



**FINAL EXAM – SEPTEMBER 2020**

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

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  $\text{Ham}(r, 2)$ , determine  $\lim_{r \rightarrow \infty} \delta_r$ .
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.

- 
1. Each question is worth 2.5 points and the maximum score is 10 points.
  2. The duration of the exam is 1.5 hours.
  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.



ΤΕΛΙΚΗ ΕΞΕΤΑΣΗ – ΣΕΠΤΕΜΒΡΙΟΣ 2020

1. Βρείτε ένα ανάγωγο πολυώνυμο βαθμού 3 πάνω από το  $\mathbb{F}_2$ , το οποίο δεν είναι πρωταρχικό, ή εξηγήστε γιατί δεν υπάρχει τέτοιο πολυώνυμο.
2.
  - i. Αποδείξτε ότι τα  $\Psi_{19}$  και  $\Psi_{27}$  είναι ανάγωγα και του ίδιου βαθμού υπέρ του  $\mathbb{F}_2$ .
  - ii. Έστω  $q$  δύναμη πρώτου και  $\zeta$  μια πρωταρχική  $n$ -στή ρίζα της μονάδας υπέρ του  $\mathbb{F}_q$ . Αποδείξτε ότι

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

*Υπόδειξη:* Παρατηρήστε ότι το σύνολο  $\{\zeta^i : i = 0, \dots, n-1\}$  αποτελείται ακριβώς από τις ρίζες του  $X^n - 1$ .

3.
  - i. Βρείτε όλα τα πρωταρχικά στοιχεία του  $\mathbb{F}_{13}$ .
  - ii. Υπενθυμίζουμε ότι ο δείκτης πληροφορίας ενός  $q$ -δικού  $(n, M, d)$ -κώδικα  $C$  είναι το  $\delta := \frac{\log_q(|C|)}{n}$ . Αν  $\delta_r$  είναι ο δείκτης πληροφορίας του  $\text{Ham}(r, 2)$ , βρείτε το  $\lim_{r \rightarrow \infty} \delta_r$ .
4. Έστω  $C$  ο δυαδικός κώδικας με γεννήτορα πίνακα τον

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

Αφού βρείτε τις παραμέτρους του  $C$ , αποκωδικοποιήστε τις λέξεις  $w_1 = 11111$  και  $w_2 = 00111$ , χρησιμοποιώντας σύνδρομα.

- 
1. Κάθε θέμα βαθμολογείται με 2,5 βαθμούς και μέγιστη βαθμολογία είναι το 10.
  2. Η διάρκεια της εξέτασης είναι 1,5 ώρα.
  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.).