•ΚΩΔΙΚΟΠΟΙΗΣΗ ΕΛΕΓΧΟΥ ΣΦΑΛΜΑΤΟΣ

•*Στόχος είναι η περιγραφή του τρόπου κατασκευής, καθώς και της συμπεριφοράς κωδίκων ανίχνευσης και διόρθωσης σφαλμάτων.*

- ***Επιμέρους στόχοι***

– *Αντικείμενο της Θεωρίας Κωδικοποίησης.*

– *Περιγραφή των διαδικασιών κωδικοποίησης και αποκωδικοποίησης γραμμικών κωδίκων.*

– *Περιγραφή διαδικασιών κωδικοποίησης και αποκωδικοποίησης κυκλικών κωδίκων, καθώς και της διαδικασίας αποκωδικοποίησης των BCH κωδίκων.*

•ΕΙΣΑΓΩΓΗ ΣΤΗ ΘΕΩΡΙΑ ΚΩΔΙΚΟΠΟΙΗΣΗΣ (ΕΝΟΤΗΤΑ 4.1)

- ***Εξεταζονται***

– *Ισομήκεις κώδικες ή Κώδικες μπλοκ*
– *Αξιοπιστία καναλιού*
– *Ρυθμός πληροφορίας*
– *Βάρος λέξης*
– *Απόσταση μεταξύ δύο λέξεων*
– *Αποκωδικοποίηση μέγιστης πιθανότητας*
– *Πρότυπο σφάλματος*
– *Απόσταση κώδικα*

•ΠΑΡΑΔΟΧΕΣ ΚΑΙ ΟΡΙΣΜΟΙ

- *Ένας **κώδικας ονομάζεται** ισομήκης κώδικας (ή κώδικας μπλοκ) **αν όλες οι κωδικές λέξεις έχουν το ίδιο μήκος**.*
- ***Παραδοχή 1:** μια κωδική λέξη μήκους n δυαδικών ψηφίων, που εισέρχεται στο κανάλι, λαμβάνεται στην έξοδό του ως λέξη μήκους και πάλι n δυαδικών ψηφίων*
- ***Παραδοχή 2:** τα σφάλματα, δηλαδή ο θόρυβος, εμφανίζονται διασκορπισμένα κατά τυχαίο τρόπο και όχι σε συστάδες (ή καταιγισμούς, bursts).*
- *Η **αξιοπιστία του καναλιού** είναι ο πραγματικός αριθμός p, 0 <= p <= 1, όπου p είναι η πιθανότητα της ορθής μεταφοράς ενός δυαδικού ψηφίου μέσω του καναλιού.*
- *Ο **ρυθμός πληροφορίας** ενός κώδικα είναι το ποσοστό της κωδικής λέξης που μεταφέρει το μήνυμα. Ο ρυθμός πληροφορίας ενός δυαδικού κώδικα C μήκους n είναι ίσος με (1/n)log2|C|. Πρότυπο σφάλματος*

•ΠΑΡΑΔΟΧΕΣ ΚΑΙ ΟΡΙΣΜΟΙ *(συνέχεια)*

- ***Βάρος (Weight)***

  *Βάρος Hamming ή απλά **βάρος**, wt(x), μιας λέξης x μήκους n ψηφίων ονομάζεται το πλήθος των ψηφίων της λέξης, τα οποία είναι ίσα με το '1'. Το βάρος παίρνει τιμές από 0 έως n.*

- ***Απόσταση (Distance)***

  *Απόσταση Hamming ή απλά **απόσταση**, d(x, y), μεταξύ δύο λέξεων x και y του ιδίου μήκους n ονομάζεται το πλήθος των θέσεων, στις οποίες οι δύο λέξεις εμφανίζουν ασυμφωνία του δυαδικού ψηφίου. Η απόσταση παίρνει τιμές από 0 έως n.*

- *Μεταξύ των δυαδικών λέξεων ορίζονται οι πράξεις της πρόσθεσης και του πολλαπλασιασμού ως ακολούθως:*

  $0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 0 = 1$ *και* $1 + 1 = 0$

  $0 \cdot 0 = 0,\ 0 \cdot 1 = 0,\ 1 \cdot 0 = 0$ *και* $1 \cdot 1 = 1.$

- *Συμβολίζουμε με π(x, y) την πιθανότητα να μεταδόθηκε η λέξη x και να ελήφθη από τον παραλήπτη η λέξη y.*

•ΚΑΠΟΙΕΣ ΣΥΝΕΠΕΙΕΣ

- *μπορούμε να αντιμετωπίσουμε τη μετάδοση κάθε δυαδικού ψηφίου ως ανεξάρτητο γεγονός. Έτσι, αν οι λέξεις x και y εμφανίζουν διαφορές σε d δυαδικά ψηφία, τότε n-d ψηφία μεταδόθηκαν σωστά και d ψηφία μεταδόθηκαν εσφαλμένα. Επομένως, $\pi(x, y)=p^{n-d}(1-p)^{d}$.*

- *Θεωρούμε ένα BSC κανάλι με ½<p<1, δύο κωδικές λέξεις x1 και x2 και μία λέξη y, όλες μήκους n ψηφίων, καθώς και ότι οι x1 και y διαφέρουν σε d1 ψηφία και οι x2 και y σε d2 ψηφία. Τότε $\pi(x1, y) <= \pi(x2, y)$ αν και μόνο αν d1 >= d2.*

- **ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΚΩΔΙΚΟΠΟΙΗΣΗΣ ΚΑΙ ΤΗΣ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗΣ**
  - *Η κωδικοποίηση συνίσταται στον προσδιορισμό ενός κώδικα, ο οποίος θα χρησιμοποιηθεί για την αποστολή των μηνυμάτων*

  - *Σε ότι αφορά την αποκωδικοποίηση, αν ο αποδέκτης λάβει μία λέξη y, μήκους n ψηφίων, η οποία είναι κωδική λέξη, τότε εξάγει το αντίστοιχο μήνυμα.*
  - Αν όμως η λέξη *y* δεν είναι κωδική λέξη [ανίχνευση σφαλμάτων] ο παραλήπτης μπορεί να χρησιμοποιήσει μια διαδικασία, την **αποκωδικοποίηση μέγιστης πιθανότητας,** για την επιλογή της κωδικής λέξης που μεταδόθηκε (διόρθωση σφαλμάτων).

  - ***Πλήρης αποκωδικοποίηση μέγιστης πιθανότητας (ΠΑΜΠ):*** *όταν μόνο μία κωδική λέξη x εμφανίζει τη μικρότερη απόσταση από τη λέξη y, τότε η y αποκωδικοποιείται ως x. Αν περισσότερες κωδικές λέξεις εμφανίζουν την ίδια απόσταση από τη λέξη y, τότε η ληφθείσα λέξη αποκωδικοποιείται ως μία από αυτές τις κωδικές λέξεις.*
  - ***Ατελής αποκωδικοποίηση μέγιστης πιθανότητας (ΑΑΜΠ).*** *Όπως ΠΑΜΠ αλλά αν υπάρχουν περισσότερες κωδικές λέξεις με την ίδια απόσταση στη λέξη y, τότε ο αποδέκτης ζητά από τον αποστολέα επανάληψη της μετάδοσης.*

• ΚΩΔΙΚΕΣ ΑΝΙΧΝΕΥΣΗΣ ΣΦΑΛΜΑΤΩΝ

- *το **πρότυπο σφάλματος**, ε = το άθροισμα της κωδικής λέξης x που μεταδόθηκε με τη λέξη y που ελήφθη στον αποδέκτη, δηλαδή ε=x+y.*
- ***απόσταση κώδικα** C = η μικρότερη από τις αποστάσεις όλων των δυνατών ζευγών κωδικών λέξεων του κώδικα. Επειδή d(x, y) = wt(x+ y), η απόσταση του κώδικα C είναι ίση με την ελάχιστη τιμή του βάρους wt(x+ y)*
- *λέμε ότι ο κώδικας ανιχνεύει το πρότυπο σφάλματος ε αν και μόνο αν x+ε=y δεν είναι κωδική λέξη*

- ***Θεώρημα 4.2***
- *Ένας κώδικας C απόστασης d ανιχνεύει όλα τα μη μηδενικά πρότυπα σφάλματος βάρους μικρότερου ή ίσου του d-1. Επίσης, υπάρχει τουλάχιστον ένα πρότυπο σφάλματος βάρους d που δεν ανιχνεύει ο κώδικας C.*

• ΚΩΔΙΚΕΣ ΔΙΟΡΘΩΣΗΣ ΣΦΑΛΜΑΤΩΝ

– ***Θεώρημα 4.3***

– *Ένας κώδικας C απόστασης d διορθώνει όλα τα πρότυπα σφάλματος βάρους μικρότερου ή ίσου του [(d-1)/2]. Επίσης, υπάρχει τουλάχιστον ένα πρότυπο σφάλματος βάρους 1+[(d-1)/2] που δεν διορθώνει ο κώδικας C.*

– **Παράδειγμα**: Θεωρούμε ένα πλήθος μηνυμάτων $|M|=2$, $k=1$, $n=3$ και $C=\{000, 111\}$. Ποια πρότυπα σφάλματος διορθώνονται από τον κώδικα σύμφωνα με το θεώρημα 4.3;

αφού η απόσταση του κώδικα είναι ίση με 3, ο κώδικας διορθώνει κάθε πρότυπο σφάλματος βάρους 1 => ο αποδέκτης συμπεραίνει την κωδική λέξη '111', εφόσον λάβει αυτή την κωδική λέξη ή μία από τις '011', '101 ή '110', δηλαδή διορθώνει τα πρότυπα σφάλματος 111+011=100, 111+101=010 και 111+110=001.

- **ΓΡΑΜΜΙΚΟΙ ΚΩΔΙΚΕΣ (ΕΝΟΤΗΤΑ 4.2)**

Εξετάζονται

- Γραμμικός κώδικας (Linear Code)
- Βάση Κώδικα (Basis for a Code)
- Διάσταση κώδικα (Dimension of Code)
- Μορφή (περιορισμένης) κλιμακωτής διάταξης γραμμών (Row Echelon Form)
- Γεννήτορας πίνακας (Generator Matrix)
- Πίνακας ελέγχου ισοτιμίας (Parity-Check Matrix)
- Συστηματικός κώδικας
- Συνομάδα (Coset)
- Μήνυμα ή ψηφία πληροφορίας και πλεονασμός ή ψηφία ελέγχου ισοτιμίας
- Σύνδρομο (Syndrome)
- Τέλειοι κώδικες (Perfect Codes)
- Κώδικες Hamming

• ΟΡΙΣΜΟΙ - ΑΝΤΙΣΤΟΙΧΙΕΣ

– *Ένας κώδικας C ονομάζεται γραμμικός αν για κάθε x, y ανήκει C, τότε (x+y) ανήκει C.*

– *Αντιστοιχία εννοιών της γραμμικής άλγεβρας και εννοιών της θεωρίας κωδικοποίησης*

Έννοιες Γραμμικής Άλγεβρας	**Έννοιες Θεωρίας Κωδικοποίησης**
Διανυσματικός υποχώρος	Γραμμικός Κώδικας
Διάνυσμα	Λέξη
Γραμμικό ανάπτυγμα υποσυνόλου S του διανυσματικού χώρου, $<S>$ (Διανυσματικός υποχώρος) Διάνυσμα του $<S>$	Γραμμικός κώδικας $C=<S>$ Κωδική λέξη του $C=<S>$
Ορθογώνιο συμπλήρωμα υποσυνόλου S	Δυϊκός κώδικας
Βάση διανυσματικού υποχώρου	Βάση γραμμικού κώδικα
Διάσταση διανυσματικού υποχώρου	Διάσταση γραμμικού κώδικα

• ΥΠΟΜΝΗΣΕΙΣ ΑΠ0 ΓΡΑΜΜΙΚΗ ΑΛΓΕΒΡΑ

- **Απαιτουνται και θεωρούνται γνωστές οι έννοιες: Γραμμικό ανάπτυγμα, ορθογώνιο συμπλήρωμα, ορθογώνια διανύσματα, βαθμωτό γινόμενο, γραμμική ανεξαρτησία, βάση διανυσματικού χώρου**

Ιδιότητες των πράξεων της πρόσθεσης και του πολλαπλασιασμού σε έναν διανυσματικό χώρο K^n

1. $(y+z) \in K^n$,
2. $\alpha.y \in K^n$,
3. $x+y=y+x$,
4. $(x+y)+z=x+(y+z)$,
5. $(\alpha.\beta).y=\alpha.(\beta.y)$,
6. $(\alpha+\beta).x=\alpha.x+\beta.y$,
7. $a.(x+y)=a.x+a.y$,
8. $(x+0)=x$,
9. $1.x=x$,
10. υπάρχει λέξη $x' \in K^n$, τέτοια ώστε $x+x'=x'+x=0$.

• ΜΕΤΑΦΟΡΑ ΠΙΝΑΚΑ ΣΕ ΜΟΡΦΗ ΚΔΓ - ΠΚΔΓ

1) Ένας πίνακας βρίσκεται σε **μορφή κλιμακωτής διάταξης γραμμών** (ΚΔΓ, row echelon form) αν όλες οι μηδενικές γραμμές είναι στο κάτω μέρος και το πρώτο ψηφίο '1' ('οδηγός') μιας γραμμής είναι σε στήλη πιο δεξιά σε σχέση με το πρώτο (τον οδηγό) '1' των προηγούμενων γραμμών.
2) Μια στήλη που περιέχει έναν 'οδηγό' '1' ονομάζεται στήλη 'οδηγός'. Αν, επιπλέον, σε κάθε στήλη οδηγό του πίνακα (δηλαδή στήλη που περιέχεται ο οδηγός '1' μιας γραμμής) δεν περιέχονται άλλα ψηφία '1' αλλά μόνο ψηφία '0', τότε ο πίνακας είναι σε **μορφή περιορισμένης κλιμακωτής διάταξης γραμμών** (ΠΚΔΓ, reduced row echelon form).
3) Κάθε πίνακας με στοιχεία '0' και '1' μπορεί να τεθεί σε μορφή ΚΔΓ και ΠΚΔΓ. Για έναν πίνακα, η μορφή ΠΚΔΓ είναι μοναδική. Αντίθετα, ο πίνακας μπορεί να έχει πολλές μορφές ΚΔΓ.
4) Η μεταφορά ενός πίνακα, του οποίου οι γραμμές αποτελούνται από τις λέξεις του κώδικα C, σε μορφή ΚΔΓ ή ΠΚΔΓ μας είναι ιδιαίτερα χρήσιμη, διότι οι μη μηδενικές γραμμές του πίνακα στη μορφή ΚΔΓ και ΠΚΔΓ απαρτίζουν ένα μέγιστης διάστασης γραμμικώς ανεξάρτητο υποσύνολο του C.

Παράδειγμα

Δίνεται ο κώδικας $C=\{0000, 1110, 0111, 1001\}$, του οποίου οι λέξεις αποτελούν τις γραμμές πίνακα P. Ζητείται ο πίνακας P σε ΚΔΓ.

Απάντηση. Εφαρμόζοντας τις δύο στοιχειώδεις πράξεις γραμμών λαμβάνουμε τη ζητούμενη μορφή ΚΔΓ του πίνακα.

$$P=\begin{bmatrix}0&0&0&0\\1&1&1&0\\0&1&1&1\\1&0&0&1\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&0&0&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&1&1&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

• ΕΥΡΕΣΗ ΒΑΣΗΣ ΔΥΑΔΙΚΟΥ ΚΩΔΙΚΑ

Τρόπος εύρεσης βάσεων των δύο κωδίκων (διανυσματικών χώρων):

του κώδικα $C=<S>$ (γραμμικού αναπτύγματος $<S>$) και του δυϊκού του κώδικα $C^{\perp}$ (ορθογωνίου συμπληρώματος $S^{\perp}$).

Αλγόριθμος 1 - Εύρεση μιας βάσης του δυϊκού κώδικα $C^{\perp}$

Η διαδικασία εύρεση μιας βάσης του δυϊκού κώδικα $C^{\perp}$ ($C=<S>$) διακρίνεται στα ακόλουθα βήματα:

1. Σχηματισμός του πίνακα P, του οποίου οι γραμμές είναι οι λέξεις του S (ή του C) και μεταφορά του P σε μορφή ΠΚΔΓ.
2. Σχηματισμός του πίνακα G, ο οποίος αποτελείται από τις μη μηδενικές γραμμές του πίνακα P σε μορφή ΠΚΔΓ και αποτελεί μια βάση του C. Ο πίνακας G είναι διάστασης lxm.
3. Σχηματισμός του πίνακα M, ο οποίος αποτελείται μόνον από εκείνες τις στήλες του πίνακα G που δεν είναι οδηγοί, δηλαδή από τις στήλες που δεν περιέχουν οδηγούς '1'. Αφού το πλήθος των στηλών οδηγών του πίνακα G είναι ίσο με το πλήθος των γραμμών του, η διάσταση του πίνακα M είναι $lx(m-l)$.
4. Σχηματισμός του πίνακα $H=\begin{bmatrix} M \\ I \end{bmatrix}$, διάστασης $mx(m-l)$, από τον πίνακα $M(lx(m-l))$ και τον πίνακα ταυτότητας I $((m-l)x(m-l))$. (Υπόμνηση: Ο πίνακας ταυτότητας I είναι αυτός που έχει τα στοιχεία της διαγωνίου του ίσα με 1 και όλα τα υπόλοιπα ίσα με 0.) Με άλλα λόγια, ο πίνακας H $(mx(m-l))$ σχηματίζεται ως εξής:
   - Στις πρώτες l γραμμές του H τοποθετούνται με τη σειρά οι γραμμές του M.
   - Στις υπόλοιπες $(m-l)$ γραμμές του H τοποθετούνται οι γραμμές του πίνακα ταυτότητας I διάστασης $(m-l)x(m-l)$.
5. Μια βάση του δυϊκού κώδικα $C^{\perp}$ αποτελείται από τις στήλες του πίνακα H (ή τις γραμμές του ανάστροφου πίνακα H^T).

• ΕΥΡΕΣΗ ΒΑΣΗΣ ΔΥΑΔΙΚΟΥ ΚΩΔΙΚΑ (παραδειγμα)

Δίνεται το σύνολο *S={11101, 10110, 01011, 11010}* και ο κώδικας *C=<S>*. Ζητείται μία βάση του $C^{\perp}$.

Απάντηση:

Σχηματίζουμε τον πίνακα *P*, ο οποίος έχει ως γραμμές τις λέξεις του *S*.
Τον πίνακα *P* μεταφέρουμε στη μορφή ΠΚΔΓ ως ακολούθως:

$$P = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow$$

$$\rightarrow \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Ο πίνακας *G*, διαστάσεων *(3x5)*, σχηματίζεται από τις μη μηδενικές γραμμές του *P* σε μορφή ΠΚΔΓ και ο πίνακας *M*, *(3x2)*, από τον πίνακα *G* με την αφαίρεση των τριών πρώτων στηλών που περιέχουν οδηγούς (πρώτα) '1'. Από τον *M* και τον πίνακα ταυτότητας *I*, *(2x2)*, παίρνουμε τον ζητούμενο πίνακα *H*, διαστάσεων *(5x2)*.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}, M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}, H = \begin{bmatrix} M \\ I \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Επομένως, μια βάση του δυϊκού κώδικα $C^{\perp}$ είναι το σύνολο *{01110, 11101}*.

• ΓΕΝΝΗΤΟΡΕΣ ΠΙΝΑΚΕΣ

- Κάθε πίνακας, του οποίου οι γραμμές αποτελούν μια βάση του κώδικα C, ονομάζεται **γεννήτορας πίνακας** για τον C.
- Το πλήθος των γραμμών του γεννήτορα πίνακα = με τη διάσταση του C.
- Αν η διάσταση ενός κώδικα $C = k$, το μήκος των κωδικών λέξεων είναι n και η απόστασή του d, τότε $C = (n, k, d)$ γραμμικό κώδικας.

Ένας γεννήτορας πίνακας G για έναν γραμμικό κώδικα (n, k, d), C, μπορεί να αξιοποιηθεί για την κωδικοποίηση λέξεων (μηνυμάτων) u μήκους k ψηφίων ως εξής:

$$c = u.G = [a_1 \quad a_2 \quad \dots \quad a_k] \begin{bmatrix} g_1 \\ g_2 \\ \cdot \\ \cdot \\ g_k \end{bmatrix} = a_1 g_1 + a_2 g_2 + \dots + a_k g_k = [b_1 \quad b_2 \quad \dots \quad b_n]$$

όπου $u = [\alpha_1\ \alpha_2 \dots \alpha_k]$ η λέξη (διάνυσμα – γραμμή) του μηνύματος και $c = [b_1\ b_2 \dots b_n]$ η κωδική λέξη (διάνυσμα – γραμμή) μήκους n ψηφίων.

- **ΠΙΝΑΚΕΣ ΕΛΕΓΧΟΥ ΙΣΟΤΙΜΙΑΣ ΚΑΙ ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗ**

– Ορισμοί

1) Ο κώδικας *C*, ο οποίος έχει γεννήτορα πίνακα *G* σε τυπική μορφή, χαρακτηρίζεται **συστηματικός κώδικας.**

2) Κάθε κωδική λέξη *c* ενός τέτοιου κώδικα *C*, μήκους *n* και διάστασης *k*, είναι ίση με *u.G*. *Θεωρώντας οτι με τη βοήθεια της αποκωδικοποίησης μέγιστης πιθανότητας (ΑΜΠ), ο δέκτης μπορεί εύκολα να ανακτήσει το μήνυμα u από το ληφθέν c= u.G =>*

στους συστηματικούς κώδικες:

τα πρώτα *k* ψηφία των κωδικών λέξεων λέγονται **ψηφία πληροφορίας** και τα υπόλοιπα *n-k* **πλεονασμός** ή **ψηφία ελέγχου ισοτιμίας.**

• ΣΥΣΤΗΜΑΤΙΚΟΙ ΚΩΔΙΚΕΣ ΚΑΙ ΙΔΙΟΤΗΤΕΣ ΣΥΝΟΜΑΔΩΝ

Αν C είναι ένας συστηματικός γραμμικός κώδικας μήκους n και x και y δύο λέξεις επίσης μήκους n ψηφίων, τότε ισχύουν :

- Κάθε λέξη x περιέχεται στη συνομάδα $C+x$.
- Αν το άθροισμα $x+y$ περιέχεται στον κώδικα C, τότε οι x και y περιέχονται στην ίδια συνομάδα. Αν το άθροισμα $x+y$ δεν περιέχεται στον κώδικα C, τότε οι x και y περιέχονται σε διαφορετικές συνομάδες.
- Αν μια λέξη x περιέχεται στη συνομάδα $C+y$, τότε ισχύει $C+x= C+y$.
- Κάθε λέξη $x \in K^n$ περιέχεται μόνο σε μία συνομάδα του C.
- Το πλήθος των λέξεων σε μια συνομάδα είναι ίσο με το πλήθος των λέξεων του κώδικα C, δηλαδή $|C+x|=|C|$.
- Το πλήθος των διαφορετικών συνομάδων του κώδικα C, διάστασης k, ισούται με 2^{n-k} και κάθε συνομάδα περιέχει 2^k λέξεις.

• ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗ ΜΕ ΒΑΣΗ ΣΥΝΟΜΑΔΕΣ

Αλγόριθμος 2 - Αποκωδικοποίηση με τη βοήθεια των συνομάδων

Η διαδικασία αποκωδικοποίησης με τη βοήθεια των συνομάδων διακρίνεται στα ακόλουθα βήματα:

1. Λήψη της λέξης y και υπολογισμός της συνομάδας $C+y$.

2. Επιλογή από τον δέκτη της λέξης ε, ελάχιστου βάρους, που περιέχεται στη συνομάδα $C+y$. Αν περισσότερες λέξεις της συνομάδας $C+y$ έχουν το ελάχιστο βάρος, τότε στην περίπτωση ΠΑΜΠ επιλέγεται αυθαίρετα μία εξ αυτών, ενώ στην περίπτωση της ΑΑΜΠ ζητείται από τον μεταδότη επανάληψη της μετάδοσης.

3. Υπολογισμός από τον δέκτη της κωδικής λέξης x που έχει μεταδοθεί προσθέτοντας τη ληφθείσα λέξη y με το πρότυπο σφάλματος ελάχιστου βάρους ε, δηλαδή $x=y+\varepsilon$.

• ΑΠΟΚΩΔΙΚΟΠΟΙΗΣΗ ΜΕ ΒΑΣΗ ΤΗΝ ΤΔΑ

Υπολογισμός πίνακα ελέγχου ισοτιμίας -> επιλογή οδηγού κάθε συνομάδας, δηλαδή τη λέξη με το μικρότερο βάρος -> υπολογισμός του συνδρόμου κάθε συνομάδας=> ΤΔΑ για ΠΑΜΠ και ΑΑΜΠ.

$$P = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow M = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, H = \begin{bmatrix} M \\ I \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

ΤΔΑ για ΠΑΜΠ

Οδηγός συνομάδας	Σύνδρομο συνομάδας
0000	*y.H=00*
0001	*(0001).H=01*
0010	*(0010).H=10*
0100	*(0100).H=11*

ΤΔΑ για ΑΑΜΠ

Οδηγός συνομάδας	Σύνδρομο συνομάδας
0000	*00*
0001	*01*
-----	*10*
0100	*11*

Αλγόριθμος 3 – Αποκωδικοποίηση στη βάση της ΤΔΑ

- Λήψη της λέξης y και υπολογισμός του συνδρόμου $y.H$.
- Εύρεση από την ΤΔΑ του οδηγού ε που αντιστοιχεί στην συνομάδα με σύνδρομο $y.H$. Αν δεν υπάρχει αντίστοιχος οδηγός της συνομάδας, τότε ζητείται αναμετάδοση.
- Υπολογισμός της μεταδοθείσας κωδικής λέξης x προσθέτοντας την y με τον οδηγό της συνομάδας ε => $x=y+\varepsilon$.

- **ΤΕΛΕΙΟΙ ΚΩΔΙΚΕΣ ΚΑΙ ΚΩΔΙΚΕΣ HAMMING**

1) Ένας γραμμικός κώδικας C μήκους n και περιττής απόστασης $d=2t+1$ χαρακτηρίζεται τέλειος κώδικας αν $|C| = \dfrac{2^n}{\left(\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{t}\right)}$.

2) Ένας κώδικας μήκους $n=2^r-1$ $(r\geq 2)$ και πίνακα ελέγχου ισοτιμίας H, ο οποίος (H) απαρτίζεται από όλες τις δυνατές μη μηδενικές λέξεις μήκους r, ονομάζεται **κώδικας Hamming μήκους** 2^r-1.

• ΚΥΚΛΙΚΟΙ ΚΩΔΙΚΕΣ (ΕΝΟΤΗΤΑ 4.3)

Εξετάζονται

Κυκλικοί κώδικες (Cyclic Codes)
Πολυώνυμο-γεννήτορας (Generator Polynomial)
BCH κώδικες

Ορισμοί

Α) Ένας γραμμικός κώδικας C καλείται **κυκλικός** αν η κυκλική μετατόπιση κάθε κωδικής λέξης είναι και αυτή κωδική λέξη.

Β) Σε έναν γραμμικό κυκλικό κώδικα C υπάρχει μία μοναδική λέξη γ, της οποίας το αντίστοιχο πολυώνυμο $\gamma(x)$ έχει τον μικρότερα βαθμό

Το πολυώνυμο ελάχιστου βαθμού που αντιστοιχεί σε αυτή τη μοναδική, μη μηδενική, λέξη του C καλείται **πολυώνυμο – γεννήτορας**.

=> για κάθε πολυώνυμο (λέξη) $c(x) \in C$, υπάρχει πολυώνυμο $a(x)$, ώστε $c(x)=a(x)\gamma(x) \ mod(1+x^n)$,

=> πολυώνυμο – γεννήτορας διαιρεί όλες τις κωδικές λέξεις $c(x) \in C$.

- **ΑΛΓΟΡΙΘΜΟΙ ΠΟΛΥΩΝΥΜΙΚΗΣ ΚΩΔΙΚΟΠΟΙΗΣΗΣ**

Αλγόριθμος 4 –Διαδικασία πολυωνυμικής κωδικοποίησης

Θεωρούμε έναν κυκλικό κώδικα C μήκους n και διάστασης k και το πολυώνυμο – γεννήτορα του C, $\gamma(x)$, του οποίου ο βαθμός είναι n-k. Αν τα k δυαδικά ψηφία πληροφορίας $a_0a_1...a_{k-1}$, παριστάνονται με το πολυώνυμο κωδικοποίησης $(a_0+ a_1x+ ...+ a_{k-1}x^{k-1})$, τότε η κωδικοποίηση =>

:

- Τα ψηφία πληροφορίας $a_0a_1...a_{k-1}$ κωδικοποιούνται ως η λέξη $c_0c_1...c_{n-1}$ που αντιστοιχεί στο πολυώνυμο $c(x)=a(x).\gamma(x)$.

- # ΑΛΓΟΡΙΘΜΟΙ ΠΟΛΥΩΝΥΜΙΚΗΣ ΚΩΔΙΚΟΠΟΙΗΣΗΣ (συν.)

Αλγόριθμος 5 - Διαδικασία πολυωνυμικής αποκωδικοποίησης

Θεωρούμε έναν κυκλικό κώδικα C μήκους n και διάστασης k και το πολυώνυμο – γεννήτορα του C, $\gamma(x)$, του οποίου ο βαθμός είναι n-k. Επίσης, τη ληφθείσα λέξη $l(x)$.

Αποκωδικοποίηση ⇔

- Υπολογισμός του συνδρόμου $\sigma(x)=l(x) \bmod \gamma(x)$.
- Υπολογισμός του $\sigma_i \leftrightarrow \sigma_i(x)=x^i\sigma(x) \bmod \gamma(x)$, για κάθε $i \geq 0$, μέχρι να βρεθεί ένα σ_j του οποίου το βάρος είναι μικρότερο ή ίσο του t, δηλαδή $wt(\sigma_j)\leq t$. (Υπόμνηση: Αν $d=2t+1$ είναι η απόσταση του κώδικα, τότε $t=\left\lfloor \frac{d-1}{2} \right\rfloor$.) Τότε το πρότυπο σφάλματος είναι $\varepsilon \leftrightarrow \varepsilon(x)= x^{n-j}\sigma_j(x) \bmod (1+x^n)$.
- Υπολογισμός της κωδικής λέξης που μεταδόθηκε $c \leftrightarrow c(x)= l(x)+\varepsilon(x)$.

• ΑΛΓΟΡΙΘΜΟΙ BCH

Ο κώδικας BCH μήκους $n=2^r-1$ είναι ο κυκλικός κώδικας που δημιουργείται από το πολυώνυμο – γεννήτορα $\gamma(x)=m_\lambda(x)m_{\lambda^3}(x)$, όπου λ είναι πρωτογενές (*primitive*) στοιχείο στο $GF(2^r)$ και $r\geq 4$.

• ΑΛΓΟΡΙΘΜΟΙ BCH

Αλγόριθμος 6 - Διαδικασία αποκωδικοποίησης BCH κωδίκων

Η διαδικασία αποκωδικοποίησης, στην περίπτωση ΑΑΜΠ και κωδίκων διόρθωσης 2 σφαλμάτων με πολυώνυμο – γεννήτορα $\gamma(x) = m_{\lambda}(x) m_{\lambda^3}(x)$:

- Υπολογισμός του συνδρόμου $lH=[\sigma_1, \sigma_3]=[l(\lambda), l(\lambda^3)]$, όπου λ το πρωτογενές (*primitive*) στοιχείο, $\lambda \in GF(2^r)$, H ο πίνακας ελέγχου ισοτιμίας (Πρόταση 4.3) και l η ληφθείσα λέξη.
- Αν $\sigma_1=\sigma_3=0$, τότε η κωδική λέξη c που μεταδόθηκε είναι η ληφθείσα λέξη l, δηλαδή $c=l$.
- Αν $\sigma_1=0$ και $\sigma_3 \neq 0$, τότε ζητείται επανάληψη της μετάδοσης.
- Αν $\sigma_1^3=\sigma_3=0$, τότε διορθώνεται ένα απλό σφάλμα στη θέση i, όπου $\sigma_1=\lambda^i$.
- Σχηματισμός της εξίσωσης $x^2 + \sigma_1 x + \frac{\sigma_3}{\sigma_1} + \sigma_1^2 = 0$ και εξέταση των ριζών της. Αν η εξίσωση έχει δύο ξεχωριστές ρίζες λ^i και λ^j, τότε διορθώνονται τα λάθη στις θέσεις i και j.
- Αν η εξίσωση του σημείου 5 δεν έχει δύο ξεχωριστές λύσεις, τότε συμπεραίνεται ότι τα σφάλματα είναι περισσότερα των δύο και ζητείται επανάληψη της μετάδοσης.