Coding and cryptography

Assignment 2 (2022-2023)

Solutions.

For the sake of clarity, below we have not included explicit calculations for long divisions, or for the Euclidean algorithm, but they should be part of your own (complete) solutions.

1. We try to divide irreducible polynomials of increasing degree into $f(x) = x^{10}+x^6+x^5+x^4+x^3+x+1$.

   (a) x and $x+1$ are each not a factor of $f(x)$ because $f(0) \neq 0$ and $f(1) \neq 0$.

   (b) Long division of x^2+x+1 into $f(x)$ shows that $f(x) = (x^2+x+1)g(x)$ with $g(x) = x^8 + x^7 + x^5 + x^2 + 1$. $g(x)$ may still contain a factor x^2+x+1, and it does; long division gives $g(x) = (x^2+x+1)h(x)$ with $h(x) = x^6+x^4+x^2+x+1$. $h(x)$ may still contain a factor x^2+x+1, but in this case long division gives $h(x) = (x^4+x^3+x^2)(x^2+x+1)+(x+1)$ as division with remainder, so this is not the case.

   (c) $h(x)$ might now be the product of 2 irreducible polynomials of degree 3, so we divide x^3+x+1 and x^3+x^2+1 into $h(x)$ using long division. This gives $h(x) = (x^3+1)(x^3+x+1)+x^2$ and $h(x) = (x^3+x^2+1)(x^3+x^2+1)+(x^2+x)$ as division with remainder, so neither is a factor.

   So $h(x)$ is irreducible: because $\deg(h(x)) = 6$, it cannot contain an irreducible factor of degree bigger than 3 unless it also contains one of degree less than 3, which we found is not the case.

   We now found $f(x) = (x^2+x+1)g(x) = (x^2+x+1)^2h(x) = (x^2+x+1)^2(x^6+x^4+x^2+x+1)$, and know that in the last expression all three factors are irreducible. So that is the required factorisation.

2. (a) Note that 9 is odd, so we compute the sets C_i in $\{0,1,\ldots,8\}$.

   $C_0 = \{0\}$, $C_1 = \{1,2,4,8,7,5\}$ because $2 \cdot 5 \equiv 1$ modulo 9, and $C_3 = \{3,6\}$ because $2 \cdot 6 \equiv 3$ modulo 9. That gives all 9 elements of $\{0,1,\ldots,14\}$, so we are done. (Note that $C_2 = C_4 = C_5 = C_7 = C_8 = C_1$ and $C_6 = C_3$, so we do not need to compute those.)

   If we let $f_0(x) = 1$, $f_1(x) = x+x^2+x^3+x^5+x^7+x^8$ and $f_3(x) = x^3+x^6$ be the corresponding polynomials, then the idempotents in $K[x]$ modulo $1+x^9$ are the eight polynomials 0, $f_0(x)$, $f_1(x)$, $f_3(x)$, $f_0(x)+f_1(x)$, $f_0(x)+f_3(x)$, $f_1(x)+f_3(x)$, and $f_0(x)+f_1(x)+f_3(x)$.

   (b) The constant term 1 in a sum of the $f_i(x)$ with $i = 0$, 1 or 3 can only come from $f_0(x)$, and the term x only from $f_1(x)$. So the idempotents that satisfy the conditions are $I_1(x) = f_0(x)+f_1(x) = 1+x+x^2+x^4+x^5+x^7+x^8$ and $I_2(x) = f_0(x)+f_1(x)+f_3(x) = 1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$.

   The generator polynomial of the corresponding code is $\gcd(I_i(x), 1+x^9)$ (In general, the generator polynomial of the smallest cyclic linear code of length n that contains $v(x)$ is $\gcd(v(x), 1+x^n)$.) This can be computed using the Euclidean algorithm.

   For $I_2(x)$ it is faster to note that $1+x^9 = (1+x)I_2(x)$, so that $\gcd(I_2(x), 1+x^9) = I_2(x)$ (but this is the first step of the Euclidean algorithm anyway).

   For $I_1(x)$ the algorithm gives that the generator polynomial is $1+x+x^2$.

   (c) We know for n odd that, if there are s irreducible factors in $1+x^n$ (necessarily distinct because n is odd), then there are 2^s divisors of $1+x^n$ in $K[x]$ as well as 2^s idempotents in $K[x]$ modulo $1+x^n$. So s is the number of distinct C_i we find. For $n = 9$ (which is odd), we find $s = 3$, hence there are $2^3 = 8$ divisors of $1+x^9$.

   Since $1+x^9$ has three distinct irreducible factors, say $1+x^9 = g_1(x)g_2(x)g_3(x)$, the factorisation of $1+x^{36} = (1+x^9)^4$ is $g_1(x)^4g_2(x)^4g_3(x)^4$, so it has $(4+1)(4+1)(4+1) = 125$ divisors in $K[x]$.

   For any n, the cyclic linear codes of length n correspond 1-1 to the divisors of $1+x^n$ in $K[x]$. The 'codes' $\{000\ldots0\}$ and K^n correspond to the divisors $1+x^n$ and 1, so the number of codes asked for in the question is $2^3-2 = 6$ for $n = 9$, and $125-2 = 123$ for $n = 36$.

3. (a)

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}

We computed the next line out of the previous one by using $\beta^4 = 1 + \beta^3$ if necessary (i.e., by replacing 0000|1 with 1001 if we shift an element in K^4 'to the right' by adding a 0 on the left).

(b) We have to check if $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{14}$ are the 15 non-zero elements of $GF(2^4)$. But this begins $1, \beta^6, \beta^{12}, \beta^3, \beta^9, 1, \beta^6, \ldots$ because $\beta^{15} = 1$. (Note that we write everything in the form β^i for $i = 0, 1, \ldots, 14$ so that we can immediately see if elements are different or not.) So α is not a primitive element of this $GF(2^4)$.

(c) We compute the set $S = \{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \ldots\}$ with the elements that we obtain from α by iterated squaring. Here $S = \{\beta^6, \beta^{12}, \beta^9, \beta^3\}$, where we again wrote everything in the form β^i for $i = 0, 1, 2, \ldots, 14$, and used that $\beta^{15} = 1$.
So $m_\alpha(x)$ has degree $|S| = 4$ and is of the form $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + x^4$ for some (unique) a_0, a_1, a_2, a_3 in K. Plugging in α for x and using the expressions for $\alpha = \beta^6$, $\alpha^2 = \beta^{12}$, $\alpha^3 = \beta^3$ and $\alpha^4 = \beta^9$ from the table gives that we must solve

$$a_0 \cdot 1000 + a_1 \cdot 1111 + a_2 \cdot 1100 + a_3 \cdot 0001 + 1010 = 0000$$

in K^4. Looking at the four positions gives the system of equations

$$\begin{cases} a_0 + a_1 + a_2 = 1 \\ a_1 + a_2 = 0 \\ a_1 = 1 \\ a_1 + a_3 = 0 \end{cases},$$

which gives the solution $a_1 = 1$ from the third equation, then $a_2 = a_3 = 1$ from the second and fourth equations, and then $a_0 = 1$ from the first equation. So $m_\alpha(x) = 1 + x + x^2 + x^3 + x^4$.

4. (a) Here $[s_1, s_3] \neq [0, 0]$ so w is not in the code. $s_1^3 = \beta^{27} = \beta^{12} \neq \beta^7 = s_3$, so we have to write down the auxiliary polynomial $z^2 + s_1 z + s_1^{-1}(s_1^3 + s_3)$, which is $z^2 + \beta^9 z + \beta^8$ because $s_1^{-1}(s_1^3 + s_3) = \beta^{-9}(\beta^{12} + \beta^7) = \beta^{-9}\beta^2 = \beta^{-5} = \beta^8$. Hence pairs (β^i, β^j) of roots satisfy $i + j \equiv 8$ modulo 15 as well as $\beta^i + \beta^j = s_1 = \beta^9$. Starting from (β^4, β^4) where $i = j$ (which itself is discarded as $\beta^4 + \beta^4 = 0 \neq s_1$) we compute $\beta^i + \beta^j$ and find:

$$\begin{array}{ll} (\beta^3, \beta^5): & \beta^{12} \\ (\beta^2, \beta^6): & \beta^5 \\ (\beta, \beta^7): & \beta^9 \end{array} \qquad \begin{array}{ll} (1, \beta^8): & \beta^6 \\ (\beta^{14}, \beta^9): & \beta^4 \\ (\beta^{13}, \beta^{10}): & \beta^{14} \\ (\beta^{12}, \beta^{11}): & \beta^8 \end{array}$$

So $\beta + \beta^7 = \beta^9$, $z^2 + \beta^9 z + \beta^8 = (z + \beta)(z + \beta^7)$, and we can modify w into a codeword v by changing the second and eighth positions. In terms of polynomials, we decode $w(x)$ to $v(x) = w(x) + x + x^7$. NB the calculations in the last column are therefore redundant in this case, but included here for the sake if (over)completeness. They would be crucial if the auxiliary polynomial did not have roots in the field.

(b) Here $[s_1, s_3] \neq [0, 0]$ so w is not in the code. Because $s_1^3 = \beta^3 = s_3$, there is exactly one error, in the position for β, i.e., the second position. In terms of polynomials, we decode $w(x)$ to $v(x) = w(x) + x$.