Faculty of Science	**Coding and cryptography (X_405041)**
Vrije Universiteit Amsterdam	**Exam 25-3-2021 (8:30-11:15)**

Note
(1) This exam consists of 8 problems.
(2) Calculators, notes, books, etc., may not be used.
(3) Do not hand in scrap, etc., and when handing in $n \geq 1$ sheets, number them $1/n, \ldots, n/n$.
(4) Justify your answers!
(5) Throughout this exam, $K = \{0, 1\}$.

Problems

(1) For each of the following linear codes in K^9, explain either why it cannot exist, or construct an example. If you give an example, do show that your code has the right properties.
  (a) A $(9, 5, 5)$-code.
  (b) A $(9, 8, 2)$-code.

(2) Let X be a matrix with as rows all the elements in K^7 of weight 3, and let $H = \begin{bmatrix} I \\ X \end{bmatrix}$.
It is given that H is the check matrix of a linear code C.
  (a) What is the rate of 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 1. 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 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 $w = 1011101$ for this code.

(4) Let C be the smallest cyclic linear code in K^{15} that contains $x^7 + x^2 + 1$.
  (a) Determine the generator polynomial of C.
  (b) Determine the distance $d(C)$.

(5) **The two parts of this problem are independent of each other.**
  (a) Factorize $f(x) = x^8+x^7+x+1$ into irreducibles in $K[x]$. (You may use without proof which polynomials in $K[x]$ are irreducible for degrees 1, 2 and 3.)
  (b) Determine the number of idempotents $I(x)$ in $K[x]$ modulo $1+x^{15}$, and use this to determine the number of divisors in $K[x]$ of $1 + x^{30}$.

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 $\alpha = \beta^2 + \beta^8$, 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 $wH = [s_1, s_3] = [\beta^7, 0]$;
  (b) w has syndrome $wH = [s_1, s_3] = [\beta^{13}, \beta^9]$.

(8) Let $n = 177$.
  (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							
1a: 4	2a: 4	3a: 7	4a: 6	5a: 9	6a: 4	7a: 8	8a: 6
1b: 4	2b: 6	3b: 4	4b: 4	5b: 7	6b: 4	7b: 8	8b: 2
	2c: 3						
Maximum total = 90							
Exam grade = 1 + Total/10							