UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2018-19)
LECTURER: G. KAPETANAKIS

## FINAL EXAM – SEPTEMBER 2019

1. i. Find all the subfields of $\mathbb{F}_{64}$.
   ii. Find all the primitive elements of $\mathbb{F}_9$.
   iii. How many monic primitive polynomials of degree 2 are there over $\mathbb{F}_3$?
2. i. Show that $f(X) = X^3 - X - 3 \in \mathbb{F}_5[X]$ is irreducible.
   ii. Let $\alpha \in \mathbb{F}_{5^3}$ be a root of $f$. Express all the roots of $f$ with respect to the basis $\{1, \alpha, \alpha^2\}$.
   iii. Compute $N(\alpha)$.
   iv. Find all the $\beta \in \mathbb{F}_{5^3}$ such that $N(\beta) = 0$.
3. i. Show that 2 is an irreducible, but not a prime element of $\mathbb{Z}[\sqrt{5}]$, where $\sqrt{5}$ is a root of $X^2 - 5 \in \mathbb{Z}[X]$.
   ii. If $\pi_q(n)$ stands for the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree $n$, compute the numbers $\pi_3(4)$ and $\pi_4(3)$.
4. Let $C$ be the linear binary code with parity-check matrix

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

   i. Find a generator matrix of $C$ and compute the parameters of $C$. How many errors can $C$ correct?
   ii. Write all the codewords of $C$ and decode the words $w_1 = 110110$ and $w_2 = 101011$.
5. Let $C$ be a code over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ with parity-check matrix

$$H = \begin{pmatrix} 1 & \alpha & 1 & 0 \\ 1 & \alpha^2 & 0 & 1 \end{pmatrix}.$$

   i. Show that $C$ is MDS.
   ii. Show that $C \oplus C^{\perp}$ is not MDS.

---

1. All exercises are equivalent, with a maximum of 10 points.
2. The duration of the exam is 2.5 hours and you are allowed to leave the classroom the earliest 30 minutes after the beginning of the exam.
3. During the exam you are not allowed to have any bags, notes, books or electronics (calculators, mobiles, tablets, laptops etc.) on or next to you.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΕΦΑΡΜΟΣΜΕΝΗ ΑΛΓΕΒΡΑ - ΜΕΜ244 (ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2018-19)
ΔΙΔΑΣΚΩΝ: Γ. ΚΑΠΕΤΑΝΑΚΗΣ

## ΕΠΑΝΑΛΗΠΤΙΚΗ ΕΞΕΤΑΣΗ – ΣΕΠΤΕΜΒΡΙΟΣ 2019

1. i. Βρείτε όλα τα υποσώματα του $\mathbb{F}_{64}$.
   ii. Βρείτε όλα τα πρωταρχικά στοιχεία του $\mathbb{F}_9$.
   iii. Πόσα μονικά πρωταρχικά πολυώνυμα βαθμού 2 έχει το $\mathbb{F}_3$;

2. i. Δείξτε ότι το $f(X) = X^3 - X - 3 \in \mathbb{F}_5[X]$ είναι ανάγωγο.
   ii. Έστω $\alpha \in \mathbb{F}_{5^3}$ ρίζα του $f$. Γράψτε όλες τις ρίζες του $f$ ως προς την βάση $\{1, \alpha, \alpha^2\}$.
   iii. Υπολογίστε το $N(\alpha)$.
   iv. Βρείτε όλα τα $\beta \in \mathbb{F}_{5^3}$ τέτοια ώστε $N(\beta) = 0$.

3. i. Δείξτε ότι το 2 είναι ανάγωγο, αλλά όχι πρώτο στον δακτύλιο $\mathbb{Z}[\sqrt{5}]$, όπου $\sqrt{5}$ ρίζα του $X^2 - 5 \in \mathbb{Z}[X]$.
   ii. Αν $\pi_q(n)$ δείχνει τον αριθμό των μονικών ανάγωγων πολυωνύμων του $\mathbb{F}_q$ βαθμού $n$, υπολογίστε τους αριθμούς $\pi_3(4)$ και $\pi_4(3)$.

4. Έστω $C$ ο δυαδικός γραμμικός κώδικας με πίνακα ελέγχου τον

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

   i. Γράψτε έναν γεννήτορα πίνακα του $C$ και βρείτε τις παραμέτρους του $C$. Πόσα λάθη διορθώνει ο $C$;
   ii. Γράψτε όλες τις κωδικολέξεις του $C$ και αποκωδικοποιείστε τις λέξεις $w_1 = 110110$ και $w_2 = 101011$.

5. Έστω $C$ κώδικας υπέρ του $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ με πίνακα ελέγχου

$$H = \begin{pmatrix} 1 & \alpha & 1 & 0 \\ 1 & \alpha^2 & 0 & 1 \end{pmatrix}.$$

   i. Δείξτε ότι ο $C$ είναι MDS.
   ii. Δείξτε ότι ο $C \oplus C^{\perp}$ δεν είναι MDS.

---

1. Όλα τα θέματα είναι ισοδύναμα και άριστα είναι το 10.
2. Η διάρκεια της εξέτασης είναι 2,5 ώρες και μπορείτε να αποχωρίσετε από την αίθουσα το νωρίτερο 30 λεπτά μετά την αρχή της εξέτασης.
3. Κατά την διάρκεια της εξέτασης δεν επιτρέπεται να έχετε πάνω σας ή δίπλα σας τσάντες, σημειώσεις, βιβλία ή ηλεκτρονικές συσκευές (αριθμομηχανές, κινητά, ταμπλέτες, φορητούς υπολογιστές κτλ.).