Faculty of Science	**Coding and cryptography (X_405041)**
Vrije Universiteit Amsterdam	**Resit 2-6-2021 (18:45-21:30)**

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

Problems

(1) For each of the following linear codes in K^7, 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 $(7, 3, 4)$-code.
 (b) A $(7, 5, 3)$-code.

(2) Let H be a matrix with as rows all vectors in K^9 of weight 1 or 8.
 (a) Verify that H satisfies the conditions to be a parity check matrix for a binary linear code C.
 (b) What is the rate of C?
 (c) Determine $d(C)$.
 (d) 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 $w = 1110110$ for this code.

(4) **All parts of this problem are independent of each other.**
 (a) Factorise $f(x) = x^8+x^7+x^5+1$ 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 generator polynomial of the smallest cyclic linear code in K^{10} that contains $x^6 + x^4 + x^3 + x^2 + 1$.
 (c) Determine the number of idempotents $I(x)$ in $K[x]$ modulo $1 + x^{17}$ that have degree 14.

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

In problems (5) and (6), $GF(2^4)$ is constructed as $K[x]$ modulo $1+x+x^4$ 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	1	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}

(5) Let β and $GF(2^4)$ be as in the table, let $\alpha=\beta^4+\beta^{12}$, 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.

(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 $wH=[s_1,s_3]=[\beta^9,\beta^{12}]$;
  (b) w has syndrome $wH=[s_1,s_3]=[1,\beta^7]$.

(7) Let $n=81$.
  (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: 5	2a: 2	3a: 7	4a: 10	5a: 4	6a: 8	7a: 5
1b: 3	2b: 3	3b: 4	4b: 7	5b: 6	6b: 8	7b: 2
	2c: 7		4c: 6			
	2d: 3					
Maximum total = 90						
Exam grade = 1 + Total/10						