Faculty of Science	**Coding and cryptography (X_405041)**
Vrije Universiteit Amsterdam	**Exam 8-6-2023 (18:45-21:30)**

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) In this problems we consider linear $(n, n-3, 3)$-codes in K^n for $n \geq 4$.
   (a) Show that there is no such code if $n > 7$.
   (b) Construct such codes for $n = 4, 5, 6$ and 7. (Hint: construct suitable check matrices H and explain why they define such codes.)

(2) Let H be a matrix with as rows all the elements in K^8 of weight 1, 3 and 5.
   (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 the distance $d(C)$ of 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 $w = 1010011$ for this code.

(4) Let $I(x)$ modulo $1 + x^{25}$ be the idempotent that contains the term x^{10} and has the smallest possible number of terms.
   (a) Compute $I(x)$.

   Now let C be the smallest cyclic linear code in K^{25} that contains $I(x)$.
   (b) Show that the generator polynomial of C is $g(x) = 1 + x^5$.
   (c) Compute the dimension of C.
   (d) Determine the distance $d(C)$ of C.

(5) In this problem, you may use without proof which polynomials in $K[x]$ are irreducible for degrees 1, 2 and 3.
   NB The two parts of this problem are independent of each other.
   (a) Factorize $f(x) = x^8 + x^3 + x$ into irreducibles in $K[x]$.
   (b) Determine the number of divisors of $1 + x^{48}$ in $K[x]$. *Hint:* $48 = 16 \cdot 3$.

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	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}

(6) Let β and $GF(2^4)$ be as in the table, let $\alpha=\beta^5+\beta^6$, 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 $d(v,w)\le 2$ for some v in C in two cases:
   (a) w has syndrome $wH=[s_1,s_3]=[0,\beta]$;
   (b) w has syndrome $wH=[s_1,s_3]=[\beta^{14},\beta^{11}]$.

(8) (a) Perform the Miller-Rabin probabilistic primality test for $n=137$ 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:	2	3a:	7	4a:	4	5a:	7	6a:	4	7a:	8	8a:	4
1b:	5	2b:	4	3b:	4	4b:	3	5b:	4	6b:	6	7b:	8	8b:	2
		2c:	6			4c:	1								
		2d:	3			4d:	4								
Maximum total = 90															
Exam grade = 1 + Total/10															