UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

Final exam, January 2020 – Answers

Question 1. i. Let $\sqrt{-5}$ be a root of $X^2+5 \in \mathbb{Z}[X]$. Show that 3 is irreducible, but not prime in $\mathbb{Z}[\sqrt{-5}]$.

ii. Compute $\phi(31)$ and find (or describe) all the primitive elements of $\mathbb{F}_{2^5}$.

Answer. i. Define the following map:

$$\nu \; : \; \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_{\geq 0}, \quad a+b\sqrt{-5} \mapsto a^2+5b^2.$$

It is trivial to check that $\nu((a+b\sqrt{-5})(c+d\sqrt{-5})) = \nu(a+b\sqrt{-5})\nu(c+d\sqrt{-5})$. It follows that the only units of $\mathbb{Z}[\sqrt{-5}]$ are ± 1. Next, assume that

$$3 = (a+b\sqrt{-5})(c+d\sqrt{-5}).$$

It follows that $\nu(a+b\sqrt{-5})\nu(c+d\sqrt{-5}) = 9$. We have three possibilities:

(a) if $\nu(a+b\sqrt{-5}) = 1$, then $a+b\sqrt{-5} = 1$, a unit,
(b) if $\nu(a+b\sqrt{-5}) = 3$, then $a^2+5b^2 = 3$, impossible and
(c) if $\nu(a+b\sqrt{-5}) = 9$, then $\nu(c+d\sqrt{-5}) = 1$ and $c+d\sqrt{-5} = 1$, a unit.

It follows that 3 is irreducible. However, $3 \mid (2+\sqrt{-5})(2-\sqrt{-5})$, but $3 \nmid (2+\sqrt{-5})$ and $3 \nmid (2-\sqrt{-5})$, that is, 3 is not prime.

ii. 31 is a prime, hence $\phi(31) = 30$. We have that $2^5 = 32$, hence $\mathbb{F}_{2^5}$ has $\phi(31) = 30$ primitive elements, i.e., all of its elements are primitive except exactly two. Since 0 and 1 cannot be primitive in $\mathbb{F}_{2^5}$, it follows that all the elements $\neq 0, 1$ are primitive. □

Question 2. Find the minimum n such that $\mathbb{F}_{2^n}$ contains all the roots of $X^{18}-1 \in \mathbb{F}_2[X]$. List all the intermediate extensions of $\mathbb{F}_{2^n}/\mathbb{F}_2$.

Answer. Over $\mathbb{F}_2$, we have that

$$X^{18}-1 = (X^9-1)^2 = (\Psi_1\Psi_3\Psi_9)^2.$$

We have that $\Psi_1 = X-1$. Also, $\mathrm{ord}_3(2) = 2$ and $\mathrm{ord}_9(2) = 6$. These facts, combined with the facts that $\phi(3) = 2$ and $\phi(9) = 6$ imply that Ψ_3 and Ψ_9 are irreducible polynomials of degree 2 and 6 respectively. It follows that $n = 6$ and the intermediate extensions of $\mathbb{F}_{2^6}/\mathbb{F}_2$ are $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^6}$. □

Question 3. i. Prove the *generalized Möbius inversion formula*: if $f : \mathbb{Z} \to G$ and $F : \mathbb{Z} \to G$, where $(G, \cdot)$ an abelian group, then

$$f(n) = \prod_{d|n} F(d) \Rightarrow F(n) = \prod_{d|n} f(d)^{\mu(n/d)}.$$

Hint: Use the identity $\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$

ii. Show that

$$\Psi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Answer. i. We have that

$$\prod_{d|n} f(d)^{\mu(n/d)} = \prod_{d|n} f\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n}\left(\prod_{k|\frac{n}{d}} F(k)\right)^{\mu(d)} = \prod_{d|n}\prod_{k|\frac{n}{d}} F(k)^{\mu(d)}$$
$$= \prod_{d|n} F(d)^{\sum_{k|\frac{n}{d}} \mu(k)}.$$

The latter combined with the identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$$

imply the desired result.

ii. We work on the abelian group $(\mathbb{F}_q(x), \cdot)$. Using the generalized Möbius inversion formula on the identity

$$x^n - 1 = \prod_{d|n} \Psi_d(x)$$

immediately yields the desired result. □

Question 4. Let α be a root of the irreducible polynomial $X^2 + X + 1 \in \mathbb{F}_2[X]$. We define the linear code C over $\mathbb{F}_4 = F_2(\alpha)$ as follows:

$$C = \{(x_1, x_2, x_3, x_4, x_5) \in F_4^5 : x_4 = \alpha x_1 + x_2 + x_3 \text{ and } x_5 = x_1 + \alpha x_2 + (\alpha + 1)x_3\}$$

i. Find a generator and a parity-check matrix of C.

ii. Show that the parameters of the code are $[5, 3, 2]$.

Answer. i. It is immediate from the definition of C that a generator matrix is

$$G = \begin{pmatrix} 1 & 0 & 0 & \alpha & 1 \\ 0 & 1 & 0 & 1 & \alpha \\ 0 & 0 & 1 & 1 & \alpha + 1 \end{pmatrix}.$$

We take advantage of the fact that G is in standard form and immediately extract the following parity-check matrix

$$H = \begin{pmatrix} \alpha & 1 & 1 & 1 & 0 \\ 1 & \alpha & \alpha + 1 & 0 & 1 \end{pmatrix}.$$

ii. Since H is a 2×5 matrix it is clear that C is an $[5, 3]$-code and it remains to show that $d(C) = 2$. Notice that H does not contain the all-zero column, i.e., $d(C) > 1$, while the first and the third columns of H are linearly dependent (multiplying the first column by $\alpha + 1$ gives us the third column), thus $d(C) \leq 2$. It follows that $d(C) = 2$. □

Question 5. Show that the Reed-Muller code $\mathcal{R}(1, 3)$ is self-dual.

Answer. We construct $\mathcal{R}(1,i)$, for $1 \leq i \leq 3$, as follows:

$$\begin{aligned}
\mathcal{R}(1,1) =& \{00, 01, 10, 11\},\\
\mathcal{R}(1,2) =& \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\},\\
\mathcal{R}(1,3) =& \{00000000, 01010101, 10101010, 11111111, 00110011, 01100110, 10011001, 1100110,\\
& 00001111, 01011010, 10100101, 11110000, 00111100, 01101001, 10010110, 11000011\}.
\end{aligned}$$

We easily confirm that $\mathcal{R}(1,3)$ is self-orthogonal, i.e. $\mathcal{R}(1,3) \subseteq \mathcal{R}(1,3)^{\perp}$. Furthermore, we know that $\mathcal{R}(1,3)$ is an $[8,4,4]$-code, hence

$$\dim(\mathcal{R}(1,3)^{\perp}) = 8 - 4 = 4 = \dim(\mathcal{R}(1,3)).$$

It follows that $\mathcal{R}(1,3) = \mathcal{R}(1,3)^{\perp}$. □

Question 6. Let C be a linear $[n,k,d]$-code over $\mathbb{F}_q$ with $d \geq 2$. Choose some $1 \leq i \leq n$ and delete the i-th coordinate of every codeword. So, we define the code

$$C_i = \{(c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n) : (c_1, \dots, c_n) \in C\}.$$

i Show that C_i has parameters $[n-1, k, d_i]$ with $d - 1 \leq d_i \leq d$.

ii If C is MDS, show that C_i is also MDS.

Answer. i. It is clear that by construction, that C_i is linear and has length $n-1$. Also, since $d \geq 2$, the deletion of one coordinate cannot result a reduction in the number of codewords, as this would imply that two codewords of C differ only in the deleted coordinate. Hence $|C_i| = |C|$, that is, $\dim(C_i) = \dim(C) = k$. Regarding the minimum distance, note that the Hamming weight of a codeword of C_i can be either equal or smaller by exactly 1, when compared with the Hamming weight of the corresponding codeword of C. It follows that $d(C_i) = d(C)$ or $d(C_i) = d(C) - 1$.

ii. Since C is MDS, we have that

$$k + d = n + 1.$$

From the previous item, C_i is an $[n-1, k, d']$-code, where $d' = d$ or $d' = d - 1$. If $d' = d$, then the parameters of C_i violate the Singleton bound, hence $d' = d - 1$. It follows that C_i is MDS. □