ΚΩΔΙΚΟΠΟΙΗΣΗ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ $\#4$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

(1) Έστω C_i κυκλικοί κώδικες πάνω από το $\mathbb{F}_q$ μήκους n με πρωτεύοντα γεννήτορα $g_i(x)$, $i = 1, 2$.
   (α') Δείξτε ότι οι κώδικες $C_1 \cap C_2$ και $C_1 + C_2$ είναι κυκλικοί.
   (β') Εκφράστε τους πρωτεύοντες γεννήτορες των $C_1 \cap C_2$ και $C_1 + C_2$ σε σχέση με αυτούς των C_1 και C_2.

(2) Έστω C ένας κυκλικός κώδικας πάνω από το $\mathbb{F}_q$ μήκους n. Μια κωδική λέξη $e(x)$ ονομάζεται idempotent αν $e(x)^2 \equiv e(x) \pmod{x^n - 1}$. Αν συμβαίνει το πολυώνυμο $e(x)$ να γεννά τον κώδικα (όχι απαραίτητα να είναι πρωτεύων γεννήτορας), τότε ονομάζεται idempotent γεννήτορας. Έστω $g(x)$ ο πρωτεύων γεννήτορας του C και $h(x) = (x^n - 1)/g(x)$. Δείξτε ότι εάν $(g(x), h(x)) = 1$ τότε ο C έχει ένα μοναδικό idempotent γεννήτορα.
Υπόδειξη: Αφού $(g(x), h(x)) = 1$, το $g(x)$ έχει αντίστροφο modulo $h(x)$. Έστω $s(x)$ αυτός ο αντίστροφος. Δείξτε ότι το $e(x) = s(x)g(x)$ έχει τις απαιτούμενες ιδιότητες. Εάν $e_1(x)$ είναι ένας άλλος idempotent γεννήτορας, δείξτε ότι $e_1(x) \equiv e(x) \pmod{x^n - 1}$.

(3) (α') Κατασκευάστε έναν narrow sense BCH κώδικα πάνω από το $\mathbb{F}_2$ μήκους 7, με απόσταση σχεδίασης $\delta = 4$. Υπολογίστε τις παραμέτρους του κώδικα σας. Πόσα λάθη διορθώνει; Πόσα λάθη ανιχνεύει; Είναι MDS;
   (β') Κατασκευάστε ένα κώδικα Reed-Solomon πάνω από το $\mathbb{F}_8$ με απόσταση σχεδίασης $\delta = 4$. Υπολογίστε τις παραμέτρους του κώδικα σας. Πόσα λάθη διορθώνει; Πόσα λάθη ανιχνεύει;
   (γ') Ποιός από τους δύο παραπάνω κώδικες πιστεύετε ότι είναι καλύτερος και γιατί;

(4) Δείξτε ότι ο κώδικας $\mathrm{Ham}(m, 2)$ είναι ένας narrow sense BCH κώδικας πάνω από το $\mathbb{F}_2$.
Υπόδειξη: Κατασκευάστε ένα narrow sense BCH κώδικα πάνω από το $\mathbb{F}_2$ με $\delta = 3$. Ελέγχοντας τον πίνακα ελέγχου (τις διαστάσεις του) συμπεράνετε ότι οι στήλες του περιλαμβάνουν όλα τα μη μηδενικά διανύσματα κατάλληλου μήκους.