ΚΩΔΙΚΟΠΟΙΗΣΗ
ΦΥΛΛΑΔΙΟ ΑΣΚΗΣΕΩΝ $\#5$

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

(1) Έστω $\alpha \in \mathbb{F}_{2^4}$ μία ρίζα του $X^4 + X + 1$ και C ο δυαδικός narrow-sense BCH κώδικας με μήκος 15 και απόσταση σχεδίασης $\delta = 5$.
 (α΄) Υπολογίστε το γεννήτορα και τις παραμέτρους του C.
 (β΄) Αποκωδικοποιήστε, σε όποια περίπτωση μπορείτε, τις παρακάτω λέξεις:
 - $w(X) = X^8 + X^7 + X^6 + 1$,
 - $w(X) = X^9 + X^6 + X^5 + X^4 + X + 1$,
 - $w(X) = X^7 + X + 1$.

(2) Έστω C ένας narrow-sense BCH κώδικας πάνω από το $\mathbb{F}_q$, με μήκος $n = q^m - 1$ και απόσταση σχεδίασης δ. Έστω $g(X) = \operatorname{lcm}(M^{(1)}, \dots, M^{(\delta-1)})$ ο γεννήτορας του C, όπου $M^{(j)} = \min(\alpha^j, \mathbb{F}_q)$ και α είναι γεννήτορας της $\mathbb{F}_q^*$. Υποθέστε ότι ισχύει $n = \delta\nu$ με $\nu \in \mathbb{N}$.
 (α΄) Δείξτε ότι τα α^j δεν είναι ρίζες του $X^\nu - 1$ για $1 \le j \le \delta - 1$.
 (β΄) Δείξτε ότι $(X^\nu - 1, g(X)) = 1$.
 (γ΄) Δείξτε ότι $g(X) | X^{\nu(\delta-1)} + \cdots + X^\nu + 1$.
 (δ΄) Δείξτε ότι η ελάχιστη απόσταση του C είναι ακριβώς δ.

(3) Δείξτε ότι για κάθε δύναμη πρώτου $q > 2$, για κάθε φυσικό $n \le q$ και για κάθε φυσικό $1 \le k \le n$ υπάρχει ένας $[n, k]$, MDS κώδικας πάνω από το $\mathbb{F}_q$.

(4) Έστω C ένας κώδικας Reed-Solomon πάνω από το $\mathbb{F}_q$ με γεννήτορα το
$$g(X) = (X - \alpha^b)(X - \alpha^{b+1}) \cdots (X - \alpha^{b+\delta-2}),$$
όπου $b \ge 1$, $\delta > 1$ και α γεννήτορας του $\mathbb{F}_q^*$.
 (α΄) Δείξτε ότι οι συντελεστές των $1, X, \dots, X^{\delta-1}$ στο πολυώνυμο $g(X)$ είναι διάφοροι του μηδενός.
 (β΄) Δείξτε ότι ο γεννήτορας του $C^\perp$ είναι το
$$g^\perp(X) = (X - \alpha^{1-b})(X - \alpha^{2-b}) \cdots (X - \alpha^{q-\delta-b}).$$