Τμήμα Μηχανικών Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδας

Θεωρία Πληροφορίας

Διάλεξη 9: Προηγμένη κωδικοποίηση Block

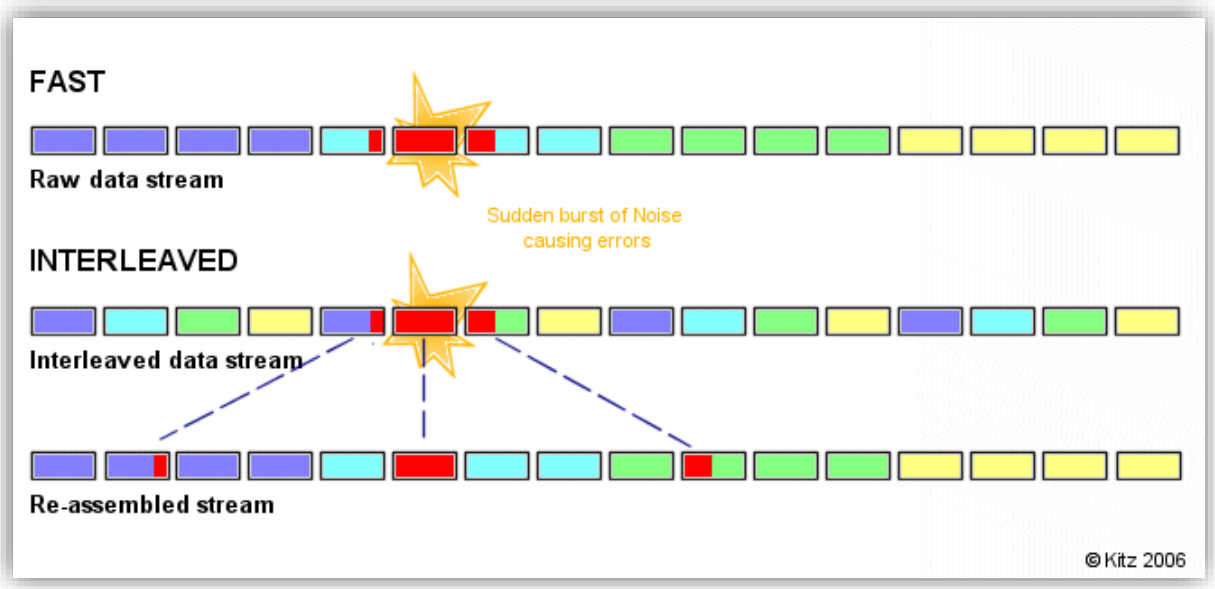
Δρ. Μιχάλης Παρασκευάς
Επίκουρος Καθηγητής

Ατζέντα

1. Διεμπλοκή (Interleaving)
2. Κώδικες Reed-Solomon

Διεμπλοκή

Interleaving



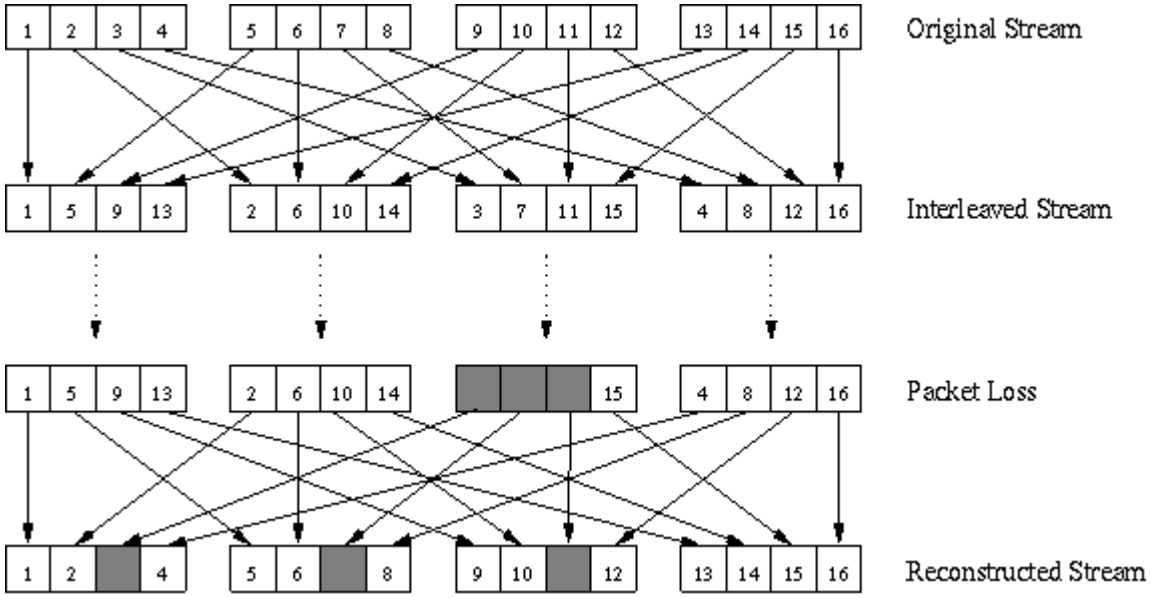
Διεμπλοκή - Γενικά

- Το πρόβλημα:
  - Σε περιπτώσεις όπου κατά την μετάδοση ψηφιακής πληροφορίας συμβαίνει κάποιο λάθος, αυτό αναμένεται να επηρεάσει συνεχόμενα bits (burst errors)
  - Σε αυτή την περίπτωση οι αλγόριθμοι ανίχνευσης και διόρθωσης λαθών αποτυγχάνουν

- Η λύση:
  - Πριν την εφαρμογή κωδικοποιήσεων καναλιού, εφαρμόζουμε Διεμπλοκή (interleaving).

Διεμπλοκή - Ορισμός

- Έστω ένα μήνυμα προς μετάδοση, το οποίο αποστέλλεται σε blocks
- Διεμπλοκή είναι η διαδικασία «ανάμιξης» blocks από bit με σκοπό την αντιμετώπιση των burst λαθών



\+

«Ενεργοποίηση» αλγορίθμων διόρθωσης λαθών

\-

Καθυστέρηση

Διεμπλοκή - Ορισμός (συνέχεια)

- Η τεχνική interleaving χρησιμοποιείται για να προσθέσει **τυχαιότητα** στις θέσεις των σφαλμάτων, ιδίως στην περίπτωση που αυτά παρουσιάζουν πυκνώματα σε μία διάσταση (τυπικά στον χρόνο).
  - οι ριπές σφαλμάτων ή η απώλεια μια συχνότητας στη μετάδοση με διαμόρφωση OFDM (Orthogonal Frequency Division Multiplexing), η οποία χρησιμοποιείται στην ψηφιακή τηλεόραση (και όχι μόνο).
- Εάν τα σφάλματα αυτά καταφέρουμε να τα διασπείρουμε, να τα απομακρύνουμε, δηλαδή, αρκετά το ένα από το άλλο, υπάρχουν περισσότερες δυνατότητες να διορθωθούν (με τους τυπικούς αλγόριθμους προληπτικής διόρθωσης σφαλμάτων).
- Έτσι στον πομπό, τα κωδικοποιημένα bits αναδιατάσσονται με συγκεκριμένο τρόπο. Στον δέκτη επανέρχονται στην αρχική τους θέση με την αντίστροφη διαδικασία πριν την αποκωδικοποίηση.
- Συγκεκριμένα **η διεμπλοκή (interleaving) είναι μια περιοδική και αναστρέψιμη αντιμετάθεση συμβόλων ή bits. Τα σύμβολα ή τα bits επανέρχονται στη σωστή σειρά στον δέκτη.**

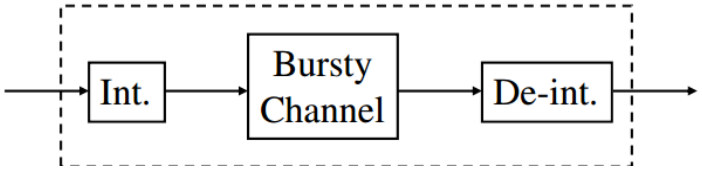
Burst Error Channels

- Τα κανάλια που παρουσιάζουν «εξάρσεις» λαθών χαρακτηρίζονται ως «κανάλια με μνήμη».

- Λόγοι εμφάνισης «εξάρσεων» λαθών:
  - Διαλείψεις σήματος (π.χ. κινητές επικοινωνίες)
  - Παρεμβολές (κανάλια πολλαπλών προσβάσεων)
  - Φθορές σε μέσα αποθήκευσης (π.χ. γρατζουνιά σε CD)

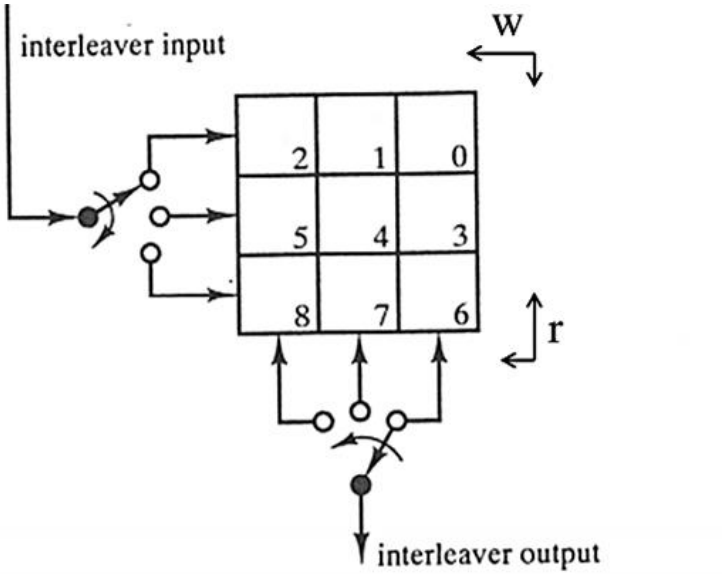
Αλγόριθμοι Διεμπλοκής - Βασικοί Ορισμοί

- Κάθε αλγόριθμος διεμπλοκής περιλαμβάνει τον διεμπλοκέα στη πλευρά του πομπού και τον αποεπεμπλοκέα στην πλευρά του δέκτη.
- **Περίοδος**: Η περίοδος του διεμπλοκέα, έστω T, είναι το πιο σύντομο χρονικό διάστημα εντός του οποίου ο αλγόριθμος αναδιάταξης των συμβόλων ή bits επαναλαμβάνεται. Συχνά η περίοδος L αντιστοιχεί στο μέγεθος μιας κωδικής λέξης (codeword).
- **Βάθος** (depth): Ως βάθος του διεμπλοκέα, έστω D, ορίζουμε την ελάχιστη απόσταση μεταξύ δύο συμβόλων (ή bits) στην έξοδο του διεμπλοκέα, όταν τα σύμβολα (ή bits) αυτά ήταν συνεχόμενα στην είσοδο αυτού.
- Η περίοδος καθορίζεται από τη δομή του διεμπλοκέα και μας δίνει το σύνολο των συμβόλων (ή bits) στο οποίο εφαρμόζεται κάθε φορά ο αλγόριθμος της αντιμετάθεσης. Το βάθος του διεμπλοκέα είναι σημαντικό στην αντιμετώπιση ριπών σφαλμάτων. Συγκεκριμένα, εάν μια ριπή σφαλμάτων έχει μήκος μικρότερο από το βάθος του διεμπλοκέα, τότε δεν θα υπάρχουν συνεχόμενα εσφαλμένα σύμβολα στην έξοδο του διεμπλοκέα (που να οφείλονται βέβαια σε αυτήν τη ριπή σφαλμάτων).
- Κύριες κατηγορίες αλγορίθμων διεμπλοκής:
  - Block διεμπλοκή
  - Διεμπλοκή με πίνακα μετάθεσης
  - Συνελικτική διεμπλοκή



Block Διεμπλοκή

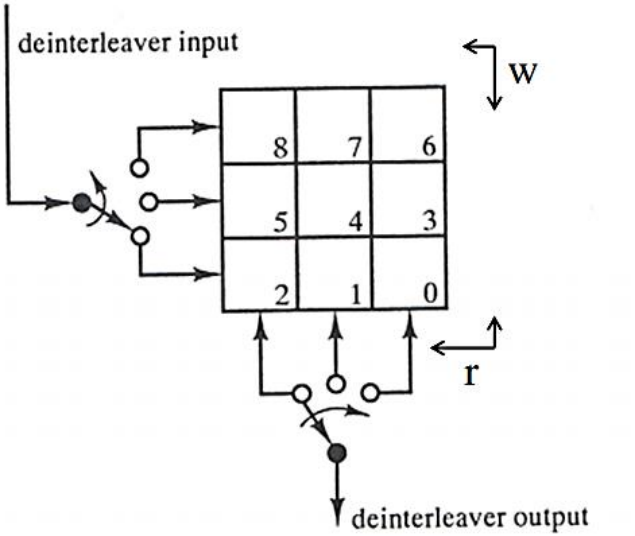
- Ένας $n \times m$ block διεμπλοκέας μεταθέτει ένα block από n·m σύμβολα χρησιμοποιώντας έναν πίνακα μνήμης $n \cdot m$ θέσεων και ακολουθώντας τα εξής βήματα:
  - **1.** Γράφει τα δεδομένα εισόδου από δεξιά προς τα αριστερά και από πάνω προς τα κάτω
  - **2**. Εξάγει τα δεδομένα προσπελαύνοντάς τα από κάτω προς τα πάνω και από δεξιά προς τα αριστερά.



- Εάν για παράδειγμα τα δεδομένα εισόδου είναι τα 012345678, τότε η έξοδος του διεμπλοκέα θα είναι 630741258

Block Απεμπλοκή

- Ένας $n \times m$ block απεμπλοκέας μεταθέτει ένα block από n·m σύμβολα χρησιμοποιώντας έναν πίνακα μνήμης $n \cdot m$ θέσεων και ακολουθώντας τα εξής βήματα:
  - **1.** Γράφει τα δεδομένα εισόδου από πάνω προς τα κάτω και από δεξιά προς τα αριστερά
  - **2**. Εξάγει τα δεδομένα προσπελαύνοντάς τα από δεξιά προς τα αριστερά και από κάτω προς τα πάνω.



- Εάν για παράδειγμα τα δεδομένα εισόδου είναι τα 630741258, τότε η έξοδος του διεμπλοκέα θα είναι 012345678

Ιδιότητες Block Διεμπλοκής

- Οι **απαιτήσεις μνήμης** τόσο και στον πομπό όσο και στον δέκτη είναι $n \cdot m$ σύμβολα.
- Η **καθυστέρηση** που εισάγεται στο σύστημα είναι $D = 2(m(n-1)+1) \approx 2\text{nm}$ σύμβολα
- Δύο διαδοχικά σύμβολα στην αρχική ροή **χωρίζονται από (n-1)** σύμβολα μετά την διεμπλοκή
- Συνήθως, κάθε γραμμή του πίνακα μνήμης αντιστοιχεί σε μία κωδική λέξη m συμβόλων
- Χρησιμοποιώντας έναν κώδικα διόρθωσης λαθών, ικανότητας διόρθωσης t – **λαθών/γραμμή**, το μήκος της μικρότερης μη-διορθώσιμης έξαρσης λαθών **είναι** $\boldsymbol{nt+1}$ **σύμβολα**

Διεμπλοκή με πίνακα μετάθεσης

- Έστω $\hat{x} = [x_1\ x_2\ x_3\ \dots x_L]$ ένα διάνυσμα εισόδου μήκους L συμβόλων
- Ο **πίνακας μετάθεσης διεμπλοκής** $\boldsymbol{P}$ είναι ένας τετραγωνικός πίνακας $L \times L$, ο οποίος έχει ένα 1 σε κάθε γραμμή και σε κάθε στήλη.
- Για παράδειγμα, ο block διεμπλοκέας του προηγούμενου παραδείγματος είναι ισοδύναμος με τον πίνακα μετάθεσης
- $$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

- Αυτό συμβαίνει γιατί:

$$P \times \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \\ 0 \\ 7 \\ 4 \\ 1 \\ 8 \\ 5 \\ 2 \end{bmatrix}$$

Απεμπλοκή με χρήση πίνακα μετάθεσης

- Ο απεμπλοκέας εκτελεί την αντίστροφη μετάθεση χρησιμοποιώντας ως πίνακα μετάθεσης τον ανάστροφο πίνακα (εξαιτίας της κατασκευής του P, ισχύει: $\mathrm{P}^{-1} = P^T$)

- Για το προηγούμενο παράδειγμα

$$\mathrm{P}^{-1} = P^T = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

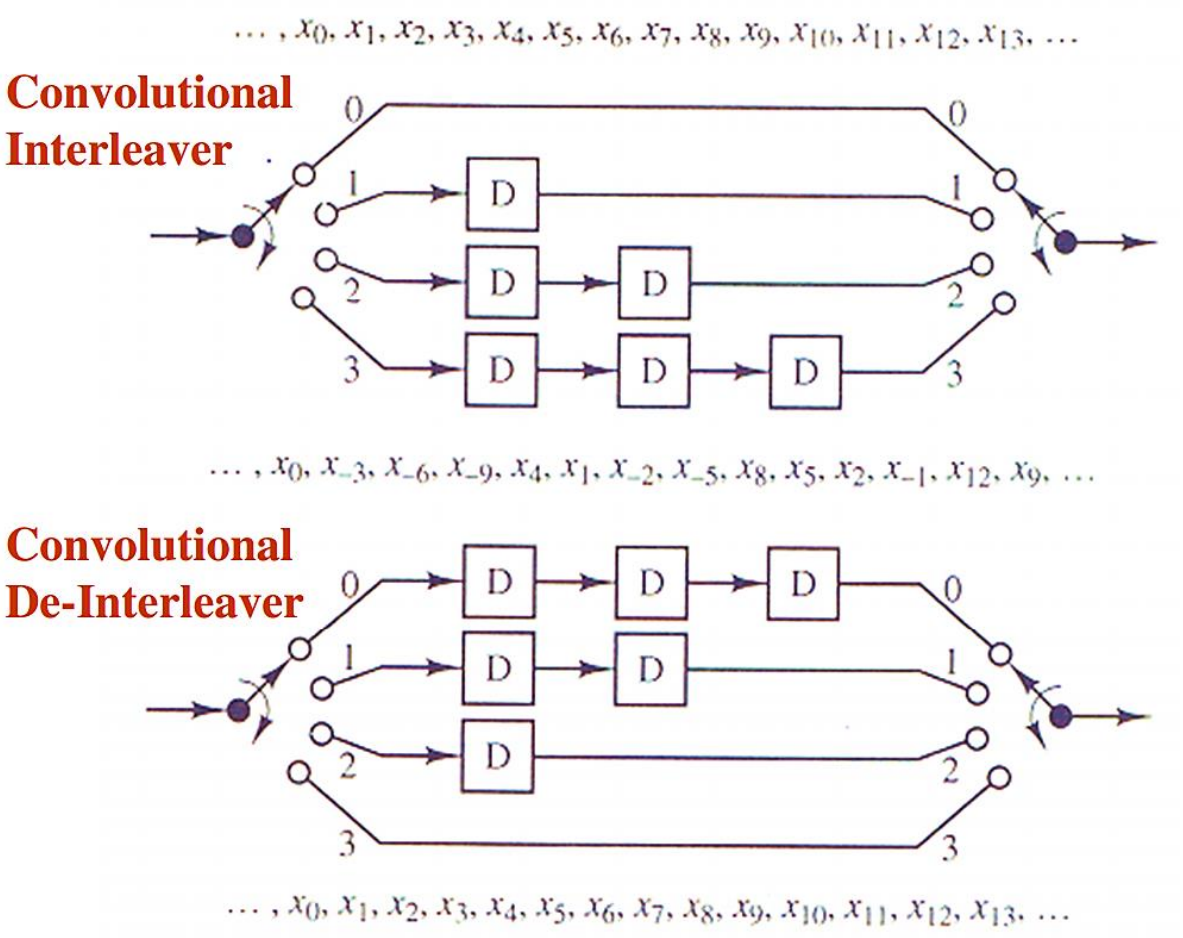
Συνελικτική διεμπλοκή

- Οι προηγούμενες μέθοδοι είναι κατάλληλες για δεδομένα που μπορούν να οργανωθούν σε block

- Στην περίπτωση όπου τα δεδομένα είναι μία συνεχή ροή συμβόλων, χρησιμοποιούμε την συνελικτική διεμπλοκή, για να αποφύγουμε την «πακετοποίηση» των δεδομένων

- Ο διεμπλοκέας/απεμπλοκέας αποτελείται από:
  - m γραμμές *καθυστέρησης*
  - η k-οστή γραμμή καθυστέρησης έχει $k-1$ στοιχεία καθυστέρησης D συμβόλων

Συνελικτική διεμπλοκή - Παράδειγμα (m=4, D=1)



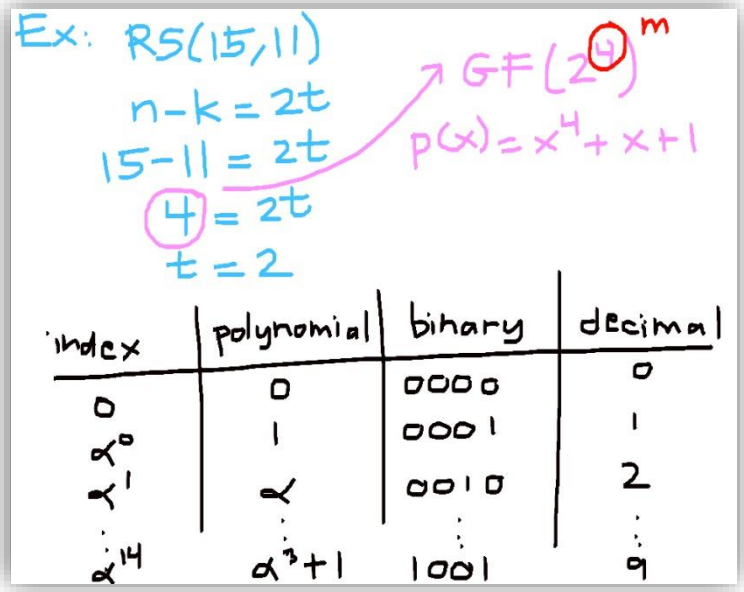
- Προσπαθήστε να καταλάβετε τα αρχικά περιεχόμενα των στοιχείων καθυστέρησης στον διεμπλοκέα

- x_{-3}
- $x_{-2}\ x_{-6}$
- $x_{-1}\ x_{-5}\ x_{-9}$

Ιδιότητες συνελικτικής διεμπλοκής

- Τυπικά, μία λέξη m συμβόλων χρησιμοποιείται, κάθε σύμβολο της οποίας ανήκει σε διαφορετική γραμμή καθυστέρησης
- Κάθε 2 διαδοχικά σύμβολα στο αρχικό μήνυμα διαχωρίζονται από $\boldsymbol{mD}$ **σύμβολα**
- Χρησιμοποιώντας έναν αλγόριθμο διόρθωσης λαθών ικανότητας t λαθών, το μήκος της μικρότερης μη διορθώσιμης έξαρσης λαθών είναι $\boldsymbol{(mD+1)t+1}$ **σύμβολα**
- Οι απαιτήσεις μνήμης τόσο στον διεμπλοκέα όσο και στο απεμπλοκέα είναι $\boldsymbol{m(m-1)D/2}$
- Η καθυστέρηση συμβόλου από άκρο σε άκρο είναι $\boldsymbol{m(m-1)D}$ σύμβολα
- Χρησιμοποιώντας τον ίδιο αλγόριθμο διόρθωσης λαθών, η συνελικτική διεμπλοκή απαιτεί μόνο την μισή μνήμη

Κώδικες Reed-Solomon



Κώδικες R-S: Γενικά Στοιχεία

- Οι κώδικες Reed-Solomon (R-S) είναι συμβολικοί (μη δυαδικοί) κυκλικοί κώδικες με σύμβολα κατασκευασμένα από ακολουθίες m-bits, όπου m ακέραιος με $m \geq 2$.
- Για τους περισσότερους συμβατικούς κώδικες R-S(n, k) ισχύει:

$$(n, k) = (2^m - 1, 2^m - 1 - 2t)$$

Όπου:

  - k είναι το πλήθος των συμβόλων δεδομένων που κωδικοποιούνται
  - n είναι το συνολικό πλήθος των συμβόλων στο block προς κωδικοποίηση (το μήκος block αυτών των κωδικών είναι $n = 2^{m\ -\ 1}$)
  - t είναι η ικανότητα διόρθωσης του κώδικα, με $n - k = 2t$

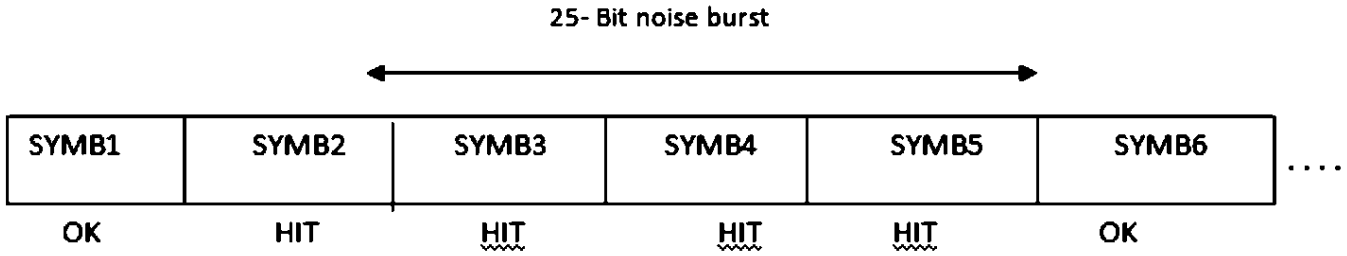
- Το πλήθος των bit ισοτιμίας που πρέπει να χρησιμοποιηθούν για την διόρθωση t λαθών υπολογίζονται από την σχέση:

$$t = (d_{\min} - 1)/2 = (n - k)/2$$

- Οι κώδικες $R - S(n, k)$ επιτυγχάνουν τη μεγαλύτερο πιθανή ελάχιστη απόσταση d_{min} από κάθε γραμμικό κώδικα. Αυτή υπολογίζεται από τη σχέση $d_{min} = n - k + 1$
- Ο R-S κωδικοποιητής επεκτείνει ένα block k συμβόλων σε ένα block n συμβόλων προσθέτοντας $(n - k)$ σύμβολα.

Κώδικες R-S: Burst Error Κανάλια

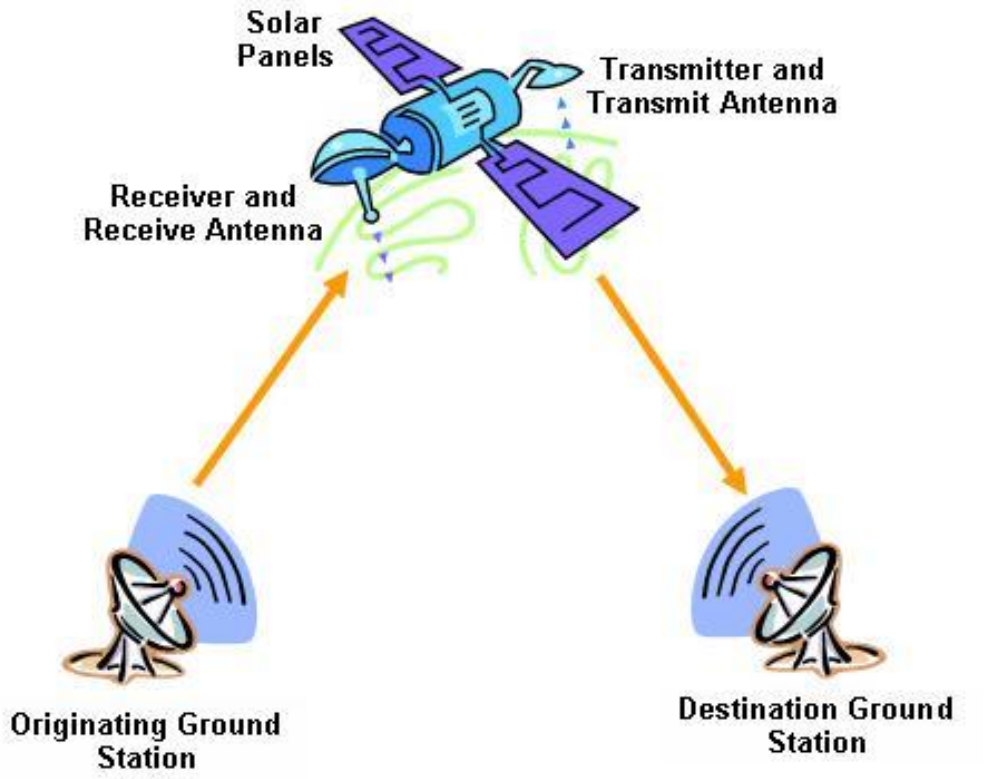
- Οι κώδικες R-S ανταποκρίνονται πολύ καλά στις εξάρσεις λαθών
- Παράδειγμα:
  - Έστω ένας κώδικας R-S(n, k) = (255, 247), όπου κάθε σύμβολο αποτελείται από m=8 bits. Αφού $n - k = 8$, ο κώδικας μπορεί να διορθώσει οποιαδήποτε 4 σύμβολα σε ένα block των 255 συμβόλων.
  - Έστω η παρουσία θορύβου «έξαρσης» ο οποίος διαρκεί 25 bit και κατανέμεται σε ένα block κατά την διάρκεια της μετάδοσης, όπως φαίνεται στο παρακάτω σχήμα:



  - Παρατηρήστε πώς ο θόρυβος διαρκεί για 25 συνεχόμενα bits και διαταράζει ακριβώς 4 σύμβολα. Ο αποκωδικοποιητής R-S θα διορθώσει τα 4 λανθασμένα σύμβολα, ανεξάρτητα από το γεγονός εάν όλο το σύμβολο είναι λανθασμένο ή εάν κάποια bits του είναι λανθασμένα.

Κώδικες R-S: Σύγχρονες Εφαρμογές

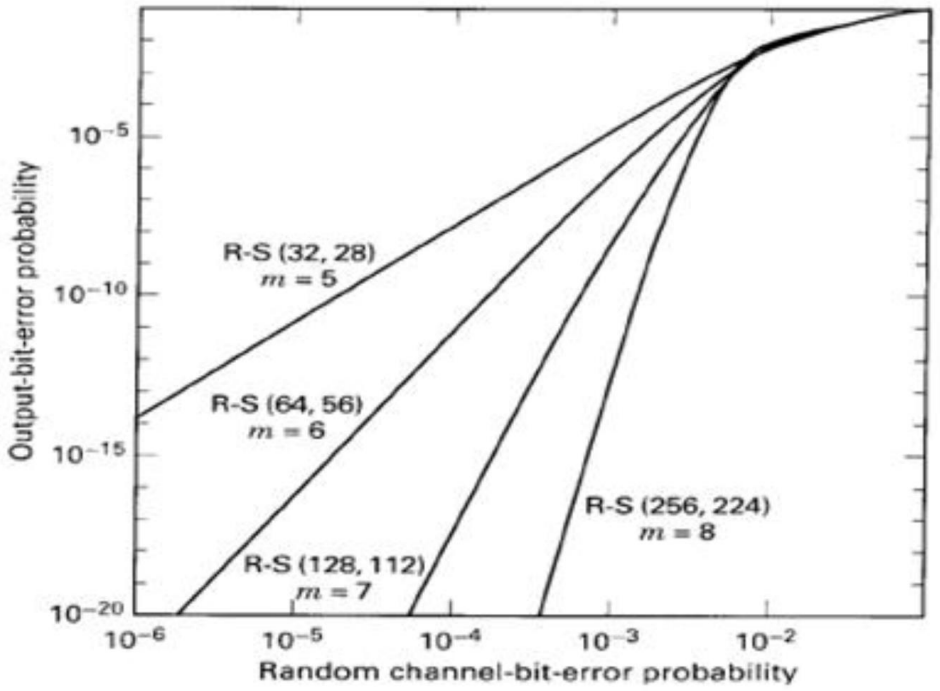
- Οι κώδικες R-S χρησιμοποιούνται σε πολλές σύγχρονες εφαρμογές όπως:
  - CDs
  - Διαστημικές και δορυφορικές επικοινωνίες (π.χ. ο κώδικας R-S(255, 223) ο οποίος αποτελεί standard κώδικα της NASA).



Κώδικες R-S

Απόδοση R-S κώδικα σε συνάρτηση του μεγέθους συμβόλου m

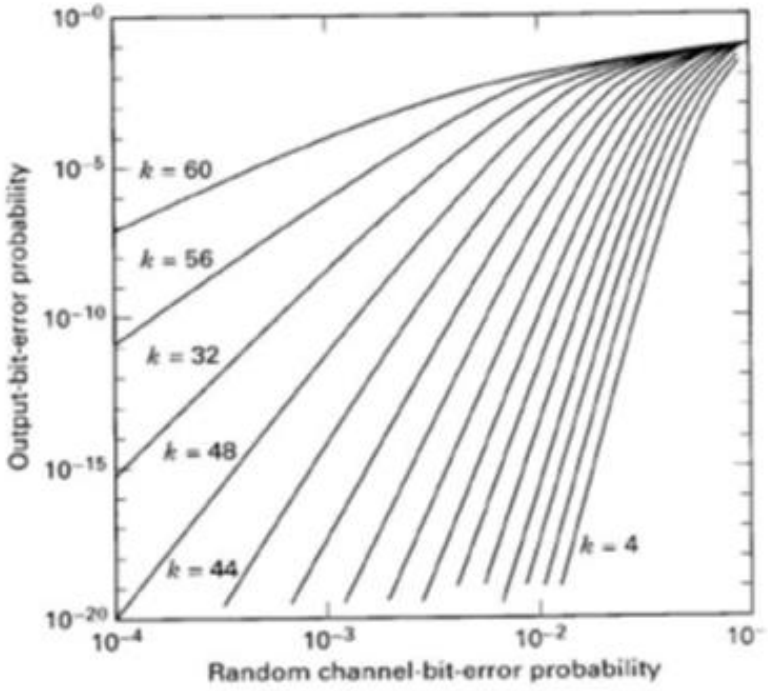
- Οι κώδικες διόρθωσης λαθών γίνονται πιο αποδοτικοί όταν το μέγεθος του block αυξάνεται.
- Εάν υποθέσουμε πως ο ρυθμός του κώδικα διατηρείται σταθερός στα 7/8 και το μέγεθος του block αυξάνεται από n = 32 σύμβολα (m = 5 bits / σύμβολο) σε n= 256 (m = 8 bits / σύμβολο), τότε το μέγεθος του block αυξάνεται από 160 bits σε 2048 bits και η απόδοση διαμορφώνεται όπως στο παρακάτω σχήμα:



Κώδικες R-S

Απόδοση R-S κώδικα σε συνάρτηση των bits πλεονασμού

- Καθώς τα bit πλεονασμού (n-k) ενός κώδικα R-S αυξάνονται (και άρα μειώνεται ο ρυθμός του κώδικα), αυξάνεται η πολυπλοκότητα υλοποίη-σης του καθώς και το απαραίτητο εύρος ζώνης.
- Το κέρδος από την αύξηση των bit πλεονασμού είναι η βελτίωση του BER, όπως φαίνεται στο παρακάτω σχήμα όπου το μήκος του κώδικα διατηρείται σταθερό στα 64 bit και τα πλεονάζοντα σύμβολα αυξάνονται από 4 σε 60.



Κώδικες R-S:
Πεπερασμένα Πεδία Galois

- Για να γίνει αντιληπτή η διαδικασία κωδικοποίησης και αποκωδικοποίησης μη δυαδικών κωδίκων, όπως είναι ο R-S, θα πρέπει να εισάγουμε την έννοια των πεπερασμένων πεδίων Galois (GF).
- Για κάθε πρώτο αριθμό p, υπάρχει ένα πεπερασμένο πεδίο GF(p) το οποίο περιέχει p στοιχεία.
- Το GF(P^m) καλείται το εκτεταμένο πεδίο του GF(p).
- Το GF(p) καλείται υποπεδίο του GF(P^m).
- Σύμβολα από το εκτεταμένο πεδίο GF(2^m) χρησιμοποιούνται για την κατασκευή των κωδίκων R-S (Το δυαδικό πεδίο GF(2) είναι υποπεδίο του GF(2^m)).
- Εκτός από τους αριθμούς 0 και 1, υπάρχουν επιπλέον μοναδικά στοιχεία στο εκτεταμένο πεδίο που τα αναπαριστούμε με ένα νέο σύμβολο α.

$$GF(2^m) = \{0, a^0, a^1, a^2, \dots, a^{2m-2}\}$$

- Ορίζουμε για κάθε μη-μηδενικό στοιχείο του πεδίου ένα πολυώνυμο $\alpha_i(x)$, όπου για $i = 0, 1, 2, \dots, 2^{m-2}$ έχουμε $\alpha^i = \alpha_i(x) = \alpha_{i,0} + \alpha_{i,1}(x)\, X + \dots + \alpha_{i,m-1}\, X_{m-1}$
- Επιλέγουμε αυτόν τον συμβολισμό για τη διευκόλυνση της κωδικοποίησης και αποκωδικοποίησης, μιας και η κωδική λέξη αποτελείται από n σύμβολα(nm bits).

Κώδικες R-S

Πεπερασμένα Πεδία Galois, Παράδειγμα για R-S (7, 3) – GF(2^3)

- Για m = 3, το πεδίο GF(2^3) έχει 8 στοιχεία (το μηδέν και 7 μη μηδενικά)
- Έτσι GF(2^3) = { 0, α^0, α^1, α^2,. . ., α^6}, με $\alpha_i = a_i(x) = a_{i,0} + a_{i,1} X + a_{i,2} X_2$
- Για να προσδιορίσουμε τους συντελεστές των α_i, εισάγουμε την έννοια των πρότυπων πολυωνύμων (primitive polynomial).
- Η κλάση πρότυπων πολυωνύμων ονομάζεται πρότυπη παρουσιάζει ενδιαφέρον γιατί μπορούμε απευθείας να ορίσουμε ένα πεδίο GF(2^m) και να το χρησιμοποιήσουμε για τον ορισμό ενός R-S κώδικα.
- Το πολυώνυμο μπορεί να βρεθεί χρησιμοποιώντας τον παρακάτω πίνακα, για διάφορες τιμές του m.

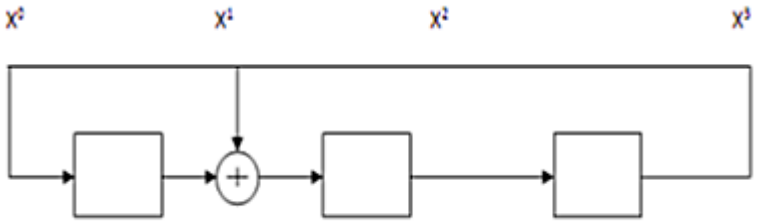
Some Primitive Polynomials

m		m	
3	$1 + X + X^3$	14	$1 + X + X^6 + X^{10} + X^{14}$
4	$1 + X + X^4$	15	$1 + X + X^{15}$
5	$1 + X^2 + X^5$	16	$1 + X + X^3 + X^{12} + X^{16}$
6	$1 + X + X^6$	17	$1 + X^3 + X^{17}$
7	$1 + X^3 + X^7$	18	$1 + X^7 + X^{18}$
8	$1 + X^2 + X^3 + X^4 + X^8$	19	$1 + X + X^2 + X^5 + X^{19}$
9	$1 + X^4 + X^9$	20	$1 + X^3 + X^{20}$
10	$1 + X^3 + X^{10}$	21	$1 + X^2 + X^{21}$
11	$1 + X^2 + X^{11}$	22	$1 + X + X^{22}$
12	$1 + X + X^4 + X^6 + X^{12}$	23	$1 + X^5 + X^{23}$
13	$1 + X + X^3 + X^4 + X^{13}$	24	$1 + X + X^2 + X^7 + X^{24}$

Κώδικες R-S

Πεπερασμένα Πεδία Galois, Παράδειγμα για R-S (7, 3) – GF(2^3) (*συνέχεια*)

- Από τον προηγούμενο πίνακα, το κατάλληλο πρότυπο πολυώνυμο είναι το $f(X)=1+X+X^3$
- Τα στοιχεία του εκτεταμένου πεδίου α μπορούν να αναπαρασταθούν από τα περιεχόμενα ενός δυαδικού ανατροφοδοτούμενου γραμμικού καταχωρητή (linear feedback shift register (LFSR)) ο οποίος σχηματίζεται από το πρότυπο πολυώνυμο.



- Αρχικοποιώντας το κύκλωμα με μία μη μηδενική κατάσταση (π.χ. 1 0 0) και εκτελώντας επαναληπτικά δεξιόστροφες ολισθήσεις , λαμβάνουμε τα σύμβολα του πεδίου.

Field elements	Basis elements X^0	X^1	X^2
0	0	0	0
α^0	1	0	0
α^1	0	1	0
α^2	0	0	1
α^3	1	1	0
α^4	0	1	1
α^5	1	1	1
α^6	1	0	1
α^7	1	0	0

Κώδικες R-S

Πεπερασμένα Πεδία Galois, Παράδειγμα για R-S (7, 3) – GF(2^3) (*συνέχεια*)

- Σύνοψη
  - Σε κάθε R-S κωδικοποίηση, πρώτα ορίζουμε τα n και k. Από αυτά υπολογίζουμε το m.
  - Βρίσκουμε το πρότυπο πολυώνυμο από τον παραπάνω πίνακα.
  - Δημιουργούμε τον LFSR και περνούμε όλες τα μη μηδενικά στοιχεία (=2^m-1).
- Πολλαπλασιασμός και πρόσθεση στο πεδίο GF(2^3)
  - Χρησιμοποιούμε τους παρακάτω πίνακα (ή αντίστοιχους για διαφορετικά m)

TABLE 8.2 Addition Table for GF(8) with $f(X) = 1 + X + X^3$

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	0	α^3	α^6	α^1	α^5	α^4	α^2
α^1	α^3	0	α^4	α^0	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α^1	α^3	α^0
α^3	α^1	α^0	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α^1	α^6	0	α^0	α^3
α^5	α^4	α^6	α^3	α^2	α^0	0	α^1
α^6	α^2	α^5	α^0	α^4	α^3	α^1	0

TABLE 8.3 Multiplication Table for GF(8) with $f(X) = 1 + X + X^3$

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
α^1	α^1	α^2	α^3	α^4	α^5	α^6	α^0
α^2	α^2	α^3	α^4	α^5	α^6	α^0	α^1
α^3	α^3	α^4	α^5	α^6	α^0	α^1	α^2
α^4	α^4	α^5	α^6	α^0	α^1	α^2	α^3
α^5	α^5	α^6	α^0	α^1	α^2	α^3	α^4
α^6	α^6	α^0	α^1	α^2	α^3	α^4	α^5

Κώδικες R-S

Παράδειγμα για R-S (7, 3) – GF(2^3) (*συνέχεια*), Κωδικοποίηση

- Για όλους τους τύπους block κωδικοποίησης, χρειαζόμαστε το πολυώνυμο γεννήτορα, που έχει την μορφή:

$$g(X) = g_0 + g_1 X + g_2 X^2 + \cdots + g_{2t-1} X^{2t-1} + X^{2t}$$

- Σχεδιάζουμε τις ρίζες του *g(X)* ως: α, α^2 , . . . , α^{2t}.

- Για τον R-S (7, 3):
  - n= 7, k=3 , t=(n-k)/2= 2, έτσι το πολυώνυμο γεννήτορας έχει βαθμό 4 (2t=4), και συνεπώς έχει 4 ρίζες: α, α_2, α_3, α_4

$$g(X) = (X - \alpha)\,(X - \alpha_2)(X - \alpha_3\,)(X - \alpha_4)$$

όπου χρησιμοποιώντας του παραπάνω πίνακες πολλαπλασιασμούς και πρόσθεσης, καταλήγουμε στο:

$$g(X) = \alpha_3 + \alpha_1 X + \alpha_0 X^2 + \alpha_3 X^3 + X^4$$

Κώδικες R-S

Παράδειγμα για R-S (7, 3) – GF(2^3) (*συνέχεια*), Κωδικοποίηση

- Εάν m(x) είναι το μήνυμα προς κωδικοποίηση, τα βήματα που ακολουθούμε είναι:
  - Πολλαπλασιάζω το m(x) με X^{n-k}.
  - Διαιρώ το αποτέλεσμα με το g(x). Έστω p(x) το υπόλοιπο.
  - Η λέξη που προκύπτει U(X) μπορεί να γραφεί ως :

$$U(X)=p(X)+m(X)X^{n-k}$$

- Στο παράδειγμα R-S(7,3)R-S, ακολουθούμε την παραπάνω διαδικασία για το μήνυμα**:**

$$\underbrace{010}_{\alpha^1} \quad \underbrace{110}_{\alpha^3} \quad \underbrace{111}_{\alpha^5}$$

$$g(X)=\alpha_3+\alpha_1 X+\alpha_0 X^2+\alpha_3 X^3+X^4$$

1. Πολλαπλασιάζουμε το μήνυμα $m(X)=\alpha^1+\alpha^3X+\alpha^5X^2$ με $X^{n-k}=X^4$. Η πράξη δίνει $\alpha^1X^4+\alpha^3X^5+\alpha^5X^6$
2. Διαιρούμε με το πολυώνυμο γεννήτορα και παίρνουμε υπόλοιπο p(X): $P(X)=\alpha^0+\alpha^2X+\alpha^4X^2+\alpha^6X^3$
3. Το πολυώνυμο της κωδικής λέξης μπορεί να γραφεί ως: $U(X)=p(X)+m(X)X^{n-k}=\alpha^0+\alpha^2X+\alpha^4X^2+\alpha^6X^3+\alpha^1X^4+\alpha^3X^5+\alpha^5X^6$

Αφού υπολογίσουμε τους συντελεστές, όπως περιεγράφηκε παραπάνω, έχουμε

$$U(X)=(100)+(001)X+(011)X^2+(101)X^3+(010)X^4+(110)X^5+(111)X^6$$

Κώδικες R-S

Παράδειγμα για R-S (7, 3) – GF(2^3) (*συνέχεια*), Αποκωδικοποίηση

- Υποθέτουμε πως κατά την διάρκεια της μετάδοσης, στην κωδική λέξη συνέβησαν λάθη, και 2 σύμβολά της άλλαξαν.
- Αναπαριστούμε το πρότυπο λάθους ως πολυώνυμο:
  $e(X) = (000) + (001)X + (011)X^2 + (001)\,X^3 + (111)\,X^4 + (000)\,X^5 + (000)X^6$

- Η λαμβανόμενη λανθασμένη κωδική λέξη (αναπαρίσταται το πολυώνυμο r(X)) είναι το άθροισμα της εκπεμπόμενης κωδικής λέξης και του προτύπου λάθους:
  $r(X) = U(X) + e(X) \Longrightarrow$
  $r(X) = (100) + (001)X + (011)X^2 + (100)\,X^3 + (101)\,X^4 + (110)\,X^5 + (111)X^6 \Longrightarrow$
  $r(X) = \alpha^0 + \alpha^2X + \alpha^4X^2 + \alpha^4X^2 + \alpha^0X^3 + \alpha^6X^4 + \alpha^3X^5 + \alpha^5X^6$

- Υπολογισμός συνδρόμου για τον R-S(7, 3) ($Si(X)|_{X=\alpha i} = r(\alpha^i)$ ($i = 1,2,\ldots\ldots n-k$))
  - $S1(\alpha) = \alpha^0 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^{10} + \alpha^8 + \alpha^{11} = \alpha^0 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^3 + \alpha^1 + \alpha^4 = \alpha^3$
  - $S2(\alpha^2) = \alpha^0 + \alpha^4 + \alpha^8 + \alpha^6 + \alpha^{14} + \alpha^{13} + \alpha^{17} = \alpha^0 + \alpha^4 + \alpha^1 + \alpha^6 + \alpha^0 + \alpha^6 + \alpha^3 = \alpha^5$
  - $S3(\alpha^3) = \alpha^0 + \alpha^5 + \alpha^{10} + \alpha^9 + \alpha^{18} + \alpha^{18} + \alpha^{23} = \alpha^0 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha^4 + \alpha^4 + \alpha 2 = \alpha^6$
  - $S4(\alpha^4) = \alpha^0 + \alpha^6 + \alpha^{12} + \alpha^{12} + \alpha^{22} + \alpha^{23} + \alpha^{29} = \alpha^0 + \alpha^6 + \alpha^5 + \alpha^5 + \alpha^1 + \alpha^2 + \alpha^1 = 0$

- Αφού υπάρχουν $S \neq 0$, η κωδική λέξη περιέχει λάθη

Κώδικες R-S

Παράδειγμα για R-S (7, 3) – GF(2^3) (*συνέχεια*), Αποκωδικοποίηση

- Το πολυώνυμο εντοπισμού λαθών είναι το $\sigma(X) = \alpha^0 + \alpha^6 X + \alpha^0 X^2$

- Βάζοντας τιμές στο σ(X) τα στοιχεία του πεδίου GF(2^3), εντοπίζουμε τα μη μηδενικά στοιχεία, τα οποία είναι και τα λανθασμένα
  - $\sigma(\alpha^0) = \alpha^0 + \alpha^6 + \alpha^0 = \alpha^6 \neq 0$
  - $\sigma(\alpha^1) = \alpha^0 + \alpha^7 + \alpha^2 = \alpha^2 \neq 0$
  - $\sigma(\alpha^2) = \alpha^0 + \alpha^8 + \alpha^4 = \alpha^6 \neq 0$
  - $\sigma(\alpha^3) = \alpha^0 + \alpha^9 + \alpha^6 = 0$ **ΛΑΘΟΣ**
  - $\sigma(\alpha^4) = \alpha^0 + \alpha^{10} + \alpha^8 = 0$ **ΛΑΘΟΣ**
  - $\sigma(\alpha^5) = \alpha^0 + \alpha^{11} + \alpha^{10} = \alpha^2 \neq 0$
  - $\sigma(\alpha^6) = \alpha^0 + \alpha^{12} + \alpha^{12} = \alpha^0 \neq 0$