Faculty of Sciences	**Coding and Cryptography**
VU University Amsterdam	**Exam 15:15-18:00 26-10-2010**

Note

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

Problems

(1) Suppose C is a binary code of length 14 with 16 codewords and distance $d = 6$. How many words in K^n can be decoded under IMLD if we only decode error patterns of weight at most $t = \lfloor \frac{d-1}{2} \rfloor$? Do not simplify your answer to a number.

(2) Let

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

(a) Explain why H is a check matrix of the code $C = \{w \text{ in } K^8 \text{ with } wH = 0\}$.
(b) Determine the distance of C.

(3) Consider all cyclic linear codes over K of length $n = 21$.
(a) Show there are only two idempotents $I(x)$ modulo $1 + x^{21}$ of degree 12.
(b) Determine the generating polynomial $g(x)$ of the cyclic linear code C corresponding to the idempotent $x^3 + x^6 + x^{12}$.
(c) What is the *rate* of the code C in (b)?

(4) Let $p(x) = 1 + x^3 + x^6$ be in $K[x]$.
(a) Show that $p(x)$ is irreducible in $K[x]$. (You may use without proof which polynomials in $K[x]$ are irreducible for degrees 1, 2 and 3.)
(b) Let $GF(2^6)$ be constructed as $K[x]$ modulo $p(x)$, and let α be the class of x. Compute α^9 and determine if α is a primitive element of $GF(2^6)$.

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. Determine the minimal polynomial in $K[x]$ of $\alpha = 1 + \beta$.

(6) Let β and $GF(2^4)$ be as in the table. Let C be the 2-error correcting BCH code of length 15 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 $w(x)$ is a received word, determine if $d(v, w) \leq 2$ for some v in C in two cases:

(a) w has syndrome $wH = [s_1, s_3] = [\beta^9, \beta^7]$;

(b) w has syndrome $wH = [s_1, s_3] = [\beta, \beta^3]$.

(7) Consider $\mathbb{Z}_{11}$.

(a) Determine a generator of $\mathbb{Z}_{11}^{\times}$.

(b) Write $2^{21} + 3^{23}$ modulo 11 as $0, 1, \ldots, 10$.

Distribution of points						
(1) 5	(2)(a) 5	(3)(a) 7	(4)(a) 11	(5) 11	(6)(a) 8	(7)(a) 5
	(2)(b) 7	(3)(b) 7	(4)(b) 7		(6)(b) 8	(7)(b) 4
		(3)(c) 5				
5	12	19	18	11	16	9

Maximum exam score = 90

Score for the course = (10+Exam score)/2 + (Total homework score)/3