Faculty of Sciences	**Coding and Cryptography**
VU University Amsterdam	**Exam 12:00-14:45 22-10-2014**

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) For each of the following codes, either explain why it does not exist or construct an example.
  (a) A linear $(6, 3, 3)$-code in K^6.
  (b) A linear $(8, 5, 4)$-code in K^8.

(2) Let
$$X = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$
and $H = \begin{bmatrix} I \\ X \end{bmatrix}$.
  (a) Verify that H satisfies the conditions to be a parity check matrix for a binary linear code C.
  (b) Determine $d(C)$.
  (c) Compute how many received words for C can be decoded under IMLD where we correct any error of weight at most 2. Do not simplify your answer to a number.

(3) Let $F = GF(2^3)$ be constructed using the primitive irreducible polynomial $1+x^2+x^3$ and let β be the class of x.
  (a) Find a parity check matrix (with entries in K) for the cyclic Hamming code of length 7 with generator polynomial $m_\beta(x)$.
  (b) Decode the received word $w = 1010101$ for this code.

(4) (a) Factor $f(x) = x^7 + x^5 + x^3 + x^2 + x + 1$ 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 of degree 4 does $f(x)$ have?

(5) (a) What is the idempotent $I(x)$ modulo $1+x^{27}$ that contains x^3 and has the smalllest possible number of terms?
  (b) Find the generator polynomial $g(x)$ of the corresponding cyclic linear code C in K^{27} and compute the rate of this code.

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

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

0000	-	1101	β^7
1000	β^0	1010	β^8
0100	β	0101	β^9
0010	β^2	1110	β^{10}
0001	β^3	0111	β^{11}
1100	β^4	1111	β^{12}
0110	β^5	1011	β^{13}
0011	β^6	1001	β^{14}

(6) Let β and $GF(2^4)$ be as in the table, let $\alpha=\beta^8+\beta^9$, and let $m_\alpha(x)$ be the minimal polynomial of α in $K[x]$.
  (i) Determine the degree of $m_\alpha(x)$ in an efficient way.
  (ii) 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 $d(v,w)\le 2$ for some v in C in two cases:
  (i) w has syndrome $wH=[s_1,s_3]=[\beta,\beta^{13}]$;
  (ii) w has syndrome $wH=[s_1,s_3]=[0,\beta^6]$.

(8) (a) Determine if a is a generator of $\mathbb{Z}_{17}^\times$ when (i) $a=2$ and (ii) $a=3$.
  (b) Compute $7^{169}+3^{89} \pmod{17}$.

Distribution of points															
(1)(a)	5	(2)(a)	4	(3)(a)	7	(4)(a)	7	(5)(a)	4	(6)(a)	4	(7)(a)	8	(8)(a)	5
(1)(b)	5	(2)(b)	6	(3)(b)	4	(4)(b)	4	(5)(b)	6	(6)(b)	6	(7)(b)	8	(8)(b)	2
		(2)(c)	5												
	10		15		11		11		10		10		16		7

Maximum total = 90
Exam score = Total score + 10