Faculty of Sciences	**Coding and Cryptography**
VU University Amsterdam	**Exam 12:00-14:45 21-10-2015**

Note

(1) This exam consists of 8 problems.
(2) Calculators, notes, books, etc., may not be used.
(3) Justify your answers!
(4) Throughout this exam, $K = \{0, 1\}$.

Problems

(1) (a) Does there exist a code in K^8 with 7 codewords and distance 5? Explain your answer.
(b) Let C be a linear $(8, 3, 2)$-code in K^8. We leave out the last position of each codeword, obtaining a linear code C' in K^7. Give the possible parameters (n', k', d') of C', and show by means of examples they all occur.

(2) Let X be a matrix with as rows all the elements in K^7 of weight 3, and let $H = \begin{bmatrix} I \\ X \end{bmatrix}$.
We view H as the check matrix of a linear code C.
(a) Determine de distance of C.
(b) Compute how many received words for C can be decoded under IMLD where we correct any error of weight at most 1. Do not simplify your answer to a number.

(3) Let $F = GF(2^3)$ be constructed using the primitive irreducible polynomial $1+x+x^3$ and let β be the class of x.
(a) Find a parity check matrix H (with entries in K) for the cyclic Hamming code C of length 7 with generator polynomial $m_\beta(x)$.
(b) Decode the received word $w = 1010000$ for this code.
(c) To each $a_0a_1 \dots a_6$ in C corresponds the polynomial $a(x) = a_0 + a_1x + \cdots + a_6x^6$. We then consider $D \subseteq C$ consisting of all $a(x)$ in C with $a(1) = 0$. What are the dimension and distance of D?

(4) (a) Factorize $f(x) = x^6 + x^5 + x + 1$ into irreducibles in $K[x]$. (You may use without proof which polynomials in $K[x]$ are irreducible for degrees 1, 2 and 3.)
(b) How many divisors in $K[x]$ does $f(x)$ have?

(5) (a) Compute the number of idempotents $I(x)$ modulo $1 + x^{21}$ that have degree at most 17.
(b) For the idempotent of degree 12 with constant term 1, find the generator polynomial $g(x)$ of the corresponding cyclic linear code C in K^{21}.

Please turn over for problems (6), (7) and (8).

In problems (6) and (7), $GF(2^4)$ is constructed as $K[x]$ modulo $1+x^3+x^4$ and β is the class of x, so $1+\beta^3+\beta^4=0$. Moreover, β is primitive, and the table for its powers is:

0000	-	1110	β^7
1000	1	0111	β^8
0100	β	1010	β^9
0010	β^2	0101	β^{10}
0001	β^3	1011	β^{11}
1001	β^4	1100	β^{12}
1101	β^5	0110	β^{13}
1111	β^6	0011	β^{14}

(6) Let β and $GF(2^4)$ be as in the table, let $\alpha=\beta^5+\beta^{12}$, and let $m_\alpha(x)$ be the minimal polynomial of α in $K[x]$.
   (a) Determine the degree of $m_\alpha(x)$ in an efficient way.
   (b) Find $m_\alpha(x)$ explicitly.

(7) Let β and $GF(2^4)$ be as in the table. Let $C\subseteq K^{15}$ be the 2-error correcting BCH code with parity check matrix

$$H=\begin{bmatrix} 1 & 1 \\ \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \vdots \\ \beta^{14} & \beta^{42} \end{bmatrix}.$$

If w is a received word, determine if $d(v,w)\leq 2$ for some v in C in two cases:
   (a) w has syndrome $wH=[s_1,s_3]=[\beta^8,\beta^8]$;
   (b) w has syndrome $wH=[s_1,s_3]=[\beta^{11},\beta^3]$.

(8) Let $n=113$.
   (a) Perform the Miller-Rabin probabilistic primality test for n with $a=2$.
   (b) Which conclusions can be drawn from the result in (a) concerning if n is prime or not?

Distribution of points							
(1)(a) 4	(2)(a) 6	(3)(a) 7	(4)(a) 7	(5)(a) 5	(6)(a) 4	(7)(a) 8	(8)(a) 5
(1)(b) 6	(2)(b) 5	(3)(b) 4	(4)(b) 4	(5)(b) 4	(6)(b) 6	(7)(b) 8	(8)(b) 2
		(3)(c) 5					
10	11	16	11	9	10	16	7

Maximum total = 90
Exam score = Total score + 10