Faculty of Sciences	**Coding and Cryptography**
VU University Amsterdam	**Exam 18:30-21:15 13-01-2014**

Note
(1) This exam consists of 7 problems.
(2) Calculators, notes, books, etc., may not be used.
(3) Justify your answers!
(4) Throughout this exam, $K = \{0, 1\}$.

Problems

(1) Let C be a binary code of length $n = 5$ and distance $d = 4$.
  (a) Show that the Hamming bound gives $|C| \leq 5$.
  (b) Show that we in fact have $|C| \leq 2$.

(2) Let $X = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, 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) Use syndromes to determine if the received word $w = 11101100$ under IMLD can be decoded, where we correct any error of weight at most 1.

(3) (a) Determine how many idempotents $I(x)$ modulo $1 + x^{21}$ have degree 16.
  (b) For the idempotent $I(x)$ from (a) with the least number of terms, determine the generator polynomial $g(x)$ of the corresponding cyclic linear code C in K^{21} and compute the rate of this code.
  (c) Determine the number of divisors in $K[x]$ of $1 + x^{21}$ and of $1 + x^{84}$.

(4) (a) Factor $f(x) = x^7 + x^2 + 1$ in $K[x]$. (You may use without proof which polynomials in $K[x]$ are irreducible for degrees 1, 2 and 3.)
  (b) How many polynomials of degree 10 have 8 divisors including $f(x)$?

Please turn over for problems (5), (6) and (7).

In problems (5) and (6), $GF(2^4)$ 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}

(5) Let β and $GF(2^4)$ be as in the table, let $\alpha=\beta^4+\beta^{14}$, 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) Is α a primitive element of $GF(2^4)$?

(6) 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:
(a) w has syndrome $wH=[s_1,s_3]=[\beta^{14},\beta^{12}]$;
(b) w has syndrome $wH=[s_1,s_3]=[\beta^6,\beta^8]$.

(7) (a) Determine if a is a generator of $\mathbb{Z}_{23}^\times$ when (i) $a=2$ and (ii) $a=5$.
(b) Compute $3^{241}+5^{83} \pmod{23}$ in an efficient way.

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

Maximum exam score = 90

Score for the course = (10+Exam score)/2 + (Total homework score)/2