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

FINAL EXAM – JANUARY 2020

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 $\mathbb{F}_{2^5}$.

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 $\mathbb{F}_{2^n}/\mathbb{F}_2$.

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

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 $[5, 3, 2]$.

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

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

---

1. Each question is worth 2 points and the maximum score is 10 points. You may answer as many and any questions you prefer.
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 2019-20)
ΔΙΔΑΣΚΩΝ: Γ. ΚΑΠΕΤΑΝΑΚΗΣ

ΤΕΛΙΚΗ ΕΞΕΤΑΣΗ – ΙΑΝΟΥΑΡΙΟΣ 2020

1. i. Έστω $\sqrt{-5}$ ρίζα του $X^2+5 \in \mathbb{Z}[X]$. Δείξτε ότι το 3 είναι ανάγωγο, αλλά όχι πρώτο στον $\mathbb{Z}[\sqrt{-5}]$.

   ii. Υπολογίστε το $\phi(31)$ και βρείτε (ή περιγράψτε) τα πρωταρχικά στοιχεία του $\mathbb{F}_{2^5}$.

2. Υπολογίστε τον ελάχιστο φυσικό αριθμό n τέτοιο ώστε το $\mathbb{F}_{2^n}$ να περιέχει όλες τις ρίζες του $X^{18}-1 \in \mathbb{F}_2[X]$. Απαριθμήστε όλες τις ενδιάμεσες επεκτάσεις της $\mathbb{F}_{2^n}/\mathbb{F}_2$.

3. i. Αποδείξτε τον *γενικευμένο τύπο αντιστροφής του Möbius*: αν $f : \mathbb{Z} \to G$ και $F : \mathbb{Z} \to G$, όπου $(G, \cdot)$ αβελιανή ομάδα, τότε

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

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

   ii. Δείξτε ότι

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

4. Έστω το ανάγωγο πολυώνυμο $X^2 + X + 1 \in \mathbb{F}_2[X]$ και α μία ρίζα του. Ορίζουμε το γραμμικό κώδικα C πάνω από το $\mathbb{F}_4 = F_2(\alpha)$ ως

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

   i. Βρείτε έναν γεννήτορα και ένα πίνακα ελέγχου του C.

   ii. Δείξτε ότι οι παράμετροι του κώδικα είναι $[5, 3, 2]$.

5. Δείξτε ότι ο κώδικας Reed-Muller $\mathcal{R}(1, 3)$ είναι αυτοδυϊκός.

6. Έστω C ένας γραμμικός $[n, k, d]$-κώδικας πάνω από το $\mathbb{F}_q$ με $d \geq 2$. Επιλέγουμε κάποιο $1 \leq i \leq n$ και διαγράφουμε την i-στη συντεταγμένη κάθε διανύσματος. Έτσι ορίζουμε τον κώδικα

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

   i Αποδείξτε ότι ο C_i έχει παραμέτρους $[n-1, k, d_i]$ με $d - 1 \leq d_i \leq d$.

   ii Εάν ο C είναι MDS δείξτε ότι και ο C_i είναι MDS.

---

1. Κάθε θέμα βαθμολογείται με 2 βαθμούς και μέγιστη βαθμολογία είναι το 10. Μπορείτε να απαντήσετε όποια και όσα θέματα προτιμάτε.
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.).