ΘΕΜΑ:
ΚΩΔΙΚΕΣ ΤΕΤΡΑΓΩΝΙΚΟΥ ΥΠΟΛΟΙΠΟΥ

ΧΡΗΣΤΟΣ ΣΑΡΟΓΛΟΥ

ΚΩΔΙΚΕΣ ΤΕΤΡΑΓΩΝΙΚΟΥ ΥΠΟΛΟΙΠΟΥ

Πρόκειται για κυκλικούς κώδικες μήκους n πάνω από το σώμα Fq, όπου ο πρώτος περιττός και q τετραγωνικό υπόλοιπο modulon.

Οι κώδικες τετραγωνικού υπολοίπου (quadratic residue codes ή QR-codes) δεν είναι τόσο καλοί όσο άλλοι, όπως π.χ. οι BCH ή οι Reed - Móller κώδικες, με την έννοια ότι δεν έχουν τόσο μεγάλη ελάχιστη απόσταση.

Για παράδειγμα στους BCH μπορούμε να διαλέξουμε οσοδήποτε μεγάλη ελάχιστη απόσταση, ενώ στους QR- κώδικες, όπως θα δούμε στη συνέχεια, η καλύτερη εκτίμηση είναι d^2-d+1$\geq$n Επιπλέον, είναι σχετικά σπάνια τα πρώτα n, για τα οποία το q είναι τετραγωνικό υπόλοιπο modulo n.

Όμως, έχουν αρκετές άλλες καλές ιδιότητες με σημαντικότερη ότι πολλοί τέλειοι κώδικες ανήκουν σε αυτήν την κατηγορία, όπως π.χ. οι δυαδικοί κώδικες του Hamming και του Golay.

Έχουν, λοιπόν, μεγάλη αξία, τόσο ιστορική όσο και πρακτική.

Ορισμός: Ένας ακέραιος α λέγεται τετραγωνικό υπόλοιπο modulo n ($n\in Z$-{0}), αν υπάρχει $k\in Z$-{0}, τέτοιος ώστε:

$$\alpha \equiv k^2 \mathrm{mod} n$$

Οι επόμενες προτάσεις είναι χρήσιμες για τον ακριβή ορισμό των QR- κωδίκων.

Πρόταση 1: Έστω p ένας πρώτος περιττός και α ένας μη μηδενικός ακέραιος. Ισχύει: $\alpha^{\frac{p-1}{2}} \equiv 1 \mathrm{mod} p$ ή $\alpha^{\frac{p-1}{2}} \equiv -1 \mathrm{mod} p$. Επιπλέον, το α είναι

τετραγωνικό υπόλοιπο modulo p ανν $\alpha^{\frac{p-1}{2}} \equiv 1 \text{mod} p$. Τέλος, υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα modulo p.

<u>Απόδειξη</u>: Επειδή ο p είναι πρώτος, ο δακτύλιος Zp είναι σώμα, και συνεπώς η ομάδας Z_p^* είναι κυκλική. Άρα, κάθε στοιχείο α αυτής ικανοποιεί: $\alpha^{p-1} \equiv 1 \text{ mod} p$. Επομένως $\alpha^{p-1} \equiv 1 \text{ mod} p$, άρα $\alpha^{p-1}-1 \equiv 0 \text{ mod} p$ $\Rightarrow \left(\alpha^{\frac{p-1}{2}} - 1\right)\left(\alpha^{\frac{p-1}{2}} + 1\right) \equiv 0 \text{ mod} p$. Λόγω του ότι το Zp είναι σώμα, έχουμε $\alpha^{\frac{p-1}{2}} - 1 \equiv 0$ ή $\alpha^{\frac{p-1}{2}} + 1 \equiv 0 \text{mod} p \Leftrightarrow \alpha^{\frac{p-1}{2}} \equiv \pm 1 \text{mod} p$.

Αν, τώρα το α είναι τετραγωνικό υπόλοιπο modp, τότε $\exists k \in Z - \{0\}$, $\alpha \equiv k^2 \text{mod} p \Rightarrow \alpha^{\frac{p-1}{2}} \equiv (k^2)^{\frac{p-1}{2}} = k^{p-1} \equiv 1 \text{ mod} p$. Αντίστροφα, έστω ότι το α δεν είναι τετραγωνικό υπόλοιπο modulo p. Έστω, ακόμη, $\lambda \in Z_p^*$ ένα στοιχείο τάξης p-1. Τότε, ισχύει $\lambda^q \equiv \alpha \text{ mod} p$, όπου q περιττός (αφού αν το q ήταν άρτιος, τότε το α θα ήταν τετραγωνικό υπόλοιπο). Επομένως, $\alpha^{\frac{p-1}{2}} \equiv (\lambda^q)^{\frac{p-1}{2}} = \lambda^{q\frac{p-1}{2}} \text{ mod} p$.

Όμως, $q \cdot \frac{p-1}{2}$ δεν διαιρείται από το p-1, δηλαδή την τάξη του λ.

Άρα, αναγκαστικά, $\lambda^{q\frac{p-1}{2}} \not\equiv 1 \text{mod} p \Rightarrow \alpha^{\frac{p-1}{2}} \not\equiv 1 \text{mod} p \Rightarrow \alpha^{\frac{p-1}{2}} \equiv -1 \text{mod} p$

Για το τελευταίο, παίρνουμε πάλι ένα στοιχείο $\lambda \in Z_p^*$ τάξης p-1. Τότε, τα στοιχεία του συνόλου $\{\lambda^\beta : \beta \le p-1, \beta \text{ θετικός άρτιος}\}$ είναι διακεκριμένα modp, αφού: $\lambda^\beta \equiv \lambda^{\beta'} \text{mod} p \Leftrightarrow \lambda^{\beta-\beta'} \equiv 1 \text{mod} p \Leftrightarrow$ β-β'=p-1 ή β-β'=0 $\Leftrightarrow$ β=β', αφού |β-β'|<p-1. Κάθε στοιχείο αυτού του συνόλου είναι τετραγωνικό

υπόλοιπο modulo p, ενώ το πλήθος των στοιχείων του είναι $\frac{p-1}{2}$. Άρα, υπάρχουν τουλάχιστον $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα modulo p. Όμοια, τα στοιχεία του συνόλου $\{\lambda^{\beta}:\beta<p-1,\ \beta$ θετικός περιττός$\}$ είναι όλα διαφορετικά ανά 2, $\frac{p-1}{2}$ το πλήθος και δεν είναι τετραγωνικά υπόλοιπα. Άρα, τελικά, υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά υπόλοιπα modulo p.

<u>Πόρισμα</u>: Το 2 είναι τετραγωνικό υπόλοιπο modulo p αν και μόνον αν $p \equiv \pm 1$ mod8.

<u>Απόδειξη</u>:

Ονομάζουμε $\alpha = 1\cdot 2\cdot 3...\frac{p-1}{2}$. Τότε, $(2.1)(2.2)(2.3)...\left(2\cdot\frac{p-1}{2}\right) = 2^{\frac{P-1}{2}}\cdot\alpha$ Άρα, το 2 είναι τετραγωνικό υπόλοιπο modulo p αν και μόνο αν $2\cdot 4\cdot 6...(p-1) \equiv 1\cdot 2\cdot 3...\frac{p-1}{2} \text{mod} p$. Το πρώτο μέλος είναι ισοδύναμο με:

$$(\Pi k_i)\cdot(\Pi(p-\lambda j)) \equiv (\Pi k_i)\cdot(\Pi(-\lambda j))\,\text{mod}p.$$
$$\underset{Ki\le\frac{p-1}{2}}{Ki\ \text{άρτιος}}\quad \underset{\lambda j<\frac{p-1}{2}}{\lambda j\ \text{περιττός}}\qquad \underset{Ki\le\frac{p-1}{2}}{Ki\ \text{άρτιος}}\quad \underset{\lambda j<\frac{p-1}{2}}{\lambda j\ \text{περιττός}}$$

Αν β το πλήθος των παραγόντων του γινομένου π (-μj), τότε ισχύει, προφανώς: 2 τετραγωνικό υπόλοιπο modulo p αν και μόνο αν $(-1)^{\beta}.\alpha \equiv \alpha$ modp $\Leftrightarrow$ $(-1)^{\beta} \equiv 1$ modp.

Επειδή το πλήθος των παραγόντων είναι $\frac{p-1}{2}$ (για το γινόμενο 2·4·6....(p-1)) και $\lambda j<\frac{p-1}{2}$ ανν $\lambda j < \left[\frac{p-1}{4}\right]$, ισχύει $\beta = \frac{p-1}{2} - \left[\frac{p-1}{4}\right]$.

Ακόμη, $(-1)^{\beta} \equiv 1 \bmod p$ ανν β άρτιος. Άρα, 2 τετραγωνικό υπόλοιπο modulo p ανν $\frac{p-1}{2}-\left[\frac{p-1}{4}\right]$ άρτιος. Θέτω $p=8t+\gamma$, όπου $t \in Z$ και $\gamma \in N$, $\gamma<8$, γ περιττός (δηλαδή γ=1 ή 3 ή 5 ή 7).

Τότε, $\frac{p-1}{2}-\left[\frac{p-1}{4}\right]=4t+\frac{\gamma-1}{2}-2t-\left[\frac{\gamma-1}{4}\right]$. Άρα, $\frac{p-1}{2}-\left[\frac{p-1}{4}\right]$ άρτιος ανν $\delta := \frac{\gamma-1}{2}-\left[\frac{\gamma-1}{4}\right]$ άρτιος.

Για γ=1, έχουμε δ=0, άρτιος. Για γ=3 έχουμε δ=1, περιττός. Για γ=5 έχουμε δ=1, περιττός. Για γ=7, έχουμε δ=2, άρτιος. Άρα, $\frac{p-1}{2}-\left[\frac{p-1}{4}\right]$ άρτιος αν και μόνο αν γ=1 ή 7 $\Leftrightarrow$ $p \equiv 1$ ή $7 \bmod 8 \Leftrightarrow p \equiv \pm 1 \bmod 8$.

Συνεπώς, το 2 είναι τετραγωνικό υπόλοιπο modulo p αν και μόνο αν $p \equiv \pm 1 \bmod 8$.

<u>Πρόταση 2</u>: Θεωρούμε το σώμα Fq, q δύναμη πρώτου και το πολυώνυμο f(x) με συντελεστές σε ένα σώμα - επέκταση του Fq. Αν για κάθε ρίζα α του f(x) και α^q είναι ρίζα του f(x), τότε $f(x) \in Fq[x]$.

<u>Απόδειξη</u>:

Έστω ότι $q=p^m$, p πρώτος και $m \in N$. Τότε το σώμα Fq, καθώς και κάθε επέκτασή του έχει χαρακτηριστική p. Υποθέτουμε ότι $f(x)=\alpha_0+\alpha_1 x+...+\alpha_{n-1}x^{n-1}$. Αν $\beta_1,...,\beta_n$ οι ρίζες του f(x), τότε $f(x)=(x-\beta_1)...(x-\beta_n)$.

Επομένως, $\alpha_k = \sum_{1\le \ell 1<\ell 2<...<\ell n-k\le n} \beta_{\ell 1}...\beta_{\ell n-k}$. Όμως, από την υπόθεση, $\beta_1^q,...,\beta_n^q$ επίσης ρίζες του f(x). Άρα, ισχύει:

$$\alpha_k = \sum_{1\le \ell_1<\ell_2<\ldots<\ell n-k\le n} \beta_{\ell 1}^q \ldots \beta_{\ell n-k}^q = \left(\sum_{1\le \ell_1<\ell_2<\ldots<\ell n-1\le n} \beta_{\ell 1} \ldots \beta_{\ell n-k} \right)^q = \alpha_k^q, \quad k=0,1,\ldots,n-1,$$ επειδή οι ρίζες $\beta_1,\ldots,\beta_n$ ανήκουν σε σώμα χαρακτηριστικής p (επέκταση του $F_q=F_{pm}$) και το q είναι δύναμη του p.

Άρα, κάθε συντελεστής του πολυωνύμου f(x) είναι και ρίζα του πολυωνύμου x^q-x.

Είναι εύκολο να διαπιστώσει κανείς ότι το σύνολο των ριζών του x^q-x, που βρίσκονται στο F_q ή σε μία επέκτασή του, αποτελεί ένα σώμα με q στοιχεία, άρα ταυτίζεται με το F_q.

Επομένως, οι συντελεστές του f(x) είναι στοιχεία του F_q.

Δίνουμε, τώρα, τον ορισμό των κωδίκων τετραγωνικού υπολοίπου.

Έστω n ένας περιττός πρώτος. Θεωρούμε το αλφάβητο F_q (q δύναμη πρώτου), όπου υποθέτουμε ότι το q είναι τετραγωνικό υπόλοιπο modulo n, δηλαδή ισχύει $q^{n-1/2} \equiv 1$ modn. Έστω, ακόμη α μία πρωταρχική n - ρίζα της μονάδας. Ορίζουμε:

$R_0 = \left\{ \lambda \in F_n^* : \exists \mu \in F_n, \lambda = \mu^2 \right\}$= Το σύνολο των τετραγωνικών υπολοίπων modulo n.

$R_1 = F_n^* - R_0$.

Ορίζουμε, επίσης, τα πολυώνυμα:

$$g_0(x) = \prod_{r\in R_0} (x - \alpha^r) \text{ και } g_1(x) = \prod_{r\in R_1} (x - \alpha^r)$$

Επειδή το πλήθος των τετραγωνικών υπολοίπων του F_n είναι ίσο με το πλήθος των στοιχείων του F_n, που δεν είναι τετραγωνικά υπόλοιπα $\left(= \frac{n-1}{2} \right)$, είναι προφανές ότι deg g_o=degg_1.

Ορισμός: Οι κώδικες με πολυώνυμο γεννήτορα τα $g_o(x)$ και $(x-1)g_o(x)$ ονομάζονται κώδικες τετραγωνικού υπολοίπου (QR-κώδικες).

Τα πολυώνυμα g_0 και g_1 έχουν συντελεστές από το F_q. Αυτό προκύπτει άμεσα από την πρόταση (2), αφού: Αν α^r, $r \in R_o$ μία οποιαδήποτε ρίζα του g_o, τότε α^{qr} είναι, επίσης, ρίζα του g_o, επειδή $q\ r \in R_o$ (αφού υποθέσαμε ότι το q είναι τετραγωνικό υπόλοιπο modn). Ομοίως, αν $r \in R_1$, τότε $qr \in R_1 \Rightarrow \alpha^{qr}$ ρίζα του g_1. Επομένως, οι κώδικες τετραγωνικού υπολοίπου είναι γραμμικοί κυκλικοί κώδικες πάνω από το σώμα F_q. Ειδικά στην περίπτωση q=2, έχουμε δει ότι ισχύει $n \equiv \pm 1 \bmod 8$.

Λήμμα: Θεωρούμε το μετασχηματισμό π_j:Fn э $i \rightarrow ij \in F_n$, $j \in F^*_n$. Εφαρμόζοντας τον π_j πάνω στις θέσεις των ψηφίων των κωδικών λέξεων, ο κώδικας $<g_o>$ απεικονίζεται στον εαυτό του, όταν $j \in R_o$ και στον $<g_1>$, όταν $j \in R_1$.

Απόδειξη:

Έστω $U \in <g_0>$ ένα κωδικό πολυώνυμο. Τότε, $\exists\ h(x) \in F_q[x]$, τέτοιο ώστε U(x)=h(x)g(x). Επομένως, αν α η πρωταρχική n-ρίζα της μονάδας, που αντιστοιχεί στο πολυώνυμο-γεννήτορα $g_o(x)$, τότε $\forall r \in R_o$, α^r ρίζα του πολυωνύμου U(x). Αν το πολυώνυμο U(x) έχει τη μορφή: $U(x)=\alpha_0+\alpha_1X+...+\alpha_{n-1}x^{n-1}$, $\alpha_i \in F_q$, i=1, ..., n-1, τότε η εικόνα του μέσω του μετασχηματισμού π_j, θα έχει τη μορφή: $f(x)=\alpha_o+\alpha_1x^{j\cdot 1}+...+\alpha_{n-1}{}^{xj\cdot(n-1)}=\alpha_0+\alpha_1(x^j)^1+...+\alpha_{n-1}(x^j)^{n-1}$. Επιπλέον, $\forall r \in F_q$, έχουμε: $f(\alpha^r)=\alpha_0+\alpha_1(\alpha^r j)^1+...+\alpha_{n-1}(\alpha^r j)^{n-1}=U(\alpha^r j)$. Αν $j \in R_o$, τότε $\alpha^r j$ ρίζα του U(x), επειδή $rj \in R_o$, $\forall r \in R_o$. Άρα, $f\alpha^r=0$, $\forall r \in R_o$. Επομένως, το πολυώνυμο f(x)

μηδενίζεται από κάθε ρίζα του $g_o(x)$, κατά συνέπεια $g(x)/f(x) \Rightarrow f \in <g_o>$. Επομένως, όταν $j \in R_o$, κάθε κωδική λέξη του $<g_o>$ απεικονίζεται σε κωδική λέξη. Άρα, η εικόνα του $<g_o>$ μέσω του πj είναι γραμμικός υπόχωρος του $<g_o>$. Όμως, ο μετασχηματισμός, αυτός (η εφαρμογή του πj στις θέσεις των ψηφίων των κωδικών λέξεων), είναι, προφανώς, γραμμικός ισομορφισμός, άρα η διάσταση της εικόνας ισούται με $\dim <g_o>$. Άρα, αναγκαστικά, ο $<g_o>$ και η εικόνα του ταυτίζονται. Ομοίως, αν $j \in R_1$, τότε $rj \in R_o$, $\forall r \in R_1$, αφού $(rj)^{(n-1/2)} = r^{\frac{n-1}{2}} j^{\frac{n-1}{2}} \equiv (-1)\cdot(-1) = 1 \bmod n$. Άρα, $U(\alpha^r j) = 0 \Rightarrow f(\alpha^r) = 0, \ \forall r \in R_1 \Rightarrow$ $g_1(x)/f(x) \Rightarrow f \in <g_1>$. Συνεπώς, κάθε κωδική λέξη του $<g_o>$ απεικονίζεται σε κωδική λέξη του $<g_1>$. Όμως, (όμοια με πριν) η εικόνα του $<g_o>$ έχει διάσταση ίση με $\dim<g_o> = n - \deg g_o = n - \frac{n-1}{2} = n - \deg g_1 = \dim < g_1 >$. Άρα, τελικά, στην περίπτωση $j \in R_1$, η εικόνα του κώδικα $<g_o>$ μέσω του μετασχηματισμού πj ταυτίζεται με τον κώδικα $<g_1>$.

<u>Θεώρημα (1)</u>: Αν c(x) ένα κωδικό πολυώνυμο του QR-κώδικα $<g_o>$, $c(1) \neq 0$ και w(c)=d, ισχύουν:

i) $d^2 \geq n$

ii) Αν $n \equiv -1 \bmod 4$, τότε $d^2 - d + 1 \geq n$.

iii) Αν $q=2$ και $n \equiv -1 \bmod 8$, τότε $d \equiv 3 \bmod 4$.

<u>Απόδειξη:</u>

(i) Έστω $c \in <g_o>$, $c(1) \neq 0$. Τότε, (x-1) δεν διαιρείται από c(x).

Επιλέγουμε $j \in R_1$, οπότε αν $\hat{c}$ η εικόνα του c μέσω του μετασχηματισμού π_j, τότε $\hat{c} \in <g_1>$, χάρη στο προηγούμενο λήμμα. Ο π_j αποτελεί, απλώς, μια

μετάθεση των συντελεστών του c. Κατά συνέπεια, ισχύει w($\hat{c}$)=w(c)=d και το άθροισμα των συντελεστών του $\hat{c}$(x) ισούται με το άθροισμα των συντελεστών του c(x). Άρα, $\hat{c}$(1)=c(1) $\neq$ 0 $\Rightarrow$ (x-1) δεν διαιρείται από $\hat{c}$(x). Επομένως, το πολυώνυμο (c· $\hat{c}$(x) είναι πολλαπλάσιο του $\frac{x^{n-1}}{x-1} = 1 + x + ... + x^{n-1} \Rightarrow \exists h(x) \in F_q[x]$, , ($\hat{c}$ c) (x)=h(x)·(1+x+...+x^{n-1}), h(1) $\neq$ 0.

Τότε, θέτω t(x)=h(x)-h(1), οπότε ($\hat{c}$ c) (x)= t(x)(1+x...+x^{n-1})+h(1)(1+...+x^{n-1}). Επειδή t(1)=0 $\Rightarrow$

(x-1)/t(x) $\Rightarrow$ x^{n-1}/t(x)(1+...+x^{n-1}).

Άρα, $\hat{c}$·c $\equiv$ h(1) (1+...+x^{n-1}) mod (x^{n-1}-1) $\Leftrightarrow$ $\hat{c}$*c=h(1)·(1+...+x^{n-1}).

Όμως, το $\hat{c}$*c έχει το πολύ d^2 μη μηδενικούς συντελεστές, και συνεπώς, $d^2 \geq$ w (h(1)(1+...+x^{n-1}))=n.

(ii) Αν n $\equiv$ -1 mod4, τότε $(-1)^{\frac{n-1}{2}} = (-1)^{\frac{(4s-1)-1}{2}} = (-1)^{2s-1} = (-1)^{-1} = -1 \equiv -1 \bmod 4$ όπου s κάποιος ακέραιος. Άρα, -1 $\in$ R_1. Συνεπώς, στην προηγούμενη απόδειξη μπορούμε να πάρουμε j=-1. Τότε, αν c(x)= $\sum_{j=1}^{d} \alpha_j x^{\ell j}$, είναι $\hat{c}(x) = \sum_{j=1}^{d} \alpha_j x^{-\ell j}$. Έχουμε λοιπόν:

$$\hat{c}c(x) = \sum_{i=1}^{d}\sum_{j=1}^{d} \alpha_i \alpha_j x^{\ell i - \ell j} = \sum_{\substack{1 \leq i,j \leq d \\ i \neq j}} \alpha_i \alpha_j x^{\ell i - \ell j} + \left(\alpha_1^2 + ... + \alpha_d^2\right).$$

Είναι φανερό, λοιπόν, ότι το πλήθος των μη μηδενικών συντελεστών του πολυωνύμου c*$\hat{c}$ είναι το πολύ d^2-d+1, και συνεπώς d^2-d+1$\geq$n.

iii) Στη δυαδική περίπτωση, όπου n ≡ -1 mod8 ⇒ n=-1mod4, είναι $\alpha_1=...=\alpha_d=1$, οπότε $\alpha_1^2+...+\alpha_d^2=1$, αφού d περιττός. Εξάλλου, για τους υπόλοιπους όρους του πολυωνύμου $\left(c*\hat{c}\right)(x)$, ισχύει: Οι όροι $x^{\ell_i-\ell_j}$ και $x^{\ell_\mu-\ell_\lambda}$ απλοποιούνται μεταξύ τους αν και μόνο αν $\ell_i-\ell_j\equiv\ell_\mu-\ell_\lambda \bmod n \Leftrightarrow$

$\ell_j-\ell_i\equiv\ell_\lambda-\ell_\mu \bmod n \Leftrightarrow$ Οι όροι $x^{\ell_j-\ell_i}$ και $x^{\ell_\lambda-\ell_\mu}$

απλοποιούνται μεταξύ τους. Άρα, αν κάποιοι όροι του πολυωνύμου απλοποιούνται, τότε απλοποιούνται κατά τετράδες. Συνεπώς, $n=d^2-d+1-4\alpha$, για κάποιο $\alpha \in N$. Επειδή d περιττός, ισχύει $d \equiv 1$ ή 3 mod4. Αν $d \equiv 1$ mod4, τότε: $n=d^2-d+1-4\alpha \equiv 1^2-1+1-4\alpha = 1-4\alpha \equiv 1 \neq -1$ mod 4, άτοπο. Άρα, αναγκαστικά $d \equiv 3$ mod4.

Στόχος μας είναι να αποδείξουμε ότι κάθε λέξη ελάχιστου βάρους του QR-κώδικα $<g_0>$ δεν διαιρείται (αν τη δούμε ως πολυώνυμο) με το x-1, οπότε η ελάχιστη απόσταση του κώδικα $<g_o>$ (άρα και του $<(x-1)g_o(x)>$, αφού $<(x-1)g_0(x)>c<g_o>$) φράσσεται από κάτω, μέσω των ανισοτήτων (i) και (ii) του προηγούμενου θεωρήματος. Ο επόμενος ορισμός θα χρησιμοποιηθεί γι΄αυτό το σκοπό.

<u>Ορισμός</u>: Έστω C ένας γραμμικός κυκλικός κώδικας και $\theta \in C$ ένα κωδικό πολυώνυμο. Αν για κάθε κωδική λέξη - πολυώνυμο $h \in C$, ισχύει: $\theta(x)*h(x)=h(x)$, τότε το πολυώνυμο $\theta(x)$ λέγεται Idempotent πολυώνυμο του κώδικα C. Σημειώνεται (εγκυκλοπαιδικά) ότι υπάρχει μοναδικό τέτοιο πολυώνυμο, για κάθε κυκλικό κώδικα.

Θεώρημα (2): Για κατάλληλη επιλογή της πρωταρχικής n-ρίζας α της μονάδας, το πολυώνυμο $\theta(x):=\sum_{r\in R_0} x^r$ είναι το idempotent πολυώνυμο του δυαδικού (q=2) QR-κώδικα $<g_o(x)>$, αν $n \equiv 1 \bmod 8$ και, αντίστοιχα, idempotent του δυαδικού QR-κώδικα $<(x-1)g_o(x)>$, αν $n \equiv -1 \bmod 8$.

Απόδειξη: Καταρχήν, ισχύει:

$$\{ir : r \in R_o\} = \begin{cases} R_o, i \in R_o \\ R_1, i \in R_1 \end{cases}.$$

Πράγματι, έχουμε ήδη δει ότι $\forall\ r \in R_o$, $ir \in R_o$, αν $i \in R_o$ και $ir \in R_1$, αν $i \in R_1$. Επίσης, $\forall r, r' \in R_o\ \ ir = ir' \Leftrightarrow r = r'$, άρα όλα τα στοιχεία του συνόλου $\{ir : r \in R_o\}$ είναι διακεκριμένα και συνεπώς πλήθος $\frac{n-1}{2}$.

Είναι: $[\theta(x)]^2 = \left(\sum_{r\in R_o} x^r\right)^2 = \sum_{r \in R_o} x^{2r}$. Αλλά, από την υπόθεση, έχουμε ότι $2 \in R_o$. Συνεπώς, ισχύει $[\theta(x)]^2=\theta(x)$. Επομένως, ισχύει $\theta(\alpha)=0$ ή 1, για όλες τις πρωταρχικές n-ρίζες της μονάδας α. Αν $i \in R_o$, τότε

$$\theta(\alpha^i) = \sum_{r\in R_o} (\alpha^i)^r = \sum_{r\in R_o} \alpha^{ri} = \sum_{r\in R_o} \alpha^r = \theta(\alpha).$$

Αν $i \in R_1$, τότε $\theta(\alpha^i)+\theta(\alpha) = \sum_{r\in R_o} \alpha^{ir} + \sum_{r\in R_1} \alpha^{ir} = \alpha + \alpha^2 + \ldots + \alpha^{n-1} =$

$=1+\alpha+\ldots+\alpha^{n-1}-1 = \frac{\alpha^{n-1}-1}{\alpha-1} - 1 = -1 = 1$, αφού $\alpha \neq 1 \Rightarrow$ α ρίζα του πολυωνύμου $\frac{x^{n-1}}{x-1}$.

Επιλέγουμε, τώρα, αρχική n-ρίζα της μονάδας α, τέτοια ώστε $\theta(\alpha)=0$. Υπάρχει τέτοιο α, αφού αν δεν υπήρχε, τότε $\forall\omega$ αρχική n-ρίζα της μονάδας,

θα ήταν θ(ω)=1. Όμως, n πρώτος, άρα όλες οι n-ρίζες της μονάδας εκτός του 1 είναι πρωταρχικές. Τότε, το πολυώνυμο θ(x)-1 θα μηδενιζόταν από όλες τις ρίζες του $\frac{x^n-1}{x-1} = 1+x+...+x^{n-1} \Rightarrow 1+x+...+x^{n-1} / [\theta(x)-1]$, άτοπο. Τότε, για θ(α)=0, έχουμε θ(α^i)=0, i $\in$ R_o και θ(α^i)=1, i $\in$ R_1. Τέλος, $\theta(1) = \sum_{r \in R_0} 1 = \frac{n-1}{2} = 0$, αν n ≡ 1 mod8 και θ(1)=1, αν n ≡ -1 mod8 (στο F_2). Συνεπώς, $(x-1) | \theta(x)$, αν n ≡ 1mod8 και (x-1)+θ(x), αν n ≡ -1mod8. Θέτω:

$$g(x) = \begin{cases} g_o(x) & , \text{αν } n \equiv -1 \bmod 8 \\ (x-1)g_o(x) & , \text{αν } n \equiv 1 \bmod 8 \end{cases}$$

Τότε, σε κάθε περίπτωση το πολυώνυμο g(x)[θ(x)-1], μηδενίζεται από όλες τις n-ρίζες της μονάδας. Δηλαδή, $(x^n-1) \mid g(x)[\theta(x)-1]$. Επομένως, g(x)θ(x)-g(x) ≡ 0 mod (x^n-1) ⇔ g(x)θ(x) ≡ g(x)mod(x^n-1) ⇔ g(x)*θ(x)=g(x). Όμως, κάθε κωδικό πολυώνυμο c(x) είναι πολλαπλάσιο του g(x)mod(x^n-1), δηλαδή υπάρχει h(x) $\in$ F_2[x], c(x)=h(x)*g(x) ⇒ θ(x)*c(x) = (θ(x)*g(x))*h(x)=g(x)*h(x)=c(x). Επομένως, το πολυώνυμο θ(x) είναι Idempotent πολυώνυμο του κώδικα <g(x)>, οπότε αποδείχτηκε ο ισχυρισμός μας.

Έστω, τώρα, α μία αρχική n-ρίζα της μονάδας και $g_0^1(x) = \prod_{r \in R_0} (x-\alpha^r)$, $g_1^1(x) = \prod_{r \in R_1} (x-\alpha^r)$. Τότε, ∀ j $\in$ F_n*, είναι: α^j αρχική n-ρίζα της μονάδας, αφού (j, n)=1, λόγω του ότι j<n και n πρώτος. Επίσης, είναι προφανές, ότι $\alpha^i = \alpha^j$ ⇔ i=j, ∀ i, j $\in$ F_n. Άρα, το σύνολο των πρωταρχικών n-ριζών της μονάδας είναι το {α^j : j $\in$ Fn*}.

Αν $g^j(x) = \prod_{r \in R_0} \left(x - \left(\alpha^j \right)^r \right)$, το πολυώνυμο γεννήτορας του QR-κώδικα, που αντιστοιχεί στην πρωταρχική n-ρίζα της μονάδας α^j, τότε:

$$g_0^j(x) = \prod_{r \in R_0} \left(x - \alpha^{rj} \right) = g_0^1(x), \text{ αν } j \in R_o$$

και $g_0^j = g_0^1$, αν $j \in R_1$.

Όμως, όπως ήδη έχει αναφερθεί, οι κώδικες $<g_o>$ και $<g_1>$ είναι ισοδύναμοι. Κατά συνέπεια, όλοι οι QR- κώδικες με πολυώνυμα, γεννήτορες τα g_0^j, $j \in F^*$,είναι ισοδύναμοι. Επομένως, η ελάχιστη απόσταση του QR-κώδικα με πολυώνυμο γεννήτορα g_o είναι ανεξάρτητη της επιλογής της αρχικής n-ρίζας της μονάδας α. Μπορούμε, λοιπόν, στη μελέτη της ελάχιστης απόστασης να υποθέτουμε ότι η α ικανοποιεί τη συνθήκη του προηγούμενου θεωρήματος, ότι δηλαδή, θ(α)=0.

Θεωρούμε, τώρα, το σύνολο {∞, 0, 1,, ..., n-1}, όπου το σύμβολο ∞ ακολουθεί όλους τους συνήθεις κανόνες των αριθμητικών πράξεων. Θεωρούμε, επίσης, το σύνολο PSL(2,n), που αποτελείται από όλους τους μετασχηματισμούς της μορφής: $x \mapsto \frac{\alpha x + b}{cx + d}$, x=∞, 0, 1, ..., n-1, όπου αd-bc=1,a,b,c,d $\in F_n$. Θα δείξουμε ότι το σύνολο PSL(2,n) αποτελεί ομάδα ως προς την πράξη της σύνθεσης και παράγεται από τους μετασχηματισμούς $S : x \mapsto x + 1$ και $T: x \mapsto -x^{-1}$, x=∞, 0, ..., n-1. Καταρχήν, αν:

$$x \mapsto \frac{\alpha x + b}{cx + d}, \alpha d - bc = 1 \text{ και } x \mapsto \frac{\alpha' x + b'}{c' x + d'}, \alpha' d' - bc = 1$$

δύο στοιχεία του PSL (2,n), τότε ο μετασχηματισμός $x \mapsto \frac{(\alpha\alpha'+bc')x + d'b + \alpha b'}{(\alpha' c + dc')x + d' d + cb'}$ είναι η σύνθεσή τους και είναι εύκολο να διαπιστώσει κανείς ότι (αα'+bc')(d'd+cb')-(d'b+αb')(α'c+dc')=1. Συνεπώς, το σύνολο PSL (2,n) είναι κλειστό ως προς την πράξη της σύνθεσης. Αν, μάλιστα, πάρουμε α'=d, b'=-b, c'=-c και d'=α, τότε ο προηγούμενος μετασχηματισμός γίνεται ο ταυτοτικός του συνόλου {∞, 0, 1, ..., n-1}, ο οποίος παίζει το ρόλο του μοναδιαίου στοιχείου. Επομένως, κάθε στοιχείο του PSL(2,n) έχει αντίστροφο, άρα το ζεύγος (PSL(2,n),0) αποτελεί ομάδα.

Τώρα, για κάθε λ ∈ F_n, ορίζουμε τον μετασχηματισμό S_λ:F_n U {∞}→ F_n U {∞}, $S_\lambda(x)=x+\lambda$. Παράγεται από τον μετασχηματισμό S ως εξής: $S_\lambda=S_o S_o...oS=S^\lambda$. Άρα, $S_\lambda \in <S, T>$. Επίσης, ο μετασχηματισμός $S_{\lambda\mu} : x \mapsto \frac{\lambda x + \lambda\mu - 1}{x + \mu}$ παράγεται από τους S_λ, S_μ, T: $S_{\lambda\mu}=S_\lambda o T_o S_\mu$. Άρα, $S_{\lambda\mu} \in <S, T>$. Τέλος, θεωρούμε τον μετασχηματισμό $s_{\lambda\mu}$:$x \mapsto \frac{\lambda x + \lambda\mu - 1}{x + \mu}$ παράγεται από τους S_λ, S_μ, T: $S_{\lambda\mu}=S_\lambda o T_o S_\mu$. Άρα, $S_{\lambda\mu} \in <S, T>$. Τέλος, θεωρούμε τον μετασχηματισμό $T_{\lambda\mu\nu}$:$x \mapsto \frac{(\lambda\nu - 1)x + \lambda\mu\nu - \nu - \mu}{\lambda x + \lambda\mu - 1}$. Τότε, $T_{\lambda\mu\nu}(x) = -\frac{x+\mu}{\lambda x + \lambda\mu - 1} + \nu =$ $\left(S_\nu o T o S_{\lambda\mu}\right)(x) \Rightarrow T_{\lambda\mu\nu} \in <S, T>$. Θέτω α=λν-1, b=λμν-ν-μ, c=λ, d=λμ-1. Παρατηρούμε ότι τα α, c, d μπορούν να πάρουν αυθαίρετες τιμές, ενώ το b ορίζεται από τη σχέση αd-bc=1. Αυτό αποδεικνύει, ακριβώς τον ισχυρισμό μας.

Έστω C ο επεκτεταμένος του κυκλικού κώδικα $<g_o>$ ως προς το σώμα F_2. Υποθέτουμε ότι το g_o αντιστοιχεί σε μια n-ρίζα της μονάδας α, για την οποία θ(α)=0. Τότε, από το θεώρημα (2), το θ είναι το Idempotent

πολυώνυμο του κώδικα $<g_o(x)>$, όταν $n \equiv -1 \bmod 8$ ή, αντίστοιχα, του κώδικα $< g_0^{(x)}(x-1) >$, όταν $n \equiv 1 \bmod 8$. Κατά συνέπεια, το πολυώνυμο θ(x) παράγει τον κώδικα <g(x)>, όπου:

$$g(x) = \begin{cases} g_o(x) & , n \equiv -1 \bmod 8 \\ (x-1)g_o(x) & , n \equiv 1 \bmod 8 \end{cases}$$

αφού οι κωδικές λέξεις του <g(x)> είναι, ακριβώς, όλα τα πολλαπλάσια του θ(x). Επομένως, ο πίνακας G, που έχει ως γραμμές του το θ(x) και όλα τα κυκλικά shift αυτού, παράγει τον κώδικα <g(x)>. Ισχυριζόμαστε ότι ο πίνακας: $I = \begin{bmatrix} 1...1 \\ c^T \mid \overline{G} \end{bmatrix}$, όπου c=(0...0), όταν $n \equiv 1 \bmod 8$ και c=(1...1), όταν $n \equiv -1 \bmod 8$, παράγει τον κώδικα C. Καταρχήν, η λέξη 1...1 μήκους n+1 ανήκει στον κώδικα C. Πράγματι, η λέξη 1...1 μήκους n αντιστοιχεί στο πολυώνυμο $1+x+...+x^{n-1}$, που όπως είδαμε είναι πολλαπλάσιο του $g_o(x)$, άρα 1...1 (μήκους n) $\in <g_o(x)>$. Το parity check symbol αυτής είναι 1, αφού n περιττός και συνεπώς 1...1 (μήκους n+1) $\in$ C. Στην περίπτωση $n \equiv 1 \bmod 8$, έχουμε $w(\theta) = \frac{n-1}{2} \equiv 0 \bmod 2$. Άρα το parity check symbol του θ και κάθε κυκλικού shift αυτού είναι το 0. Επίσης, η λέξη 1...1 (μήκους n+1) δεν ανήκει στον επεκτεταμένο του κώδικα $<(x-1)g_o(x)>$. Ο πίνακας $\left[\begin{array}{c|c} 0 & \\ \vdots & G \\ 0 & \end{array}\right]$ παράγει τον τελευταίο, ο οποίος είναι γραμμικός υπόχωρος του C και έχει διάσταση n-deg $[(x-1)g_o(x)]$=n-deg g_o-1=dimC-1. Κατά συνέπεια, ο πίνακας

$\left[\begin{array}{c|c} 1 & \cdots\ 1 \\ 0 & \\ \vdots & \overline{G} \\ 0 & \end{array}\right]$ παράγει έναν υπόχωρο του C με διάσταση ίση με dimC, οπότε παράγει τον κώδικα C. Στην περίπτωση $n \equiv -1 \bmod 8$, έχουμε: $w(\theta) = \frac{n-1}{2} \equiv 1 \bmod 2$, άρα το parity check symbol του θ και κάθε κυκλικού shift αυτού είναι 1. Επομένως, ο πίνακας $\left[\begin{array}{c|c} 1 & \\ \vdots & G \\ 1 & \end{array}\right]$ παράγει τον κώδικα C, και αφού 1...1 (μήκους n) $\in$ C, και οι γραμμές του πίνακα $\left[\begin{array}{c|c} 1 & \cdots\ 1 \\ \vdots & \overline{G} \\ 1 & \end{array}\right]$ παράγουν τον κώδικα C.

Σημείωση: Όταν λέμε ότι ο κώδικας παράγεται από έναν πίνακα δεν εννοούμε ότι πρόκειται για γεννήτορα πίνακα του εν λόγω κώδικα. Δεν εννοούμε ότι οι γραμμές του είναι γραμμικώς ανεξάρτητες, απλώς απαιτούμε να παράγουν τον κώδικα (ως διανύσματα του F_q^n). Αντίστοιχα ισχύουν και όταν λέμε ότι ένα πολυώνυμο παράγει κάποιον κυκλικό κώδικα.

Υποθέτουμε, τώρα, ότι τα σύμβολα ∞, 0, 1,..., n-1 χαρακτηρίζουν τις θέσεις των ψηφίων των κωδικών λέξεων του επεκτεταμένου κώδικα C του δυαδικού QR-κώδικα με πολυώνυμο γεννήτορα το g_0.

Δείξαμε πριν ότι ο πίνακας: $I = \left[\begin{array}{c|c} 1 \cdots 1 & \\ C^T & \overline{G} \end{array}\right]$ παράγει τον κώδικα C, για κατάλληλη επιλογή της n-ρίζας της μονάδας α, που αντιστοιχεί στο πολυώνυμο g. Η αρχική θέση των ψηφίων (δηλαδή η θέση ∞) συμβολίζει το parity check symbol των κωδικών λέξεων του κώδικα $<g_0>$. Τότε, ο

μετασχηματισμός S:x $\rightarrow$ x+1, x=∞, 0, 1, ...,n-1 απεικονίζει την τυχούσα γραμμή $\alpha_\infty\alpha_0....\ \alpha_{n-1}$ του πίνακα I στο διάνυσμα, $\alpha_\infty\alpha_{n-1}\alpha_0...\alpha_{n-2}$, αφού $\infty \xrightarrow{S} \infty,\ 0 \xrightarrow{S} 1, ..., n-1 \xrightarrow{S} 0$. Συνεπώς, ο S απεικονίζει κάθε γραμμή του πίνακα I σε στοιχείο του εαυτού του. Αποδεικνύεται το ίδιο και για τον μετασχηματισμό T: x $\rightarrow$ x^{-1} (μάλιστα, η εικόνα κάθε γραμμής του πίνακα I μέσω του T γράφεται ως γραμμικός συνδυασμός το πολύ τριών γραμμών του I). Όμως, δείξαμε προηγουμένως ότι η ομάδα PSL (2, n) παράγεται από τους S και T. Άρα, κάθε στοιχείο αυτής απεικονίζει τον κώδικα C σε κάποιον υποκώδικα αυτού. Όμως, ο C και η εικόνα του είναι γραμμικώς ισόμορφοι, άρα αναγκαστικά ίσοι. Άρα, κάθε στοιχείο της PSL (2,n) αφήνει τον C αναλλοίωτο.

Θεώρημα (3): Κάθε κωδική λέξη c ελάχιστου βάρους του δυαδικού κώδικα $<g_0(x)>$ ικανοποιεί τη συνθήκη $C(1) \neq 0$. Επομένως, ικανοποιεί και τις σχέσεις (i) - (iii) του θεωρήματος (1) (άρα, και η ελάχιστη απόσταση του κώδικα ικανοποιεί τις ίδιες σχέσεις).

Απόδειξη: Έστω ότι $c=c_0\ ...c_{n-1}$. Τότε, η λέξη $c'= c_\infty\ c_0...\ c_{n-1}$ είναι στοιχείο του κώδικα C.

Θεωρούμε ένα μετασχηματισμό $R: x \rightarrow \frac{ax+b}{cx+d}$, ad-bc=1, x=$\infty$, 0, 1, ..., n-1 από την ομάδα PSL (2,n). Τότε:

$R(\infty)=\frac{a}{c}$, όταν a . c $\neq$0. Προφανώς, επιλέγοντας κατάλληλα τα a και c, το R(∞) μπορεί να πάρει όλες τις τιμές του συνόλου F_n^*. Αν c(1)=0, τότε W(c) άρτιο $\Rightarrow$ C_∞=0. Επιλέγουμε α και c τέτοια ώστε $C_{R^{-1}(\infty)}=1$. Τότε, από τα

προηγούμενα έχουμε: C^R: $C_{R^{-1}(\infty)}C_{R^{-1}(0)}...C_{R^{-1}(n-1)} \in C$. Επίσης, $w(c^R)= w(c')= 0 + w(c)= w(c)$ και $c_{R^{-1}(\infty)} = 1$, το parity check της λέξης $c_{R^{-1}(0)}...c_{R^{-1}(n-1)}$, που προφανώς ανήκει στον κώδικα $<g_0>$.

Όμως, $$W\left(C_{R^{-1}(0)}....C_{R^{-1}(n-1)}\right) = W\left(C^R\right) - W\left(C_{R^{-1}(\infty)}\right) = W(C) - 1 < W(C),$$

άτοπο επειδή η C υποτέθηκε κωδική λέξη ελάχιστου βάρους. Κατά συνέπεια, ισχύει $c(1) \neq 0$.

ΠΑΡΑΔΕΙΓΜΑ

Έστω, ότι q=2 και n=7. Τότε, n πρώτος και $n \equiv -1 \bmod 8$.

Το πλήθος των τετραγωνικών υπολοίπων στο F_7 είναι $\frac{7-1}{2} = 3$. Έχουμε, a priori, ότι τα στοιχεία 1 και 2 είναι τετράγωνα στο σώμα F_7. Επιπλέον, $5^2 = 25 = 3 \cdot 7+4 \equiv 4 \bmod 7$. Άρα και το 4 είναι τετραγωνικό υπόλοιπο. Επομένως, τα τετραγωνικά υπόλοιπα στο σώμα F_7 είναι, ακριβώς, τα στοιχεία 1, 2, 4. Τότε, σύμφωνα με το θεώρημα (2), για κατάλληλη επιλογή της αρχικής n-ρίζας της μονάδας α, το πολυώνυμο $x+x^2+x^4$ είναι το Idempotent πολυώνυμο του κώδικα με γεννήτορα πολυώνυμο το $g_0(x)$. Άρα, $g_0(x) | x+x^2+x^4$.

Αναλύουμε το x^7-1 σε γινόμενο αναγωγών πολυωνύμων στο F_2 [x] : $x^7-1 = (x-1) \cdot (x^3+x+1) \cdot (x^3+x2+1)$. Από αυτά τα 3, το μόνο που διαιρεί το $x+x^2+x^4$ είναι το πολυώνυμο x^3+x+1. Άρα, αναγκαστικά $g_0(x) = x^3+x+1$ και $g_1(x) = x^3+x^2+1$, (με δεδομένη την επιλογή της ρίζας α). Ο κώδικας $<g_0>$ είναι ο [7,4] - κώδικας. Η amming, που ως γνωστόν είναι τέλειος κώδικας. Ακόμη, $d^2-d+1 \geq 7 \Rightarrow d \geq 3$. Όμως, $d<7 \Rightarrow d=3$ ή 4 ή 5 ή 6. Τέλος, από τη σχέση $d \equiv 3 \bmod 4$ προκύπτει, ότι η ελάχιστη απόσταση του κώδικα είναι 3. Όμως, όπως είναι γνωστό, όλοι οι δυαδικοί κώδικες Hamming είναι ισοδύναμοι. Άρα, όλοι οι δυαδικοί κώδικες Hamming είναι ισοδύναμοι προς τον QR-κώδικα $<x^3+x+1>$.

Πληροφοριακά, και μόνο, αναφέρουμε ότι ο δυαδικός κώδικας του Golay, έχει μήκος $23 \equiv -1 \bmod 8$. Ο κώδικας, αυτός, είναι άλλος ένας τέλειος κώδικας τετραγωνικού υπολοίπου.