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

Final exam, September 2020 – Answers

**Question 1.** Find an irreducible polynomial of degree 3 over $\mathbb{F}_2$, that is not primitive, or explain why such polynomial does not exist.

*Answer.* Notice that, trivially, all polynomials over $\mathbb{F}_2$ are monic. We have that there are

$$\frac{\phi(2^3-1)}{3} = \frac{\phi(7)}{3} = \frac{6}{3} = 2$$

primitive polynomials of degree 3 over $\mathbb{F}_2$. Likewise, there are

$$\frac{1}{3}\sum_{d|3} \mu(d) 2^{3/d} = \frac{2^3-2}{3} = \frac{6}{3} = 2$$

irreducible polynomials of degree 3 over $\mathbb{F}_2$. Since all primitive polynomials are also irreducible, this means that, in this case, the opposite is also true. Hence there are no irreducible polynomials of degree 3 over $\mathbb{F}_2$ that are not primitive. □

**Question 2.** i. Prove that $\Psi_{19}$ and $\Psi_{27}$ are both irreducible and of the same degree over $\mathbb{F}_2$.

ii. Let $q$ be a prime power and let $\zeta$ be a primitive $n$-th root of unity over $\mathbb{F}_q$. Prove that

$$\sum_{i=0}^{n-1} \zeta^i = \begin{cases} 0, & \text{if } n \neq 1, \\ 1, & \text{if } n = 1. \end{cases}$$

*Hint:* Observe that $\{\zeta^i \ : \ i = 0, \dots, n-1\}$ are exactly the roots of $X^n - 1$.

*Answer.* i. First, observe that

$$\deg(\Psi_{19}) = \phi(19) = 18 = \phi(27) = \deg(\Psi_{27}).$$

Further, we have that $\Psi_{19}$ factors into $\phi(19)/d$ distinct monic irreducible polynomials of degree $d$, where $d$ is the order of 2 modulo 19. We easily verify that, in this case, $d = 18 = \phi(19)$, that is, $\Psi_{19}$ is irreducible. Similarly, $\Psi_{27}$ is also irreducible.

ii. The result is trivial when $n = 1$. Assume that $n > 1$. Observe that $\{\zeta^i \ : \ i = 0, \dots, n-1\}$ are exactly the roots of $X^n - 1$. Thus

$$X^n - 1 = (X-1)(X-\zeta)\cdots(X-\zeta^{n-1}).$$

In the above polynomial equation, observe that the coefficient of $X^{n-1}$ on the LHS is 0 and the coefficient of $X^{n-1}$ on the RHS is $-1-\zeta-\cdots-\zeta^{n-1}$. The result follows. □

**Question 3.** i. Find all the primitive elements of $\mathbb{F}_{13}$.

ii. Recall that the *information rate* of a $q$-ary $(n, M, d)$-code $C$ is $\delta := \frac{\log_q(|C|)}{n}$. If $\delta_r$ stands for the information rate of $\mathrm{Ham}(r, 2)$, determine $\lim_{r\to\infty} \delta_r$.

*Answer.* i. First, we notice that we have $\phi(13-1) = \phi(12) = 4$ primitive elements in $\mathbb{F}_{13}$. Moreover, the order of an element of $\mathbb{F}_{13}^*$ must divide 12, i.e., it may be $1, 2, 3, 4, 6$ or 12. We check that $\text{ord}(2) = 12$, as $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^3 = 8 \neq 1$, $2^4 = 16 = 3 \neq 1$ and $2^6 = 2^4 2^2 = 3 \cdot 4 = 12 \neq 1$. It follows that 2 is primitive in $\mathbb{F}_{13}$. It follows that the primitive elements of $\mathbb{F}_{13}$ are

$$\{2^i \ : \ 1 \leq i \leq 12, \gcd(i, 12) = 1\} = \{2^1, 2^5, 2^7, 2^{11}\} = \{2, 6, 11, 7\}.$$

ii. We have that $\text{Ham}(r, 2)$ is a binary $[2^r - 1, 2^r - 1 - r, 3]$-code. It follows that $\delta_r = \frac{2^r - 1 - r}{2^r - 1}$, hence $\lim_{r \to \infty} \delta_r = 1$. □

**Question 4.** Let $C$ be the binary code with generator matrix

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

After you determine the parameters of $C$, decode the words $w_1 = 11111$ and $w_2 = 00111$, using syndrome decoding.

*Answer.* Note that $G$ is in standard form. It follows that

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

is a parity-check matrix for $C$. From $H$, we get that $C$ is a binary $[5, 2, 3]$-code. It follows that we will have a total of 8 syndromes and, since $C$ corrects 1 error, all words of Hamming weight up to 1 will appear as coset leaders, while we will have to find two more words (of weight 2), that will correspond to the remaining syndromes. So, we get that a syndrome look-up table is the following:

| Coset leader | Syndrome |
|---|---|
| 00000 | 000 |
| 10000 | 110 |
| 01000 | 011 |
| 00100 | 100 |
| 00010 | 010 |
| 00001 | 001 |
| 11000* | 101 |
| 01100* | 111 |

We compute $S(w_1) = 010$, so the error is $e_1 = 00010$ and we decode to 11101. Finally, we compute $S(w_2) = 111$, which means that we decode only in the case of complete decoding and in which case, we may assume that the error term is $e_2 = 01100$ and we may decode to 01011. □