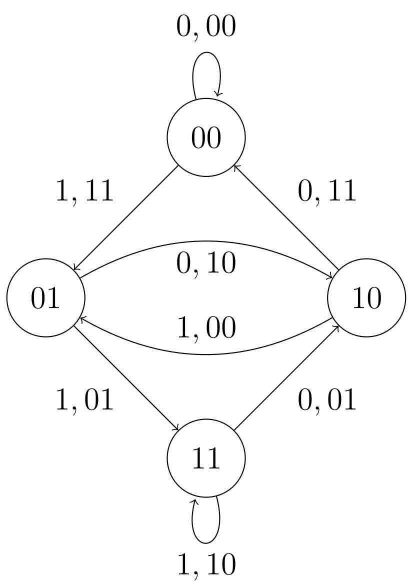
c) Use the Berlekamp-Massey algorithm to show that the sequence $s_0 = \alpha^3 + \alpha^2$, $s_1 = \alpha^3 + \alpha^2 + \alpha + 1$, $s_2 = \alpha^2 + \alpha$, $s_3 = \alpha^3 + \alpha$ is generated by the linear recurrence

$$s_{N+1} = (\alpha^3 + \alpha^2)s_N + (\alpha^2 + \alpha)s_{N-1}.$$

Hint: The Berlekamp-Massey algorithm is given in the appendix.

d) We received $y(x) = x^{12} + x^{11} + x^9 + x^8 + x^7 + x^3 + 1$. Compute the first four syndromes. Use these to find the error locator polynomial $C(D)$ and the error vector $e(x)$. Given that we encode using $c(x) = m(x)g(x)$, decode $y(x)$.

Problem 3 The convolutional code $\mathcal{C}$ is given by the state machine



a) Give generating polynomials for the convolution code. Encode the message 01100.

b) Use Trellis decoding to decode 11 10 10 10 01 10 11.

Appendix

The Berlekamp-Massey
In: A sequence $s_0, s_1, \ldots, s_{n-1}$ of elements from $\mathbb{F}_{2^r}$.
Out: A linear recurrence for the sequence given by $C(D) = 1 + \sum_{i=1}^{L} c_i D^i$.

1. Start with $C(D) = 1$, $L = 0$, $m = -1$, $B(D) = 1$, $\Delta = 1$, $\Delta' = 1$.
2. For N from 0 to $n-1$, inclusive, do:
   (a) Compute the discrepancy $\Delta = s_N + \sum_{i=1}^{L} c_i s_{N-i}$.
   (b) If $\Delta \neq 0$:
      i. Remember the old recurrence: $T(D) \leftarrow C(D)$.
      ii. Compute the new recurrence: $C(D) \leftarrow C(D) + B(D) \cdot D^{N-m} \cdot \Delta/\Delta'$.
      iii. If $L \leq N/2$:
         A. Compute new length: $L \leftarrow N + 1 - L$.
         B. Remember where the length last changed: $m \leftarrow N$, $\Delta' \leftarrow \Delta$, $B(D) \leftarrow T(D)$.