Θεωρία Πληροφορίας
Επανάληψη

Σπύρος Δενάζης
sdena@ee.upatras.gr

© 2006, Σπύρος Δενάζης

Χρήσιμα Στοιχεία από Συνδυαστική

- Πολλαπλασιαστικός Κανόνας
- Διακεκριμένα – Μη Διακεκριμένα Στοιχεία
- Πλήθος Μεταθέσεων
- Πλήθος Διατάξεων
- Πλήθος Συνδυασμών
- Δειγματοληψίες Πληθυσμών
  - Επανάθεση – Χωρίς Επανάθεση – Διατεταγμένο – Μη Διατεταγμένο

©2006, Σπύρος Δενάζης

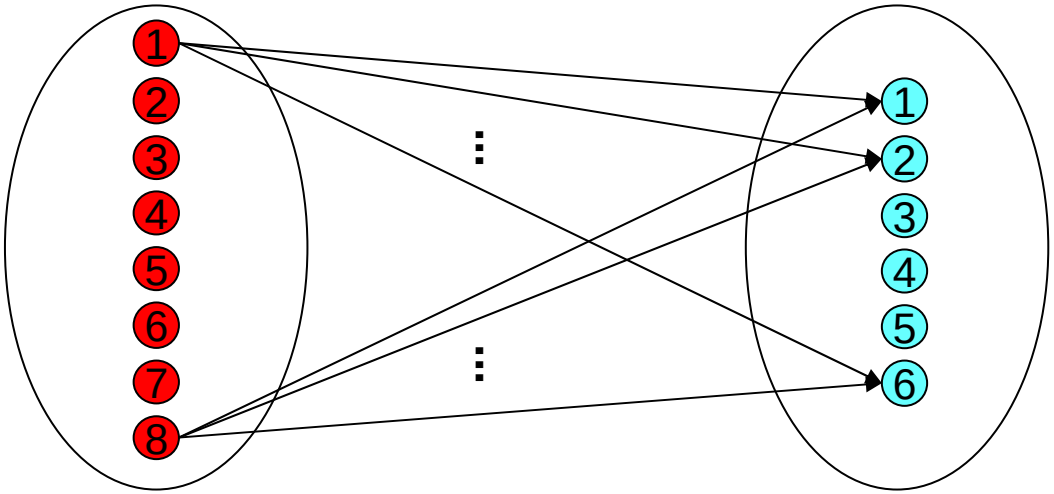
Βασικές Αρχές Συνδυαστικής …

- **<u>Θεώρημα 1.</u>** ***Πολλαπλασιαστικός Κανόνας (m*n)***
  - Έστω ένα σύνολο $A=\{\alpha_1,\alpha_2,...,\alpha_m\}$ με m στοιχεία και ένα άλλο σύνολο $B=\{b_1,b_2,\ldots,b_n\}$ με n στοιχεία. Τότε ο αριθμός όλων των δυνατόν ζευγών τύπου (α_i,b_j), i=1,…,m, j=1,…n, είναι **m*n**
  - Ή, αν μια διαδικασία μπορεί να αναλυθεί τμηματικά σε δύο διαδοχικά βήματα έτσι ώστε κατά τη διάρκεια του 1ου βήματος είναι δυνατόν να πάρουμε m πιθανά αποτελέσματα ενώ κατά τη διάρκεια του 2ου βήματος κάθε ένα από τα m αποτελέσματα είναι δυνατόν να δώσει n επιπλέον πιθανά αποτελέσματα τότε το πλήθος όλων των δυνατών αποτελεσμάτων και για τα δύο βήματα της διαδικασίας είναι **m*n**
- **<u>Θεώρημα 2.</u>** Γενίκευση πολλαπλασιαστικού κανόνα m*n για περισσότερα από δύο σύνολα
  - Έστω A_1, A_2, ... A_κ, σύνολα με το κάθε ένα με n_1, n_2,… n_k στοιχεία. Τότε ο αριθμός των κ-δων που μπορούν να δημιουργηθούν είναι $n_1*n_2*\ldots*n_k$
  - Η εναλλακτικά, για περισσότερα των δύο βημάτων

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής …

- **<u>Παράδειγμα 1</u>**
  - Ποιο είναι το πλήθος όλων των δυνατών ζευγών που μπορούμε να δημιουργήσουμε από 8 άνδρες και 6 γυναίκες;
  - 8*6=48



©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής …

- **<u>Παράδειγμα 2</u>**
  - Υποθέστε ότι θέλετε να φτιάξετε πινακίδες αυτοκινήτων οι οποίες αποτελούνται από 7 αλφαριθμητικούς χαρακτήρες εκ των οποίων οι πρώτοι 3 είναι γράμματα και οι υπόλοιποι 4 είναι ψηφία. Υπολογίστε, το σύνολο των πινακίδων που μπορείτε να διαθέσετε στις παρακάτω περιπτώσεις
  - Ο κάθε αριθμός του αυτοκινήτου δεν μπορεί να περιλαμβάνει δύο ίδια γράμματα ή αριθμούς
    - 24*23*22*10*9*8*7
  - Ο κάθε αριθμός του αυτοκινήτου είναι δυνατόν να περιλαμβάνει επαναλήψεις χαρακτήρων
    - $24*24*24*10*10*10*10 = 24^3*10^4$
  - Εάν επιτρέπεται η επανάληψη χαρακτήρων πόσες πινακίδες αποτελούνται από μόνο φωνήεντα και από ζυγά ψηφία;
    - 7*7*7*5*5*5*5

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

- **<u>Παράδειγμα 3</u>**
  - Υποθέστε ότι ένα κυλικείο προσφέρει 6 διαφορετικά είδη κρουασάν, 8 διαφορετικά είδη σάντουιτς, και 5 διαφορετικά είδη ροφημάτων (ζεστό εσπρέσσο, ζεστό τσάι, κρύο τσάι, κρύο εσπρέσσο και κρύα φρέσκια πορτοκαλάδα). Κάποιος αναλαμβάνει να εκτελέσει την παρακάτω παραγγελία, είτε ένα κρουασάν και ένα οποιοδήποτε ζεστό ρόφημα, είτε ένα σάντουιτς και ένα κρύο ρόφημα. Ποιοι είναι όλοι οι δυνατοί συνδυασμοί εκτέλεσης της παραγγελίας;
    - 6 είδη κρουασάν * 2 είδη ζεστών ροφημάτων
    - 8 είδη σάντουιτς * 3 είδη κρύων ροφημάτων
    - Συνολικά 6*2+8*3=36 διαφορετικοί τρόποι εκτέλεσης της παραγγελίας

©2006, Σπύρος Δενάζης

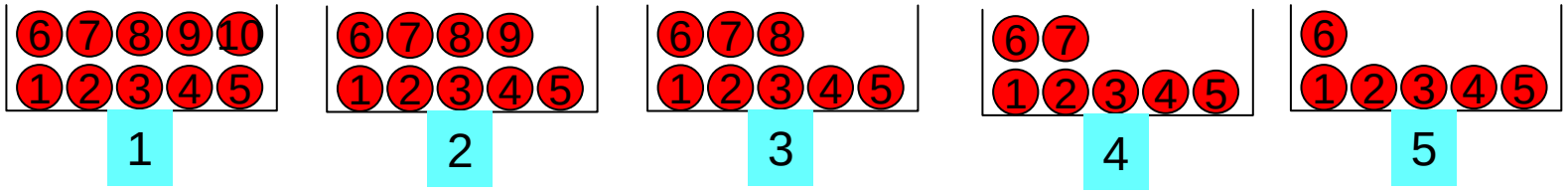
Βασικές Αρχές Συνδυαστικής ...

- **<u>Ορισμός 1</u>**: ***Μετάθεση*** **n** (διακεκριμένων) στοιχείων λέγεται κάθε τοποθέτησή τους σε <u>*σειρά*</u> πάνω σε ευθεία γραμμή.
- **<u>Ορισμός 2</u>**: ***Διάταξη*** **n** (διακεκριμένων) στοιχείων ανά r, $1 \le r \le n$, λέγεται κάθε τοποθέτηση r στοιχείων από τα n σε <u>*σειρά*</u> πάνω σε ευθεία γραμμή.
- Η μετάθεση **n** στοιχείων είναι ειδική περίπτωση της διάταξης στοιχείων
- Μας ενδιαφέρει η σειρά αβγ≠γβα
- Σε πολλά προβλήματα μας ενδιαφέρει ο αριθμός των διατάξεων που μπορούν να γίνουν από **n** στοιχεία.
- <u>Εφαρμογή των πολλαπλασιαστικών κανόνων οδηγεί στα παρακάτω θεωρήματα που υπολογίζουν τον αριθμό μεταθέσεων και διατάξεων</u>

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

- **<u>Παράδειγμα 4</u>**
  - Σε μία τάξη 10 φοιτητών θέλουμε να επιλέξουμε 5 και να τους τοποθετήσουμε σε μια διάταξη των 5. Ποιος είναι ο συνολικός αριθμός των διαφορετικών διατάξεων;
    - Εφαρμογή πολλαπλασιαστικού κανόνα



    - 10*9*8*7*6= 10*9*8*7*6* $\frac{5*4*3*2*1}{5*4*3*2*1}$ = 10!/5!

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής …

- **<u>Θεώρημα 3.</u>** (Πλήθος Μεταθέσεων)
  - Έστω P_n^n (ή $(n)_n$) το πλήθος (αριθμός) των μεταθέσεων **n** *<u>διακεκριμένων</u>* στοιχείων είναι: $P_n^n = n(n-1)\ldots 2*1 = n!$
- **<u>Θεώρημα 4.</u>** (Πλήθος Διατάξεων)
  - Έστω P_r^n (ή $(n)_r$) το πλήθος (αριθμός) των διατάξεων **n** *<u>διακεκριμένων</u>* στοιχείων ανά r. Τότε $P_r^n = n(n-1)\ldots(n-r+1) = n!/(n-r)!$

©2006, Σπύρος Δενάζης

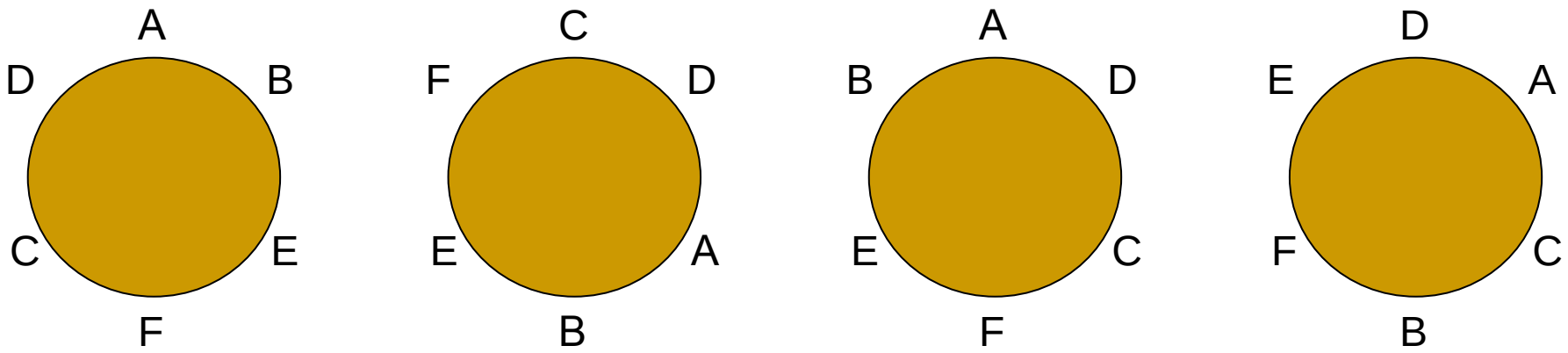
Βασικές Αρχές Συνδυαστικής …

- **<u>Θεώρημα 5.</u>** Διάταξη με μη διακεκριμένα στοιχεία
  - Έστω **n** *<u>μη διακεκριμένα</u>* στοιχεία από τα οποία r_1 είναι όμοια μεταξύ τους, r_2 είναι επίσης όμοια κ.ο.κ, όπου $r_1+r_2+\ldots+r_k=n$. Ο αριθμός των διατάξεων **n** μη διακεκριμένων στοιχείων δίνεται από τους τύπους των πολυωνυμικών συντελεστών. Οι μεταθέσεις αυτές λέγονται και *επαναληπτικές*
- *Πολυωνυμικοί Συντελεστές*
  - Έστω οι ακέραιοι και θετικοί αριθμοί $r_1,r_2,\ldots r_k$ με $r_1+r_2+\ldots+r_k=n$. Ο αριθμός των τρόπων με τους οποίους ένας πληθυσμός από **n** διακεκριμένα στοιχεία μπορεί να χωριστεί σε k μέρη, το πρώτο με r_1 στοιχεία, το δεύτερο με r_2 στοιχεία, κ.ο.κ είναι
  - $$C^n_{r_1,r_2,\ldots,r_k} = \frac{n!}{r_1!r_2!\ldots r_k!} = \binom{n}{r_1}\binom{n-r_1}{r_2}\ldots\binom{n-r_1-\ldots-r_{k-2}}{r_{k-1}}$$
  - **<u>Παράδειγμα 5</u>**: Βρείτε όλες τις δυνατές μεταθέσεις της λέξης ΜΑΘΗΜΑΤΙΚΑ $\frac{10!}{2!3!1!1!1!1!1!} = 151200$

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής …

- **<u>Παράδειγμα 6</u>**
  - Δίδεται ότι 6 άνθρωποι A,B,C,D,E,F κάθονται γύρω από μια στρογγυλή τράπεζα. Ποιος είναι ο αριθμός των διαφορετικών διατάξεων αν θεωρήσουμε ότι οι διατάξεις που προκύπτουν από περιστροφή των θέσεων είναι ίδιες;

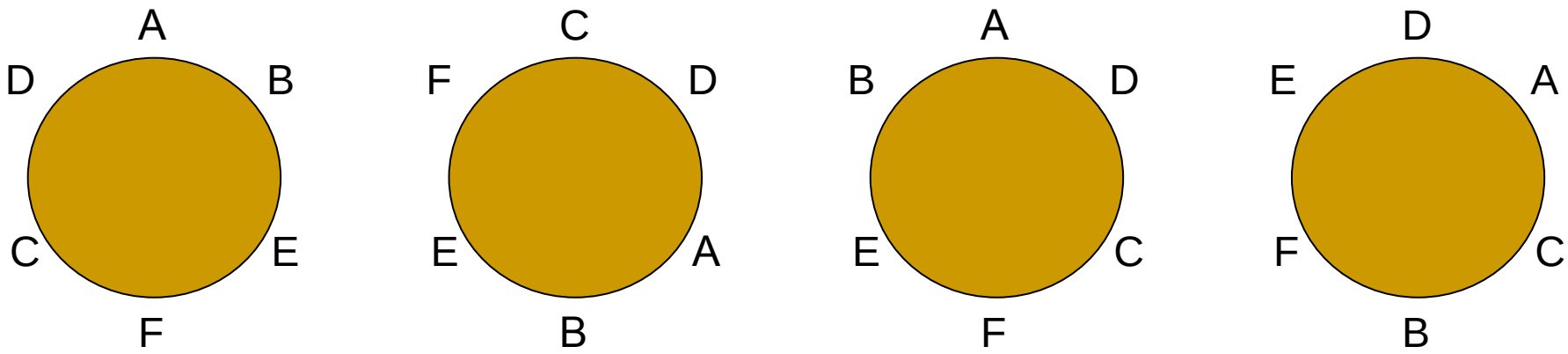


- **Λύση (<u>1ος Τρόπος</u>)**
  - Το πλήθος όλων των δυνατών μεταθέσεων είναι 6!, π.χ ABEFCD, CDABEF, ADCFEB, DACBFE
  - Κάθε μια από αυτές τις μεταθέσεις έχει 6 μεταθέσεις οι οποίες ανήκουν σε περιστροφή της μετάθεσης στον κύκλο
  - Άρα το πλήθος των διατάξεων είναι 6!/6=5!

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής …

- **<u>Παράδειγμα 6</u>**
  - Δίδεται ότι 6 άνθρωποι A,B,C,D,E,F κάθονται γύρω από μια στρογγυλή τράπεζα. Ποιος είναι ο αριθμός των διαφορετικών διατάξεων αν θεωρήσουμε ότι οι διατάξεις που προκύπτουν από περιστροφή των θέσεων είναι ίδιες;

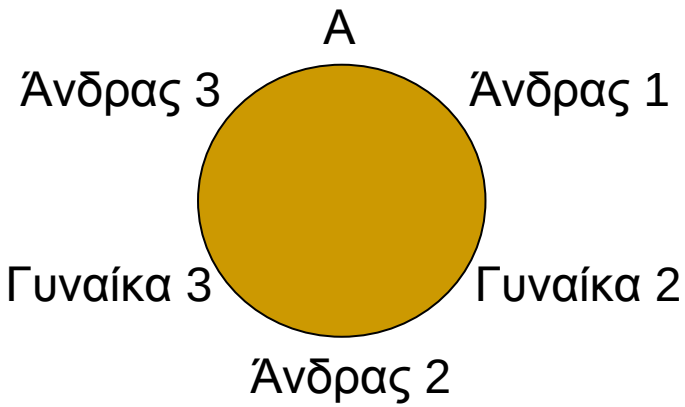


- **Λύση (<u>2ος Τρόπος</u>)**
  - Εάν επιλέξουμε έναν αντιπρόσωπο από τους έξη ανθρώπους π.χ τον A και τον βάλουμε σε μία από τις θέσεις τότε απομένουν 5 θέσεις να καταληφθούν από τους υπόλοιπους 5. Αυτό είναι δυνατόν να γίνει με 5! τρόπους

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής …

- **<u>Παράδειγμα 7</u>**
  - Αν οι 6 αυτοί άνθρωποι αποτελούν ζευγάρια με τα A,B,C να είναι γυναικείου φύλου και τα D,E,F ανδρικού φύλου με πόσους διαφορετικούς τρόπους μπορούν να τοποθετηθούν γύρω από μια στρογγυλή τράπεζα έτσι ώστε τα δύο φύλα να κάθονται εναλλάξ. Πάλι θεωρούμε ότι οι διατάξεις που προκύπτουν από περιστροφή των θέσεων είναι ίδιες;



- **Λύση (βάσει του 2ου Τρόπου του παραδείγματος 6)**
  - Εάν επιλέξουμε έναν αντιπρόσωπο από τους έξη ανθρώπους π.χ τον A που είναι γυναίκα τότε μένουν πέντε θέσεις όπως στο σχήμα να τοποθετηθούν οι υπόλοιποι με τη συγκεκριμένη διάταξη. Για τη θέση του Άνδρα 1 έχουμε 3 επιλογές για τη θέση της Γυναίκας 2 έχουμε 2 επιλογές, για τη θέση του Άνδρα 2 έχουμε 2 επιλογές αφού την μία θέση ήδη την καταλάβαμε και τέλος για τις θέσεις Γυναίκα 3 και Άνδρα 3 έχουμε από μία επιλογή.
  - Με βάση τον πολλαπλασιαστικό κανόνα έχουμε 3*2*2*1*1=12 διαφορετικές διατάξεις

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

- **<u>Ορισμός 3</u>**: Κάθε σύνολο r στοιχείων, 1≤r≤n, από **n** (διακεκριμένα) στοιχεία λέγεται ***συνδυασμός*** των n στοιχείων ανά r.
  - Δεν είναι διατεταγμένα δηλ. δεν μας ενδιαφέρει η σειρά, αβγ=γβα=βαγ=βγα
- **<u>Θεώρημα 6.</u>**
  - Έστω C_r^n (ή $\binom{n}{r}$) το πλήθος (αριθμός) των συνδυασμών **n** διακεκριμένων στοιχείων ανά r. Τότε με δεδομένο ότι από κάθε συνδυασμό μπορούμε να δημιουργήσουμε r! διατάξεις,

$$\binom{n}{r} = C_r^n = \frac{n!}{r!(n-r)!} = \frac{P_r^n}{r!}$$

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

- Οι συνδυασμοί μπορούν να χρησιμοποιηθούν για να βρούμε τους τρόπους με τους οποίους μπορούμε να χωρίσουμε ένα σύνολο **n** στοιχείων σε δύο ομάδες, η μία με r στοιχεία και η άλλη με n-r. Ο αριθμός αυτός είναι $\binom{n}{r}$

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

- **<u>Θεώρημα 7.</u>**
  - Για όλους τους φυσικούς αριθμούς n,r, n≥r ισχύει:

$$\binom{n}{r} = \binom{n}{n-r} \qquad \binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$$

  - Υπενθύμιση $\binom{n}{0} = \binom{n}{n} = 1$ και $\binom{n}{r} = 0,\ r < 0,$ ή $r > n$

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής …

- **<u>Παράδειγμα 8</u>**
  - Για να κερδίσει κάποιος στο Λόττο πρέπει να βρει 5 αριθμούς από το σύνολο το πιθανών πεντάδων που μπορεί να δημιουργηθούν από τους αριθμούς 1 έως 49. Επιπλέον θα πρέπει να βρει και ένα αριθμό (τον έκτο) από το 1 έως 42. Ποιο είναι το σύνολο όλων των δυνατών συνδυασμών;
  - Το σύνολο όλων των δυνατών συνδυασμών για τις πεντάδες αριθμών από το 1-49 είναι
  - $$\binom{49}{5}$$
  - Για κάθε ένα από αυτούς τους συνδυασμούς υπάρχουν επιπλέον 42 επιλογές για την έκτη θέση
  - Εφαρμόζοντας τον πολλαπλασιαστικό κανόνα έχουμε ότι το σύνολο των συνδυασμών είναι $\binom{49}{5} * 42$

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

- **<u>Παράδειγμα 9</u>**
  - Έστω ένα σύνολο με N διακεκριμένα στοιχεία από τα οποία Np είναι τύπου A και Nq είναι τύπου B, όπου 0≤p≤1, 0≤q≤1, και p+q=1. Να βρεθεί α) Ο αριθμός των συνδυασμών των N στοιχείων ανά **n** και β) Από αυτούς τους συνδυασμούς πόσοι περιέχουν ακριβώς x στοιχεία τύπου A;
- **<u>Λύση</u>**
  - α) $\binom{N}{n}$
  - β) Εφαρμόζοντας τον πολλαπλασιαστικό κανόνα

$$\binom{Np}{x}\binom{Nq}{n-x}$$

©2006, Σπύρος Δενάζης

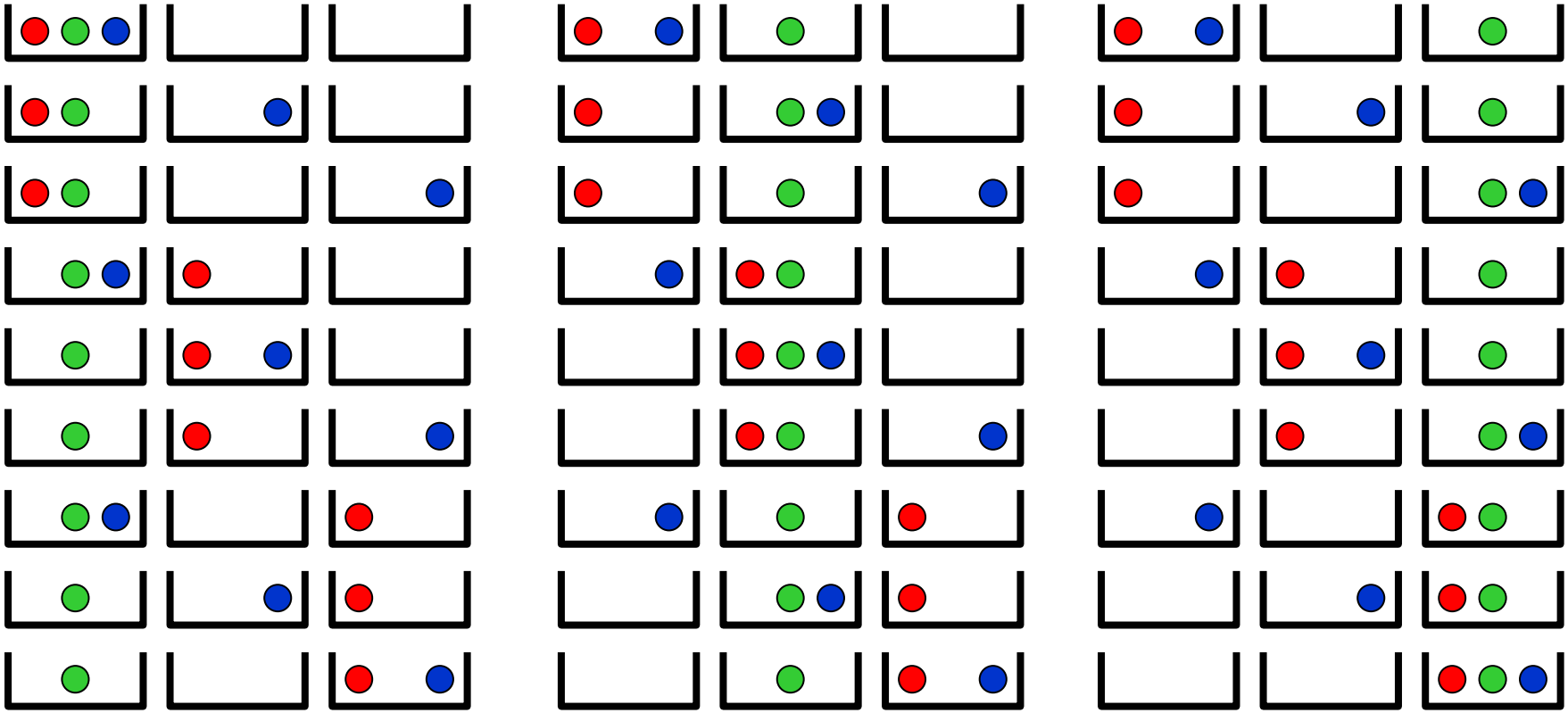
Βασικές Αρχές Συνδυαστικής ...

- **<u>Θεώρημα 8.</u>** Κυψέλες – Μπαλάκια (Διακεκριμένα)
  - Έστω **n** κυψέλες και r διακεκριμένα μπαλάκια τα οποία ρίχνονται στις κυψέλες. Τότε ο αριθμός των τρόπων με τους οποίους τα μπαλάκια μπορούν να τοποθετηθούν στις κυψέλες είναι $\mathbf{n^r}$.
  - Σημείωση: Κάθε κυψέλη μπορεί να φιλοξενήσει περισσότερα από ένα μπαλάκι

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

- Τρία διακεκριμένα μπαλάκια σε τρεις κυψέλες, $3^3=27$



- ΠΡΟΠΟ, 13 ομάδες, 3 σημεία, $3^{13}=1.500.000$

©2006, Σπύρος Δενάζης

Βασικές Αρχές Συνδυαστικής ...

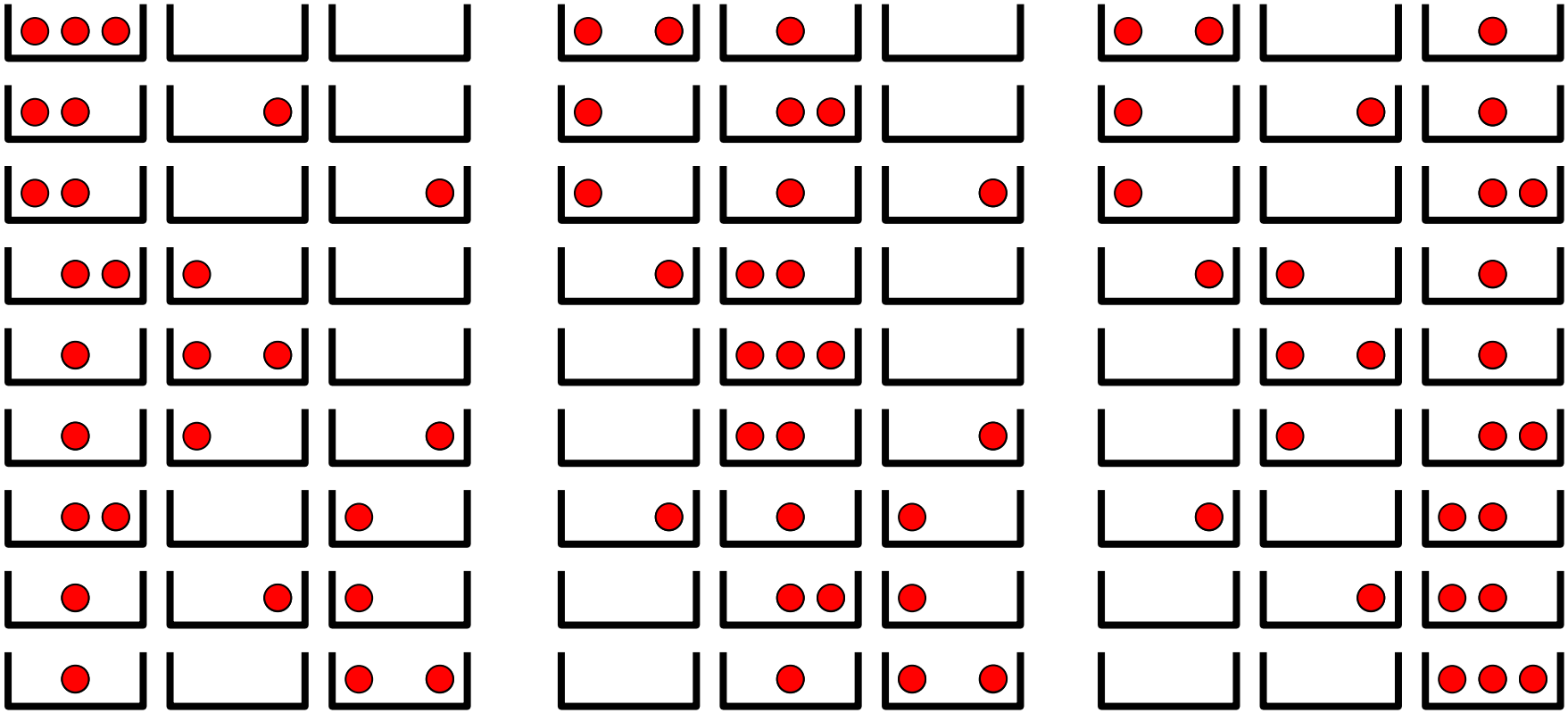
- **<u>Θεώρημα 8.</u>** Κυψέλες – Μπαλάκια (Μη Διακεκριμένα)
  - Έστω **n** κυψέλες και r <u>μη</u> διακεκριμένα (δηλ. ίδια) μπαλάκια τα οποία ρίχνονται στις κυψέλες. Τότε ο αριθμός των τρόπων με τους οποίους τα r μπαλάκια μπορούν να τοποθετηθούν στις κυψέλες είναι:

$$\binom{n+r-1}{r} = \binom{n+r-1}{n-1}$$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Συνδυαστική)...

- Τρία μη διακεκριμένα μπαλάκια σε τρεις κυψέλες, 10 τρόποι



©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Συνδυαστική)...

- **Δειγματολειψίες από πεπερασμένους πληθυσμούς**
  - Ν το μέγεθος του πληθυσμού και **n** το μέγεθος του δείγματος
  - Κατά τη δειγματολειψία τα μέλη του δείγματος εκλέγονται διαδοχικά το ένα κατόπιν του άλλου
  - Σε κάθε επιλεγόμενο μέλος μετρούμε τις τιμές μίας ή περισσοτέρων μεταβλητών
- Τρόποι επιλογών
  - *Δείγμα χωρίς επανάθεση – μη διατεταγμένο*
    - αριθμός δειγμάτων: $\binom{N}{n}$
  - *Δείγμα χωρίς επανάθεση – διατεταγμένο*
    - αριθμός δειγμάτων: $P_n^N = \frac{N!}{(N-n)!}$
  - *Δείγμα με επανάθεση –διατεταγμένο*
    - αριθμός δειγμάτων: N^n,
    - Τα μέλη Ν του πληθυσμού είναι οι κυψέλες και **n** το μέγεθος του δείγματος
  - *Δείγμα με επανάθεση – μη διατεταγμένο*
    - αριθμός δειγμάτων: $\binom{N+n-1}{n} = \binom{N+n-1}{N-1}$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Συνδυαστική)

- **Άσκηση**
  - Τα γράμματα το κώδικα Morse σχηματίζονται με τελείες και παύλες (επαναλήψεις επιτρέπονται). Πόσα διαφορετικά γράμματα μπορούμε να σχηματίσουμε αν κάθε γράμμα γίνεται με τέσσερα **<u>το πολύ</u>** σύμβολα.
  - Δείγμα με επανάθεση διατεταγμένο, N^n
  - $n=1,2,3,4$, $N=2$, $2^1+2^2+2^3+2^4=30$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Συνδυαστική)

- **Άσκηση**
  - α) Έστω ένα σύνολο το οποίο αποτελείται από N διακεκριμένα στοιχεία. Να βρεθεί το πλήθος των διατεταγμένων n-άδων οι οποίες δημιουργούνται με επανάθεση
  - β) Αν υποθέσουμε ότι από αυτά τα N διακεκριμένα στοιχεία τα N_1 είναι τύπου 1 και τα N_2 είναι τύπου 2, με $N_1+N_2=N$, να βρεθεί το πλήθος των διατεταγμένων n-άδων οι οποίες δημιουργούνται με επανάθεση και οι οποίες περιέχουν ακριβώς κ στοιχεία τύπου N_1.
  - ***<u>Απάντηση</u>***
    - α) N^n
    - β) $\binom{n}{k} N_1^k * N_2^{n-k}$
    - Εφόσον k είναι τύπου 1 υπάρχουν N_1^k τρόποι διάταξης με επανάθεση και άρα τα n-k διατάσσονται με N_2^{n-k} τρόπους. Με βάση τον πολλαπλασιαστικό κανόνα κάθε μία από τις N_1^k διατάξεις μπορεί δημιουργήσει ένα συνδυασμό με κάθε μία από τις N_2^{n-k} διατάξεις η οποία θα αποτελείται από n στοιχεία εκ των οποίων τα k θα είναι τύπου 1 και τα n-k θα είναι τύπου 2 εκ κατασκευής. Κάθε ένας τέτοιος συνδυασμός από n στοιχεία μπορεί να δημιουργήσει $\binom{n}{k}$ διαφορετικούς συνδυασμούς. Άρα το συνολικό πλήθος των διατεταγμένων n-άδων οι οποίες περιέχουν ακριβώς k στοιχεία τύπου 1 είναι $\binom{n}{k} N_1^k * N_2^{n-k}$
    - Παρατηρείστε ότι $\sum_{k=0}^{n} \binom{n}{k} N_1^k \cdot N_2^{n-k} = (N_1 + N_2)^n = N^n$

©2006, Σπύρος Δενάζης

Χρήσιμα Στοιχεία από Πιθανότητες

- Βασικές Έννοιες Πιθανοτήτων
  - Τυχαίες Μεταβλητές
    - Διακριτές, Συνεχείς
  - Πιθανότητες Τυχαίων Μεταβλητών
    - Συνάρτηση Πιθανότητας, Αθροιστικές, Συνάρτηση Πυκνότητας Πιθανότητας
  - Είδη Πιθανοτήτων Πολυδιάστατων Τυχαίων Μεταβλητών
    - Συνδυασμένες πιθανότητες
    - Περιθωριακές
    - Δεσμευμένες ή Υπό συνθήκη
  - Ιδιότητες
  - Κανόνας του Bayes
    - Εκ των προτέρων
    - Εκ των υστέρων

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων ...

- Ενδεχόμενο
  - Το αποτέλεσμα ενός πειράματος
- Στοιχειώδες Ενδεχόμενο ή Δειγματικό Σημείο
  - Το ατομικό αδιαίρετο αποτέλεσμα
- Δειγματικός Χώρος, S
  - Το σύνολο όλων των *στοιχειωδών ενδεχομένων* ενός πειράματος λέγεται δειγματικός χώρος
- Τα ενδεχόμενα χωρίζονται σε,
  - Απλά: Το δειγματικό σημείο
  - Σύνθετο: Κάθε υποσύνολο του S
- Ο δειγματικός χώρος μπορεί να είναι πεπερασμένος, αριθμήσιμος ή μή αριθμήσιμος (συνεχής)
- Οι έννοιες του δειγματικού χώρου ταυτίζονται με αυτές των συνόλων και υποσυνόλων

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων ...

- Τυχαία μεταβλητή X, είναι μία μονοσήμαντη συνάρτηση με πεδίο ορισμού το δειγματόχωρο S και πεδίο τιμών ένα υποσύνολο πραγματικών αριθμών
  - $S=(s_1,s_2, \ldots, s_n) \rightarrow (x_1,x_2, \ldots,x_n)$
- X λέμε ότι είναι διακριτή αν το πεδίο τιμών της είναι πεπερασμένο ή απείρως αριθμήσιμο (S πεπερασμένο και αριθμήσιμο)
- X λέμε ότι είναι συνεχής αν το πεδίο τιμών της είναι συνεχές (S συνεχής)
- Κάθε ενδεχόμενο s_i μπορεί να συμβεί με πιθανότητα $P(S=s_i)=P(X=x_i)=p_i$.
- Η $P(X=x_i)=p_i$ λέγεται συνάρτηση πιθανότητας μάζας και το σύνολο των πιθανοτήτων αυτών είναι $P=\{p_1,p_2,\ldots,p_n\}$
- Η συνάρτηση πιθανότητας μάζας πληροί τα ακόλουθα αξιώματα
  - $p(x_i)\geq 0$, για κάθε i
  - $\sum_{i=1}^{n} p(x_i) = 1, \quad P(S) = 1$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων ...

- Συνάρτηση κατανομής, F, αθροιστικής πιθανότητας διακριτής τυχαίας μεταβλητής
  - $$F(X \le x) = \sum_{x_i \le x} p(x_i), \quad \forall x \in (-\infty, \infty)$$
- Συνάρτηση κατανομής μιας συνεχούς τυχαίας μεταβλητής
  - $$F(X \le x) = P\left[X \in (-\infty, x)\right] = \int_{-\infty}^{x} f(y)dy$$
- Η μή αρνητική συνάρτηση f(x) καλείται συνάρτηση πυκνότητας πιθανότητας και ισχύουν τα εξής
  - $$\int_B f(x)dx = P(X \in B), \quad \int_{-\infty}^{\infty} f(x)dx = 1$$
- Ιδιότητες της συνάρτησης κατανομής
  - $0 \le F(X \le x) \le 1$, για κάθε x
  - $F(X \le x_i) \le F(X \le x_j)$ αν $x_i \le x_j$, είναι δηλ. μη φθίνουσα
  - $$\lim_{x \to \infty} F(x) = 1, \quad \lim_{x \to -\infty} F(x) = 0$$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων ...

- Πολυδιάστατες Τυχαίες Μεταβλητές
  - Η έννοια της πολυδιάστατης τ.μ. αποτελεί γενίκευση της μονοδιάστατης τ.μ.
  - Είναι μία απεικόνιση του δειγματικού χώρου S στον Ευκλείδιο χώρο R^n και συμβολίζεται $(X_1, X_2,\ldots, X_n)$
  - Διακρίνονται επίσης σε διακριτές και συνεχείς
  - Οι τ.μ. $X_1, X_2, \ldots, X_n$, είναι οι συνιστώσες της πολυδιάστατης τ.μ. και λέγονται και *περιθωριακές* ή *ακραίες* τ.μ.
- Πολυδιάστατες Κατανομές
  - Η κατανομή της πολυδιάστατης τ.μ. εκφράζει τον τρόπο με τον οποίο η μοναδιαία μάζα πιθανότητας κατανέμεται στο χώρο R^n.
  - Η από κοινού ή συνδυασμένη συνάρτηση πιθανότητας είναι
    - Διακριτή: $P_{X1,X2,\ldots Xn}(x_1,x_2,\ldots,x_n)=P(X_1=x_1,X_2=x_2,\ldots,X_n=x_n)$
    - Συνεχής: $f_{X1,X2,\ldots Xn}(x_1,x_2,\ldots,x_n)$ (συνάρτηση πυκνότητας πιθανότητας)
  - Συνδυασμένη αθροιστική συνάρτηση κατανομής
    - $F_{X1,X2,\ldots Xn}(x_1,x_2,\ldots,x_n)=P(X_1\leq x_1,X_2 \leq x_2,\ldots,X_n \leq x_n)$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων ...

- Έστω δύο τ.μ. X,Y, με δειγματόχωρους $X=(x_1,x_2,\ldots,x_n)$ και $Y=(y_1,y_2,\ldots,y_m)$
- Η συνδυασμένη τ.μ. (X,Y) ή XY παίρνει τιμές από τα διατεταγμένα ζεύγη (x,y)
- Η συνδυασμένη συνάρτηση πιθανότητας της (X,Y)
  - $P(X=x_i,Y=y_j)=p_{ij}$
- Περιθωριακή ή ακραία συνάρτηση πιθανότητας
  - $p(x_i)=\sum_{j=1}^{m} p(x_i,y_j)=\sum_{j=1}^{m} p_{ij}, \quad p(y_j)=\sum_{i=1}^{n} p(x_i,y_j)=\sum_{i=1}^{n} p_{ij}$
- Δεσμευμένη ή Υπό συνθήκη πιθανότητα
  - $p(x_i/y_j)=\dfrac{p(x_i,y_j)}{p(y_j)}$ αν $p(y_j)\neq 0$, αν $p(y_j)=0$ δεν ορίζεται

©2006, Σπύρος Δενάζης

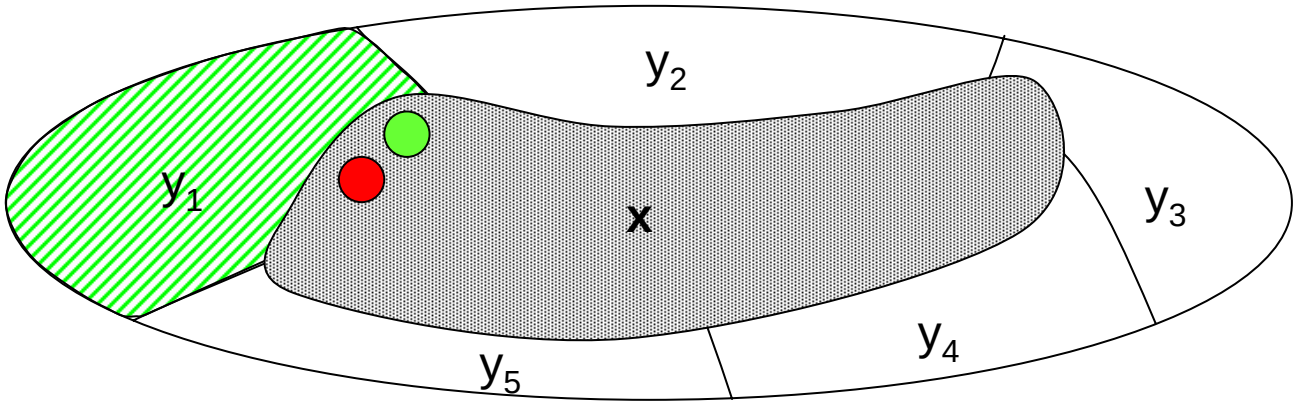
... Στοιχεία Πιθανοτήτων (Ιδιότητες)...

- **Κανόνας Γινομένου**
  - $p(x,y)=p(x/y)p(y)=p(y/x)p(x)$
  - $p(x/y)=p(x,y) / p(y)$, & $p(y/x)=p(x,y) / p(x)$
- **Αθροιστικός Κανόνας ή Θεώρημα Ολικής Πιθανότητας**
  - $p(x)= \sum p(x,y)=\sum p(x/y)p(y), \forall y \in Y$
- **Ανεξαρτησία Τυχαίων Μεταβλητών**
  - $p(x,y)=p(x)p(y)$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Bayes)...

- Θεώρημα Bayes
  - $$p(x/y) = \frac{p(x,y)}{p(y)} = \frac{p(y/x)p(x)}{p(y)} = \frac{p(y/x)p(x)}{\sum_{x'} p(y/x')p(x')}$$
  - $$\boxed{p(y/x) = \frac{p(x,y)}{p(x)} = \frac{p(x/y)p(y)}{p(x)} = \frac{p(x/y)p(y)}{\sum_{y'} p(x/y')p(y')}}$$



©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Bayes)...

- **Άσκηση**
  - Έστω δύο δοχεία Δ_1 και Δ_2. Το Δ_1 περιέχει 2 άσπρες μπάλες και 8 κόκκινες μπάλες. Το Δ_2 περιέχει 6 άσπρες μπάλες και 4 κόκκινες μπάλες. Επιλέγουμε τυχαία ένα από τα δύο δοχεία και κατόπιν επιλέγουμε μία μπάλα από το επιλεγμένο δοχείο. Έστω ότι η μπάλα που επιλέχθηκε είναι άσπρη. Να βρέθει η πιθανότητα να έχει επιλεγεί το δοχείο Δ_1. Ομοίως για το Δ_2.
- **Λύση**
  - Το γεγονός το οποίο θεωρούμε ότι δεν είμαστε σε θέση να παρατηρήσουμε είναι η επιλογή του δοχείου.
  - Γνωρίζουμε όμως και τον τρόπο αλλά και τις πιθανότητες να επιλέξουμε ένα δοχείο, δηλ. $P(\Delta_1)=P(\Delta_2)=1/2$
  - Ζητείται ο υπολογισμός της πιθανότητας P(Δ1/Μπάλα είναι άσπρη)
  - Τέλος γνωρίζουμε και τις δεσμευμένες πιθανότητες $P(A/\Delta_1)=2/10$, $P(K/\Delta_1)=$ [illegible] $P(K/\Delta_2)=4/10$.
  - Εφαρμό[illegible]υ Bayes για τ[illegible]

Εκ των υστέρων πιθανότητα

Εκ των προτέρων πιθανότητα

$$P(\Delta_1 / A) = \frac{P(\Delta_1, A)}{P(A)} = \frac{P(A/\Delta_1)P(\Delta_1)}{P(A/\Delta_1)P(\Delta_1) + P(A/\Delta_2)P(\Delta_2)} = \frac{2/10 * 1/2}{2/10 * 1/2 + 6/10 * 1/2} = 1/4$$

$$P(\Delta_2 / A) = \frac{P(A/\Delta_2)P(\Delta_2)}{P(A/\Delta_1)P(\Delta_1) + P(A/\Delta_2)P(\Delta_2)} = 3/4$$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Bayes)...

- Άσκηση
  - Ένα τεστ καρκίνου έχει αποδειχθεί ότι έχει πιστότητα 95%. Ένας άνδρας υποβάλλεται σε αυτό το τεστ ανίχνευσης καρκίνου. Με βάση την ηλικία του και το ιστορικό έχει βρεθεί ότι μόλις το 1% εμφανίζει καρκίνο. Αν το αποτέλεσμα του τεστ είναι θετικό να βρεθεί ποιά είναι η πιθανότητα ο άνδρας να έχει πραγματικά καρκίνο;
- Λύση
  - Έστω τα γεγονότα, α=1 έχει καρκίνο και α=0 δεν έχει
  - Η εκ των προτέρων πιθανότητες είναι P(α=0)=0.99 και P(α=1)=0.01
  - Έστω β=1 το τέστ είναι θετικό και β=0 το τεστ είναι αρνητικό
  - Η εκ των υστέρων πιθανότητα είναι P(α=1/β=1).
  - $$P(\alpha=1/\beta=1)=\frac{P(a=1,\beta=1)}{P(\beta=1)}$$

    $$=\frac{P(\beta=1/\alpha=1)P(\alpha=1)}{P(\beta=1/\alpha=1)P(\alpha=1)+P(\beta=1/\alpha=0)P(\alpha=0)}$$

    $$=\frac{0.95\times0.01}{0.95\times0.01+0.05\times0.99}=0.16!!!$$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Bayes)...

- **Άσκηση**
  - Ένα δοχείο περιέχει K μπάλες από τις οποίες B είναι μαύρες και K-B είναι άσπρες. Επιλέγουμε μία μπάλα τυχαία από το δοχείο. Εκτελούμε το πείραμα διαδοχικά N φορές. Να βρεθεί η πιθανότητα μάζας του αριθμού των μαύρων μπαλών, n_B.
- **Απάντηση**
  - Η Διωνυμική κατανομή με f_B=K/B
  - $$P(n_B) = \binom{N}{n_B} f_B^{n_B} (1 - f_B)^{N - n_B}, \quad n_B = 0,1,\ldots,N$$

©2006, Σπύρος Δενάζης

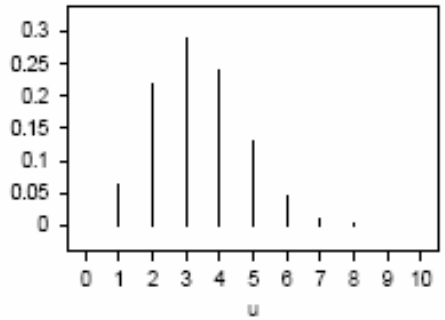
... Στοιχεία Πιθανοτήτων (Bayes)...

- **Άσκηση**
  - Έστω ότι υπάρχουν 11 δοχεία τα οποία αριθμούνται από το σύνολο $u \in \{0,1,2,...,10\}$ και το καθένα περιέχει 10 μπάλες. Το δοχείο u περιέχει u μαύρες μπάλες και 10-u άσπρες μπάλες. Επιλέγουμε τυχαία ένα δοχείο u, και από το επιλεγμένο δοχείο επιλέγουμε N φορές μία μπάλα επανατοποθετώντας την μπάλα πίσω στο επιλεγμένο δοχείο. Εάν μετά από N=10 επιλογές, n_B=3 μαύρες μπάλες έχουν επιλεγεί ποιά είναι η πιθανότητα οι μπάλες αυτές να προέρχονται από το δοχείο u;
- **Απάντηση**
  - Οι εκ των προτέρων πιθανότητες είναι: $P(u)$, $P(n_B/u)$
  - Οι εκ των υστέρων πιθανότητα είναι: $P(u/n_B)$
  - Η πιθανότητα να επιλέξουμε μία μαύρη μπάλα από το δοχείο u ειναι $f_u=u/10$

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Bayes)...

- Συνέχεια λύσης
  - $$P(u/n_B) = \frac{P(u,n_B)}{P(n_B)}$$
    $$= \frac{P(n_B/u)P(u)}{P(n_B)}$$
    $$= \frac{1}{P(n_B)}\frac{1}{11}\binom{N}{n_B} f_u^{n_B}(1-f_u)^{N-n_B}$$
    $$P(n_B) = \sum_{i=0}^{10} P(n_B/u_i)P(u_i)$$
    $$= 0.083 \quad (n_B = 3 \wedge N = 10)$$



u	$P(u \mid n_B = 3, N)$
0	0
1	0.063
2	0.22
3	0.29
4	0.24
5	0.13
6	0.047
7	0.0099
8	0.00086
9	0.0000096
10	0

©2006, Σπύρος Δενάζης

... Στοιχεία Πιθανοτήτων (Bayes).

- Παρατηρήσεις
  - Η εκ των υστέρων πιθανότητα να είχαμε επιλέξει το δοχείο u=0 είναι 0
    - Δεν υπάρχουν μαύρες μπάλες
  - Η εκ των υστέρων πιθανότητα να είχαμε επιλέξει το δοχείο u=10 είναι 0
    - Δεν υπάρχουν άσπρες μπάλες
- Η εκ των προτέρων πιθανότητες αντιστοιχούν στα συμπεράσματα που βγάζει ένας παρατηρητής που παρακολουθεί μία διαδικασία εκτός ενώ οι εκ των υστέρων πιθανότητες αντιστοιχούν σε ένα παρατηρητή που είναι εντός συστήματος, όπως συνήθως συμβαίνει και τις περισσότερες φορές.
- Ποια είναι η πιθανότητα ένας παρατηρητής που είναι μέσα στο σύστημα της άσκησης να λάβει μια μαύρη μπάλα στην N+1 επιλογή;
  - P(N+1 επιλογή να είναι πάλι μαύρη μπάλα / n_B=3 και N=10)
  - $P(E_{N+1}=\text{Μαύρη}/n_b,N)=\sum P(E_{N+1}=\text{Μαύρη}/u,n_b,N).P(u/n_b,N)$, για όλα τα δοχεία u
  - $P(E_{N+1}=\text{Μαύρη}/u,n_b,N)= f_u=u/10$
  - $P(E_{N+1}=\text{Μαύρη}/n_b,N)= \sum f_u.P(u/n_b,N)=0.333$,

©2006, Σπύρος Δενάζης

Χρήσιμα Στοιχεία από το Μέτρο Ποσότητας Πληροφορίας

- Πληροφορία
- Εντροπία – Μέση Ποσότητα πληροφορία
- Ιδιότητες Εντροπίας
  - Συνεχής
  - Συμμετρική
  - Μέγιστο Εντροπίας
  - Αθροιστικότητα
- Μέτρο πληροφορίας τυχαίων μεταβλητών
  - Συνδυασμένη
  - Δεσμευμένη ή Υπό συνθήκη
  - Περιθωριακή
- Αμοιβαία Πληροφορία
- Σχετική Εντροπία
- Ανισότητα Jensen και οι χρήσεις της
- Εντροπία
  - Πηγών Συμβόλων
  - Πηγών Μηνυμάτων

©2006, Σπύρος Δενάζης

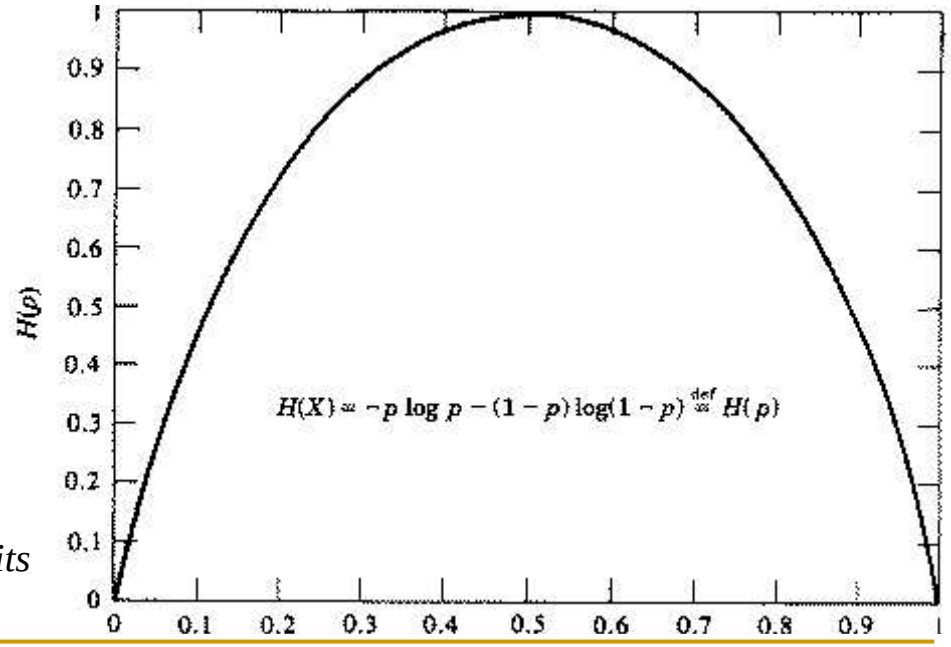
... Εντροπία ...

- Αν X είναι μία διακριτή τυχαία μεταβλητή με δειγματόχωρο $X=\{x_1,x_2,\ldots,x_n\}$ και συνάρτηση πιθανότητας μάζας $p(x_i)$,τότε η μέση ποσότητα πληροφορίας της X, H(X), δίνεται από τη σχέση
- $$\boxed{H(X) = -\sum_{i=1}^{n} p(x_i)\log p(x_i)}$$
- Η Μέση Πληροφορία ονομάζεται και **εντροπία** και εναλλακτικά συμβολίζεται με H(p)
- Η εντροπία δεν εξαρτάται από τις τιμές της τ.μ X αλλά από την κατανομή της, δηλ. τις τιμές που πέρνει η πιθανότητα μάζας, και μετριέται σε bits.
- Με δεδομένο ότι η μέση τιμή της συνάρτησης μιας τυχαίας μεταβλητής είναι $E[g(X)]=\sum g(x)p(x)$, τότε
  - $H(X)= E[\log(1/p(x)]$
- **<u>Λήμμα 1</u>**: $H(X)\geq 0$
- **<u>Λήμμα 2</u>**: $H_b(X)=(\log_b a)H_a(X)$
  - Υπενθυμίζεται ότι $\log_b x=\log_b a*\log_a x$

©2006, Σπύρος Δενάζης

… Εντροπία …

- **Παράδειγμα 1**
  - Έστω X μία τυχαία μεταβλητή με δύο ενδεχόμενα p και (1-p).
  - H(p)=-p*log(p)-(1-p)*log(1-p)
  - Η μέγιστη τιμή της εντροπίας είναι όταν τα δύο ενδεχόμενα είναι ισοπίθανα



- **Παράδειγμα 2**

$$X = \begin{cases} a & \text{με πιθανότητα } 1/2 \\ b & \text{με πιθανότητα } 1/4 \\ c & \text{με πιθανότητα } 1/8 \\ d & \text{με πιθανότητα } 1/8 \end{cases}$$

$$\mathrm{H(X)} = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} = \frac{7}{4} bits$$

©2006, Σπύρος Δενάζης

… Εντροπία …

- **Συνδυασμένη ή από κοινού εντροπία**
  - Η Συνδυασμένη ή από κοινού εντροπία H(X,Y) ενός ζεύγους δύο διακριτών τυχαίων μεταβλητών με πιθανότητα μάζας p(x,y) ορίζεται ως
  - $$\boxed{\mathrm{H}(\mathrm{X},\mathrm{Y}) = -\sum_x \sum_y p(x,y) \log\, p(x,y)}$$
  - H[X,Y]=-E[log p(x,y)]

©2006, Σπύρος Δενάζης

… Εντροπία …

- **Δεσμευμένη ή υπό συνθήκη εντροπία**
  - $H(x_i/y_j)=-p(x_i/y_j)\log p(x_i/y_j)$
  - $$\mathrm{H}(\mathrm{X}/Y=y)=-\sum_x p(x/y)\log p(x/y)$$
  - $$\mathrm{H}(\mathrm{X}/\mathrm{Y})=-\sum_y p(y)\sum_x p(x/y)\log p(x/y)$$
    $$=-\sum_y p(y)H\left(X/Y=y\right)=-\sum_x\sum_y p(x,y)\log p(x/y)$$
  - $$\boxed{\mathrm{H}(\mathrm{X}/\mathrm{Y})=-\sum_x\sum_y p(x,y)\log p(x/y)}$$
  - $$\boxed{\mathrm{H}(Y/X)=-\sum_x\sum_y p(x,y)\log p(y/x)}$$

©2006, Σπύρος Δενάζης

… Εντροπία …

- **<u>Θεώρημα 1</u>: Αθροιστικός Κανόνας**
  - $H(X,Y)=H(X)+H(Y/X)$
- Το θεώρημα αυτό μας λέει ότι η εντροπία της συνδυασμένης τυχαίας μεταβλητής (X,Y) ισούται με την εντροπία της μίας από αυτές, X, συν την εξαρτημένη εντροπία της άλλης τ.μ., Y, όταν έχει συμβεί η X.
- Ισχύει επίσης,
  - $H(X,Y)=H(Y)+H(X/Y)$
  - $H(X)-H(X/Y)=H(Y)-H(Y/X)$
- Προσοχή!
  - $H(X/Y)\neq H(Y/X)$
- Εάν X,Y είναι ανεξάρτητες τ.μ τότε $H(X,Y)=H(X)+H(Y)$
- **<u>Πρόταση</u>**: $H(X,Y/Z)=H(X/Z)+H(Y/X,Z)$

©2006, Σπύρος Δενάζης

… Εντροπία.

- **<u>Παράδειγμα 1</u>**: Έστω (X,Y) έχουν την παρακάτω πιθανότητα μάζας

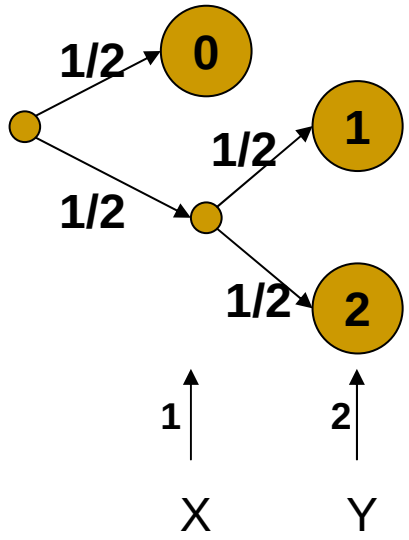
Y \ X	1	2	3	4		P(y)
1	1/8	1/16	1/32	1/32	→	1/4
2	1/16	1/8	1/32	1/32	→	1/4
3	1/16	1/16	1/16	1/16	→	1/4
4	1/4	0	0	0	→	1/4
P(x)	1/2	1/4	1/8	1/8		

- p(x/y)=p(x,y)/p(y)
- H(X)=7/4 bits και H(Y)=2 bits
- H(X/Y)=11/8 bits και H(Y/X)=13/8 bits
- H(X,Y)=27/8 bits

©2006, Σπύρος Δενάζης

Αθροιστική Ιδιότητα Εντροπίας ...

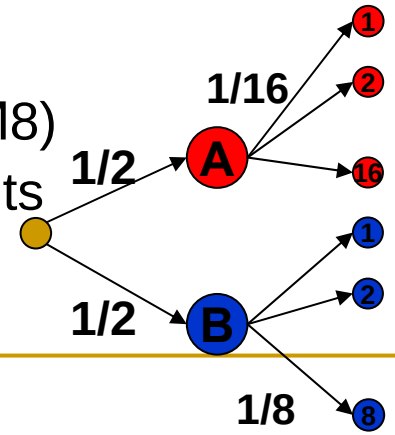
- **<u>Παράδειγμα 2</u>:** Ας υποθέσουμε ότι η τ.μ Z = {0,1,2} ως εξής (βλ. σχήμα)
  - Τότε p(0)=1/2, p(1)=1/4, p(2)=1/4
  - Ποια είναι η εντροπία της X;
    - H(Z)=- [p(0)log p(0)+ p(1)log p(1)+ p(2)log p(2)] = 1/2*log2+ 1/4*log4+ 1/4*log4 =3/2 bits
- Υπάρχει και 2ος τρόπος υπολογισμού της πληροφορίας ιδιαίτερα όταν αυτή μας αποκαλύπτεται σταδιακά;
  - Στο παράδειγμά μας μαθαίνουμε πρώτα εάν Z=0. Εάν όχι τότε μαθαίνουμε ποια από τις δύο τιμές λαμβάνουμε.
  - Η Πληροφορία ότι {Z=0 ή όχι 0} ισοδυναμεί με 1 bit αφού H(1/2,1/2)
  - Εάν η Z δεν είναι μηδέν στο πρώτο βήμα τότε λαμβάνουμε νέα πληροφορία στο δεύτερο βήμα μας η οποία και αυτή είναι 1 bit. Η μόνη διαφορά τώρα είναι ότι η πληροφορία αυτή λαμβάνεται μόνο κατά το ήμισυ των προσπαθειών, δηλ. με πιθανότητα ½.
    - H(Z)=H(1/2,1/2)+1/2*H(1/2,1/2)=1+1/2=3/2 bits
- Μια άλλη εξήγηση του 2ου τρόπου. Εάν θεωρήσουμε το αποτέλεσμα του 1ου βήματος ως μία μεταβλητή X={0,1} και το αποτέλεσμα του 2ου βήματος ως μια άλλη μεταβλητή Y ={0,1} τότε,
  - H(Z)=H(X,Y)=H(X) + H(Y/X) =1+1/2*H(Y/X=0)+1/2*H(Y/X=1)=1+0+1/2*H(1/2,1/2)



©2006, Σπύρος Δενάζης

Αθροιστική Ιδιότητα Εντροπίας ...

- **<u>Άσκηση</u>**
  - Έστω δύο δοχεία Α, Β. Το Α περιέχει 16 κόκκινες αριθμημένες μπάλες από το 1-16 και το Β περιέχει 8 μπλε αριθμημένες μπάλες από το 1-8. Έστω Χ η τυχαία μεταβλητή η οποία συμβολίζει το χρώμα και τον αριθμό της μπάλας που επιλέγεται αφού προηγηθεί η επιλογή κάποιου εκ των δύο δοχείων. Η επιλογή των δοχείων Α, Β γίνεται με την ίδια πιθανότητα. Η δε πιθανότητα επιλογής μιας αριθμημένης μπάλας από το επιλεγμένο δοχείο είναι ίδια. Να βρεθεί η εντροπία της Χ.
    - X={K1,...,K16,M1,...,M8}, Δ={K, M}
    - H(X)=H(Δ)+1/2*H(K1,...,K16)+1/2*H(M1,...,M8)
    - H(X)=$\log_2 2$+1/2*{$\log_2 16$+$\log_2 8$}=1+7/2=4.5 bits



©2006, Σπύρος Δενάζης

Αθροιστική Ιδιότητα Εντροπίας ...

- <u>Παράδειγμα 4</u>
  - Μία τράπουλα έχει 52 χαρτιά. Αυτά χωρίζονται σε 4 κατηγορίες, σπαθιά, μπαστούνια, καρό και κούπες. Κάθε κατηγορία έχει 13 χαρτιά η κάθε μία ενώ τα σπαθιά και τα μπαστούνια είναι μαύρου χρώματος και τα καρό και οι κούπες κόκκινου χρώματος. Το τυχαίο πείραμα συνιστάται στο τράβηγμα ενός χαρτιού από την τράπουλα. Θεωρούμε ότι η πιθανότητα να τραβήξουμε το κάθε χαρτί είναι η ίδια.
    - Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται το χαρτί που τραβήξαμε;
    - Αν μας γνωστοποιηθούν διαδοχικά το χρώμα, μετά η κατηγορία και μετά ο αριθμός ποια είναι η ποσότητα της πληροφορίας που θα έχουμε λάβει; Ποια είναι η ποσότητα της πληροφορίας σε κάθε ένα από τα στάδια;
    - Δοθέντος ότι γνωρίζουμε το χρώμα, ποια είναι η ποσότητα της πληροφορίας που λαμβάνουμε όταν μας γνωστοποιείται ο αριθμός;
    - Δοθέντος ότι γνωρίζουμε το χρώμα, ποια είναι η ποσότητα της πληροφορίας που λαμβάνουμε όταν μας γνωστοποιείται η κατηγορία;

©2006, Σπύρος Δενάζης

Αθροιστική Ιδιότητα Εντροπίας ...

- **<u>Απάντηση</u>**
  - Έστω X,Y,Z οι τ.μ που συμβολίζουν χρώμα, κατηγορία, αριθμό.
  - Ποια ποσότητα πληροφορίας λαμβάνουμε όταν μας γνωστοποιείται το χαρτί που τραβήξαμε;
    - H(Z)=-log(1/52)=5.7 bits
  - Αν μας γνωστοποιηθούν διαδοχικά το χρώμα, μετά η κατηγορία και μετά ο αριθμός ποια είναι η ποσότητα της πληροφορίας που θα έχουμε λάβει; Ποια είναι η ποσότητα της πληροφορίας σε κάθε ένα από τα στάδια;
    - *1ο Στάδιο: Χρώμα*
      - H(1/2,1/2)=-log(1/2)=1 bits
    - *2ο Στάδιο: Κατηγορία*
      - H(Y/X)=1/2*H(Y/X=μαύρο)+1/2*H(Y/X=κόκκινο)=1/2*H(1/2,1/2)+1/2*H(1/2,1/2)=H(1/2,1/2)=-log(1/2)=1 bits
    - *3ο Στάδιο: Αριθμός*
      - H(Z/X,Y)=1/4*H(1/13,1/13,…,1/13)+...+ 1/4*H(1/13,1/13,…,1/13)=H(1/13,1/13,…,1/13)=-log(1/13)=3.7 bits
    - Δηλαδή αποτελεί γενίκευση του παρακάτω τύπου
      - H(X,Y,Z)=H(X)+H(Y,Z/X)=H(X)+H(Y/X)+H(Z/X,Y)=H(1/2,1/2)+H(1/2,1/2)+H(1/13,1/13,...,1/13)=1+1+3.7 bits
    - ΠΡΟΣΟΧΗ: Η πληροφορία του συνδυασμένου γεγονότος (χρώμα, κατηγορία), H(X,Y)=H(1/4,1/4,1/4,1/4)= 2 bits, ΔΕΝ ΕΙΝΑΙ ΙΣΗ με H(Y/X)=H(1/2,1/2)=1 bits

©2006, Σπύρος Δενάζης

Αμοιβαία Πληροφορία ...

- Έστω δύο τ.μ. X, Y με συνδυασμένη πιθανότητα μάζας p(x,y) και περιθωριακές πιθανότητες μάζας, p(x) και p(y), αντίστοιχα. Τότε η ***αμοιβαία πληροφορία I(X;Y)*** ορίζεται ως η σχετική εντροπία μεταξύ της συνδυασμένης κατανομής και του γινομένου p(x)p(y)

$$\boxed{\begin{aligned} I(X;Y) &= \sum_x \sum_y p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \\ &= D\big(p(x,y) \,\|\, p(x)p(y)\big) \end{aligned}}$$

  - Εναλλακτικά συμβολίζει την ποσότητα πληροφορίας που περιέχει μια τμ X για μια άλλη τμ Y.

©2006, Σπύρος Δενάζης

Αμοιβαία Πληροφορία ...

$$I(X;Y) = \sum_x \sum_y p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$$

$$= \sum_x \sum_y p(x,y) \log \frac{p(x/y)\cancel{p(y)}}{p(x)\cancel{p(y)}}$$

$$\log \frac{p(x/y)}{p(x)} = \log p(x/y) - \log p(x)$$

$$= -\sum_x \sum_y p(x,y) \log p(x) + \sum_x \sum_y p(x,y) \log p(x/y)$$

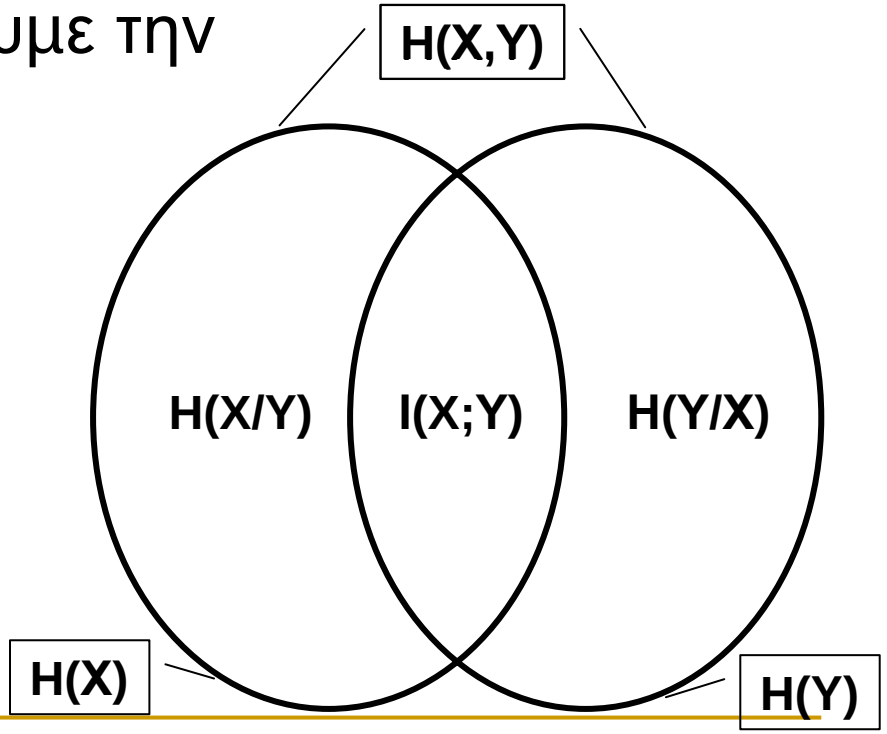
$$= -\sum_x p(x) \log p(x) - \left[-\sum_x \sum_y p(x,y) \log p(x/y) \right]$$

$$\boxed{= H(X) - H(X/Y)}$$

©2006, Σπύρος Δενάζης

Αμοιβαία Πληροφορία ...

- Συμπεραίνουμε ότι η αμοιβαία πληροφορία I(X;Y) είναι η μείωση της αβεβαιότητας της X εξαιτίας του γεγονότος ότι γνωρίζουμε την Y!!
- **Θεώρημα 4**: Ισχύουν
  - I(X;Y)= H(X)-H(X/Y)
  - I(X;Y)=H(Y)-H(Y/X)
  - I(X;Y)=H(X)+H(Y)-H(X,Y)
  - I(X;Y)=I(Y;X)
  - I(X;X)=H(X)



©2006, Σπύρος Δενάζης

Αμοιβαία Πληροφορία ...

- **<u>Παράδειγμα 6</u>**: Έστω (X,Y) έχουν την παρακάτω πιθανότητα μάζας

Y \ X	1	2	3	4		P(y)
1	1/8	1/16	1/32	1/32	→	1/4
2	1/16	1/8	1/32	1/32	→	1/4
3	1/16	1/16	1/16	1/16	→	1/4
4	1/4	0	0	0	→	1/4
P(x)	1/2	1/4	1/8	1/8		

- H(X)=7/4 bits και H(Y)=2 bits
- H(X/Y)=11/8 bits και H(Y/X)=13/8 bits
- H(X,Y)=27/8 bits
- I(X;Y)=H(X)-H(X/Y)=H(Y)-H(Y/X)=3/8 bits

©2006, Σπύρος Δενάζης

Ανισότητες...

- **Θεώρημα 9:**
  - Έστω X μία τ.μ. με πλήθος στοιχείων n. Τότε ισχύει
    - $H(X) \leq \log n$
  - Η ισότητα ισχύει εάν η κατανομή της X είναι ομοιόμορφη, δηλ. $p(x)=1/n, \forall x \in X$
- **Θεώρημα 10**: (Η εξάρτηση μειώνει την εντροπία)
  - $H(X/Y) \leq H(X)$
  - Η ισότητα ισχύει εάν X,Y είναι ανεξάρτητες μεταβλητές
- **Θεώρημα 11:** (Ανώτατο Όριο εντροπίας πολυδιάστατης τ.μ)
  - Έστω $X_1, X_2, \ldots, X_n$ τ.μ με συνδυασμένη πιθανότητα μάζας $p(x_1, x_2, \ldots, x_n)$. Τότε ισχύει
  - $H(X_1, X_2, \cdots, X_n) \leq \sum_{i=1}^{n} H(X_i)$
  - Με την ισότητα να ισχύει στην περίπτωση που οι τ.μ. είναι ανεξάρτητες.

©2006, Σπύρος Δενάζης

Ανισότητες ...

- **<u>Άσκηση</u>**
  - Έστω ότι η τ.μ (X,Y) έχει την παρακάτω συνδυασμένη μάζα πιθανότητας

Y \ X	1	2	P(y)
1	0	3/4	→ 3/4
2	1/8	1/8	→ 1/4
P(x)	1/8	7/8	

  - H(X)=H(1/8,7/8)=0.544 bits
  - H(X/Y=1)=0 bits και H(X/Y=2)=1 bit
  - H(X,Y)=3/4 H(X/Y=1)+1/4 H(X/Y=2)=0.25 bits
  - Παρατηρείστε ότι η αβεβαιότητα της X αυξάνεται στην περίπτωση που γνωρίζουμε το γεγονός Y=2 και ελαττώνεται όταν γνωρίζουμε το γεγονός Y=1. Παρόλα αυτά η μέση πληροφορία ή η αβεβαιότητα ελαττώνεται για την X/Y

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων

- **Διακριτή Πηγή Πληροφορίας**
  - Παράγει ακολουθίες **συμβόλων** (ή γραμμάτων), s_i
  - **Αλφάβητο πηγής** είναι το σύνολο των συμβόλων
    - $S=(s_1,s_2,\ldots,s_n)$, όπου n είναι το πλήθος των συμβόλων
  - Παράγει διαδοχικές ακολουθίες συμβόλων που ονομάζονται **μηνύματα**
    - Το πλήθος των δυνατών μηνυμάτων μήκους l είναι n^l
  - Η Παραγωγή των συμβόλων λαμβάνει χώρα με κάποια πιθανότητα, p_i
  - Η παραγωγή κάθε συμβόλου γίνεται
    - Είτε ανεξάρτητα αυτών που έχουν προηγηθεί οπότε αναφερόμαστε σε **διακριτή πηγή χωρίς μνήμη**
    - Είτε εξαρτάται στατιστικά αυτών που έχουν προηγηθεί οπότε αναφερόμαστε σε **διακριτή πηγή με μνήμη**

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων ...

- **Ποσότητα πληροφορίας της πηγής χωρίς μνήμη**
- Μέση ποσότητα πληροφορίας ή εντροπία των συμβόλων (bits/symbol)
  - $H(S) = -\sum_{i=1}^{n} p_i \log p_i$
- Μέγιστη μέση ποσότητα πληροφορίας (bits/symbol)
  - $\max H(S) = -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} = \log n$
- Πλεονασμός διακριτής πηγής, [0,1]
  - $red = 1 - \frac{H(S)}{\max H(S)} = 1 - \frac{H(S)}{\log n}$
- Μέσος Ρυθμός Πληροφορίας της πηγής (bits/sec)
  - $R = r_S H(S)$

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων ...

- **Παράδειγμα:** S={0,1} με p(0)=3/4 και p(1)=1/4
  - H(S)=0.815 bits/symbol
  - maxH(S)=log2=1 bit/symbol
  - red=1-0.815/1=0.19
- **Άσκηση**
  - S={Χ,Ψ,Ω} και P={0.25,0.5,0.25}. Αν η πηγή παράγει σύμβολα με ρυθμό 1000 σύμβολα/sec να βρεθούν
    - H(S), maxH(S), red, R

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων ...

- Μέσο πληροφοριακό περιεχόμενο μηνυμάτων της πηγής
  - Εάν γνωρίζουμε ότι η πηγή παράγει μηνύματα μήκους l, με δεδομένο ότι το πλήθος του συνόλου $M=(m_1,m_2,\ldots,m_n)$, των μηνυμάτων είναι n^l, και η πιθανότητα εμφάνισης ενός μηνύματος m_i είναι $p(m_i)$, τότε το μέσο πληροφοριακό περιεχόμενο των μηνυμάτων είναι
    - $H(M) = -\sum_{i=1}^{n^l} p(m_i)\log p(m_i)$
    - Αποδεικνύται ότι H(M)= l*H(S), δηλαδή το μέσο πληροφοριακό περιεχόμενο ενός μηνύματος είναι ίσο με το άθροισμα της πληροφορίας που μεταφέρουν τα σύμβολα που το αποτελούν.
- **Παράδειγμα:** Τα μηνύματα μήκους 2 που δημιουργούνται από την πηγή των συμβόλων του προηγούμενου παραδείγματος είναι M={00,01,10,11} πλήθους 4 και οι πιθανότητες να συμβούν είναι p(00)=9/16, p(01)=p(10)=3/16, p(11)=1/16. Τότε H(M)=1.63 bits/μήνυμα=2*0.815

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων ...

- ***Άσκηση***
  - Μια πηγή πληροφορίας παράγει σύμβολα, τα οποία ανήκουν στο αλφάβητο *S={τ, υ, φ, χ, ψ, ω}.* Οι πιθανότητες των συμβόλων αυτών είναι ¼, ¼, 1/8, 1/8, 1/8 και 1/8, αντίστοιχα.
  - Θεωρώντας την πηγή χωρίς μνήμη, ζητείται να υπολογίσετε
  - α) Το σύμβολο με το μεγαλύτερο και το μικρότερο πληροφορικό περιεχόμενο της πηγής.
  - β) Το μέσο πληροφορικό περιεχόμενο των συμβόλων της πηγής,
  - γ) Το μέσο πληροφορικό περιεχόμενο των μηνυμάτων της πηγής αποτελούμενων από δύο σύμβολα.
  - δ) Τον πλεονασμό της πηγής (*log6=2,585*) και
  - ε) Το μέσο ρυθμό πληροφορίας της πηγής για ρυθμό 500 συμβόλων /sec.

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων ...

- ***<u>Απάντηση</u>***
  - α) Τα σύμβολα με το μεγαλύτερο πληροφορικό περιεχόμενο είναι αυτά που έχουν την μικρότερη πιθανότητα δηλαδή *H(i)=-log(1/8)=3 bits* όπου *i*=φ,χ,ψ,ω. Αντίθετα τα σύμβολα με το μικρότερο πληροφορικό περιεχόμενο είναι αυτά που έχουν την μικρότερη πιθανότητα δηλαδή *H(i)=-log(1/4)=2 bits* όπου *i*=τ,υ.
  - β) Το μέσο πληροφορικό περιεχόμενο των συμβόλων της πηγής
    - $$H(S) = -\sum_{i=1}^{6} p_i \log p_i = -\frac{1}{4}\log\frac{1}{4} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} = (20/8) = 2{,}5 \text{ bits/symbol.}$$

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων ...

- **<u>Απάντηση (συνέχεια)</u>**
  - γ) Για τον υπολογισμό του μέσου πληροφορικού περιεχομένου των μηνυμάτων της πηγής αποτελούμενων από 2 σύμβολα, υπολογίζουμε πρώτα τις (συνδυασμένες) πιθανότητες δημιουργίας των μηνυμάτων αυτών. Αφού η πηγή είναι χωρίς μνήμη, για τον υπολογισμό της πιθανότητας κάθε μηνύματος αρκεί να πολλαπλασιάσουμε τις πιθανότητες παραγωγής των συμβόλων από τα οποία αποτελείται. Συνολικά έχουμε 36 μηνύματα. Παρατηρούμε ότι από τα 36 μηνύματα, 4 έχουν πιθανότητα παραγωγής ίση με (1/16), 16 μηνύματα έχουν πιθανότητα παραγωγής (1/64) και 16 μηνύματα έχουν πιθανότητα παραγωγής (1/32).
  - p1=p(τ,τ)=1/16, p2=p(τ,υ)=1/16, p3=p(τ,φ)=1/32, p4=p(τ,χ)=1/32, p5=p(τ,ψ)=1/32, p6=p(τ,ω)=1/32,
  - p7=p(υ,τ)=1/16, p8=p(υ,υ)=1/16, p9=p(υ,φ)=1/32, p10=p(υ,χ)=1/32, p11=p(υ,ψ)=1/32, p12=p(υ,ω)=1/32,
  - p13=p(φ,τ)=1/32, p14=p(φ,υ)=1/32, p15=p(φ,φ)=1/64, p16=p(φ,χ)=1/64, p17=p(φ,ψ)=1/64, p18=p(φ,ω)=1/64,
  - p19=p(χ,τ)=1/32, p20=p(χ,υ)=1/32, p21=p(χ,φ)=1/64, p22=p(χ,χ)=1/64, p23=p(χ,ψ)=1/64, p24=p(χ,ω)=1/64,
  - p25=p(ψ,τ)=1/32, p26=p(ψ,υ)=1/32, p27=p(ψ,φ)=1/64, p28=p(ψ,χ)=1/64, p29=p(ψ,ψ)=1/64, p30=p(ψ,ω)=1/64,
  - p31=p(ω,τ)=1/32, p32=p(ω,υ)=1/32, p33=p(ω,φ)=1/64, p34=p(ω,χ)=1/64, p35=p(ω,ψ)=1/64, p36=p(ω,ω)=1/64.

©2006, Σπύρος Δενάζης

Εντροπία Συμβόλων και Διακριτών Μηνυμάτων ...

- **<u>Απάντηση (συνέχεια)</u>**
  - Επομένως

$$H(M) = -\sum_{i=1}^{36} p_i \log p_i = -4\frac{1}{16}\log\frac{1}{16} - 16\frac{1}{64}\log\frac{1}{64} - 16\frac{1}{32}\log\frac{1}{32} = (320/64) = 5 \text{ bits/message.}$$

  - Παρατηρείστε ότι H(M)=2 H(S)
  - Αυτό συμβαίνει λόγω του ότι η πηγή είναι χωρίς μνήμη
  - δ) red=1-H(S)/maxH(S)=1-H(S)/log6=1-(2,5/2,585)=1-0,967=0,0328.
  - ε) R=rH(S)=500x(2,5)=1250 bits/sec.

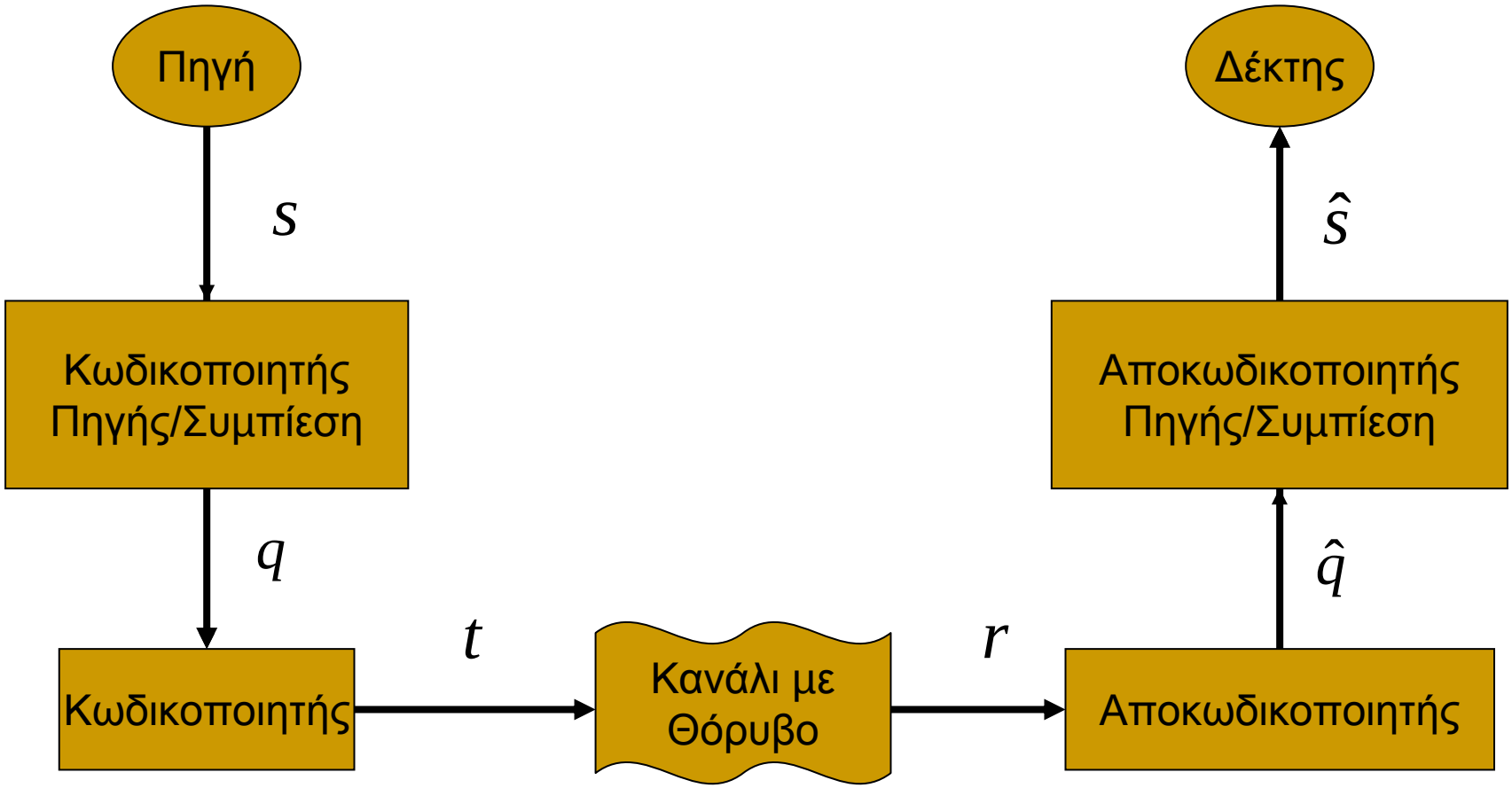
©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής

- Επικοινωνιακό μοντέλο
- Διακριτές Πηγές Πληροφορίας
  - Με μνήμη
  - Χωρίς μνήμη
- Κωδικοποίηση Πηγής
  - Κωδικό Αλφάβητο, Κωδικές Λέξεις
- Κώδικες Πηγών
  - Ιδιάζοντες
  - Μοναδικά Αποκωδικοποιήσιμοι
  - Άμεσοι
  - Πλήρεις
- Ανισότητα Kraft
- Θεώρημα Κωδικοποίησης
  - Βέλτιστα Μήκη Κωδικών Λέξεων
- Αλγόριθμοι Κωδικοποίησης Πηγών Συμβόλων
  - FANO, SHANNON, HUFFMAN,

©2006, Σπύρος Δενάζης

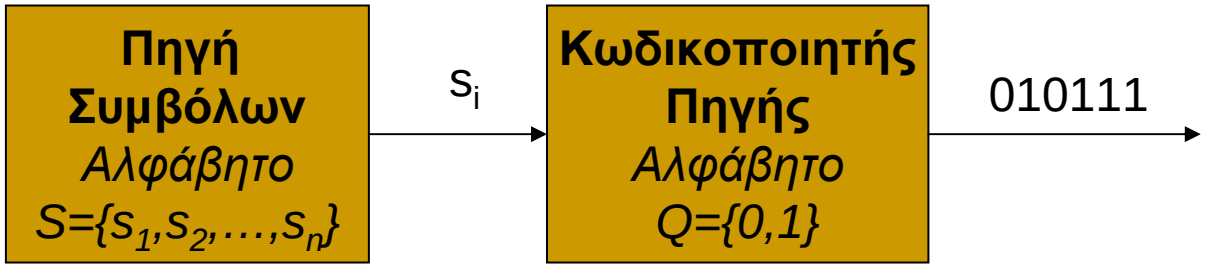
Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...



©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Κωδικοποίηση/συμπίεση της πηγής
  - Είναι η διαδικασία αντιστοίχισης του αλφάβητου των συμβόλων σε ένα άλλο αλφάβητο.
  - Το καινούριο αυτό αλφάβητο ονομάζεται **κωδικό αλφάβητο** και τα μέλη ονομάζονται **κωδικά σύμβολα**.
  - Οι ακολουθίες των κωδικών συμβόλων που αντιστοιχούν σε σύμβολα της πηγής λέγονται **κωδικές λέξεις**



©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Ερωτήματα που προκύπτουν από τις σχέσεις που διέπουν τα σύμβολα και τους κώδικες και τις κωδικές λέξεις
  - Πως μπορούμε να κατασκευάσουμε άμεσους κώδικες με το ελάχιστο προσδοκόμενο μήκος για την συμπιεσμένη αναπαράσταση των συμβόλων μιας πηγής;
  - Υπάρχει σχέση μεταξύ συμβόλου και μήκους κωδικής λέξης;
  - Το πληροφοριακό περιεχόμενο της πηγής των συμβόλων πως επηρεάζει την παραγωγή των κωδικών λέξεων και με ποιό τρόπο;

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Απαιτήσεις για χρησιμότητα κωδικών
  - Κάθε ακολουθία κωδικών λέξεων πρέπει να μπορεί να αποκωδικοποιηθεί με μοναδικό τρόπο
  - Η αποκωδικοποίηση πρέπει να γίνεται εύκολα και άμεσα
  - Ο κώδικας πρέπει να πετυχαίνει τη βέλτιστη δυνατή συμπίεση

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- **Ορισμοί**
  - **Μη ιδιάζων κώδικας**
    - Όταν όλες οι κωδικές λέξεις είναι διαφορετικές
  - **Μοναδικά αποκωδικοποιήσιμος**
    - Όταν και οι ακολουθίες των κωδικών λέξεων είναι διαφορετικές
  - **Άμεσος ή Προθεματικός κώδικας**
    - Κάθε μοναδικά αποκωδικοποίησιμος κώδικας που επιτρέπει την άμεση αποκωδικοποίηση της κωδικής λέξης χωρίς να χρειάζεται να λάβει υπόψη του τις επόμενες κωδικές λέξεις.
    - Ο άμεσος κώδικας αποτελείται από κωδικές λέξεις οι οποίες δεν αποτελούν μέρος (προθέματα άλλων)

©2006, Σπύρος Δενάζης

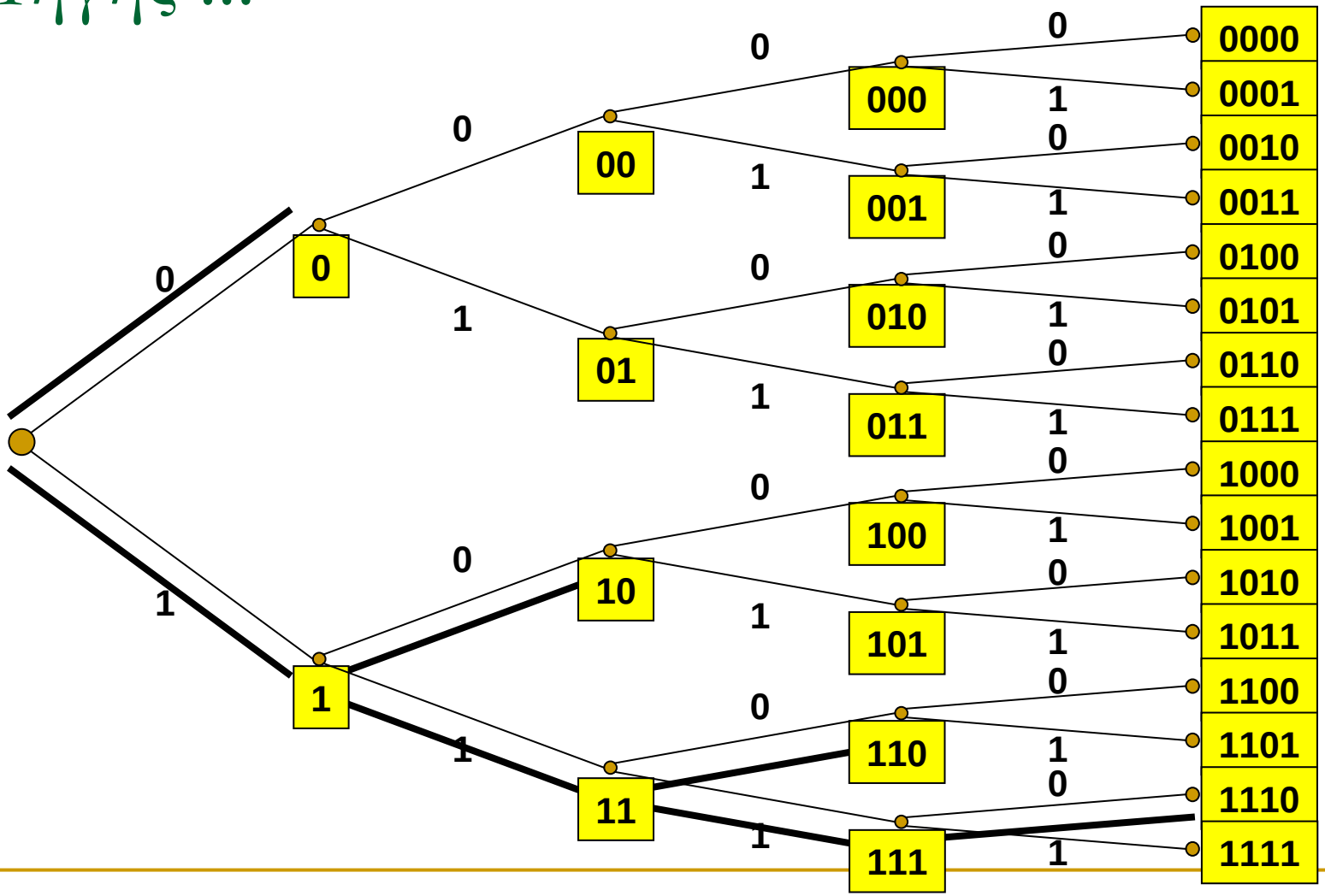
Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- **Παράδειγμα**
  - Μη ιδιάζων, I,II,III,IV
  - Μοναδικά αποκωδικοποιήσιμος, II,III,IV. Ο I δεν είναι αφού ΦΦΦΦ, ΦΦΨ, ΨΨ όλα έχουν κωδική λέξη την ίδια, 0000
  - Άμεσοι κώδικες, II και III
  - Ο κώδικας IV δεν είναι άμεσος αφού χρειάζεται να γνωρίζουμε ψηφία που ανήκουν στην επόμενη κωδική λέξη, π.χ. 011011100?

	I	**II**	**III**	**IV**
Φ	0	00	0	0
Χ	11	01	10	01
Ψ	00	10	110	011
Ω	01	11	1110	0111

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

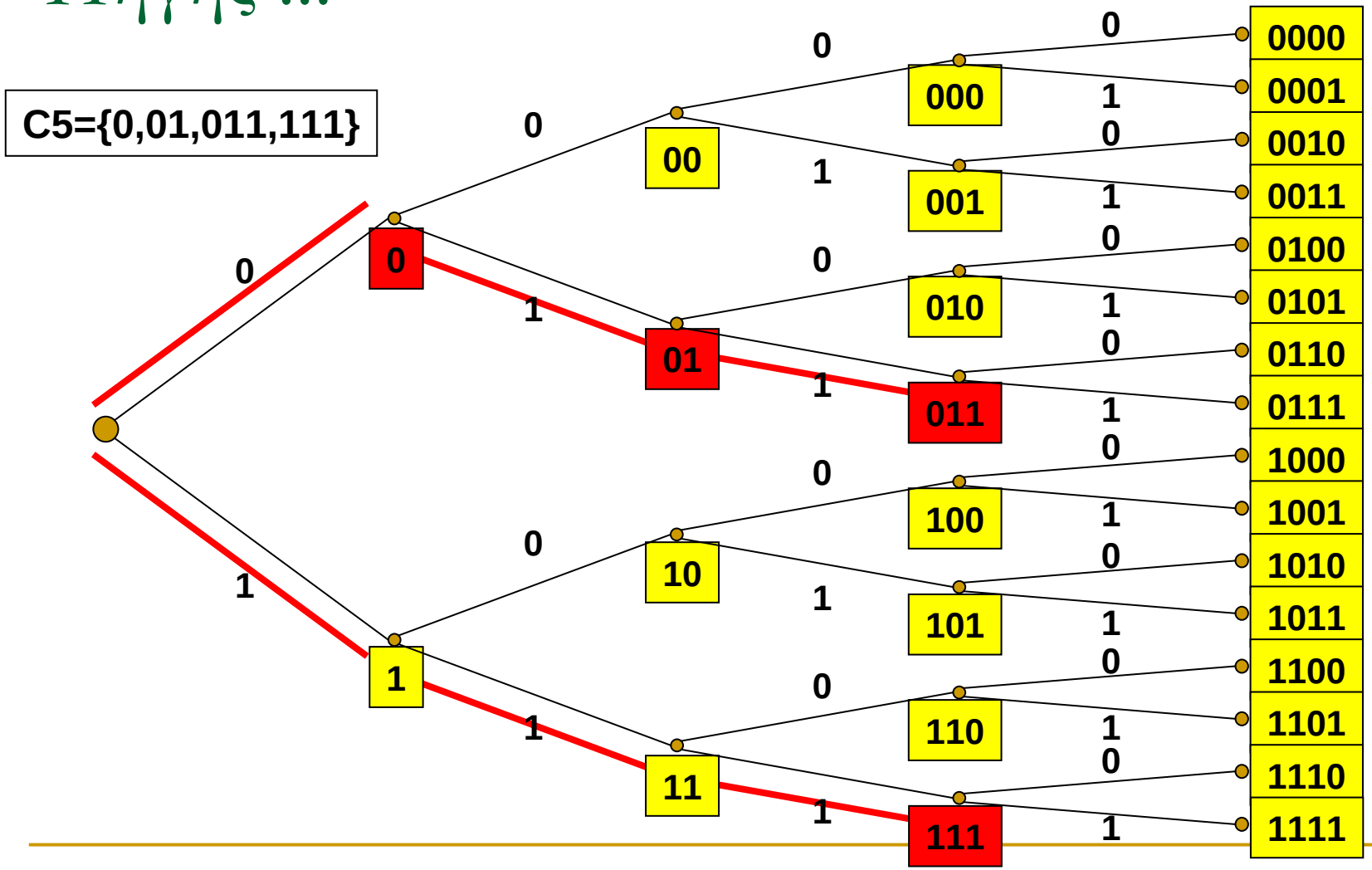

0
1
0
1
0
1

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Παραδείγματα άλλων άμεσων και μη αμέσων κωδικών
  - C1={0,101} **Άμεσος**
  - C2={1,101} **Μη άμεσος**
  - C3={0,10,110,111} **Άμεσος**
  - C4={00,01,10,11} **Άμεσος**
  - C5={0,01,011,111} **Μη άμεσος**

©2006, Σπύρος Δενάζης

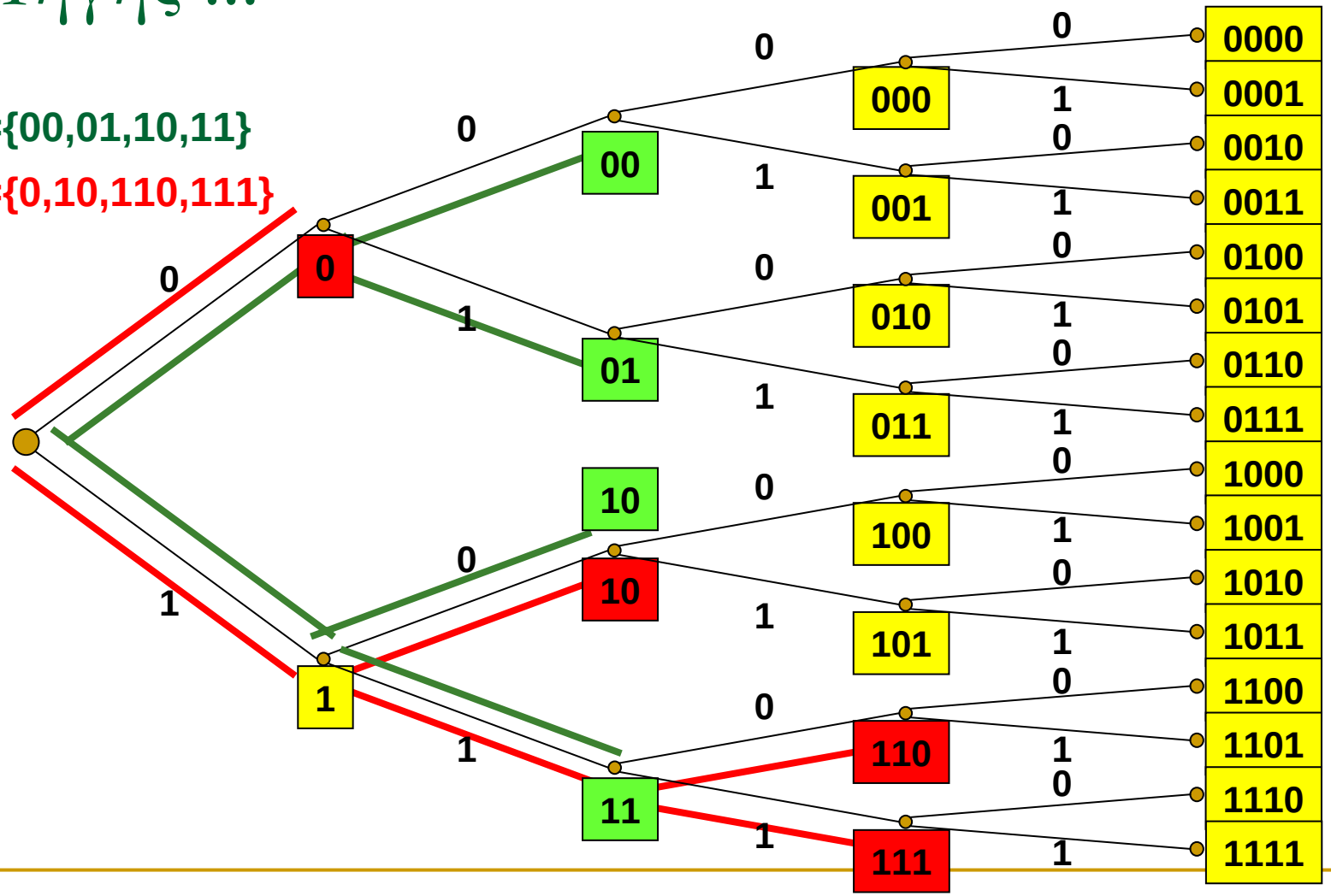
Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...


C5={0,01,011,111}
0
1
0
1
0
1

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

C4={00,01,10,11}

C3={0,10,110,111}


0
1
0
1
0
1

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Παίρνοντας τον κώδικα C4={00,01,10,11} και μειώνοντας το μήκος μίας εκ των κωδικών λέξεων, 00→0, τότε μπορούμε να διατηρήσουμε την δυνατότητα της άμεσης αποκωδικοποίησης μόνο αν αυξήσουμε το μήκος άλλων κωδικών λέξεων. Φαίνεται λοιπόν ότι υπάρχει ένα κόστος που καλούμαστε να πληρώσουμε στην περίπτωση που θέλουμε μικρότερου μήκους λέξεις. Με άλλα λόγια μικρού μήκους κωδικές λέξεις έχουν μεγάλο κόστος.
- Ας εξετάσουμε τον κώδικα με λέξεις μήκους 3. Το πλήθος των λέξεων είναι $2^3=8$. Ο κώδικας αυτός είναι άμεσος και μοναδικά αποκωδικοποιήσιμος. Αν κάνουμε την αντικατάσταση 000→0 τότε ο κώδικας που προκύπτει με όλες τις υπόλοιπες λέξεις μήκους 3 είναι ο {0, 100,101,110,111}. Φαίνεται λοιπόν ότι κωδικές λέξεις μήκους 3 κοστίζουν 2^2 λιγότερο αν θέλουμε να διατηρήσουμε την μοναδικότητα της αποκωδικοποίησης.
- Αν θεωρήσουμε τώρα ότι έχουμε ένα μέγιστο ποσό, έστω 1, να διαθέσουμε για την δημιουργία άμεσων και μοναδικά αποκωδικοποιήσιμων κωδικών όπου το κόστος κάθε λέξης μήκους l είναι 2^{-l} τότε κάθε συνδυασμός μήκους κωδικών λέξεων δεν θα πρέπει να υπερβαίνει την 1 εάν θέλουμε να είναι μοναδικά αποκωδικοποιήσιμος. Δηλ.

$$\boxed{\sum_{i=1}^{n} 2^{-l_i} \leq 1}$$

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- **<u>Θεώρημα 12:</u>** Ανισότητα του Kraft
  - Για κάθε άμεσο κώδικα με πλήθος κωδικών συμβόλων του κωδικού αλφαβήτου q και μήκη των κωδικών λέξεων l_i, όπου i=1,2,…,n και n το πλήθος των συμβόλων της πηγής ισχύει,
    - $$\boxed{\sum_{i=1}^{n} q^{-l_i} \leq 1}$$
  - Αντίστροφα, αν για ένα σύνολο μηκών κωδικών λέξεων ισχύει η ανισότητα Kraft τότε υπάρχει ένας άμεσος κώδικας του οποίου οι κωδικές λέξεις έχουν αυτά τα μήκη.

©2006, Σπύρος Δενάζης

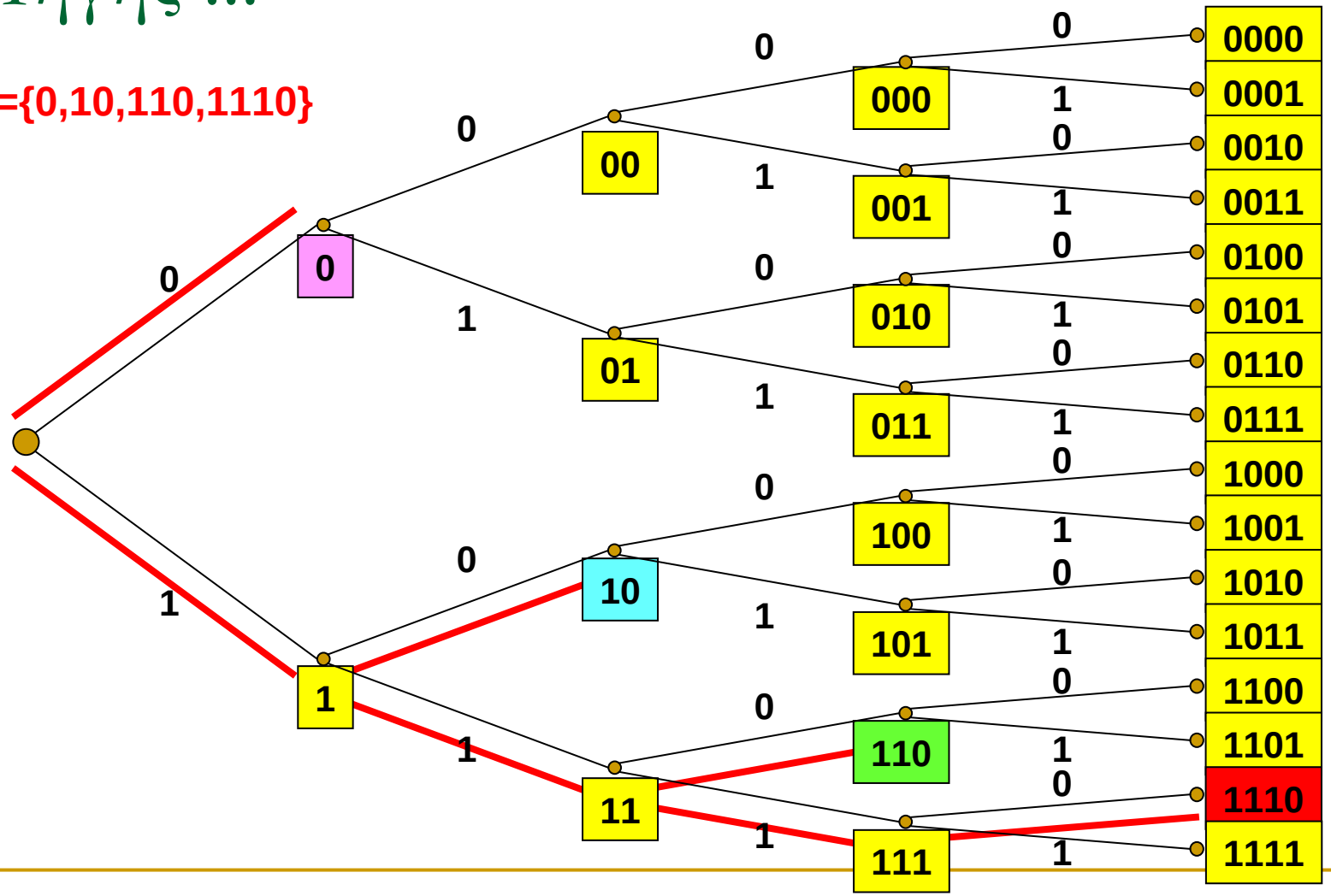
Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- **<u>Απόδειξη</u>**
  - Τέτοιοι κώδικες (άμεσοι και αποκωδικοποιήσιμοι) έχουν κωδικές λέξεις οι οποίες έχουν ένα μέγιστο μήκος, π.χ l_{max}. Όλες οι λέξεις σε αυτό το επίπεδο είναι είτε μέρος του συνόλου των κωδικών λέξεων είτε <u>απόγονοι</u> άλλων κωδικών λέξεων οι οποίες βρίσκονται σε μικρότερα επίπεδα.
  - Το πλήθος των απογόνων μιας <u>κωδικής λέξης</u> του επιπέδου l_i, που βρίσκονται στο επίπεδο l_{max}, ισούται με το πλήθος των λέξεων μήκους l_{max}-l_i και άρα είναι $q^{l_{max}-l_i}$.
  - Καθένα από τα σύνολα αυτά των απογόνων κωδικών λέξεων δεν έχει κανένα κοινό στοιχείο μεταξύ τους
  - Επίσης το άθροισμα των απογόνων αυτών δεν μπορεί να ξεπεράσει το $q^{l_{max}}$ που είναι όλο το σύνολο των λέξεων (όχι κατ' ανάγκη κωδικών μήκους l_{max})
  - Επομένως ισχύει $\boxed{\sum_{i=1}^{n} q^{(l_{max}-l_i)} \le q^{l_{max}} \Rightarrow \sum_{i=1}^{n} q^{-l_i} \le 1}$

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

C={0,10,110,1110}


0
1
0
1
0
1

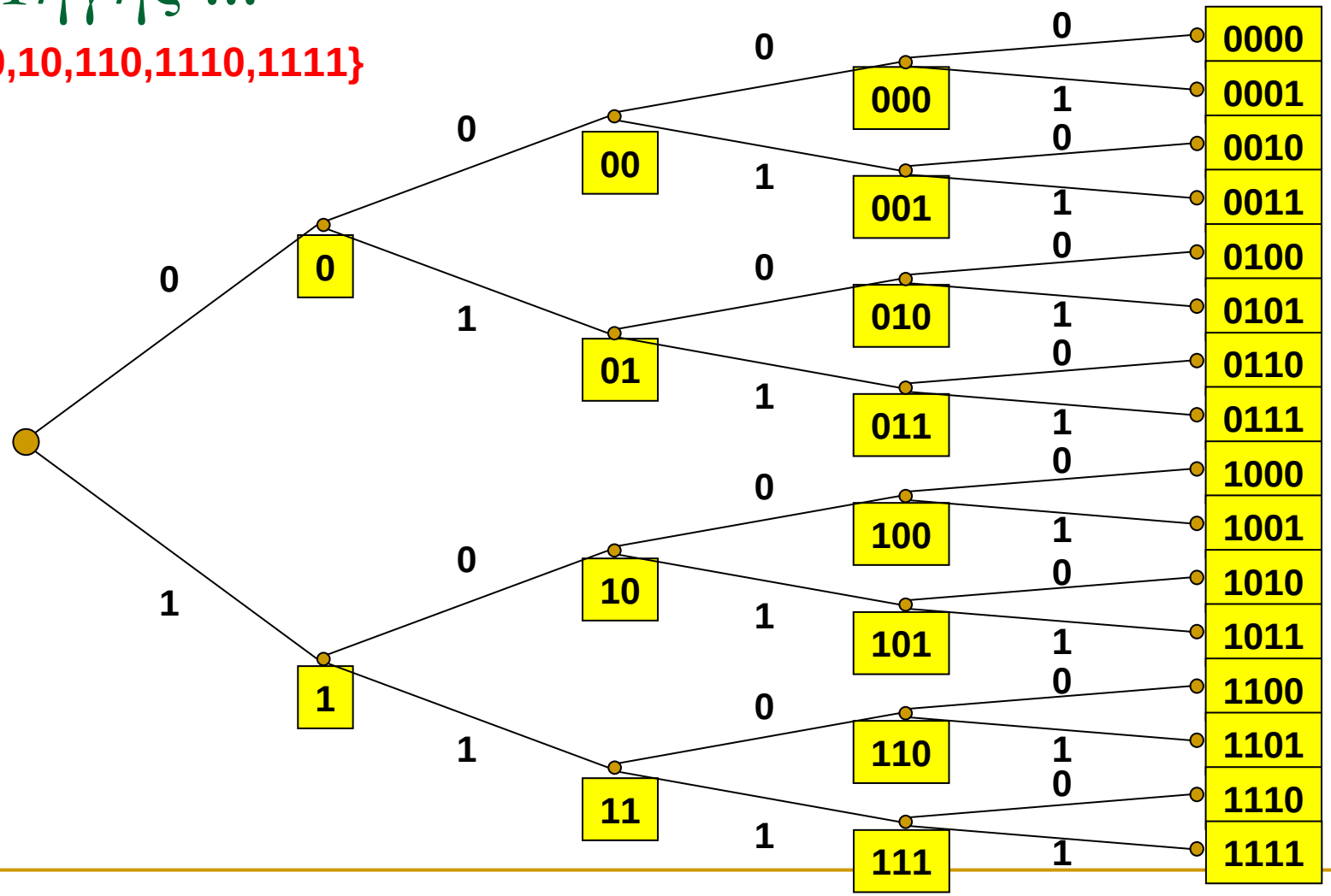
Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Συνέχεια απόδειξης ανισότητας Kraft (αντίστροφο)
  - Έστω $l_1, l_2,..., l_n$, μήκη λέξεων που ικανοποιούν την ανισότητα Kraft, τότε είναι δυνατόν να κατασκευαστεί ένα δέντρο όπως αυτό που είδαμε προηγουμένως.
  - Επιλέγοντας μια κωδική λέξη μήκους l_1, διαγράφουμε όλους τους απογόνους της. Μετά επιλέγουμε από το δένδρο που απομένει μια λέξη μήκους l_2, και διαγράφουμε τους απογόνους της κ.ο.κ μέχρι l_n.
  - **Προσοχή:** Το θεώρημα μας λέει ότι υπάρχει άμεσος κώδικας με μήκη l_i και όχι ότι κάθε κώδικας με μήκη l_i είναι που πληροί την ανισότητα είναι άμεσος

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής …

C={0,10,110,1110,1111}


0
1
0
1
0
1

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Με τις πιθανότητες εμφάνισης των συμβόλων τι γίνεται;
- Μπορούμε να βρούμε ένα κώδικα (άμεσο και αποκωδικοποιήσιμο) του οποίου οι κωδικές λέξεις να έχουν το βέλτιστο δυνατό μήκος; Να έχουν δηλαδή τη κατά μέσο όρο τη μικρότερη τιμή μήκους κωδικής λέξης;
  - $\min \sum_i p_i l_i$
- Υπάρχει σχέση μήκους λέξης και πιθανότητας εμφάνισης συμβόλου πηγής;
- Αν αντιστοιχίσουμε κωδικές λέξεις μικρού μήκους σε σύμβολα με μεγάλη πιθανότητα εμφάνισης θα μειωθεί το μέσο μήκος της κωδικής λέξης;
- Ξέρουμε όμως ότι μικρού μήκους κωδικές λέξεις έχουν μεγάλο κόστο αφού χρειάζεται να εισάγουμε μεγάλου μήκους κωδικές λέξεις για την πλήρη αντιστοίχιση των συμβόλων πηγής.
- **Ποια είναι η βέλτιστη συμπίεση που είναι δυνατόν να επιτευχθεί;**

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- **<u>Θεώρημα 13:</u>** *Κωδικοποίησης Πηγής*
  - Έστω μια πηγή παράγει $S=\{s_1,s_2,\ldots,s_n\}$ σύμβολα με πιθανότητα εμφάνισης κάθε συμβόλου $\{p_1,p_2,\ldots,p_n\}$. Τα σύμβολα αυτά κωδικοποιούνται από ένα κωδικό αλφάβητο q συμβόλων και αντιστοιχίζονται σε άμεσο και αποκωδικοποιήσιμο κώδικα n κωδικών λέξεων μήκους l_i η κάθε μία, i=1,2,…,n. Αν H(C) είναι το μέσο πληροφοριακό περιεχόμενο των συμβόλων της πηγής τότε ισχύει,
  - $$\boxed{\frac{H(C)}{\log q} \le \sum_{i=1}^{n} p_i l_i}$$
- Για q=2, το βέλτιστο (ελάχιστο) **μέσο** μήκος κωδικής λέξης είναι ίσο με το μέσο πληροφοριακό περιεχόμενο της πηγής των συμβόλων και δεν μπορεί να είναι μικρότερο από αυτό.
- Για ποιές τιμές των l_i ισχύει η ισότητα του θεωρήματος της κωδικοποίησης της πηγής;
- **Ελάχιστο του μήκους των κωδικών λέξεων**
  - Η ισότητα ισχύει όταν $$\boxed{l_i = \log_q\left(\frac{1}{p_i}\right)}$$

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Βέλτιστες κωδικές λέξεις για q=2
  - Η μέση τιμή του μήκους των λέξεων ενός κώδικα ελαχιστοποιείται και είναι ίση με την εντροπία της πηγής όταν τα μήκη της κάθε κωδικής λέξης είναι ίσα με το πληροφοριακό περιεχόμενο του κάθε συμβόλου
  - $$\boxed{l_i = \log_2\left(\frac{1}{p_i}\right)}$$
- Αντίστροφα, οποιαδήποτε επιλογή κώδικα και κωδικών λέξεων έμμεσα ορίζει και μία κατανομή πιθανότητας $\{q_i\}$,
  - $\boxed{q_i = 2^{-l_i} / z}$,z=1 όταν ο κώδικας είναι πλήρης

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Δεν μπορούμε λοιπόν να συμπιέσουμε λιγότερο από την εντροπία της πηγής.
- Πρακτικά πόσο κοντά σε αυτή την τιμή μπορούμε να φτάσουμε;
- **Θεώρημα 14:**
  - Για κάθε τ.μ X υπάρχει ένας άμεσος και μοναδικά αποκωδικοποιήσιμος κώδικας C του οποίου η μέση τιμή μήκους, L(C,X), ικανοποιεί τη σχέση
    - $H(X) \leq L(C,X) < H(X)+1$
  - Ο κώδικας αυτός έχει κωδικές λέξεις μήκους
    - $l_i^* = \lceil \log_2(1/p_i) \rceil$ όπου $\lceil \chi \rceil$ είναι ο μικρότερος ακέραιος που είναι μεγαλύτερος του χ.

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Ποιο είναι λοιπόν το κόστος χρησιμοποίησης ενός κώδικα του οποίου τα μήκη δεν είναι τα βέλτιστα;
- Ας υποθέσουμε ότι $\{p_i\}$ είναι οι πραγματικές πιθανότητες της πηγής των συμβόλων και ο κώδικας που χρησιμοποιούμε έχει μήκη κωδικών λέξεων l_i^*
  - $q_i=2^{-l_i^*} \Rightarrow l_i^*=-\log(q_i)$
  - $$L(C,X)=\sum_i p_i \ell_i^* = -\sum_i p_i \log(q_i)$$
    $$= -\sum_i p_i \log\left(\frac{p_i q_i}{p_i}\right)$$
    $$= -\sum_i p_i \log(p_i) + \sum_i p_i \log\left(\frac{p_i}{q_i}\right)$$
    $$= H(X) + D(p \| q)$$
  - Εναλλακτικά ορίζουμε ως **επίδοση του κώδικα** το λόγο **H(X)/L(C,X)**

©2006, Σπύρος Δενάζης

Συμπίεση Πληροφορίας ή Κωδικοποίηση Πηγής ...

- Αλγόριθμοι κωδικοποίησης
  - FANO
  - SHANNON
  - HUFFMAN
- JPEG και MPEG χρησιμοποιούν μεταξύ άλλων και τον αλγόριθμο Huffman

©2006, Σπύρος Δενάζης

Αλγόριθμος Κωδικοποίησης FANO …

- **<u>Βήμα 1ο</u>**: Τα σύμβολα (ή τα μηνύματα) ταξινομούνται έτσι ώστε οι πιθανότητές τους είναι σε φθίνουσα ακολουθία.
- **<u>Βήμα 2ο</u>**: Στη συνέχεια τα σύμβολα χωρίζονται σε ομάδες ο αριθμός των οποίων είναι ίσος με τον αριθμό των κωδικών συμβόλων (στην περίπτωση δυαδικού κώδικα η ομάδες χωρισμού συμβόλων είναι δύο).
  - Το κριτήριο σχηματισμού της κάθε ομάδας είναι τέτοιο ώστε αφενός να διατηρείται η σειρά των συμβόλων όπως αυτή έχει καθοριστεί από το βήμα 1
  - Αφετέρου δε να ελαχιστοποείται η σχέση
  - $$\left|\sum_{i=1}^{k} p_i - \sum_{i=k+1}^{n} p_i\right|$$
- **<u>Βήμα 3ο</u>**: Για κάθε μία ομάδα συμβόλων που δημιουργήσαμε αντιστοιχίζουμε ένα από τα κωδικά σύμβολα ως το πρώτο τον κωδικών λεξεων που θα προκύψουν
- **<u>Βήμα 4ο</u>**: Επαναλαμβάνουμε τα βήματα 2 & 3 για κάθε μία από τις ομάδες προσθέτοντας κάθε φορά και από ένα κωδικό σύμβολο στην κωδική λέξη μέχρι να δημιουργήσουμε ομάδες με ένα μόνο σύμβολο
- Ο αλγόριθμος FANO δημιουργεί κώδικες όπου όλες οι κωδικές λέξεις είναι του ίδιου μήκους εάν η διαίρεση σε υποομάδες γίνεται πάντα με την ίδια πιθανότητα.

©2006, Σπύρος Δενάζης

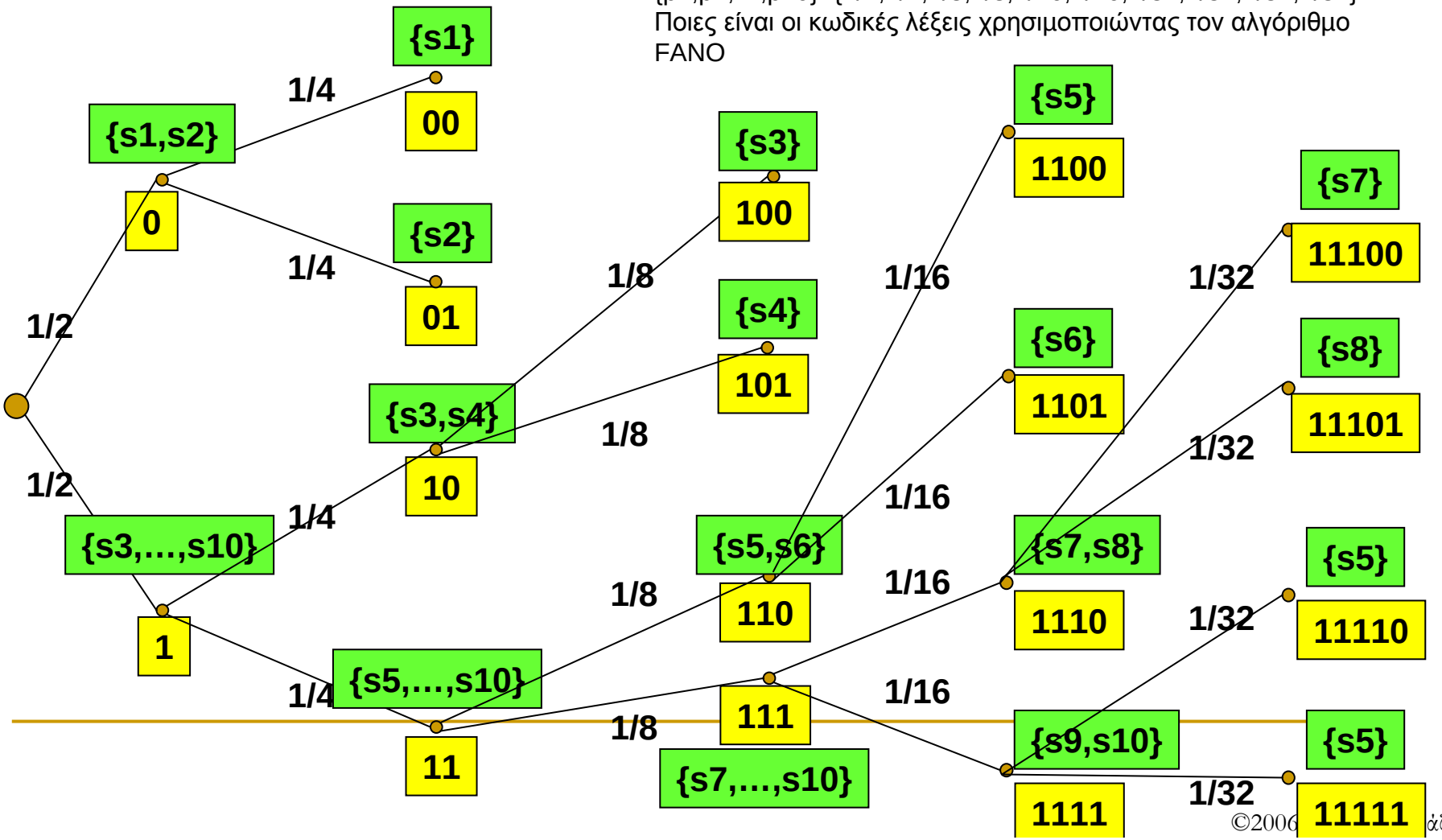
Αλγόριθμος Κωδικοποίησης FANO …

Παράδειγμα

S={s1,s2,…,s10}

{p1,p2,…,p10}={1/4,1/4,1/8,1/8,1/16,1/16,1/32,1/32,1/32,1/32}

Ποιες είναι οι κωδικές λέξεις χρησιμοποιώντας τον αλγόριθμο FANO



©2006 ...άζης

Αλγόριθμος κωδικοποίησης SHANNON …

- **<u>Βήμα 1ο</u>**: Τα σύμβολα (ή τα μηνύματα) ταξινομούνται έτσι ώστε οι πιθανότητές τους είναι σε φθίνουσα ακολουθία, όπως ακριβώς και του FANO.
- **<u>Βήμα 2ο</u>**: Για κάθε σύμβολο s_i του οποίου η πιθανότητα εμφάνισης είναι $p(s_i)$ υπολογίζεται η αθροιστική πιθανότητα P_j ως εξής:
  - $$P_i = \sum_{j=1}^{i-1} p(s_j), \quad P_1 = 0, \quad i = 2,\ldots,n$$
- **<u>Βήμα 3ο</u>**: Το μήκος της κωδικής λέξης που αντιστοιχεί στο σύμβολο s_i ισούται με τον ακέραιο αριθμό l_i, που πληροί τη σχέση
  - $$l_i = \lceil \log_2 (1/p(s_i)) \rceil$$
- **<u>Βήμα 4ο</u>**: Η κωδική λέξη c_i που αντιστοιχεί στο σύμβολο πηγής s_i είναι το δυαδικό ανάπτυγμα του κλάσματος P_i (μόνο τα πρώτα l_i bits αναπτύγματος)

©2006, Σπύρος Δενάζης

Αλγόριθμος κωδικοποίησης SHANNON …

- Μετατροπή δεκαδικού κλασματικού αριθμού σε δυαδικό
  - Ισχύει ότι το δυαδικό ανάπτυγμα ενός δεκαδικού αριθμού F είναι
    - $F = \sum_{i=1}^{k} \left(\frac{\alpha_i}{2} \right)^i = 0.\alpha_1 \alpha_2 \ldots \alpha_k$ όπου τα α_i είναι 0 ή 1
  - Πολλαπλασιάζοντας το F με το 2 έχουμε ότι
    - $2F = a_1 + \sum_{i=2}^{k} \left(\frac{\alpha_i}{2} \right)^i$
  - Από αυτό προκύπτει ότι το α_1 ισούται με 0 εάν 2F <1 και 1 εάν 2F≥1
  - Ομοίως το α_2 ισούται με 0 εάν το $2(2F-\alpha_1)<1$ και 1 εάν $2(2F-\alpha_1) \geq 1$, κοκ

©2006, Σπύρος Δενάζης

Αλγόριθμος κωδικοποίησης SHANNON …

- Παράδειγμα μετατροπής δεκαδικού κλάσματος σε δυαδικό
  - F=0.375
    - $2F=2*0.375=0.75 < 1 \Rightarrow \alpha_1=0$
    - $2(2F-\alpha_1)=2*0.75=1.5 \geq 1 \Rightarrow \alpha_2=1$
    - $2(2(2F-\alpha_1)-\alpha 2)=2(1.5-1)=1 \geq 1 \Rightarrow \alpha_3=1$
    - Άρα το δυαδικό ανάπτυγμα του 0.375 είναι 0.011
  - F=0.327
    - $2*0.327=0.654 < 1 \Rightarrow \alpha_1=0$
    - $2*0.654=1.308 \geq 1 \Rightarrow \alpha_2=1$
    - $2*(1.308-1)=0.616 < 1 \Rightarrow \alpha_3=0$
    - $2*0.616=1.232 \geq 1 \Rightarrow \alpha_4=1$
    - $2*(1.232-1)=0.464 < 1 \Rightarrow \alpha_5=0$
    - $2*0.464=0.928 < 1 \Rightarrow \alpha_6=0$
    - $2*0.928=1.956 \geq 1 \Rightarrow \alpha_7=1$
    - $2*(1.956-1)=1.912 \geq 1 \Rightarrow \alpha_8=1$
    - $2*(1.912-1)=1.824 \geq 1 \Rightarrow \alpha_9=1$
    - Άρα το δυαδικό ανάπτυγμα του 0.327 είναι 0.010100111…
    - Παρατηρούμε ότι είναι δυνατόν το δυαδικό ανάπτυγμα ενός κλάσματος να αποτελείται από άπειρα δυαδικά ψηφία

©2006, Σπύρος Δενάζης

Αλγόριθμος κωδικοποίησης SHANNON …

Παράδειγμα

Σύμβολα Πηγής	Πιθανότητες Συμβόλων
S_1	1/4
S_2	1/4
S_3	1/8
S_4	1/8
S_5	1/16
S_6	1/16
S_7	1/32
S_8	1/32
S_9	1/32
S_{10}	1/32

©2006, Σπύρος Δενάζης

Κωδικοποίηση HUFFMAN ...

- Δοθέντος μιας πηγής συμβόλων με πιθανότητες εμφάνισης p_i, πως μπορούμε να σχεδιάσουμε ένα βέλτιστο άμεσο κώδικα;
- Με τον όρο βέλτιστο εννοούμε ελαχιστοποίηση του μέσου μήκους των κωδικών λέξεων ακεραίου μήκους.
- Η διαδικασία Huffman βασίζεται σε δύο παρατηρήσεις που έχουν σχέση με βέλτιστους κώδικες:
  - Σε έναν βέλτιστο κώδικα τα σύμβολα που εμφανίζονται συχνότερα (μεγαλύτερη πιθανότητα εμφάνισης) θα πρέπει να αντιστοιχούν σε μικρότερες κωδικές λέξεις απ' ότι σύμβολα με μικρότερη συχνότητα εμφάνισης
  - Σε ένα βέλτιστο κώδικα τα δύο σύμβολα με τη μικρότερη πιθανότητα εμφάνισης αντιστοιχούν σε κωδικές λέξεις ίδιου μήκους

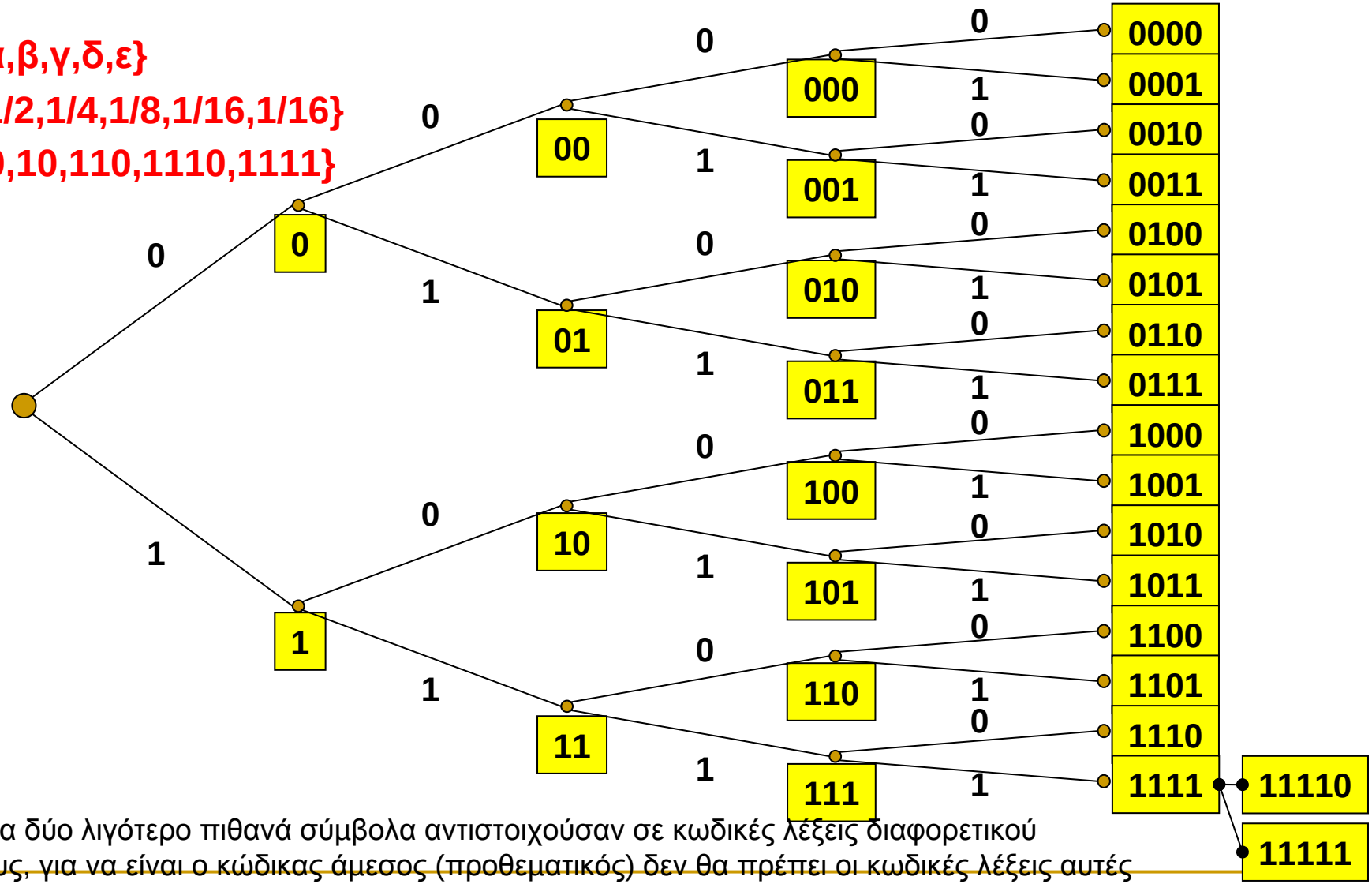
©2006, Σπύρος Δενάζης

Κωδικοποίηση HUFFMAN ...

S={α,β,γ,δ,ε}

P={1/2,1/4,1/8,1/16,1/16}

C={0,10,110,1110,1111}


0
1
0
1
0
1

Κωδικοποίηση HUFFMAN ...

- Ας δούμε πως μπορούμε να χρησιμοποιήσουμε τις προηγούμενες παρατηρήσεις για να δημιουργήσουμε ένα αλγόριθμο βέλτιστου κώδικα
- Παράδειγμα
  - $A=\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5\}$, $P(\alpha_1)=P(\alpha_3)=0.2$, $P(\alpha_2)=0.4$, $P(\alpha_4)=P(\alpha_5)=0.1$, και $c(\alpha_i)$ συμβολίζει την κωδική λέξη που αντιστοιχεί στο σύμβολο α_i
  - Η εντροπία της πηγής είναι H(A)=2.122 bits/σύμβολο
  - Τα δύο σύμβολα με την μικρότερη πιθανότητα είναι τα α4 και α5 των οποίων οι κωδικές λέξεις είναι ίδιου μήκους και διαφέρουν κατά 0 και 1
    - $c(\alpha_4)=a_1*0$
    - $c(\alpha_5)=a_1*1$
      - όπου * υποδηλώνει την προσθήκη 0 ή 1 στην ήδη υπάρχουσα ακολουθία a_1 bits
  - Αν δηλώσουμε τώρα ένα νέο αλφάβητο $A'=\{\alpha_1,\alpha_2,\alpha_3,\alpha_4'\}$, με $P(\alpha_1)=P(\alpha_3)=0.2$, $P(\alpha_2)=0.4$, $P(\alpha_4')=0.2$, τότε οι κωδικές λέξεις που αντιστοιχούν σε αυτό το αλφάβητο δίνονται από τον πίνακα
  - Ομοίως στο αλφάβητο A΄, τα α_3,α_4' επίσης διαφέρουν κατά 0 και 1
    - $c(\alpha_3)=a_2*0$
    - $c(\alpha_4')=a_2*1 \Rightarrow a_1= a_2*1 \Rightarrow c(\alpha_4)=a_2*10$ και $c(\alpha_5)=a_2*11$

α_i	p_i	$c(\alpha_i)$
α_2	0.4	$c(\alpha_1)$
α_1	0.2	$c(\alpha_2)$
α_3	0.2	$c(\alpha_3)$
α_4'	0.2	a_1

©2006, Σπύρος Δενάζης

Κωδικοποίηση HUFFMAN ...

- Δημιουργώντας διαδοχικά ένα νέο αλφάβητο Α΄΄ με ένα ακόμα λιγότερο σύμβολα έχουμε
- $A'' = \{\alpha_2, \alpha_3', \alpha_1\}$, με $P(\alpha_2)=0.4$, $P(\alpha_3')= P(\alpha_2)= 0.2$, τότε οι κωδικές λέξεις που αντιστοιχούν σε αυτό το αλφάβητο δίνονται από τον πίνακα

α_i	p_i	$c(\alpha_i)$
α_2	0.4	$c(\alpha_2)$
α_3'	0.4	a_2
α_1	0.2	$c(\alpha_1)$

- $c(\alpha_3')=a_3*0 \Rightarrow a_2= a_3*0$
- $c(\alpha_1)=a_3*1$
- Από το προηγούμενο βήμα έχουμε
  - $c(\alpha_3)=a_2*0 = a_3*00$
  - $c(\alpha_4)=a_2*10 = a_3*010$
  - $c(\alpha_5)=a_2*11 = a_3*011$
- Τέλος συνδυάζοντας τα α3΄ και α1 έχουμε

α_i	p_i	$c(\alpha_i)$
α_3''	0.6	a_3
α_2	0.4	$c(\alpha_2)$

- $c(\alpha_3'')=0 \Rightarrow a_3= 0$
- $c(\alpha_2)=1$
- Άρα ο συνολικός βέλτιστος κώδικας είναι

α_i	p_i	$c(\alpha_i)$
α_2	0.4	1
α_1	0.4	01
α_3	0.2	000
α_4	0.2	0010
α_5	0.2	0011

©2006, Σπύρος Δενάζης

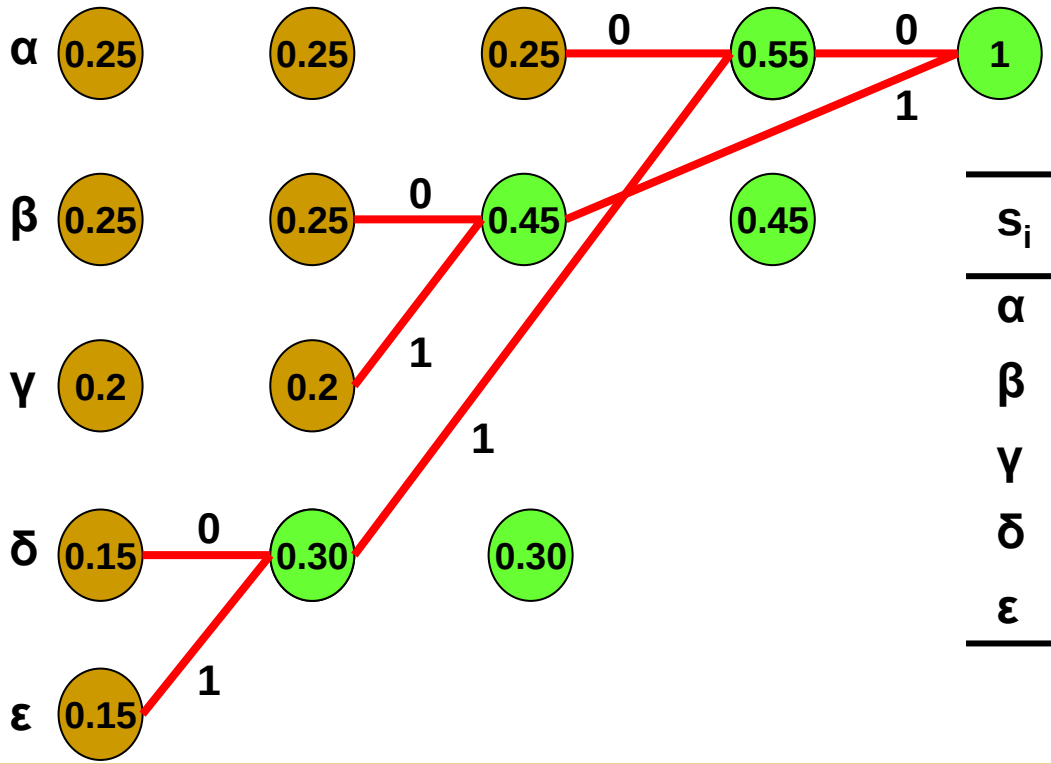
Κωδικοποίηση HUFFMAN ...

- **Αλγόριθμος κωδικοποίησης HUFFMAN**
  - Ο αλγόριθμος Huffman κατασκευάζει το δυαδικό δέντρο αρχίζοντας από τα φύλλα του και προχωράει προς τη ρίζα του.
  - **Βήμα 1ο**: Τα σύμβολα (ή τα μηνύματα) ταξινομούνται έτσι ώστε οι πιθανότητές τους είναι σε φθίνουσα ακολουθία.
  - **Βήμα 2ο**: Στη συνέχεια παίρνουμε τα δύο σύμβολα με τις μικρότερες πιθανότητες. Γι' αυτά μέσα από την διαδικασία του αλγορίθμου θα αναθέσουμε, τις μακρύτερες δυνατές κωδικές λέξεις έτσι ώστε αυτές να έχουν το ίδιο μήκος και να διαφέρουν στο τελευταίο τους ψηφίο.
    - Το βήμα αυτό θα δημιουργήσει το τελευταίο από τα ψηφία της κωδικής λέξης
  - **Βήμα 3ο**: Συνδυάζοντας τα δύο σύμβολα που επιλέξαμε στο βήμα 2 σε ένα και αναθέτοντας στο συνδυασμένο σύμβολο το άθροισμα των πιθανοτήτων των επιμέρους συμβόλων επαναλαμβάνουμε τη διαδικασία από το βήμα 1 μεταξύ των συμβόλων που απομένουν και του συμβόλου που δημιουργήσαμε μέχρις ότου καταλήξουμε σε ένα σύμβολο με πιθανότητα 1.
  - **Βήμα 4ο**: Οι κωδικές λέξεις που αντιστοιχούν στο κάθε σύμβολο αποτελούνται από τις ακολουθίες 0 και 1 που δημιουργούνται αν διατρέξουμε το δένδρο που δημιουργήθηκε από τον κόμβο με το μοναδικό σύμβολο προς τα σύμβολα από τα οποία ξεκινήσαμε

©2006, Σπύρος Δενάζης

Κωδικοποίηση HUFFMAN ...

- **Παράδειγμα**



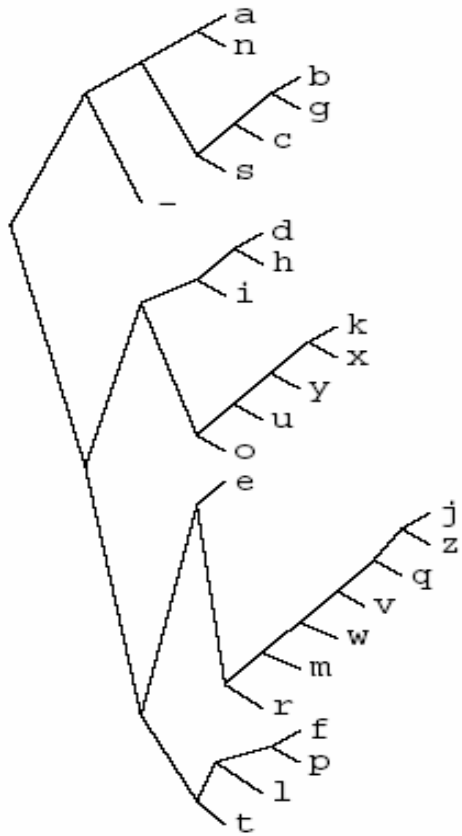
s_i	p_i	H	l_i	$C(s_i)$
α	0,25	2.0	2	00
β	0.25	2.0	2	10
γ	0.2	2.3	2	11
δ	0.15	2.7	3	010
ε	0.15	2.7	3	011
		2.2855	2.30	

©2006, Σπύρος Δενάζης

Κωδικοποίηση HUFFMAN ...

- Παράδειγμα
  - Παρατηρείστε τις διαφορές που υπάρχουν μεταξύ βέλτιστου μήκους και ελάχιστου μήκους
  - H(X)=4.11 bits
  - L(C,X)=4.15 bits

a_i	p_i	$\log_2 \frac{1}{p_i}$	l_i	$c(a_i)$
a	0.0575	4.1	4	0000
b	0.0128	6.3	6	001000
c	0.0263	5.2	5	00101
d	0.0285	5.1	5	10000
e	0.0913	3.5	4	1100
f	0.0173	5.9	6	111000
g	0.0133	6.2	6	001001
h	0.0313	5.0	5	10001
i	0.0599	4.1	4	1001
j	0.0006	10.7	10	1101000000
k	0.0084	6.9	7	1010000
l	0.0335	4.9	5	11101
m	0.0235	5.4	6	110101
n	0.0596	4.1	4	0001
o	0.0689	3.9	4	1011
p	0.0192	5.7	6	111001
q	0.0008	10.3	9	110100001
r	0.0508	4.3	5	11011
s	0.0567	4.1	4	0011
t	0.0706	3.8	4	1111
u	0.0334	4.9	5	10101
v	0.0069	7.2	8	11010001
w	0.0119	6.4	7	1101001
x	0.0073	7.1	7	1010001
y	0.0164	5.9	6	101001
z	0.0007	10.4	10	1101000001
–	0.1928	2.4	2	01



©2006, Σπύρος Δενάζης

Κωδικοποίηση HUFFMAN ...

- Παρατηρήσεις σχετικά με τον αλγόριθμο Huffman
  - Αποδεικνύεται ότι κανένας άλλος αλγόριθμος δεν μπορεί να οδηγήσει στην κατασκευή κώδικα με μικρότερο μέσο μήκος κωδικών λέξεων για ένα δεδομένο αλφάβητο πηγής.
  - Η κατασκευή του δένδρου γίνεται από τα φύλλα προς τη ρίζα του δένδρου,
  - Σε αντίθεση με τον αλγόριθμο FANO όπου δημιουργεί το δένδρο από τη ρίζα του προς τα φύλλα διαιρώντας κάθε φορά το σύνολο συμβόλων σε δύο σύνολα. Ένας τέτοιος αλγόριθμος είναι πάντα λιγότερο βέλτιστος.

©2006, Σπύρος Δενάζης

Κώδικες Ακολουθιών Συμβόλων.

- Μειονεκτήματα αλγορίθμου Huffman
  - Υπόθεση: Τα σύμβολα της πηγής παράγονται ανεξάρτητα το ένα από το άλλο. Τι γίνεται όμως αν τα σύμβολα αυτά εξαρτώνται από το ποια σύμβολα έχουν παραχθεί στο άμεσο παρελθόν;
  - Γνωρίζουμε ότι ο αλγόριθμος Huffman παράγει βέλτιστο κώδικα και άρα βάσει του θεωρήματος ισχύει ότι
    - $H(X) \leq L(C,X) < H(X)+1$
    - Άρα κατά μέσο όρο και ανά σύμβολο έχουμε πλεονάζοντα bits μεταξύ 0 και 1.
    - Αν η εντροπία H(X) της πηγής είναι μεγάλη τότε το πλεονάζον αυτό bit, L(C,X)-H(X), θα ήταν αμελητέο στην παραγωγή μηνυμάτων. Αν όμως η εντροπία είναι μικρότερη από 1 bit τότε το πλεονάζον bit θα ήταν καθοριστικό στην παραγωγή μηνυμάτων.
  - Χρειάζεται να ξέρουμε τις πιθανότητες εμφάνισης εκ των προτέρων. Αν όχι τότε θα πρέπει να συλλέξουμε πρώτα τα στατιστικά μιας πηγής και μετά να εφαρμόσουμε τον αλγόριθμο
- **Έτσι λοιπόν παρόλο που οι κώδικες Huffman θεωρούνται βέλτιστοι αυτό αφορά στην παραγωγή συμβόλων και όχι στην παραγωγή μηνυμάτων που είναι και αυτό που χρειαζόμαστε στην πράξη.**

©2006, Σπύρος Δενάζης

Κώδικες Ακολουθιών Συμβόλων...

- **<u>Παράδειγμα</u>**
  - Έστω μία πηγή με αλφάβητο $A=\{\alpha_1,\alpha_2,\alpha_3\}$ και $P=\{0.8,0.02,0.18\}$.
  - $H(A)=0,816$ bits/symbol
  - Εφαρμόζοντας τον αλγόριθμο του Huffman παίρνουμε τις εξής κωδικές λέξεις και μήκη

α_i	p_i	H	l_i	$C(\alpha_i)$
α_1	0.8	0.322	1	0
α_2	0. 02	5.644	2	11
α_3	0.18	2.474	2	10
		0,816	1,2	
		H(A)	L(C,A)	

  - Παρατηρούμε ότι το μέσο μήκος κωδικής λέξης είναι 1.2 bits/symbol το οποίο απέχει κατά 47% από την εντροπία δηλαδή υπάρχει πλεονασμός κατά 0.384 bits/symbol.
  - Σε επίπεδο μηνυμάτων (ακολουθίες συμβόλων) αυτός ο πλεονασμός παίζει καθοριστικό ρόλο
    - Π.χ. Για ακολουθίες μηνυμάτων που αποτελούνται από N=1000 σύμβολα τότε σύμφωνα με την κωδικοποίηση κατά Huffman θα παράγαμε κατά μέσο όρο 384 bits περισσότερα από τα 816 που είναι τα αναγκαία
  - Τι πρέπει να γίνει;

©2006, Σπύρος Δενάζης

Κώδικες Ακολουθιών Συμβόλων...

- **Παράδειγμα (συνέχεια)**
  - Να εφαρμόσουμε τον αλγόριθμο όχι σε επίπεδο συμβόλων αλλά σε επίπεδο μηνυμάτων.
  - Έτσι για μηνύματα δύο συμβόλων έχουμε
  - Το μέσο μήκος κάθε κωδικής λέξης που αντιστοιχεί σε μήνυμα 2 συμβόλων είναι 1.7228 bits και άρα κάθε σύμβολο το μέσο μήκος κωδικής λέξης ανά σύμβολο είναι 1.7228/2=0.8614 bits το οποίο συγκρινόμενο με την εντροπία H(A)=0.816 είναι μόλις κατά 5.5% προσαυξημένο
  - Το πρόβλημα που παρουσιάζει αυτή η μέθοδος στην πράξη είναι ότι χρειάζεται να υπολογίσουμε όλες τις πιθανότητες των πιθανών μηνυμάτων. Για ένα αλφάβητο με n σύμβολα και μηνύματα μήκους m τότε το σύνολο όλων των μηνυμάτων είναι m^n, δηλαδή για ένα αλφάβητο 5 συμβόλων και μηνύματα μήκους 10 θα χρειαστεί να υπολογίσουμε περίπου 10 εκ. πιθανότητες πρώτα!!

α_i	p_i	H	l_i	$C(\alpha_i)$
$\alpha_1\alpha_1$	0.64	0.644	1	0
$\alpha_1\alpha_2$	0. 016	5.966	5	10101
$\alpha_1\alpha_3$	0.144	2.796	2	11
$\alpha_2\alpha_1$	0.016	5.966	6	101000
$\alpha_2\alpha_2$	0. 0004	11.288	8	10100101
$\alpha_2\alpha_3$	0.0036	8.118	7	1010011
$\alpha_3\alpha_1$	0. 144	2.796	3	100
$\alpha_3\alpha_2$	0.0036	8.118	8	10100100
$\alpha_3\alpha_3$	0.0324	4.948	4	1011
		1,632	1,7228	
		$H(A^2)$	$L(C,A^2)$	
		2*H(A)	$L(C,A^2)/2=0,861$	

©2006, Σπύρος Δενάζης

Θεώρημα Κωδικοποίησης Πηγής ...

- **<u>Θεώρημα Shannon Κωδικοποίησης Πηγής</u>**
  - Έστω X μια τ.μ. παραγωγής συμβόλων πηγής με εντροπία H(X)=*H* bits. Για κάθε δ>0 και 0<θ<1, υπάρχει ένας θετικός ακέραιος αριθμός N_0, τέτοιος ώστε για κάθε $N>N_0$, ισχύει

$$\left|\frac{1}{N}\Pi_{\theta}\left(\mathrm{X}^{\mathrm{N}}\right)-H\right|<\delta$$

©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...

- Οι πηγές παραγωγής συμβόλων που συναντήσαμε μέχρι τώρα υποθέταμε ότι παράγουν ακολουθίες συμβόλων στις οποίες το κάθε σύμβολο έχει παραχθεί ανεξάρτητα από το τι έχει συμβεί στο παρελθόν.
- Τέτοιου είδους πηγές δεν αντιστοιχούν σε πραγματικά φαινόμενα αφού συνήθως η παραγωγή συμβόλων πηγής παρουσιάζει στατιστικές εξαρτήσεις μεταξύ των.
- Οι εξαρτήσεις αυτές μπορεί να επηρεάζουν την παραγωγή συμβόλων τα οποία είτε απέχουν μεγάλα χρονικά διαστήματα μεταξύ τους είτε μόλις λίγα σύμβολα.
- Μια ειδική περίπτωση είναι όταν η παραγωγή ενός συμβόλου παρουσιάζει στατιστικές εξαρτήσεις μόνο με το αμέσως προηγούμενό του.
- Τέτοιου είδους διαδικασίες ονομάζονται Μαρκοβιανές διαδικασίες ή αλυσίδες και οι πηγές οι οποίες υπόκεινται σε αυτές, πηγές Markoff

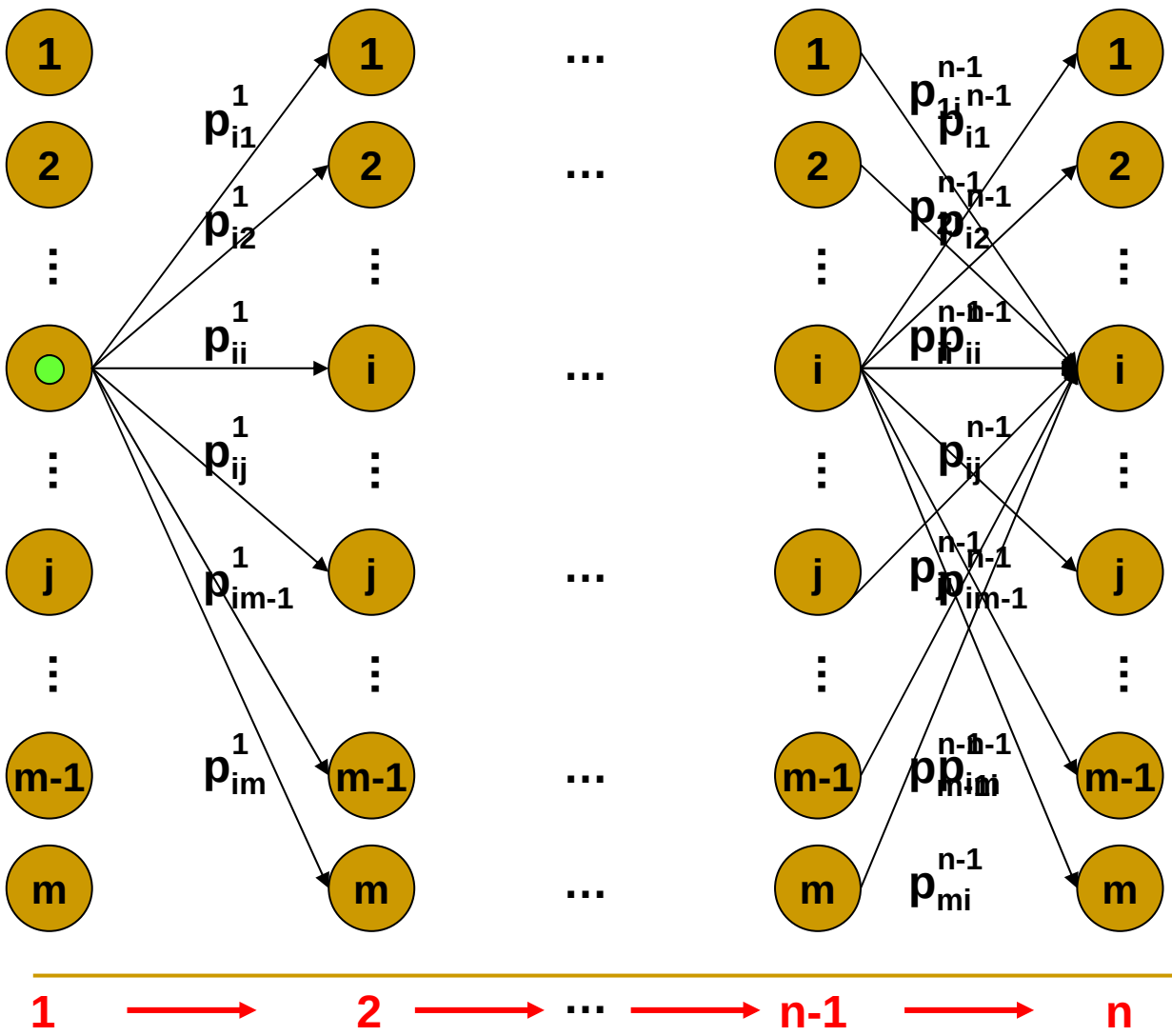
©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...

- **Διαδικασίες Markoff**
  - Έστω $\{Y_1,Y_2,...,Y_n\}$ μια ακολουθία τ.μ. Έτσι ώστε κάθε μία τ.μ. Y_i, $i=1,2,\ldots,n$, παίρνει τιμές από το σύνολο συμβόλων $S=\{s_1,s_2, \ldots,s_m\}$
  - Η τυχαία αυτή διαδικασία ορίζεται από τη συνδυασμένη συνάρτηση μάζας πιθανότητας
    - $P\{(Y_1,Y_2,...,Y_n)=(y_1,y_2,...,y_n)\}=p(y_1,y_2,...,y_n)$, $y_i \in S$
  - Εάν ισχύει ότι
    - $P\{Y_{n+1}= y_{n+1}/ Y_n= y_n, Y_{n-1}= y_{n-1},\ldots, Y_1= y_1\}= P\{Y_{n+1}= y_{n+1}/ Y_n= y_n)$
    - Τότε λέμε ότι η $\{Y_1,Y_2,...,Y_n\}$ είναι μία διαδικασία Markoff
  - Εφαρμόζοντας επαναληπτικά το τύπο που συνδέει τη συνδυασμένη συνάρτηση μάζας πιθανότητας με την εξαρτημένη βρίσκουμε ότι
    - $p(y_1,y_2,...,y_n)= p(y_n/y_{n-1})\, p(y_{n-1}/y_{n-2}) \ldots p(y_2/y_1)\, p(y_1)$

©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...



$$p_i(n) = \sum_{j=1}^{m} p_j(n-1)\, p_{ji}^{n-1}$$

Χρονικά Αμετάβλητη Μαρκοβιανή Αλυσίδα
Πίνακας Μετάβασης

$$P = [P_{ij}]$$

Στατική Μαρκοβιανή Αλυσίδα

$$\pi = \pi P$$

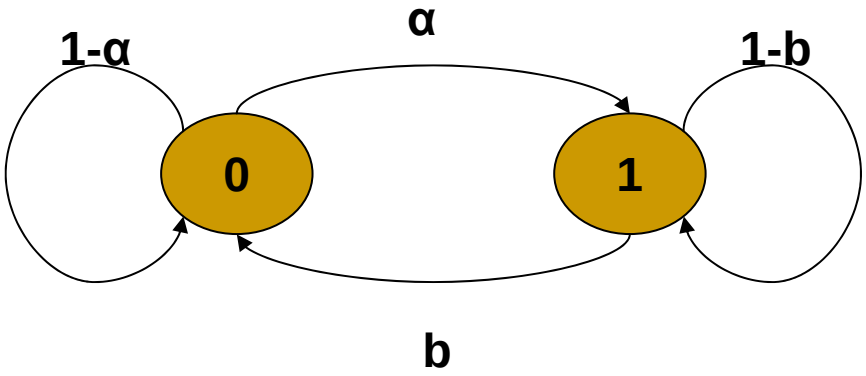
1 → 2 → ... → n-1 → n

©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...

- **Παράδειγμα**
  - Έστω μία στατική πηγή Markoff με πίνακα μετάβασης

$$P = \left[P_{ij}\right] = \begin{bmatrix} 1-a & a \\ b & 1-b \end{bmatrix}$$



$$\begin{bmatrix} \pi_0 & \pi_1 \end{bmatrix} = \begin{bmatrix} \pi_0 & \pi_1 \end{bmatrix} \begin{bmatrix} 1-a & a \\ b & 1-b \end{bmatrix}$$

$$\pi_0 = (1-a)\pi_0 + b\pi_1$$

$$\pi_1 = a\pi_0 + (1-b)\pi_1$$

$$\pi_0 + \pi_1 = 1$$

$$\boxed{\pi_0 = \frac{a}{a+b}}$$

$$\boxed{\pi_1 = \frac{b}{a+b}}$$

©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...

- **Εντροπία των πηγών Markoff**
  - Η εντροπία της πηγής ορίζεται ως ο μέσος όρος της εντροπίας συμβόλων που εκπέμπονται από κάθε κατάσταση
  - Εάν X, Y είναι τ.μ των συμβόλων που εκπέμπονται από την πηγή Markoff τότε ισχύει
    - $$H(X/Y=i) = -\sum_{j=1}^{m} P_{ij} \log P_{ij} \quad bits/symbol$$
    - $$H(X/Y) = \sum_{i=1}^{m} \pi_i \sum_{j=1}^{m} P_{ij} \log P_{ij} \quad bits/symbol$$

©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...

- **Μηνύματα που παράγονται από πηγές Markoff**
  - Έστω X η τ.μ. μιας πηγής συμβόλων {0,1}
  - X^N, η τ.μ. που συμβολίζει όλες τις ακολουθίες συμβόλων ‘0’ και ‘1’, μήκους N.
    - Το πλήθος των ακολουθιών συμβόλων ‘0’ και ‘1’, μήκους N, που μπορούν να δημιουργηθούν είναι 2^N.
  - Εάν m_i, i=1,2,…,2^N είναι μία από τις ακολουθίες της X^N, τότε η εντροπία της πηγής που παράγει μηνύματα μήκους N είναι
    - $$\boxed{H\left(X^N\right) = -\sum_{i=1}^{2^N} p(m_i)\log\, p(m_i)}$$
  - Η μέση ποσότητα πληροφορίας ανά σύμβολο είναι
    - $$\boxed{\frac{1}{N}H\left(X^N\right)}$$
  - **Πρόταση**
    - Η Μέση ποσότητα πληροφορίας των συμβόλων της πηγής $H(X^N)$, η οποία είναι μία μονότονα αύξουσα συνάρτηση του N, ισχύει
      - $$\lim_{N\to\infty}\left(\frac{1}{N}H\left(X^N\right)\right) = \sum_{i=1}^{m}\pi_i\sum_{j=1}^{m}P_{ij}\log P_{ij} \quad bits/symbol$$

©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...

- **Παράδειγμα**
  - Έστω μία στατική πηγή Markoff η οποία παράγει τα σύμβολα φ, χ, ψ, βάσει του πίνακα μετάβασης

$$\begin{array}{c|ccc} & \varphi & \chi & \psi \\ \hline \varphi & 1/2 & 1/2 & 0 \\ \chi & 1/4 & 0 & 3/4 \\ \psi & 1/3 & 1/3 & 1/3 \end{array}$$

$$\pi = \pi P,$$

$$\left[\pi_\varphi = 10/27, \quad \pi_\chi = 8/27, \quad \pi_\psi = 9/27\right]$$

$P(\chi\psi)=P(\psi/\chi)\pi_\chi=(3/4)*(8/27)$

X^2	p_i	$H(x_i^2)$	l_i	$C(s_i)$ (FANO)
φφ	5/27	2.433	2	01
φχ	5/27	2.433	3	100
φψ	0	0	-	-
χφ	2/27	3.755	4	1011
χχ	0	0	-	-
χψ	6/27	2.17	2	00
ψφ	3/27	3.17	3	110
ψχ	3/27	3.17	3	111
ψψ	3/27	3.17	4	1010
		2.72	2.78	(1.39 bits/symbol)
		$H(X^2)$	$L(C,X^2)$	

©2006, Σπύρος Δενάζης

Διακριτές Πηγές Πληροφορίας Με Μνήμη ...

- **Παράδειγμα (συνέχεια)**
  - Εφαρμόζοντας τον αλγόριθμο Huffman για κάθε σύμβολο φ, χ, ψ ξεχωριστά τότε

X	π_i	$H(x_i)$	l_i	$C(s_i)$
φ	10/27	1.433	1	0
χ	8/27	1.756	2	10
ψ	9/27	1.585	2	11
		1.58	1.63	
		H(X)	L(C,X)	

$H(X^2)$	2.72
$L(C,X^2)$	2.78
$L(C,X^2)/2$	1.39
H(X)	1.58
L(C,X)	1.63
2*L(C,X)	3.26
H(X/Y)	1.14

?

$$\pi_\varphi\left[p_{\varphi\varphi}\log p_{\varphi\varphi}+p_{\varphi\chi}\log p_{\varphi\chi}+p_{\varphi\psi}\log p_{\varphi\psi}\right]+$$
$$\pi_\chi\left[p_{\chi\varphi}\log p_{\chi\varphi}+p_{\chi\chi}\log p_{\chi\chi}+p_{\chi\psi}\log p_{\chi\psi}\right]+$$
$$\pi_\psi\left[p_{\psi\varphi}\log p_{\psi\varphi}+p_{\psi\chi}\log p_{\psi\chi}+p_{\psi\psi}\log p_{\psi\psi}\right]$$

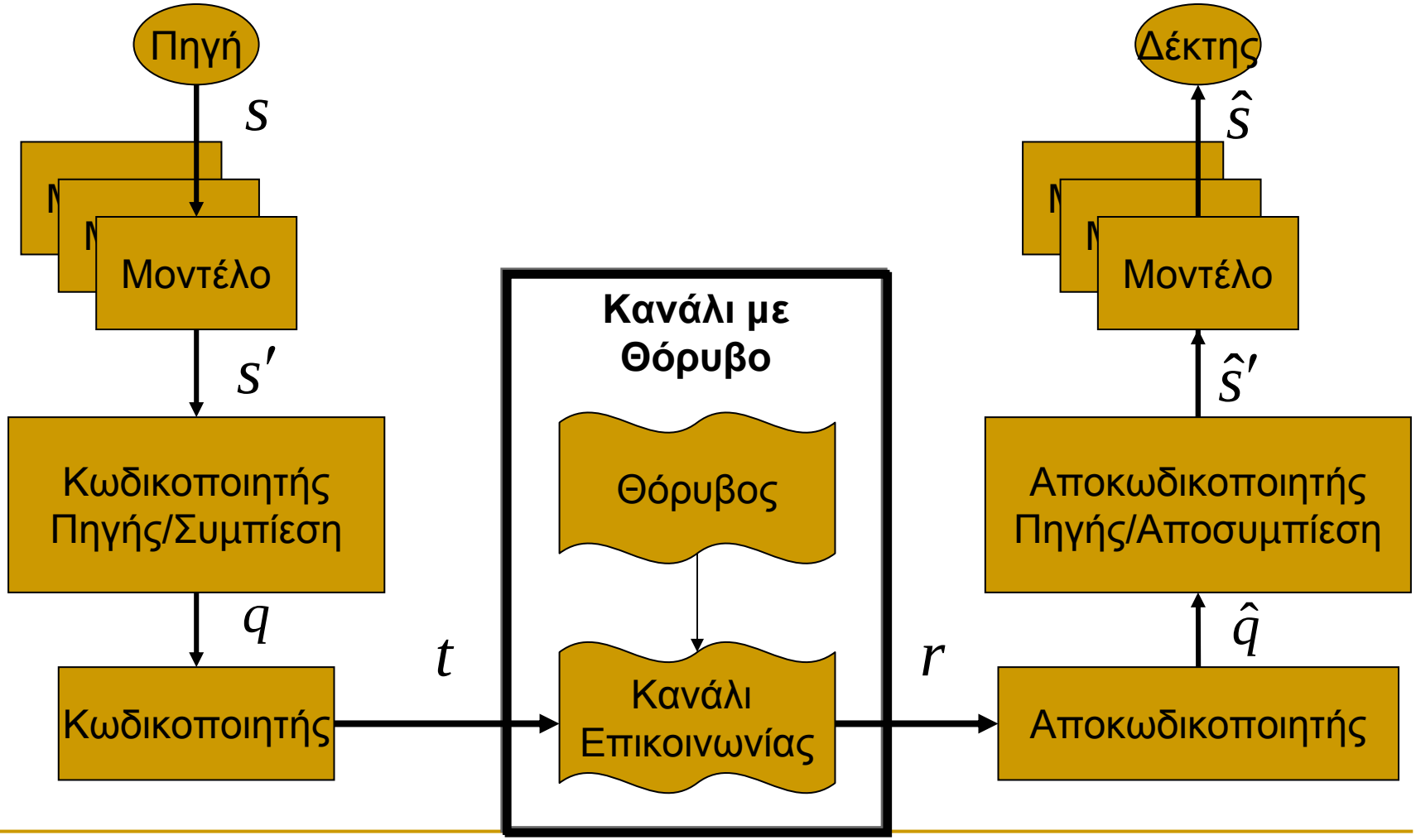
©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας

- Διακριτά Κανάλια Επικοινωνίας Χωρίς Μνήμη
- Σχέσεις Πληροφορίας εισόδου – εξόδου
- Αμοιβαία Πληροφορία
- Χωρητικότητα διακριτών καναλιών χωρίς μνήμη
- Θεμελιώδες Θεώρημα Πληροφορίας

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...



©2006, Σπύρος Δενάζης

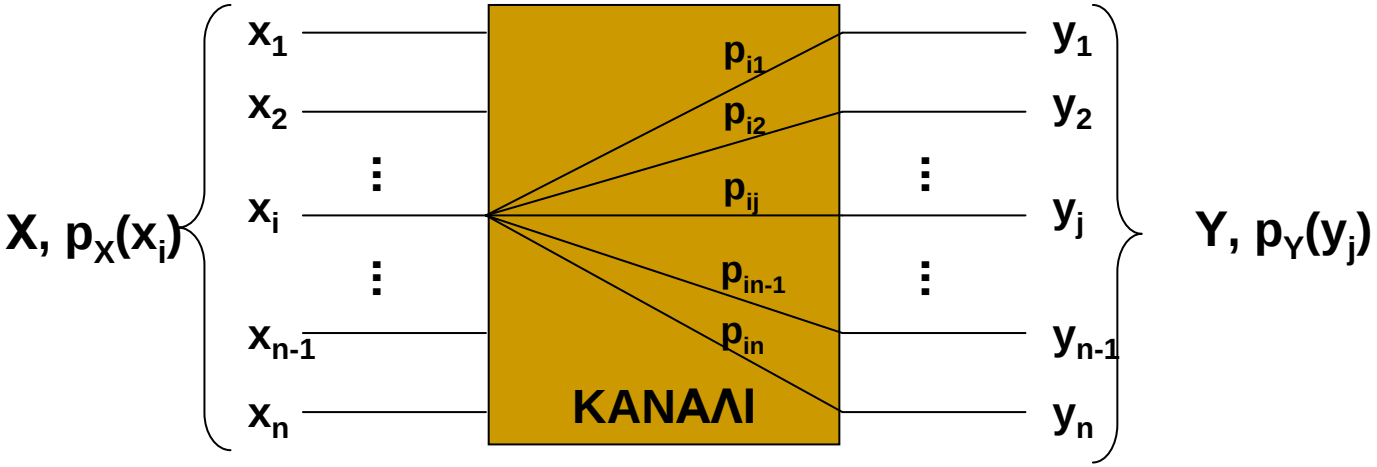
Κανάλια Επικοινωνίας ...

- Είδη Καναλιών
  - Διακριτά Κανάλια
    - Χωρίς Μνήμη
    - Με Μνήμη
  - Συνεχή Κανάλια
    - Χωρίς Μνήμη
    - Με Μνήμη
- Ποσότητα πληροφορίας που μεταφέρεται πάνω από ένα κανάλι χωρίς μνήμη
- Χωρητικότητα διακριτού Καναλιού, C, παρουσία θορύβου.
- 2° Θεμελιώδες θεώρημα κωδικοποίησης καναλιού του Shannon
- Χωρητικότητα συνεχούς Καναλιού, C, παρουσία προσθετικού θορύβου

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- Διακριτά Κανάλια Χωρίς Μνήμη



$$[p_{Y/X}(y_j/x_i)]=[p_{ij}]=[P_{Y/X}]$$

$$[P_Y]=[P_X]\,[P_{Y/X}]$$

$$[P_X]=[p_X(x_1)\ p_X(x_2)\ \dots\ p_X(x_N)\ ]$$

$$[P_Y]=[p_Y(y_1)\ p_Y(y_2)\ \dots\ p_Y(y_N)\ ]$$

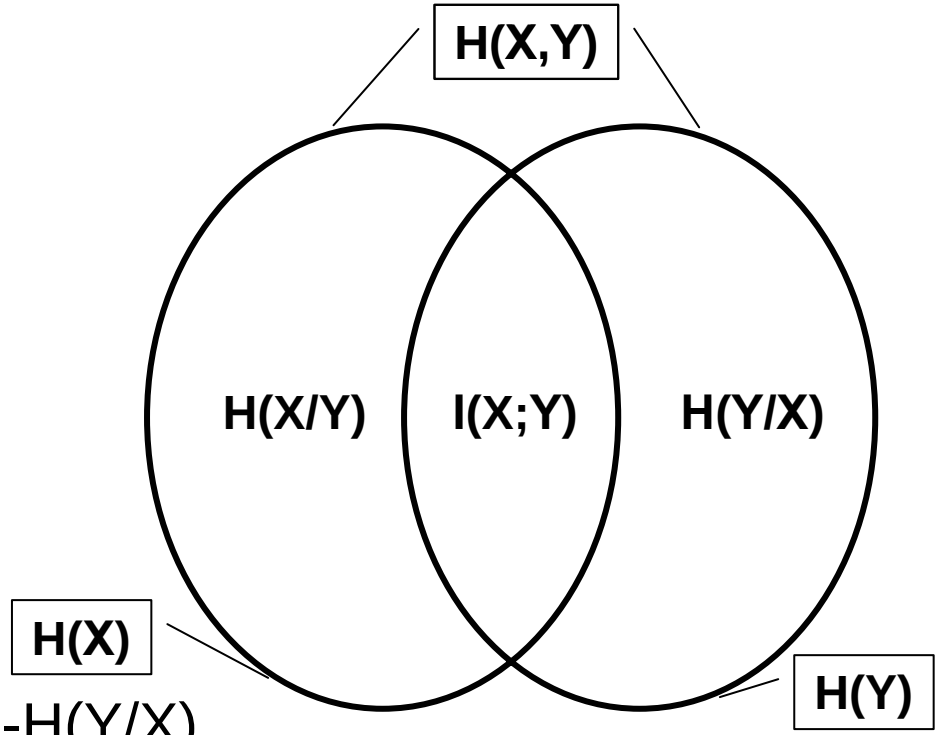
$$p_Y(y_j)=\sum_{i=1}^{N} p_X(x_i)p_{ij},\ j=1,\dots,N$$

Συγκρίνετε αυτούς τους τύπους με τους αντίστοιχους της στατικής Μαρκοβιανής αλυσίδας

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **<u>Υπενθύμιση</u>**
  - Συνδυασμένη Εντροπία
    - $\mathrm{H}(\mathrm{X},\mathrm{Y}) = -\sum_x \sum_y p(x,y) \log p(x,y)$
    - H(X,Y)=H(X)+H(Y/X)
  - Δεσμευμένη Εντροπία
    - $\mathrm{H}(\mathrm{X}/\mathrm{Y}) = -\sum_x \sum_y p(x,y) \log p(x/y)$
  - Αμοιβαία Πληροφορία
    - I(X;Y)= H(X)-H(X/Y)=H(Y)-H(Y/X)
    - Είναι το μέγεθος εκείνο που μετράει το ποσό της μείωσης της αβεβαιότητας της X όταν γίνει γνωστό το Y.
    - Τη μέση πληροφορία της X που μεταφέρεται στη Y.



©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***<u>Δυαδικό κανάλι χωρίς θόρυβο</u>***

$$x_1 \quad 0 \xrightarrow{1} 0 \quad y_1$$

X, $p_X(x_i)$ **Y, $p_Y(y_j)$**

$$x_2 \quad 1 \xrightarrow[1]{} 1 \quad y_2$$

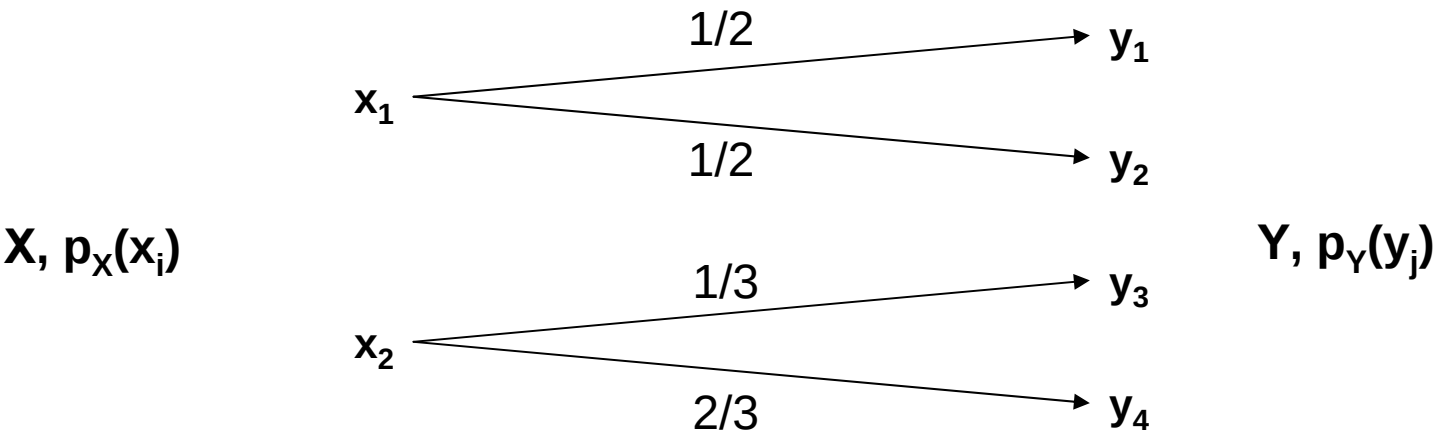
$$\begin{bmatrix} p_Y(0) & p_Y(1) \end{bmatrix} = \begin{bmatrix} p_x(0) & p_x(1) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$p_Y(0) = p_x(0)$$
$$p_Y(1) = p_x(1)$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***<u>Ενθόρυβο κανάλι με μη επικαλυπτόμενες εξόδους</u>***



$$\begin{bmatrix} p_Y(y_1) & p_Y(y_2) & p_Y(y_3) & p_Y(y_4) \end{bmatrix} = \begin{bmatrix} p_x(x_1) & p_x(x_2) \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/3 & 2/3 \end{bmatrix}$$

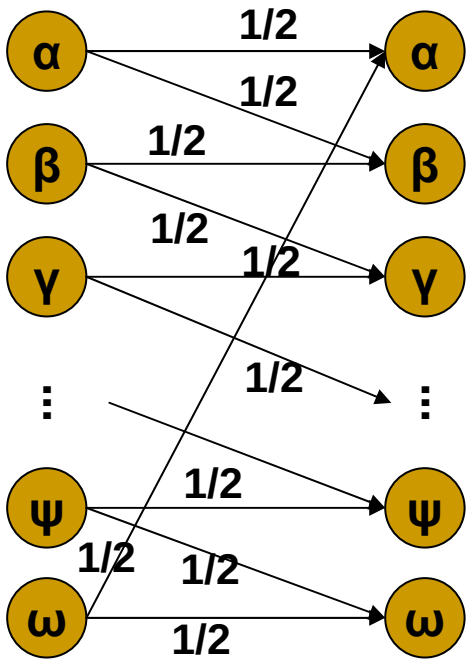
$$p_Y(y_1) = \frac{1}{2} p_x(x_1), \quad p_Y(y_2) = \frac{1}{2} p_x(x_1)$$

$$p_Y(y_3) = \frac{1}{3} p_x(x_2), \quad p_Y(y_4) = \frac{2}{3} p_x(x_2)$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***<u>Ενθόρυβη Γραφομηχανή</u>***
    - {α,β,γ,δ,...,χ,ψ,ω}

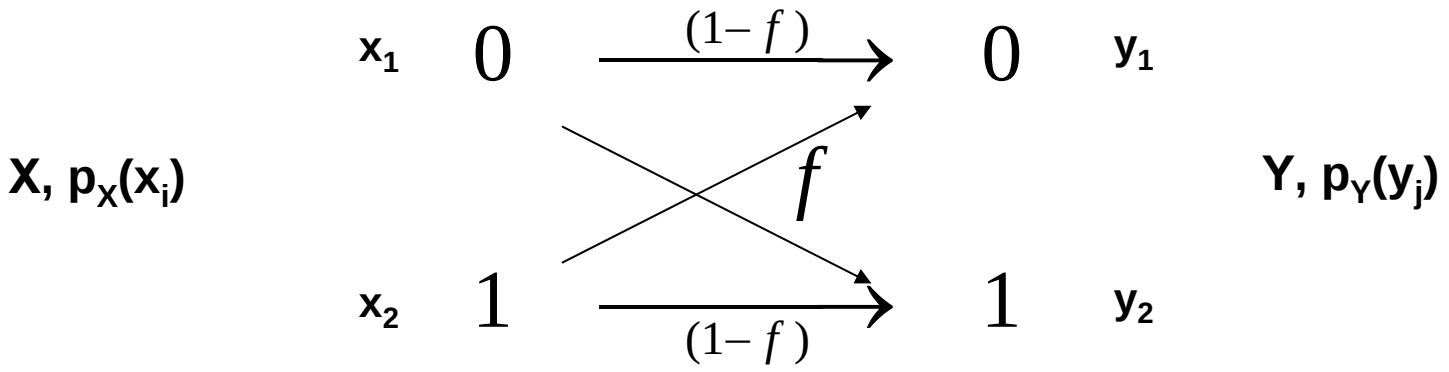


$$
\begin{array}{c}
 \\ \alpha \\ \beta \\ \gamma \\ \delta \\ \varepsilon \\ \vdots \\ \chi \\ \psi \\ \omega
\end{array}
\begin{array}{c}
\begin{array}{ccccccccc} \alpha & \beta & \gamma & \delta & \varepsilon & \cdots & \chi & \psi & \omega \end{array} \\
\begin{bmatrix}
1/2 & 1/2 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 1/2 & 1/2 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 1/2 & 1/2 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 1/2 & 1/2 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1/2 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & 0 & \cdots & 1/2 & 1/2 & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1/2 & 1/2 \\
1/2 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1/2
\end{bmatrix}
\end{array}
$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***<u>Δυαδικό συμμετρικό κανάλι</u>***



$$\begin{bmatrix} p_Y(0) & p_Y(1) \end{bmatrix} = \begin{bmatrix} p_x(0) & p_x(1) \end{bmatrix} \begin{bmatrix} 1-f & f \\ f & 1-f \end{bmatrix}$$

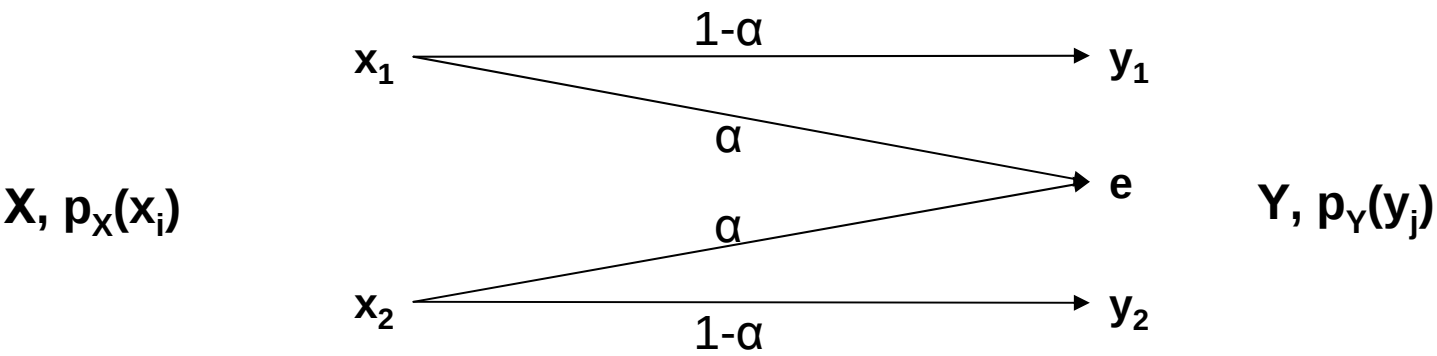
$$p_Y(0) = (1-f)p_x(0) + fp_x(1)$$

$$p_Y(1) = fp_x(0) + (1-f)p_x(1)$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***<u>Δυαδικό κανάλι με αποσβέσεις</u>***



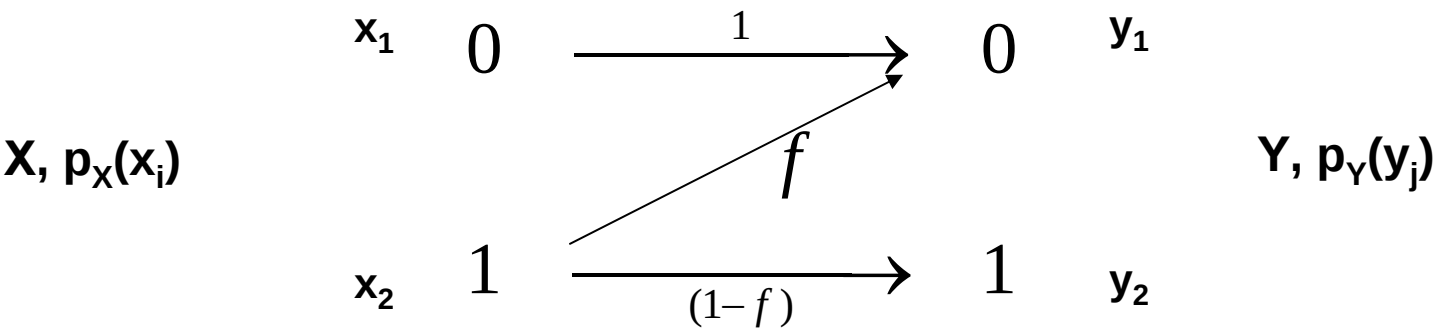
$$\begin{bmatrix} p_Y(y_1) & p_Y(e) & p_Y(y_2) \end{bmatrix} = \begin{bmatrix} p_x(x_1) & p_x(x_2) \end{bmatrix} \begin{bmatrix} 1-a & a & 0 \\ 0 & a & 1-a \end{bmatrix}$$

$$p_Y(y_1) = (1-a)p_x(x_1),$$
$$p_Y(e) = a(p_x(x_1) + p_x(x_2)) = a,$$
$$p_Y(y_2) = (1-a)p_x(x_2)$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***Το κανάλι Z***



$$[p_Y(0) \quad p_Y(1)] = [p_x(0) \quad p_x(1)] \begin{bmatrix} 1 & 0 \\ f & 1-f \end{bmatrix}$$

$$p_Y(0) = p_x(0) + f p_x(1)$$
$$p_Y(1) = (1-f) p_x(1)$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***Συμμετρικά κανάλια***
  - ***Ορισμοί***
    - Ένα κανάλι λέγεται *συμμετρικό* εάν οι γραμμές του πίνακα μετάβασης $[p_{ij}]=[P_{Y/X}]$ μπορούν να προκύψουν από συνδυασμούς των στοιχείων της κάθε γραμμής και το ίδιο να συμβαίνει και για τις στήλες
    - Ένα κανάλι λέγεται *μερικώς συμμετρικό* (weakly symmetric) εάν εάν οι γραμμές του πίνακα μετάβασης $[p_{ij}]=[P_{Y/X}]$ μπορούν να προκύψουν από συνδυασμούς των στοιχείων της κάθε γραμμής και το άθροισμα των στοιχείων της κάθε στήλης να είναι πάντα το ίδιο

Συμμετρικό Κανάλι

$$[p_{ij}]=\begin{bmatrix} 0.3 & 0.2 & 0.5 \\ 0.5 & 0.3 & 0.2 \\ 0.2 & 0.5 & 0.3 \end{bmatrix}$$

Μερικώς Συμμετρικό Κανάλι

$$[p_{ij}]=\begin{bmatrix} \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \end{bmatrix}$$

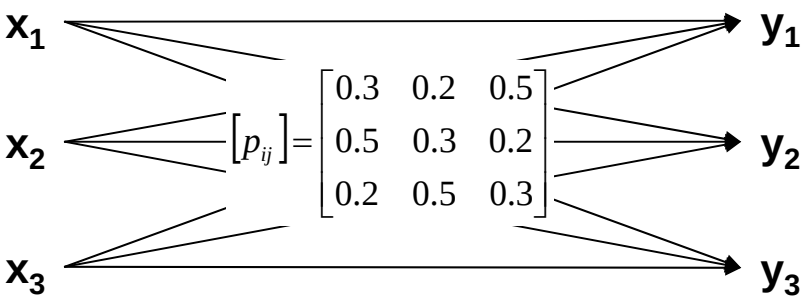
$$\begin{matrix} \| & \| & \| \\ \frac{2}{3} & \frac{2}{3} & \frac{2}{3} \end{matrix}$$

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***<u>Συμμετρικό κανάλι</u>***

X, $p_X(x_i)$



Y, $p_Y(y_j)$

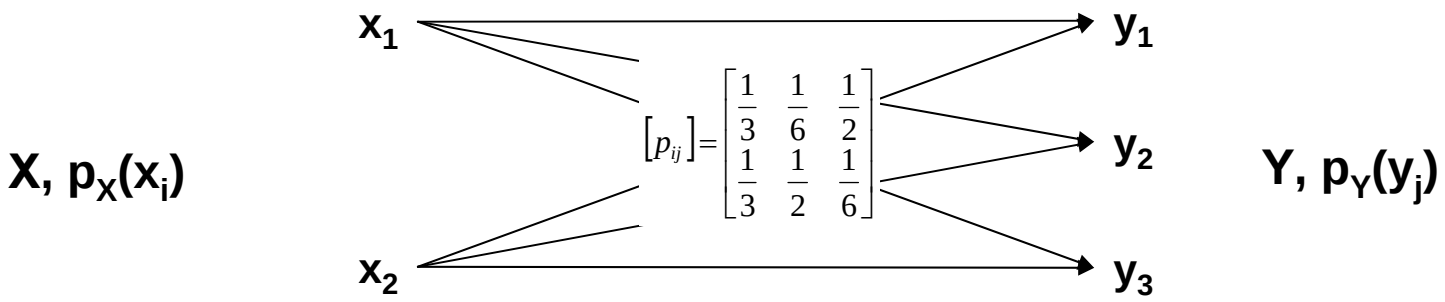
$$\begin{bmatrix} p_Y(y_1) & p_Y(y_2) & p_Y(y_3) \end{bmatrix} = \begin{bmatrix} p_x(x_1) & p_x(x_2) & p_x(x_3) \end{bmatrix} \begin{bmatrix} 0.3 & 0.2 & 0.5 \\ 0.5 & 0.3 & 0.2 \\ 0.2 & 0.5 & 0.3 \end{bmatrix}$$

$$p_Y(y_1) = 0.3\,p_x(x_1) + 0.5\,p_x(x_2) + 0.2\,p_x(x_3),$$
$$p_Y(y_2) = 0.2\,p_x(x_1) + 0.3\,p_x(x_2) + 0.5\,p_x(x_3),$$
$$p_Y(y_3) = 0.5\,p_x(x_1) + 0.2\,p_x(x_2) + 0.3\,p_x(x_3)$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **Παραδείγματα Διακριτών Καναλιών**
  - ***Μερικώς Συμμετρικό κανάλι***



$$\begin{bmatrix} p_Y(y_1) & p_Y(y_2) & p_Y(y_3) \end{bmatrix} = \begin{bmatrix} p_x(x_1) & p_x(x_2) \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6} \end{bmatrix}$$

$$p_Y(y_1) = \frac{1}{3} p_x(x_1) + \frac{1}{3} p_x(x_2),$$

$$p_Y(y_2) = \frac{1}{6} p_x(x_1) + \frac{1}{2} p_x(x_2),$$

$$p_Y(y_3) = \frac{1}{2} p_x(x_1) + \frac{1}{6} p_x(x_2)$$

©2006, Σπύρος Ξενάζης

Κανάλια Επικοινωνίας ...

- **<u>Πιθανότητες Εισόδου Καναλιού εάν γνωρίζουμε την έξοδο (Κανόνας Bayes)</u>**
- $$p(x/y)=\frac{p(x,y)}{p(y)}=\frac{p(y/x)p(x)}{p(y)}=\frac{p(y/x)p(x)}{\sum_{x'}p(y/x')p(x')}$$
- **1.** Έστω ένα **<u>δυαδικό συμμετρικό κανάλι</u>** επικοινωνίας όπου *f*=0.15 και $P_X=\{p_X(0)=0.9,\ p_X(1)=0.1\}$. Υποθέτοντας ότι y=1 τότε είναι δυνατόν να υπολογίσουμε την πιθανότητα το σύμβολο που μεταδόθηκε να ήταν επίσης 1
  - $$p(x=1/y=1)=\frac{p(x=1,y=1)}{p(y=1)}=\frac{p(y=1/x=1)p(x=1)}{p(y=1)}=\frac{p(y=1/x=1)p(x=1)}{\sum_{i=0,1}p(y=1/x=i)p(x=i)}$$
  - $$p(x=1/y=1)=\frac{0.85\times 0.1}{0.85\times 0.1+0.85\times 0.9}=0.39$$
- **2.** Έστω ένα **<u>κανάλι επικοινωνίας Z</u>** όπου *f*=0.15 και $P_X=\{p_X(0)=0.9,\ p_X(1)=0.1\}$. Υποθέτοντας ότι y=1 τότε είναι δυνατόν να υπολογίσουμε την πιθανότητα το σύμβολο που μεταδόθηκε να ήταν επίσης 1
  - $$p(x=1/y=1)=\frac{0.85\times 0.1}{0.85\times 0.1+0.85\times 0}=1.0$$

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **<u>Πληροφορία η οποία μεταφέρεται από το κανάλι.</u>**
  - Με τον όρο πληροφορία πάνω από το κανάλι εννοούμε το ποσοστό της πληροφορίας που μεταφέρεται τελικά χωρίς λάθος μέσα από το κανάλι.
  - Στόχος μας είναι να βρούμε τρόπους ώστε τα bits τα οποία στέλνουμε να μπορούν να ανακτηθούν (παραληφθούν) με πολύ μικρή πιθανότητα λάθους.
  - Με άλλα λόγια θέλουμε να μετρήσουμε την πληροφορία η οποία σχετίζεται με τη X (είσοδος στο κανάλι) και η οποία εμπεριέχεται στην Y (έξοδος στο κανάλι) δηλ. την αμοιβαία πληροφορία I(X;Y)
    - **I(X;Y)=H(X)-H(X/Y)=H(Y)-H(Y/X)**
  - Πρακτικά αυτό που μας ενδιαφέρει είναι να βρούμε τρόπους έτσι ώστε τα bits (η πληροφορία) τα οποία στέλνονται πάνω από το κανάλι να μπορούν να ανακτηθούν με τέτοιο τρόπο ουτοσώστε η πιθανότητα λάθους να είναι αμελητέα.
  - Αντί του συμβολισμού I(X;Y) χρησιμοποιείται και ο συμβολισμός R και τότε μιλάμε για **ρυθμό μετάδοσης**

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- Ορισμένες ερμηνείες σχετικά με τις ποσότητες της πληροφορίας
  - H(X/Y): Καλείται και **αβεβαιότητα** αφού εκφράζει ακριβώς το πόσο αβέβαιοι είμαστε ως προς το σύμβολο της εισόδου x αν στην έξοδο έχει ληφθεί το y. Σχετίζεται με τις *εκ των υστέρων* πιθανότητες
  - H(Y/X): Μπορεί να εκληφθεί και ως μέση αβεβαιότητα ως προς το y αν είναι γνωστό το x.
  - H(X), H(Y) αντιπροσωπεύουν την μέση ποσότητα πληροφορίας που μεταφέρεται από τις εισόδους και τις εξόδους του συστήματος και κατ' αντιστοιχία τον μέσο αριθμό bits κάθε κωδικής λέξης.
  - I(X;Y): Η Αμοιβαία πληροφορία συμβολίζει το πληροφορικό περιεχόμενο που μεταδόθηκε τελικά πάνω από το κανάλι, δηλ. H(X)-H(X/Y)

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **<u>Αμοιβαία Πληροφορία Καναλιών</u>**
  - **1.** Έστω ένα **<u>δυαδικό συμμετρικό κανάλι</u>** επικοινωνίας όπου f=0.15
  - *<u>Περίπτωση 1η</u>*: $P_X=\{p_X(0)=0.9, p_X(1)=0.1\}$.
    - Εφαρμόζοντας τον τύπο με τους πίνακες είναι δυνατόν να υπολογίσουμε $P_Y=\{p_Y(0)=0.78, p_Y(1)=0.22\}$.
    - I(X;Y)=H(Y)-H(Y/X)=H(0.22)-H(0.15)=0.76-0.61=<u>0.15 bits</u>
    - H(X)=0.47 bits
  - *<u>Περίπτωση 2η</u>*: $P_X=\{p_X(0)=0.5, p_X(1)=0.5\}$.
    - Εφαρμόζοντας τον τύπο με τους πίνακες είναι δυνατόν να υπολογίσουμε $P_Y=\{p_Y(0)=0.5, p_Y(1)=0.5\}$.
    - I(X;Y)=H(Y)-H(Y/X)= H(0.5)-H(0.15)=1-0.61=<u>0.39 bits</u>
    - H(X)=1 bit
  - Παρατηρούμε ότι η αμοιβαία πληροφορία παίρνει την μέγιστη τιμή της στη $2^η$ περίπτωση όταν μεγιστοποιείται το P_x

©2006, Σπύρος Δενάζης

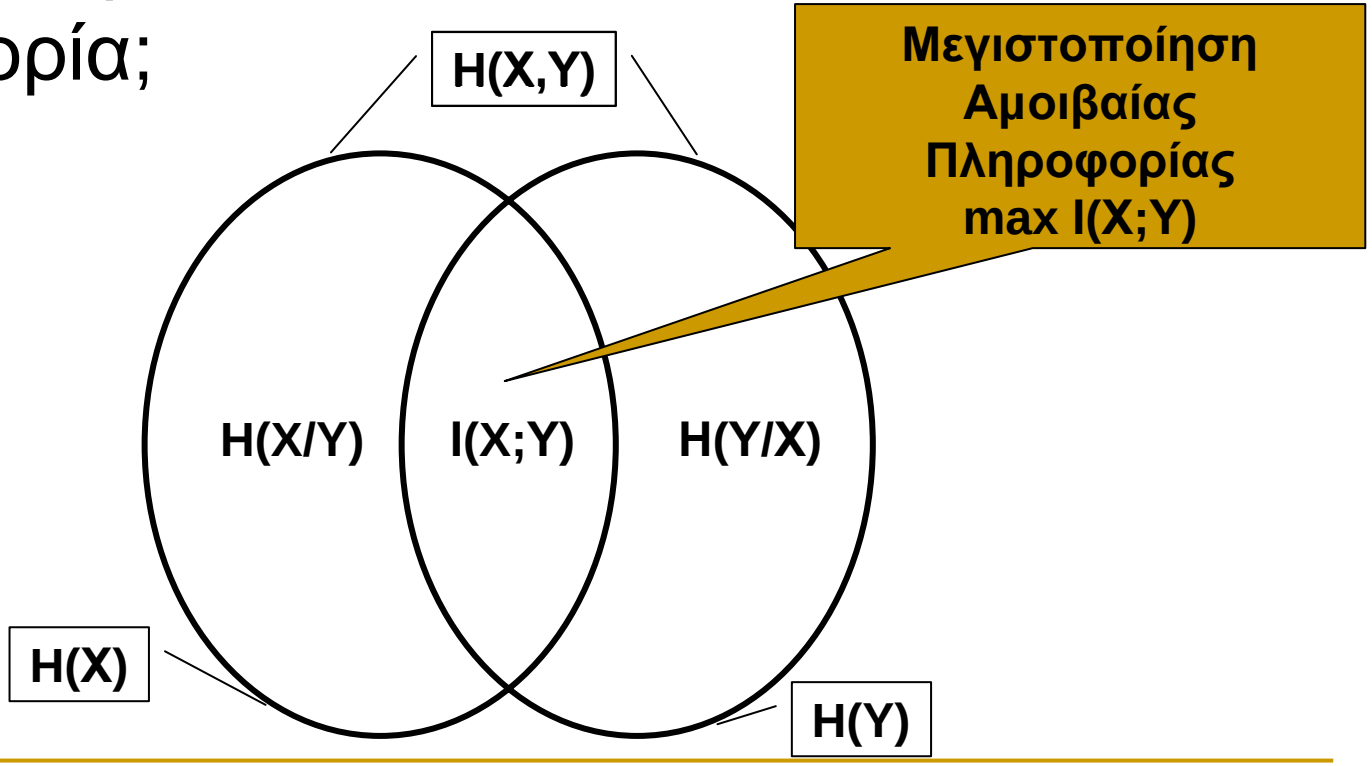
Κανάλια Επικοινωνίας ...

- **<u>Αμοιβαία Πληροφορία Καναλιών</u>**
  - **2.** Έστω ένα **<u>κανάλι επικοινωνίας Z</u>** όπου *f*=0.15
  - *<u>Περίπτωση 1η:</u>* $P_X=\{p_X(0)=0.9, p_X(1)=0.1\}$.
    - Ομοίως, $P_Y=\{p_Y(0)=0.915, p_Y(1)=0.085\}$.
    - I(X;Y)=H(Y)-H(Y/X)= H(0.085)-[0.9*H(0)+0.1*H(0.15)] =<u>0.36 bits</u>
    - H(X)=0.47 bits
  - *<u>Περίπτωση 2η:</u>* $P_X=\{p_X(0)=0.5, p_X(1)=0.5\}$.
    - Ομοίως, $P_Y=\{p_Y(0)=0.575, p_Y(1)=0.425\}$.
    - I(X;Y)=H(Y)-H(Y/X)= H(0.575)-[0.5*H(0)+0.5*H(0.15)]=0.98-0.3=<u>0.679 bits</u>
    - H(X)=0.47 bits
  - Παρατηρούμε ότι και στην περίπτωση του καναλιού Z η αμοιβαία πληροφορία παίρνει την μέγιστη τιμή της επίσης στη $2^η$ περίπτωση όταν μεγιστοποιείται το P_x
  - Παρατηρείστε ότι το Z κανάλι έχει μεγαλύτερη πιστότητα απ' ότι το συμμετρικό κανάλι.

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- Τι πρέπει λοιπόν να κάνουμε για να μεταδώσουμε όσο το δυνατόν περισσότερη πληροφορία;



©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **<u>Μεγιστοποίηση Αμοιβαίας Πληροφορίας</u>**
  - Η αμοιβαία πληροφορία παρατηρούμε ότι εξαρτάται από την κατανομή P_X της τ.μ. X της εισόδου στο κανάλι.
  - Για να μεγιστοποιήσουμε την max I(X;Y) θα πρέπει να βρούμε την καλύτερη δυνατή κατανομή P_X.
  - Έτσι λοιπόν καλήγουμε στο συμπέρασμα ότι η χωρητικότητα C, του καναλιού Q, είναι:
    - $$\boxed{C(Q)=\max_{P_X} I(X;Y)}$$
    - Η κατανομή P_X η οποία μεγιστοποιεί την παραπάνω σχέση λέγεται βέλτιστη κατανομή.
    - Μπορεί να υπάρχουν παραπάνω από μία βέλτιστες κατανομές.
  - Από τα παραπάνω είναι φανερό ότι ο τρόπος με τον οποίο ορίσαμε την χωρητικότητα καναλιού C, αντιστοιχεί σε εκείνο το μέγεθος το οποίο μετρά την ποσότητα της πληροφορίας που είναι δυνατόν να μεταφερθεί πάνω από ένα ενθόρυβο διακριτό κανάλι χωρίς μνήμη.

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **<u>Μεγιστοποίηση Αμοιβαίας Πληροφορίας Καναλιών</u>**
  - **1. <u>Δυαδικό Κανάλι Χωρίς Θόρυβο</u>**
    - $C(Q)=\max_{P_X} I(X;Y)=1$ bit, Προσοχή: $I(X,Y)=H(X)$
  - **2. <u>Ενθόρυβο κανάλι με μη επικαλυπτόμενες εξόδους</u>**
    - $C(Q)=\max_{P_X} I(X;Y)=1$ bit
  - **3. <u>Ενθόρυβη γραφομηχανή</u>**, $p_{ii}=p_{i,i+1}=1/2$, i=α,β,...,ψ,ω.
    - Παρατηρούμε ότι κάθε ένα γράμμα είτε λαμβάνεται σωστά είτε λαμβάνεται το επόμενό του με πιθανότητα ½. Με δεδομένο ότι έχουμε 24 διαφορετικά σύμβολα εάν μεταδίδαμε μόνο κάθε δεύτερο σύμβολο δηλ. β,δ,ζ,θ,...,χ,ω, τότε μόνο αυτά τα 12 σύμβολα από τα 24 θα μπορούσαν να μεταδοθούν και στη συνέχεια να αποκωδικοποιηθούν χωρίς σφάλματα. Με άλλα λόγια η χωρητικότητα του καναλιού είναι log12 bits
    - Στο ίδιο συμπέρασμα θα καταλήγαμε εάν χρησιμοποιούσαμε τον ορισμό
      - $\max_{P_X} I(X;Y)=\max_{P_X} [H(Y)-H(Y/X)]=\max_{P_X} H(Y) -1=\log24-1=\log12$

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **Μεγιστοποίηση Αμοιβαίας Πληροφορίας Καναλιών**
  - **Δυαδικό συμμετρικό κανάλι, *f*.**
    - $I(X;Y)=H(Y)-H(Y/X)$
      $=H(Y)-\sum p(x)H(Y/X=x)$
      $=H(Y)- \sum p(x)H(f)$
      $=H(Y)-H(f)$
      $\leq 1-H(f)$
  - **Δυαδικό κανάλι απόσβεσης, α.**
    - $\max I(X;Y)=\max(H(Y)-H(Y/X))$
      $=\max(H(Y)-H(\alpha))$
      $=\max H(Y)-H(\alpha)$
    - Θα μπορούσε να είναι max H(Y)=log3 αλλά αυτή η τιμή δεν είναι εφικτή για καμμία τιμή της $p_X(x_i)$, i=1,2
    - Αν θέσουμε $p_X(x_1)=1-\pi$, και $p_X(x_2)=\pi$, τότε από τα $p_Y(y_i)$, i=1,e,2 δίνονται από τους τύπους (βλ. διαφάνεια 10) τότε
      - $\max H(Y)=\max H((1-\alpha)\pi,\alpha,(1-\alpha)(1-\pi))=\max[(1-\alpha)*H(\pi)+H(\alpha)]=(1-\alpha)*\max H(\pi)+H(\alpha)$
    - Οπότε προκύπτει ότι
      - $\max I(X;Y)=\max H(Y)-H(\alpha)=(1-\alpha)*\max H(\pi)+H(\alpha)-H(\alpha)=1-\alpha$

π=1/2

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **<u>Μεγιστοποίηση Αμοιβαίας Πληροφορίας Καναλιών</u>**
  - **<u>Κανάλι Z, *f*.</u>**
    - Αν θέσουμε $p_X(x_1=0)=1-\pi$, και $p_X(x_2=1)=\pi$, τότε από τα $p_Y(y_i)$, i=1,2 δίνονται από τους τύπους (βλ. διαφάνεια 11) τότε
      - $H(Y)=H((1-f)\pi)$
      - $H(Y/X)=\pi*H(Y/X=1)=\pi*H(f)$
    - Οπότε $\max I(X;Y)=\max(H(Y)-H(Y/X))$

      $=\max\mathbf{(}H((1-f)\pi) - \pi*H(f)\mathbf{)}$
    - Για f=0.15 μπορούμε να βρούμε ότι μεγιστοποιείται όταν π=0.445 και άρα C=0.685
    - Παρατηρείστε ότι $p_X(x_1=0)=0.555$, και $p_X(x_2=1)=0.445$, που είναι διαφορετική από την $p_X(x_1=0)=0.5$, και $p_X(x_2=1)=0.5$, η οποία μεγιστοποιεί την εντροπία, H(X)

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- ***<u>Κώδικες Ομάδων Διόρθωσης Λαθών:</u>***
  - Αντί να προσθέτουμε πλεονάζουσα πληροφορία ανά bit θα προσθέτουμε ανά ομάδες
  - Κώδικας Ομάδας ορίζεται το σύστημα εκείνο κωδικοποίησης κατά το οποίο μηνύματα πηγής **s**, μήκους K, μετατρέπονται σε μηνύματα μετάδοσης **t**, μήκους N, όπου N>K.
  - Τα πλεονάζοντα bits, N-K, ονομάζονται bits ισοτιμίας (parity)
  - Εάν τα πλεονάζοντα bits προκύπτουν ως γραμμικές συναρτήσεις των bits της πηγής **s**, τότε ο κώδικας λέμε ότι είναι γραμμικός.

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- **<u>Θεώρημα Shannon για Διακριτά Κανάλια χωρίς μνήμη</u>**
  - Για κάθε διακριτό κανάλι χωρίς μνήμη, η χωρητικότητα καναλιού έχει την ακόλουθη ιδιότητα
    - C=max I(X;Y)
  - Για κάθε ε>0 και R<C, για μεγάλα N, υπάρχει ομαδικός κώδικας (για διόρθωση λαθών) μήκους N και ρυθμού ροής πληροφορίας ≥ R, τέτοιος ώστε η μέγιστη πιθανότητα, p_{BM}, λανθασμένης λήψης του κώδικα N είναι <ε
  - Για αυθαίρετες πιθανότητες λάθους p_b, τότε ο ρυθμός μετάδοσης $R(p_b)$ που δίνεται από τη σχέση είναι εφικτός
    - $R(p_b) = \dfrac{C}{1 - H(p_b)}$
  - Για κάθε p_b, δεν είναι εφικτός ρυθμός μετάδοσης μεγαλύτερος του $R(p_b)$

©2006, Σπύρος Δενάζης

Κανάλια Επικοινωνίας ...

- Αυτό που μας λέει το θεώρημα είναι ότι
  - *Κάθε διακριτό κανάλι χαρακτηρίζεται από ένα μέγεθος που είναι η χωρητικότητά του, C.*
  - *Όσο η πηγή μας μεταδίδει πληροφορία η οποία είναι μικρότερη της χωρητικότητας C του καναλιού, είναι δυνατόν να βρούμε ομαδικούς κώδικες (N,K) διόρθωσης λαθών έτσι ώστε το ενθόρυβο κανάλι να μεταδίδει πληροφορία με απειροελάχιστη πιθανότητα λάθους. Να συμπεριφέρεται δηλαδή σαν κανάλι χωρίς θόρυβο.*

©2006, Σπύρος Δενάζης

- **<u>Άσκηση</u>**
  - Δίνεται ένα διακριτό κανάλι χωρίς μνήμη. Στην είσοδο του καναλιού εμφανίζονται τα σύμβολα x_i, $i=1, 2,$ με πιθανότητα εμφάνισης του x_1, $p(x_1)=a$. Στην έξοδο του καναλιού λαμβάνονται τα σύμβολα y_j, $j=1, 2, 3, 4$ όπου οι πιθανότητες μετάβασης $p_{ij}=p(y_j/x_i)$ περιέχονται στον ακόλουθο πίνακα μετάβασης του καναλιού.

$$P = \begin{bmatrix} 0{,}8 & 0 & 0{,}1 & 0{,}1 \\ 0 & 0{,}8 & 0{,}1 & 0{,}1 \end{bmatrix}.$$

  - α) Να υπολογιστεί η ποσότητα πληροφορίας των συμβόλων εξόδου, $H(Y)$.
  - β) Να υπολογιστεί η αβεβαιότητα $H(Y/X)$.
  - γ) Να υπολογιστεί η χωρητικότητα του καναλιού.

©2006, Σπύρος Δενάζης

- **<u>Απάντηση</u>**
  - α) Πρώτα πρέπει να υπολογίσουμε τις πιθανότητες λήψης των κωδικών συμβόλων y_j, $j=1, 2, 3, 4$. Είναι
  - $p(y_1)= p(y_1,x_1)+ p(y_1,x_2)=p(x_1)\ p(y_1/x_1)+ p(x_2)\ p(y_1/x_2)=a(0,8)+(1-a)(0)=0,8\alpha.$
  - Κατά ανάλογο τρόπο υπολογίζουμε
  - $p(y_2)= p(y_2,x_1)+ p(y_2,x_2)=p(x_1)\ p(y_2/x_1)+ p(x_2)\ p(y_2/x_2)=0,8(1-\alpha),$
  - $p(y_3)= p(y_3,x_1)+ p(y_3,x_2)=p(x_1)\ p(y_3/x_1)+ p(x_2)\ p(y_3/x_2)=\alpha(0,1)+(1-\alpha)(0,1)=0,1,$
  - $p(y_4)= p(y_4,x_1)+ p(y_4,x_2)=p(x_1)\ p(y_4/x_1)+ p(x_2)\ p(y_4/x_2)=0,1.$
  - Από τις πιθανότητες αυτές, των οποίων το άθροισμα είναι 1, υπολογίζουμε τη μέση πληροφορία της εξόδου του καναλιού.
  - $H(Y)=-p(y_1)\log p(y_1)-p(y_2)\log p(y_2)-p(y_3)\log p(y_3)-p(y_4)\log p(y_4)=$
  - $=-0,8\alpha\log(0,8\alpha)-0,8(1-a)\log(0,8(1-a)) -2(0,1)\log(0,1)$
  - $=0,66-0,8\alpha\log(0,8\alpha)-0,8(1-a)\log(0,8(1-a)).$

©2006, Σπύρος Δενάζης

- β) Πρώτα υπολογίζουμε τις συνδυασμένες πιθανότητες των συμβόλων εισόδου και εξόδου του καναλιού (δείτε και το ερώτημα 1).
- Είναι $p(x_1,y_1)= p(y_1,x_1)= p(x_1)\ p(y_1/x_1)=0,8\alpha,$
- $p(x_1,y_2)= p(y_2,x_1)= p(x_1)\ p(y_2/x_1)=0,$
- $p(x_1,y_3)= p(y_3,x_1)= p(x_1)\ p(y_3/x_1)=0,1a,$
- $p(x_1,y_4)= p(y_4,x_1)= p(x_1)\ p(y_4/x_1)=0,1a,$
- $p(x_2,y_1)= p(y_1,x_2)= p(x_2)\ p(y_1/x_2)=0,$
- $p(x_2,y_2)= p(y_2,x_2)= p(x_2)\ p(y_2/x_2)=0,8(1-a),$
- $p(x_2,y_3)= p(y_3,x_2)= p(x_2)\ p(y_3/x_2)=0,1(1-a),$
- $p(x_2,y_4)= p(y_4,x_2)= p(x_2)\ p(y_4/x_2)=0,1(1-a).$
- Τώρα υπολογίζουμε την αβεβαιότητα του καναλιού
- $H(Y/X)=-p(x_1,y_1)\log p(y_1/x_1) - p(x_1,y_2)\log p(y_2/x_1) - p(x_1,y_3)\log p(y_3/x_1) - p(x_1,y_4)\log p(y_4/x_1)-p(x_2,y_1)\log p(y_1/x_2) -p(x_2,y_2)\log p(y_2/x_2) - p(x_2,y_3)\log p(y_3/x_2) -p(x_2,y_4)\log p(y_4/x_2)=$
- $-0,8a.\log 0,8+0-0,1a\log 0,1-0,1a\log 0,1-0-0,8(1-a)\log 0,8-0,1(1-a)\log 0,1-0,1(1a)\log 0,1=-0,8\log 0,8-0,1\log 0,1-0,1\log 0,1=0,2575+0,66.$

©2006, Σπύρος Δενάζης

- γ) Για τον προσδιορισμό της χωρητικότητας του καναλιού θα πρέπει να βρούμε τις πιθανότητες εμφάνισης των συμβόλων της εισόδου, για τις οποίες μεγιστοποιείται η αμοιβαία πληροφορία μεταξύ της εισόδου και της εξόδου του καναλιού, δηλαδή την τιμή *α.*
- Είναι

$$
\begin{aligned}
C &= \max_{p(x)} I(X;Y) = \max_{p(x)}[H(Y) - H(Y/X)] \\
&= \max_{p(x)}\left[0{,}66 - 0{,}8a\log(0{,}8a) - 0{,}8(1-a)\log(0{,}8(1-a)) - 0{,}2575 - 0{,}66)\right] \\
&= \max_{p(x)}\left[-0{,}8a\log(0{,}8a) - 0{,}8(1-a)\log(0{,}8(1-a)) - 0{,}2575\right].
\end{aligned}
$$

- Η συνάρτηση αυτή μεγιστοποιείται όπως γνωρίζουμε για την τιμή του a που μηδενίζει την πρώτη της παράγωγο.

©2006, Σπύρος Δενάζης

- Επομένως,

$$\frac{dI(X;Y)}{da} = \left[-0{,}8a\log(0{,}8a) - 0{,}8(1-a)\log(0{,}8(1-a) - 0{,}2575\right]'$$

$$= -0{,}8\left[(a)'\log(0{,}8a) + a(\log(0{,}8a))'\right]$$

$$-0{,}8\left[(1-a)'\log(0{,}8(1-a)) + (1-a)(\log(1-a))'\right]$$

$$= -0{,}8\left[\log(0{,}8a) + a\frac{\log e}{a}\right] - 0{,}8\left[(-1)\log(0{,}8(1-a)) + (1-a)(-1)\frac{1}{1-a}\log e\right]$$

$$= -0{,}8\log(0{,}8a) - 0{,}8\log e + 0{,}8\log(0{,}8(1-a)) + 0{,}8\log e$$

$$= -0{,}8\left[\log(0{,}8a) - \log(0{,}8(1-a))\right] = -0{,}8\log\frac{0{,}8a}{0{,}8(1-a)} = 0 \Rightarrow$$

$$\log\frac{a}{1-a} = 0 \Rightarrow \left(\frac{a}{1-a}\right) = 2^0 = 1 \Rightarrow a = \frac{1}{2}.$$

- Θέτοντας ανωτέρω την τιμή αυτή του *a*, λαμβάνουμε τη χωρητικότητα του καναλιού
- *C=0,8 bits/symbol.*

©2006, Σπύρος Δενάζης

Συνεχή Κανάλια Επικοινωνίας ...

- Έστω X, Y συνεχείς τμ με συνάρτηση πυκνότητας f (x), f (y), αντίστοιχα
- Συνεχή ποσότητα πληροφορίας, H(X)
  - $H(X) = -\int_{-\infty}^{+\infty} f(x)\log_2 f(x)dx$
- Συνδυασμένη ποσότητα πληροφορίας, H(X,Y)
  - $H(X,Y) = -\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\log_2 f(x,y)dxdy$
- Υπό συνθήκη ποσότητα πληροφορίας, H(X/Y)
  - $H(X/Y) = -\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\log_2 f(x/y)dxdy$
- Αμοιβαία ποσότητα πληροφορίας, I(X;Y)
  - $I(X;Y) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\log_2 \frac{f(x,y)}{f(x)f(y)}dxdy$

©2006, Σπύρος Δενάζης

Συνεχή Κανάλια Επικοινωνίας ...

- Στα συνεχή κανάλια επικοινωνίας η κωδικοποίηση και αποκωδικοποίηση ερμηνεύονται διαφορετικά σε σχέση με τα διακριτά κανάλια
- Με την κωδικοποίηση εννοούμε διαμόρφωση πλάτους και συχνότητας ή τη φραγή εύρους με τη χρήση φίλτρων
- Έτσι με τη διαμόρφωση το σήμα μετατρέπεται σε μορφή κατάλληλη για το συνεχές κανάλι
- Κατά τη μετάδοση του σήματος υπεισέρχεται θόρυβος (προσθετικός ή πολλαπλασιαστικός) και γι' αυτό το σήμα θα πρέπει να ανασκευαστεί στην έξοδο.
- Ο προσθετικός θόρυβος μπορεί να είναι είτε γκαουσιανός είτε κρουστικός
  - Ο γκαουσιανός θόρυβος
  - Κρουστικός (χαρακτηρίζεται από καταιγισμό παλμών θορύβου μεγάλου πλάτους

©2006, Σπύρος Δενάζης

Συνεχή Κανάλια Επικοινωνίας χωρίς μνήμη

- Υποθέτουμε ότι στην είσοδο του καναλιού έχουμε ένα συνεχές σήμα x(t) και στην έξοδο επίσης ένα σήμα y(t).
- Έστω ότι παίρνουμε N δείγματα αυτών των σημάτων.
- Τότε για τη συνάρτηση πυκνότητας πιθανότητας του σήματος που λαμβάνεται στην έξοδο του καναλιού y(t) δεδομένου του σήματος εισόδου x(t) ισχύει
  - $f(y/x)=f(y_1,y_2,\ldots,y_N/x_1, x_2, \ldots,x_N)$
- Αν ένα δείγμα του σήματος εισόδου εξαρτάται μόνο από το αντίστοιχό του στην είσοδο τότε το κανάλι είναι συνεχές χωρίς μνήμη
- Σε τέτοια περίπτωση τα μέτρα ποσότητας της πληροφορίας μπορούν να οριστούν στη βάση του ζεύγους δειγμάτων X, Y
  - Τα X, Y είναι τμ που αναπαριστούν τα δείγματα των σημάτων εισόδου και εξόδου x(t) και y(t).
- Μπορούμε να ορίσουμε όπως και στην περίπτωση διακριτών καναλιών την αμοιβαία ποσότητα πληροφορίας που είναι και ο ρυθμός μετάδοσης της πληροφορίας
  - $$I(X;Y)=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\log_2 \frac{f(x,y)}{f(x)f(y)}\,dxdy$$

©2006, Σπύρος Δενάζης

Συνεχή Κανάλια Επικοινωνίας χωρίς μνήμη

- **<u>Ορισμός χωρητικότητας συνεχούς καναλιού χωρίς μνήμη</u>**
  - $C = \max_{f(x)} I(X;Y) = \max_{f(x)} \{H(Y) - H(Y/X)\}$
- Για την περίπτωση αθροιστικών καναλιών όπου ο στατιστικά ανεξάρτητος θόρυβος n(t) προστίθεται στο μεταδιδόμενο σήμα x(t) (X+N=Y) ισχύει:
- f(y/x)= f(x+n/x)=f(n/x)=f(n), εφόσον ο θόρυβος είναι στατιστικά ανεξάρτητος του σήματος εισόδου
- Στην περίπτωση του αθροιστικού καναλιού, η επενέργεια του θορύβου στη χωρητικότητα του καναλιού αντανακλάται στην υπό συνθήκη ποσότητα πληροφορίας H(Y/X). Μπορούμε να υπολογίσουμε την ποσότητα πληροφορίας H(Y/X) ως εξής:

©2006, Σπύρος Δενάζης

Συνεχή Κανάλια Επικοινωνίας χωρίς μνήμη

- $$H(Y/X) = -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log f(y/x)\,dx\,dy$$
$$= -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x)f(y/x)\log f(y/x)\,dx\,dy$$
$$= -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x)f(n)\log f(n)\,dx\,dn$$
$$= -\int_{-\infty}^{\infty} f(n)\log f(n)\,dn = H(N).$$
- Η χωρητικότητα αθροιστικού καναλιού δίνεται από την παρακάτω σχέση
- C=max I (X;Y) =max {H(Y) – H (Y/X) }=max (H(Y) – H(N))=max H(Y) – H(N)
  (f(x)) *(f(x))* *(f(x))* *(f(x))*

©2006, Σπύρος Δενάζης

Χωρητικότητα Γκαουσιανού καναλιού ...

- Μπορεί να αποδειχθεί ότι η ποσότητα πληροφορίας μιας συνεχούς πηγής πληροφορίας με σταθερή ισχύ, σ^2, είναι ίση με H(N) = log(σ√2πe) bits/δείγμα και ισχύει για κανονική συνάρτηση πυκνότητας πιθανότητας, f(n). Το αποτέλεσμα αυτό μπορεί να επεκταθεί και να εκφραστεί σε bits/sec λαμβάνοντας υπόψη το πλήθος των δειγμάτων M, το οποίο είναι ίσο με το διπλάσιο του εύρους ζώνης του σήματος W, δηλαδή M = 2W. Άρα:

$$H(N) = \log\left(\sigma\sqrt{2\pi e}\right) \text{ bits / δείγμα}$$

$$= M\frac{1}{2}\log\left(2\pi e\sigma^2\right) \text{ bits / sec}$$

$$= 2W\frac{1}{2}\log\left(2\pi e\sigma^2\right) = W\log\left(2\pi e\sigma^2\right) \text{ bits / sec.}$$

©2006, Σπύρος Δενάζης

Χωρητικότητα Γκαουσιανού καναλιού ...

- Από την άλλη πλευρά, η μέγιστη τιμή της ποσότητας πληροφορίας του σήματος της εξόδου λαμβάνεται όταν είναι κανονικά κατανεμημένο, με ισχύ σ^2_y. Αλλά τότε, αφού και ο λευκός θόρυβος ακολουθεί την κανονική κατανομή, το σήμα εισόδου πρέπει να είναι και αυτό γκαουσιανό. Επομένως, αφού Y = X + N και $\sigma^2_y = \sigma^2_x + \sigma^2_n$, η μέγιστη τιμή της ποσότητας πληροφορίας του σήματος εισόδου ως προς τη συνάρτηση πυκνότητας πιθανότητας του σήματος εισόδου δίνεται από την ακόλουθη σχέση:

$$\max_{f(x)} H(Y) = \log\sqrt{\sigma_x^2+\sigma_n^2}\left(\sqrt{2\pi e}\right) \text{ bits / δείγμα}$$

$$= \frac{1}{2}\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} \text{ bits / δείγμα}$$

$$= W\log\left\{2\pi e\left(\sigma_x^2+\sigma_n^2\right)\right\} \text{ bits / sec.}$$

©2006, Σπύρος Δενάζης

Χωρητικότητα Γκαουσιανού καναλιού ...

- Έχοντας υπολογίσει την ποσότητα πληροφορίας του λευκού θορύβου και τη μέγιστη τιμή της ποσότητας πληροφορίας του σήματος εξόδου για την περίπτωση περιορισμένης μέσης ισχύος, μπορούμε πλέον να υπολογίσουμε τη χωρητικότητα του συνεχούς καναλιού με αθροιστικό λευκό θόρυβο:

$$
\begin{aligned}
C &= \max_{f(x)} \left\{ H(Y) \right\} - H(N) \text{ bits / sec} \\
&= W \log \left\{ 2\pi e \left(\sigma_x^2 + \sigma_n^2 \right) \right\} - W \log \left\{ 2\pi e \sigma_n^2 \right\} \\
&= W \log \frac{\sigma_x^2 + \sigma_n^2}{\sigma_n^2} = W \log \left\{ 1 + \frac{\sigma_x^2}{\sigma_n^2} \right\} \text{ bits / sec.}
\end{aligned}
$$

©2006, Σπύρος Δενάζης

Χωρητικότητα Γκαουσιανού καναλιού ...

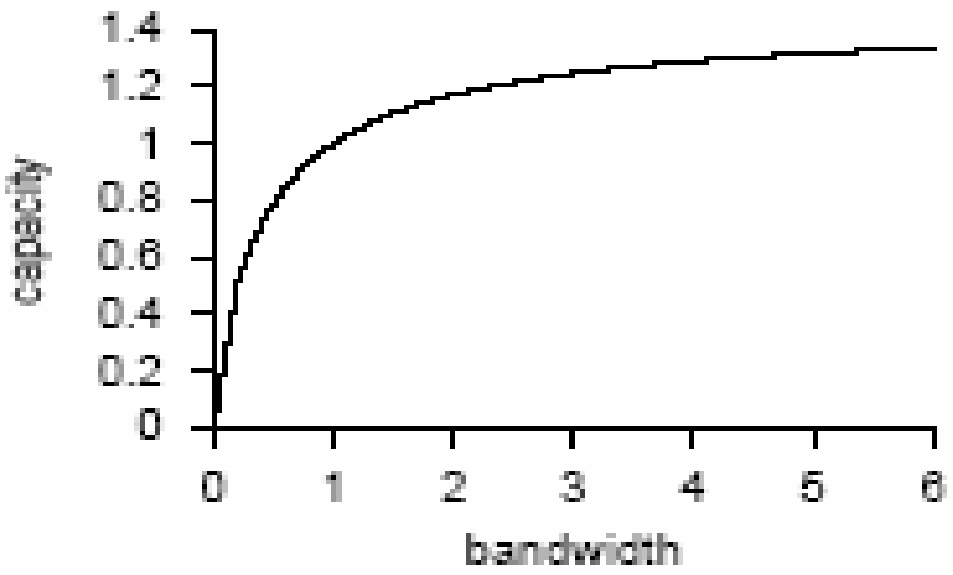
- Η χωρητικότητα καναλιού στην περίπτωση αθροιστικού γκαουσιανού λευκού θορύβου
  - $C=W \log\{1+\sigma_x^2/\sigma_n^2\}$ bits/sec,
- W=εύρος ζώνης καναλιού , σ_x^2= S = ισχύς σήματος, σ_n^2 =Ισχύς θορύβου=N=No.W, No=πυκνότητα φασματικής ισχύος (noise power spectrum) και
- **$C=W \log\{1+S/N\}$ bits/sec**
- Βασικοί παράγοντες για C = W, S και N
- Για S ισχύει: Αυξάνοντας S αυξάνει και η C
  - Αυξάνοντας S προσδίδει μεγαλύτερη δυνατότητα για μεγαλύτερο αριθμό σταθμών εισόδου με αρκετή απόσταση μεταξύ τους και άρα μεγαλύτερη ανοσία σε θόρυβο και bits/μετάδοση είναι δυνατόν
  - Για κάτι τέτοιο όμως χρειάζεται μεγάλη αύξηση του S και για αυτό η αύξηση είναι αργή και λογαριθμική.

©2006, Σπύρος Δενάζης

Χωρητικότητα Γκαουσιανού καναλιού ...

Εύρος Ζώνης

- Η αύξηση του W έχει δύο αντίθετα αποτελέσματα: Αυξημένο W σημαίνει δυνατότητα για μετάδοση περισσότερων δειγμάτων/sec (γραμμική αύξηση στην εξίσωση) αλλά σημαίνει επίσης και υψηλότερο θόρυβο εισόδου στο δέκτη (log μείωση στην εξίσωση)
- Για να διευκρινιστεί το συνολικό αποτέλεσμα της αύξησης του W στην C αρκεί να βρεί την τιμή της εξίσωσης με W→∞ :
- lim C (W→∞)= (S/No) . loge= 1.44 S/No
- Ως συμπέρασμα σε αντίθεση με την περίπτωση ισχύος, μόνο με την αύξηση του W δεν είναι δυνατόν να αυξηθεί το C σε οποιαδήποτε επιθυμητή τιμή.



©2006, Σπύρος Δενάζης

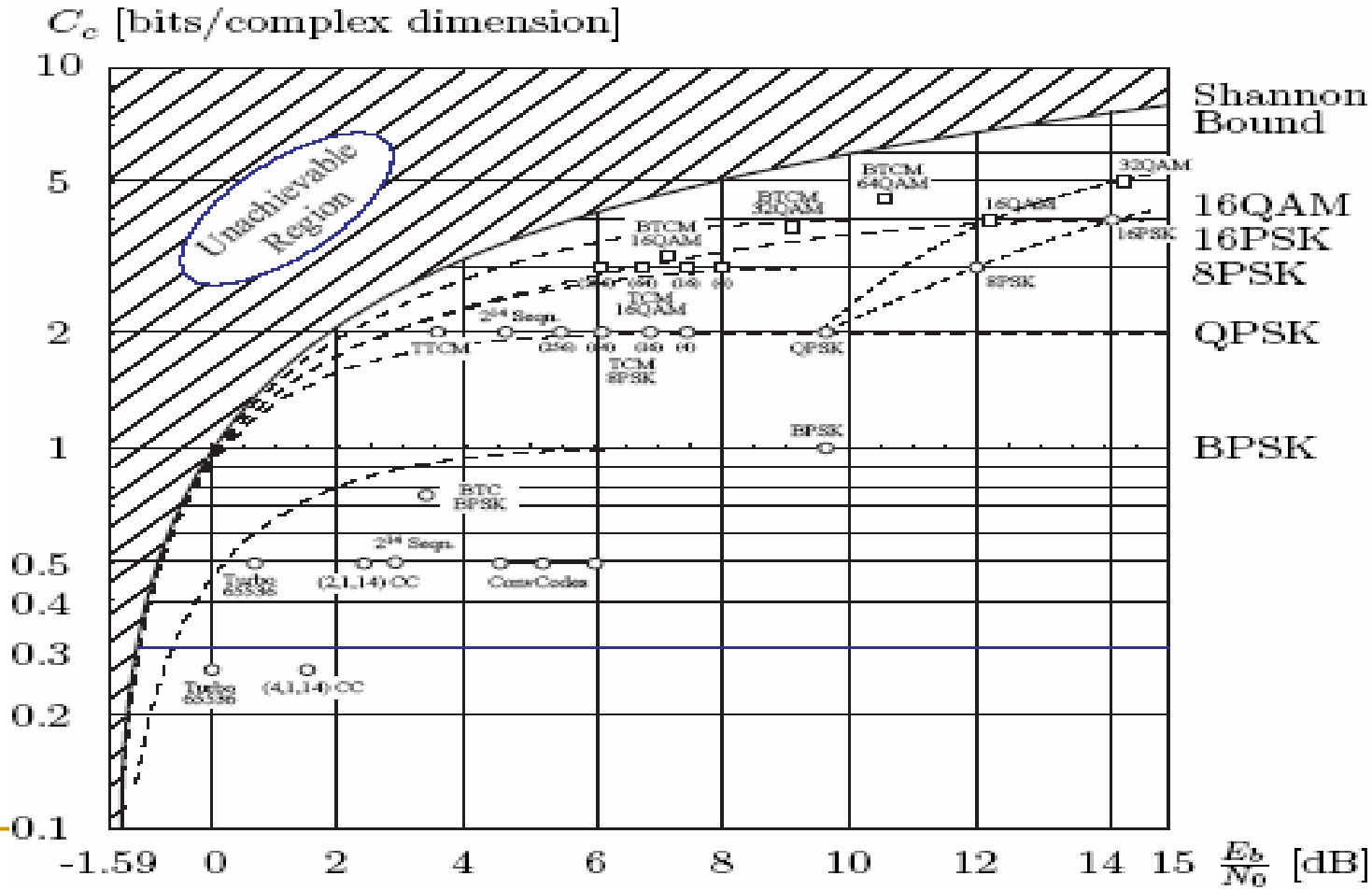
Χωρητικότητα Γκαουσιανού καναλιού ...

- Δεδομένου ότι για κάθε πρακτικό σύστημα τηλεπικοινωνιών πρέπει να ισχύει R=ρυθμός μετάδοσης < C. Άρα και στην περίπτωση του Γκαουσιανού καναλιού (AWGN κανάλι):
  - $R < W \log\{1+S/(No.W)\}$.
- Διαιρώντας και τα δύο μέλη με W και ορίζοντας r = R/W (=spectral bit rate):
  - $r < \log\{1+S/(No.W)\}$
- Θεωρώντας ότι E_b = ενέργεια του σήματος/bit, τότε ισχύει $E_b = S/R$, οπότε:
  - $r < \log\{1+r\, E_b/No\}$
- Η σχέση αυτή ($r = R/W$ συναρτήσει του E_b) απεικονίζεται στην επόμενη διαφάνεια.
- Η καμπύλη που ορίζεται από την ισότητα δηλ η $r = \log\{1+r\, E_b/No\}$ διαιρεί ουσιαστικά το γράφημα σε δύο περιοχές. Στην περιοχή κάτω από την καμπύλη όπου είναι δυνατή η αξιόπιστη μετάδοση και η περιοχή πάνω από την καμπύλη όπου κάτι τέτοιο δεν είναι δυνατόν
- Η απόδοση κάθε συστήματος σηματοδοτείται από ένα σημείο στο γράφημα και όσο εγγύτερα κείται το σημείο αυτό στην καμπύλη τόσο εγγύτερα και η απόδοση του συστήματος σε ένα ιδανικό σύστημα

©2006, Σπύρος Δενάζης

Χωρητικότητα Γκαουσιανού καναλιού.

- Τέλος από την καμπύλη μπορεί να δειχθεί ότι η τιμή $E_b/No=\ln 2= 0.693 \sim -1.592$ dB αποτελεί το απόλυτο ελάχιστο προκειμένου να έχουμε αξιόπιστη επικοινωνία, δηλ θα πρέπει να ισχύει $E_b/No > 0.693$



©2006, Σπύρος Δενάζης

- **<u>Άσκηση</u>**
  - Υποθέστε ότι μεταφέρεται ψηφιοποιημένη τηλεοπτική εικόνα από μία πηγή η οποία χρησιμοποιεί ανάλυση 480 x 500 pixels και για κάθε pixel η χρωματική πληροφορία μπορεί να πάρει 32 διαφορετικές τιμές έντασης. Στη διάρκεια του δευτερολέπτου μεταδίδονται 30 πλαίσια.
  - α) Βρείτε το ρυθμό, R, μετάδοσης της πηγής.
  - β) Αν η τηλεοπτική εικόνα μεταδοθεί σε κανάλι εύρους ζώνης 4.5 MHz με signal-to-noise ratio 35 dB, να βρείτε την χωρητικότητα του καναλιού σε bps.

©2006, Σπύρος Δενάζης

- **<u>Απάντηση</u>**
  - α) Το συνολικό πλήθος των pixels ανά πλαίσιο είναι *480*500 =240000*. Λαμβάνοντας υπόψη και τις 32 διαφορετικές τιμές χρωματικής πληροφορίας έχουμε *5*240000 bits/frame =1200000 bits/frame*.
  - Έτσι, σε 1 sec μεταδίδονται 30 πλαίσια και επομένως *R=30*1200000 bits =36000000bits* = ***36Mbps*** **.**
  - β) Έχουμε
    - **C=W log{1+S/N } bits/sec**
    - $\mathrm{SNR} = 10\log_{10}(\frac{S}{N}) = 35 \Rightarrow \log_{10}(\frac{S}{N}) = 3{,}5 \Rightarrow \frac{S}{N} = 10^{3,5} \approx 3162{,}27$
    - W=4,5 MHz
  - Επομένως,
    - $C = 4{,}5\log_2(1+3162{,}27)\,bits/\sec = 4{,}5*10^6*11{,}627 \approx 52{,}32 Mbps.$

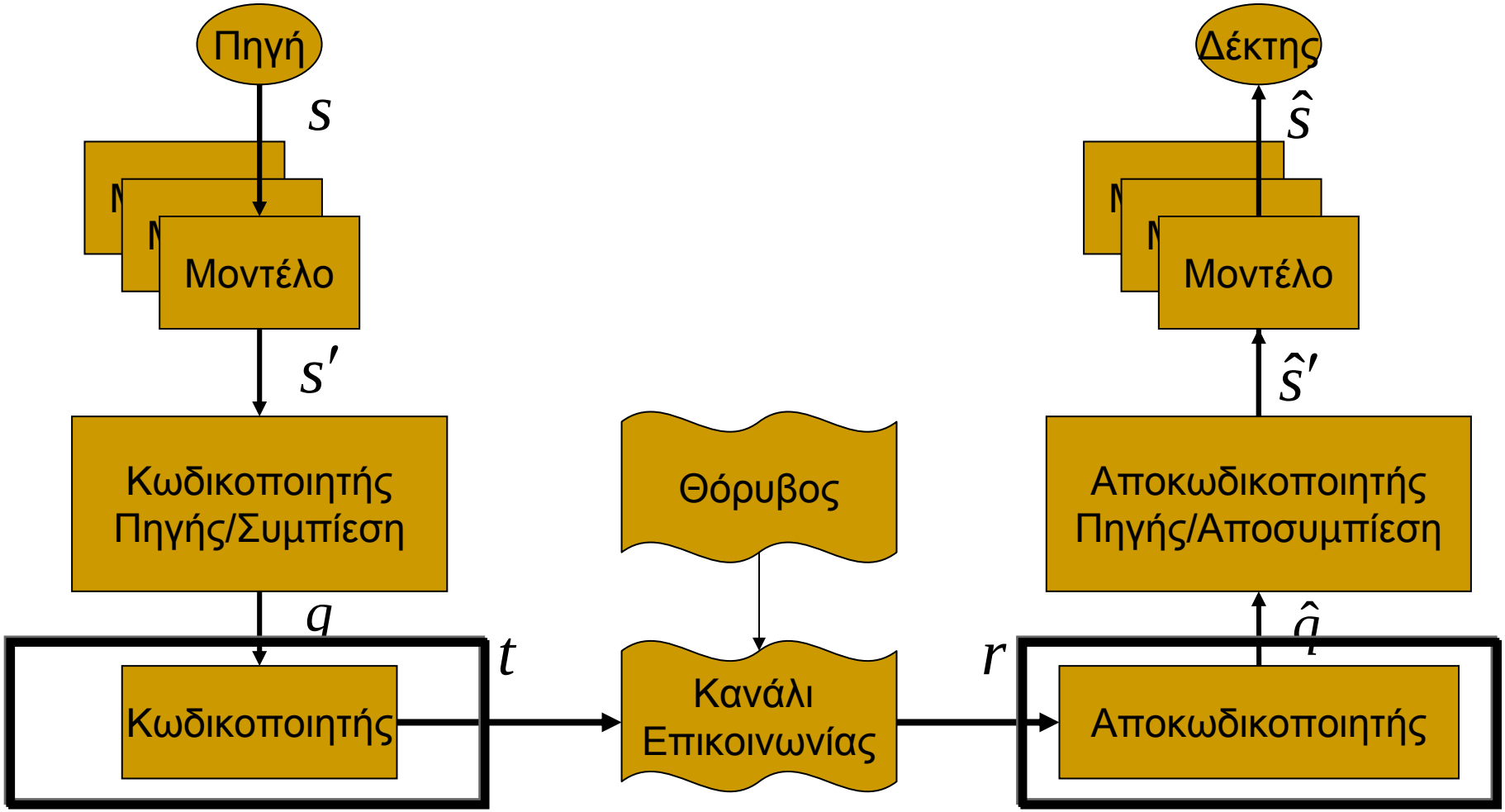
©2006, Σπύρος Δενάζης

Κωδικοποίηση Διόρθωση Λαθών

- Ανίχνευση + Διόρθωση Λαθών
- Ισομήκης Κώδικες
- Γραμμικοί Κώδικες
- Κώδικες Hamming
- Τέλειοι Κώδικες
- Δυϊκοί Κώδικες
- Κυκλικοί Κώδικες

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση



©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- Η **Θεωρία Κωδικοποίησης** είναι η μελέτη μεθόδων για την αποτελεσματική και ορθή μεταφορά της πληροφορίας από την πηγή στον προορισμό.
- Βασικός στόχος = *Ανίχνευση* + *Διόρθωση* λαθών. Για τον σκοπό αυτό προστίθεται όσος πλεονασμός είναι απαραίτητος για επιθυμητή μείωση της πιθανότητας σφάλματος μετάδοσης
- Οι κωδικές λέξεις είναι ακολουθίες δυαδικών ψηφίων π.χ. C ={00, 10, 01, 11}. Το πλήθος των κωδικών λέξεων ενός κώδικα C συμβολίζεται με |C|.
- Ένας κώδικας ονομάζεται ***ισομήκης κώδικας*** (ή κώδικας μπλοκ) αν όλες οι κωδικές λέξεις έχουν το ίδιο μήκος.

- **<u>Βασικές Παραδοχές</u>**
- Ο δέκτης έχει την δυνατότητα να λάβει όλες τις λέξεις που μεταδόθηκαν, με ή χωρίς σφάλματα. Π.χ. εάν σε είσοδο 01001 τότε σε έξοδο λανθασμένη ίσως αλλά ισομήκης ακολουθία ψηφίων δηλ. 00101 αλλά όχι 0011
- Τα σφάλματα, δηλαδή ο θόρυβος, εμφανίζονται διασκορπισμένα κατά τυχαίο τρόπο και όχι σε συστάδες (bursts). Η πιθανότητα δηλ να αλλοιωθεί ένα bit κατά τη μετάδοση είναι η ίδια με αυτή οποιουδήποτε άλλου bit και δεν επηρεάζεται από σφάλματα σε γειτονικά δυαδικά ψηφία.

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- ***Αξιοπιστία*** ενός δυαδικού συμμετρικού καναλιού είναι ο πραγματικός αριθμός p, $0 \le p \le 1$, όπου p είναι η πιθανότητα της ορθής μεταφοράς ενός δυαδικού ψηφίου μέσω του καναλιού.
  - Επειδή κάθε κανάλι αξιοπιστίας $0 \le p \le 1/2$ μπορεί να μετατραπεί σε ένα κανάλι $1/2 \le p \le 1$, θα θεωρούμε ότι $1/2 \le p \le 1$.

- Ο **<u>ρυθμός πληροφορίας</u>** ενός κώδικα είναι το ποσοστό της αρχικής πληροφορίας (δηλ. τα ψηφία πληροφορίας πριν την κωδικοποίηση) που μεταφέρεται από την κωδική λέξη. Ο ρυθμός πληροφορίας ενός δυαδικού κώδικα C μήκους n είναι ίσος με $(1/n)\log_2|C|$, κείται δε μεταξύ 0 ($|C|=1$) και 1($|C| = 2^n$)
  - π.χ. εάν C1 = {00, 10, 01, 11}, τότε ο ρυθμός πληροφορίας είναι: $(1/n)\log_2|C1| = (1/2)\log_2 4 = 1$).
  - Εάν C2 = {000, 101, 011, 110}, τότε ο ρυθμός πληροφορίας είναι: $(1/n)\log_2|C2| = (1/3)\log_2 4 = 2/3$).
  - Έστω ότι μεταδίδεται το μήνυμα 0010 και παραλαμβάνεται το 0011. Δεν υπάρχει δυνατότητα ανίχνευσης στην περίπτωση του C1.
  - Αν όμως χρησιμοποιήσουμε τον C2 όπου το τελευταίο ψηφίο κάθε κωδικής λέξης είναι το ψηφίο ελέγχου ισοτιμίας τότε όταν στείλουμε την κωδική λέξη 000 και παραλάβουμε την λέξη 001, αυτή δεν αποτελεί κωδική λέξη και έτσι καταλαβαίνουμε ότι παραλάβαμε λάθος.
  - Δεν είναι πάντοτε δυνατή η ανίχνευση και ακόμα δυσκολότερη η διόρθωση

- Βασικές Πράξεις που ορίζονται μεταξύ των δυαδικών λέξεων:
  - (XOR) πρόσθεση : 0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1 και 1 + 1 = 0
  - (AND) πολ/σμός: 0 . 0 = 0, 0 . 1 = 0, 1 . 0 = 0 και 1 . 1 = 1.

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- **<u>Ορισμός</u>**: ***Βάρος (Weight) 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
  - **<u>Παράδειγμα:</u>** Για x1 = 000000, x2 = 000010, x3 = 110001 wt(x1)=0, wt(x2)=1, wt(x3)=3

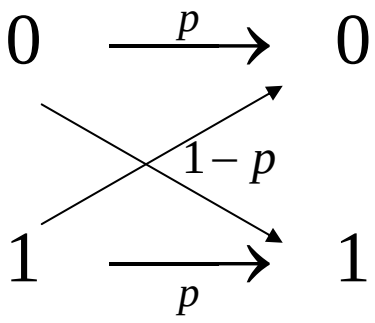
- **<u>Ορισμός</u>**: ***Απόσταση (Distance) Hamming*** ή απλά απόσταση, d(x, y), μεταξύ δύο λέξεων x και y του ιδίου μήκους n ονομάζεται το πλήθος των θέσεων, στις οποίες οι δύο λέξεις εμφανίζουν ασυμφωνία του δυαδικού ψηφίου. Η απόσταση παίρνει τιμές από 0 έως n.

- Εύκολα μπορεί να παρατηρηθεί ότι d(x,y)=wt(x+y)
  - **<u>Παράδειγμα</u>**: d(x1, x2)= wt(x1+x2) = wt(000000 +000010)= wt(000010)=1 d(x1, x3)=wt (x1+x3)=wt(110001)=3, d(x2, x3) = wt(110011)=4

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- Βασική υπόθεση ότι έχομε σχεδόν αποκλειστικά δυαδικό συμμετρικό κανάλι (Binary Symmetric Channel)



- Έστω π(x, y) η πιθανότητα να μεταδόθηκε η λέξη x και να ελήφθη από τον παραλήπτη η λέξη y.
- Εάν οι λέξεις x,y μήκους n διαφέρουν κατά d ψηφία τότε n-d ψηφία μεταδόθηκαν σωστά και d εσφαλμένα και ισχύει: $\pi(x,y)=p^{n-d}(1-p)^{d}$.

- **<u>Θεώρημα</u>**
- 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 π(x1, y) ≤ π(x2, y) αν και μόνο αν d1 ≥ d2.
- <u>Απόδειξη</u> Για να ισχύει η ανισότητα π(x1, y) ≤ π(x2, y) αρκεί να ισχύει
- $p^{n-d1}(1-p)^{d1} \le p^{n-d2}(1-p)^{d2}$ ή $(p/(1-p))^{d2-d1} \le 1$. Εφόσον ισχύει $(p/(1-p))>1$ τότε $d2 \le d1$.

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- **<u>Γενικά για κωδικοποίηση</u>**:
- Πρώτα επιλέγεται ένας θετικός ακέραιος k, το μήκος κάθε δυαδικής λέξης που αντιστοιχεί σε ένα μήνυμα. Το μήκος των λέξεων επιλέγεται $2^k \geq |M|$, όπου |M| είναι το πλήθος των δυνατών μηνυμάτων.
- Επιπλέον, επιλέγεται το πλήθος των n-k δυαδικών ψηφίων που θα προστεθούν σε κάθε λέξη (πλεονασμός) έτσι ώστε να μπορεί να ανιχνεύεται ή και να διορθώνεται το επιθυμητό πλήθος σφαλμάτων. Έτσι προκύπτουν οι κωδικές λέξεις που αντιστοιχούν στα δυνατά μηνύματα, μήκους n ψηφίων,
  - Τα πλεονάζοντα bits, n-k, ονομάζονται bits ισοτιμίας (parity)
  - Εάν τα πλεονάζοντα bits προκύπτουν ως γραμμικές συναρτήσεις των bits της πηγής s, τότε ο κώδικας είναι γραμμικός.
- Εάν τα μη κωδικοποιημένα k δυαδικά ψηφία (ψηφία πληροφορίας) μεταδίδονται μαζί με τα (n-k) πλεονάζοντα που παράγονται κατά την κωδικοποίηση, τότε ο κώδικας ονομάζεται συστηματικός-σε αντίθετη περίπτωση είναι μη-συστηματικός λ.χ.
  - Εάν u1, u2, u3 ψηφία πληροφορίας και η κωδική λέξη είναι u1,u2,u3,x4 με x4=bit ισοτιμίας=u1+u2+u3 ο κώδικας είναι συστηματικός
  - Εάν η κωδικοποιημένη λέξη είναι η x1, x2, x3 με x1= u1+u2, x2=u1+u3, x3=u2+u3 τότε ο κώδικας είναι μη συστηματικός

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- **<u>Γενικά για αποκωδικοποίηση:</u>**
- Έστω x,y η αποσταλείσα/ληφθείσα λέξη. Εάν y ≠x και το y δεν είναι κωδική λέξη, y∉ C (ανίχνευση λάθους), τότε για λήψη απόφασης χρησιμοποιείται η **Αποκωδικοποίηση Μεγίστης Πιθανότητας (ΑΜΠ)** :
- Αν υπάρχει μόνο μία κωδική λέξη x, η οποία εμφανίζει την μικρότερη απόσταση από τη λέξη y, σε σύγκριση με όλες τις άλλες κωδικές λέξεις, τότε η y αποκωδικοποιείται ως x*(<u>μεγιστοποίηση της πιθανότητας π(x,y)</u>)*
- Εάν υπάρχουν περισσότερες κωδικές λέξεις με ίδια απόσταση από τη y:
  - Είτε ο αποδέκτης αποκωδικοποιεί αυθαίρετα τη ληφθείσα λέξη ως μία από αυτές τις κωδικές λέξεις => **Πλήρης Αποκωδικοποίηση Μέγιστης Πιθανότητας (ΠΑΜΠ)**
  - Είτε επαναλαμβάνεται η μετάδοση => **Ατελής Αποκωδικοποίηση Μέγιστης Πιθανότητας (ΑΑΜΠ).** Επανάληψη μετάδοσης μπορεί να ζητηθεί και όταν,υπάρχει μια μόνο κωδική λέξη εγγύτερη στη λέξη y, με πολύ μεγάλη απόσταση
- **<u>Παράδειγμα</u>**:Εάν |M|=2, k = 1, n = 3 και C={000, 111}, βασιζόμενοι στην ΑΑΜΠ:
  - Ο αποδέκτης αποφασίζει για «111», εφόσον είτε y= 111 ή y= «011», «101 ή «110», καθώς έχουν μικρότερη απόσταση προς την «111» από ό,τι προς «000».
  - Συμπεραίνει την κωδική λέξη «000» σε οποιαδήποτε από τις υπόλοιπες τέσσερις δυαδικές ακολουθίες. Η περίπτωση της ίσης απόστασης της ληφθείσας λέξης δεν είναι δυνατή με τον κώδικα αυτό

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- **ΠΡΟΤΥΠΟ ΣΦΑΛΜΑΤΟΣ - ΑΠΟΣΤΑΣΗ ΚΩΔΙΚΑ**
- Ως ***Πρότυπο σφάλματος***, ε ορίζεται το άθροισμα της κωδικής λέξης x που μεταδόθηκε με τη λέξη y που ελήφθη στον αποδέκτη, δηλαδή $\varepsilon = x + y$.
- Λέμε ότι ο κώδικας C ανιχνεύει το πρότυπο σφάλματος ε, αν και μόνο αν $x + \varepsilon = y$ δεν είναι κωδική λέξη, (για κάθε) $\forall\ x \in C$.
- Ως ***Απόσταση ενός κώδικα*** C ορίζεται η μικρότερη από τις (Hamming) αποστάσεις όλων των δυνατών ζευγών κωδικών λέξεων του κώδικα.
- Δεδομένου ότι $d(x, y) = wt(x + y)$, η απόσταση του κώδικα C είναι ίση με την ελάχιστη τιμή του βάρους $wt(x + y)$, με $x, y \in C$ και $x \neq y$.
- **Παράδειγμα**
  - Έστω ο C = {0000, 1010, 1111} Εάν η 1010 μεταδόθηκε τρεις φορές και ο δέκτης έλαβε με τη σειρά τις λέξεις 0100, 1001 και 1010 τότε τα αντίστοιχα πρότυπα σφάλματος είναι 1010 + 0100 = 1110, 1010 + 1001 = 0011και 1010 + 1010 = 0000. Η απόσταση δε του κώδικα είναι ίση με d(0000, 1010) =d(1010, 1111) =wt (1010 +1111) =wt (0101) = 2.

©2006, Σπύρος Δενάζης

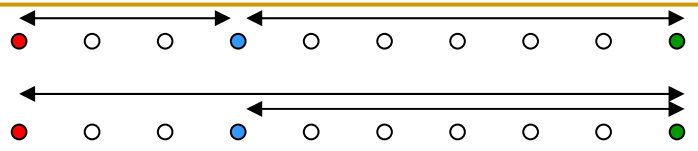
Εισαγωγή στην Κωδικοποίηση

- **Ανίχνευση Σφαλμάτων:**
- ***Θεώρημα Ανίχνευσης Σφαλμάτων***
  - Ένας κώδικας **C απόστασης d ανιχνεύει όλα τα μη μηδενικά πρότυπα σφάλματος ε βάρους μικρότερου ή ίσου του d – 1**, ενώ υπάρχει τουλάχιστον ένα πρότυπο ε βάρους d που δεν ανιχνεύει ο κώδικας C.
  - **Απόδειξη:** Έστω ε με $wt(\varepsilon) \leq d-1$ και $x \in C$. Τότε $d(x, x + \varepsilon) = wt(x + x + \varepsilon) = wt(\varepsilon) \leq d - 1 < d$. Άρα η λέξη $y = x + \varepsilon$ δεν ανήκει στον C (εφόσον απόσταση C =d) και συνεπώς ανιχνεύσιμη. Εάν $\varepsilon = x+y$ με $wt(\varepsilon)=d$ τότε υπάρχει τουλάχιστον ένα τέτοιο ε με $y=x+\varepsilon \in C$ και άρα y μη ανιχνεύσιμο σφάλμα
- **Παράδειγμα:** Ο κώδικας C = {000, 111} έχει απόσταση d= wt(000 +111) =wt(111)=3. Άρα ανιχνεύεται από τον κώδικα κάθε πρότυπο σφάλματος ε βάρους 1 ή 2 (όπως τα 011 , 100 κλπ.). Δεν ανιχνεύει όμως το πρότυπο σφάλματος «111» βάρους 3 (λ.χ. $y= 000+\varepsilon= 000+111=111 \in C$)

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- **Διόρθωση Σφαλμάτων**
- **Ορισμός:** Ένας κώδικας C **διορθώνει** το πρότυπο σφάλματος ε αν $\forall$ x $\in$ C, τότε η r = x + ε είναι εγγύτερα στη x από ό,τι σε οποιαδήποτε άλλη λέξη z $\in$ C. Ένας κώδικας C καλείται β – διόρθωσης, αν διορθώνει όλα τα ε με wt(ε) ≤ β και δεν διορθώνει τουλάχιστον ένα ε βάρους β + 1.
- ***Θεώρημα Διόρθωσης Σφαλμάτων***
- Ένας κώδικας C απόστασης d **διορθώνει** όλα τα πρότυπα σφάλματος βάρους **t μικρότερου ή ίσου του ⌊(d – 1)/2⌋**(*) και υπάρχει τουλάχιστον ένα πρότυπο σφάλματος βάρους 1 + t που δεν διορθώνει ο κώδικας C.
  - ***Ισοδύναμη διατύπωση***: Ένας κώδικας C για να μπορεί να διορθώσει t σφάλματα θα πρέπει να έχει απόσταση **d≥2t+1**
  - **Απόδειξη:** Έστω ε με ε>0 και wt(ε) ≤ d-1 και x,y $\in$ C , x≠y. Για το 1ο σκέλος αρκεί να δειχθεί ότι d(x, x + ε) < d(y, x + ε). Γενικά μεταξύ των αποστάσεων τριών λέξεων ίσου μήκους, ισχύει: d(y, x + ε) + d(x + ε, x) ≥d(y, x) ≥d. Λαμβάνοντας υπόψη ότι d(x + ε, x) = wt(x + ε + x) = wt(ε) και wt(ε) ≤ (d – 1)/2 ή 2wt(ε) + 1 ≤ d, ισχύει d(y, x + ε) + wt(ε) ≥d ≥ 2wt(ε) + 1 και άρα d(y, x + ε) ≥wt(ε) + 1 =d(x, x + ε) + 1.
  - Επομένως, d(x, x + ε) < d(y, x + ε) και προκύπτει ότι ο κώδικας διορθώνει το πρότυπο σφάλματος ε. Ομοίως αποδεικνύεται και το 2ο σκέλος



d(y, x) + d(x, z) ≥d(y, z)

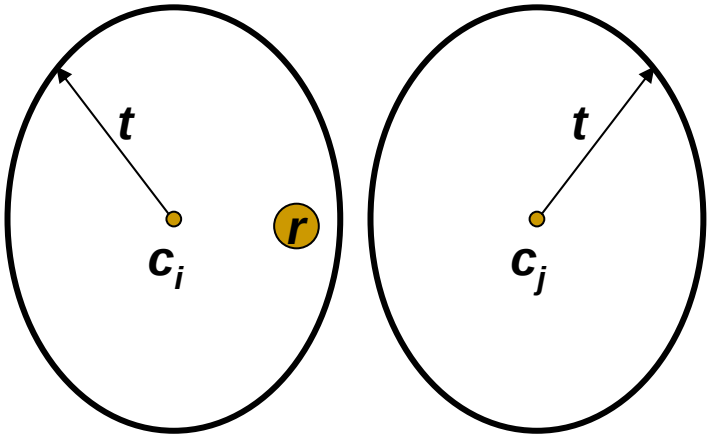
d(y, z) + d(z, x) ≥d(y, z)

(*) ⌊χ⌋= με το μεγαλύτερο ακέραιο v≤χ

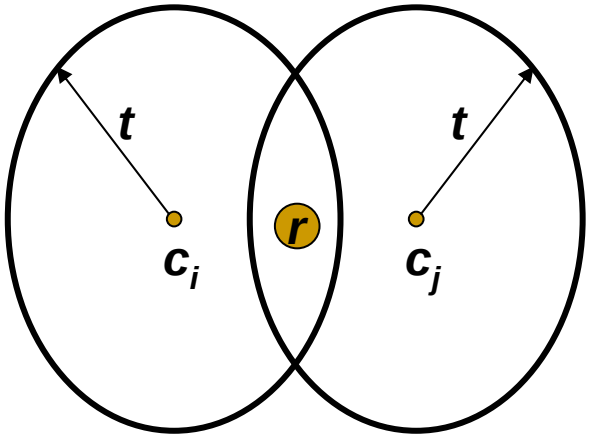
©2006, Σπύρος Δενάξης

Εισαγωγή στην Κωδικοποίηση

- Γραφική Απόδειξη του Θεωρήματος Διόρθωσης Σφαλμάτων



α) Απόσταση Hamming $d(c_i,c_j)\geq 2t+1$



β) Απόσταση Hamming $d(c_i,c_j)<2t+1$

- Στην (α) περίπτωση οι σφαίρες Hamming με κέντρα κωδικές λέξεις και ακτίνα t είναι μη επικαλυπτόμενες οπότε τα σφάλματα (όπως το r) που κείνται στην περιοχή τους είναι διορθώσιμα κατά ΑΜΠ σε αντίθεση με (β) περίπτωση όπου οι σφαίρες επικαλύπτονται και άρα κάποια σφάλματα που ανήκουν στην τομή των περιοχών ισαπέχουν από κωδικές λέξεις και συνεπώς είναι μη διορθώσιμα.

©2006, Σπύρος Δενάζης

Εισαγωγή στην Κωδικοποίηση

- **<u>Παράδειγμα:</u>** Ποια πρότυπα σφάλματος διορθώνονται από C = {000, 111};
- Σύμφωνα με το θεώρημα, αφού η απόσταση του κώδικα είναι d= 3, διορθώνει κάθε πρότυπο σφάλματος βάρους $t \leq \lfloor (3 - 1)/2 \rfloor = 1$.
- Όπως εδείχθη στο προηγούμενο παράδειγμα, ο αποδέκτης συμπεραίνει την κωδική λέξη «111», εφόσον (λάβει αυτήν ή λάβει μία από τις «011», «101 ή «110», δηλαδή διορθώνει:
  - τα πρότυπα σφάλματος ε1= 111 + 011 = 100, ε2=111 + 101 = 010 και ε3=111 + 110 = 001 στην περίπτωση μετάδοσης της λέξης «111».
- Ομοίως ο αποδέκτης συμπεραίνει την «000», εφόσον λάβει αυτήν ή λάβει μία από τις «001», «010» ή «100», δηλαδή διορθώνει:
  - Τα πρότυπα σφάλματος 1000 + 100 = 100, 000 + 010 = 010 και 000 + 001 = 001.
- Συνεπώς ο κώδικας C διορθώνει τα πρότυπα σφάλματος 100, 010 και 001,
- ο C δεν διορθώνει πρότυπα σφάλματος βάρους μεγαλύτερου του 1.
  - π.χ., κατά τη μετάδοση της λέξης «111», αν εμφανιστεί το πρότυπο σφάλματος «110», δηλαδή ληφθεί η λέξη «001», ο κώδικας τη διορθώνει εσφαλμένα σε «000».

©2006, Σπύρος Δενάζης

ΓΡΑΜΜΙΚΟΙ ΚΩΔΙΚΕΣ

(Linear Block Codes)

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες

- **<u>Εισαγωγή - Ορισμοί - Ιδιότητες</u>**
- Ένας κώδικας C ονομάζεται ***γραμμικός*** αν $\forall$ x,y$\in$C, τότε και (x + y)$\in$C. Π.χ. ο C = {00, 11} είναι γραμμικός, ενώ ο C = {00, 10, 11} δεν είναι γραμμικός, αφού η 11 + 10 = 01 δεν είναι κωδική λέξη.
- Κάθε λέξη ενός γραμμικού κώδικα αποτελείται από τα bits του αρχικού μηνύματος και από ένα αριθμό πλεοναζόντων bits ισοτιμίας που προκύπτουν ως γραμμικές συναρτήσεις των bits του αρχικού μηνύματος
- Κάθε γραμμικός κώδικας περιέχει τη μηδενική λέξη, (προκύπτουσα από το άθροισμα μιας κωδικής λέξης με τον εαυτό της).
- Πλεονεκτήματα γραμμικών κωδίκων σε σχέση με μη γραμμικούς.
  - Η απόσταση ενός γραμμικού κώδικα είναι ίση με το ελάχιστο των βαρών των μη μηδενικών κωδικών λέξεων.
  - Η κωδικοποίηση ενός γραμμικού κώδικα είναι πιο απλή και έχει μικρότερες αποθηκευτικές απαιτήσεις.
  - Υπάρχει μία πιο απλή διαδικασία αποκωδικοποίησης μέγιστης πιθανότητας (ΠΑΜΠ ή ΑΑΜΠ) από ότι έχει αναφερθεί έως τώρα
  - Η περιγραφή των συνόλων των προτύπων σφάλματος που ανιχνεύει ή διορθώνει ένας γραμμικός κώδικας είναι πιο εύκολη από ό,τι στη γενική περίπτωση.

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες - Μαθηματικό Υπόβαθρο

- Υπάρχει στενή αντιστοιχία εννοιών της γραμμικής άλγεβρας και εννοιών της θεωρίας κωδικοποίησης
  - Απαραίτητη η εμβάθυνση στις παρακάτω έννοιες της γραμμικής άλγεβρας για σαφέστερη κατανόηση των γραμμικών κωδίκων

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

Γραμμικοί Κώδικες-Μαθηματικό Υπόβαθρο

- Ο διανυσματικός χώρος K^n ($K = \{0, 1\}$), απαρτίζεται από τις βαθμωτές ποσότητες (scalars) 0 και 1 και το σύνολο των διανυσμάτων (ή λέξεων) μήκους n, καθώς και από τις πράξεις της πρόσθεσης διανυσμάτων (λέξεων) και του πολ/σμού βαθμωτών ποσοτήτων με διανύσματα που ικανοποιούν μία σειρά ιδιοτήτων
- ***Ιδιότητες των πράξεων της πρόσθεσης και του πολλαπλασιασμού στο K^n***
  - όπου x, y, z διανύσματα (ή λέξεις του ιδίου μήκους n), α και β οι βαθμωτές ποσότητες του διανυσματικού χώρου K^n και 0 η μηδενική λέξη.

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

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες-Μαθηματικό Υπόβαθρο

- Ένα μη κενό υποσύνολο S του διανυσματικού χώρου K^n είναι ένας υποχώρος αυτού, αν για κάθε ζεύγος διανυσμάτων (λέξεων) y, z $\in$ S, ισχύει (y + z) $\in$ S και α $\cdot$ y $\in$ S για κάθε βαθμωτή ποσότητα α. Άρα C είναι ένας γραμμικός κώδικας αν και μόνο αν C είναι υποχώρος του K^n.
- Το σύνολο όλων των γραμμικών συνδυασμών των διανυσμάτων (ή λέξεων) ενός συνόλου S = {z1, z2,…, zk} ονομάζεται το ***γραμμικό ανάπτυγμα του S και συμβολίζεται με <S>.***
  - Μια λέξη y είναι γραμμικός συνδυασμός των λέξεων z1,…, zk αν $\exists$ βαθμωτές ποσότητες α1,…, αk τέτοιες ώστε: y = a1 $\cdot$ z1+ …+ αk $\cdot$ zk.
- Το γραμμικό ανάπτυγμα <S> κάθε υποσυνόλου S του K^n είναι υποχώρος του K^n. ***Το <S> καλείται γραμμικός κώδικας*** προκύπτων εκ του S.
- Το γραμμικό ανάπτυγμα <S> του υποσυνόλου S του K^n περιέχει τη μηδενική λέξη, όλες τις λέξεις του S και τα επί μέρους αθροίσματά τους
- **<u>Παράδειγμα:</u>** Το γραμμικό ανάπτυγμα του υποσυνόλου S = {00011, 11100} αποτελείται από τις ακόλουθες λέξεις: 00000, 00011, 11100, 00011 + 11100 = 11111. Επομένως, <S> ={00000, 00011, 11100, 11111}.
- Το ***βαθμωτό γινόμενο δύο διανυσμάτων*** x = (α1,…, αn) και y = (β1,,…, βn) στο K^n ορίζεται ως x $\cdot$ y= α1 $\cdot$ β1 + … + αn $\cdot$ βn. Π.χ.Το γινόμενο των x = 00011 και y=11100 στο K^5 είναι: 00011 $\cdot$ 11100 = 0 $\cdot$ 1+0 $\cdot$ 1+0 $\cdot$ 1+1 $\cdot$ 0 +1 $\cdot$ 0 = 0+0+0+0+0=0.

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες-Μαθηματικό Υπόβαθρο

- ***Δύο διανύσματα (λέξεις) x και y είναι ορθογώνια αν x ·y = 0***. Ένα διάνυσμα (λέξη) x χαρακτηρίζεται ορθογώνιο σε ένα σύνολο S, αν το x είναι ορθογώνιο σε κάθε διάνυσμα (λέξη) $y \in S$.
- Το σύνολο όλων των διανυσμάτων, που είναι ορθογώνια ενός συνόλου S, συμβολίζεται με $S^{\perp}$ και ονομάζεται το ***ορθογώνιο συμπλήρωμα*** του S.
  - Για κάθε υποσύνολο S του διανυσματικού χώρου K^n, το ορθογώνιο συμπλήρωμά του, $S^{\perp}$, είναι επίσης υποχώρος του K^n.
  - Για κάθε διανυσματικό χώρο K^n, αν C = <S>, τότε $C^{\perp} = S^{\perp}$. (Δηλ. το ορθογώνιο συμπλήρωμα του γραμμικού αναπτύγματος <S> ισούται με το ορθογώνιο συμπλήρωμα του S, $S^{\perp}$.)
  - Το ορθογώνιο συμπλήρωμα $C^{\perp}$ καλείται ***δυϊκός κώδικας*** του κώδικα C, όπου S υποσύνολο του διανυσματικού χώρου K^n , C = <S> και $C^{\perp} = S^{\perp}$
- **<u>Παράδειγμα</u>**: Για να υπολογίσομε το ορθογώνιο συμπλήρωμα του S = {0001, 1100} $C^{\perp} = S^{\perp}$ αρκεί να βρούμε όλα τα x = (α1, α2, α3, α4), με x · 0001 = 0 και x · 1100 = 0.
  - Έχομε 0 · α1 +0 · α2 + 0 · α3 + 1 · α4 = 0 ⇒ α4 = 0.
  - Από το δεύτερο γινόμενο 1 · α1 + 1 · α2 + 0 · α3 + 0 · α4 = 0 ⇒, α1 + α2 = 0, ⇒ α1 = α2 = 0 ή α1 = α2=1. Το α3 = 0 ή 1.
  - Συνεπώς, α1 = α2 = 0 είτε α1 = α2 = 1, α3 = 0 είτε α3 = 1 και α4 = 0.
  - Οι συνδυασμοί των παραπάνω επιλογών οδηγούν στο ορθογώνιο συμπλήρωμα $C^{\perp} = S^{\perp}$ = {0000, 0010, 1100, 1110}.

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες-Μαθηματικό Υπόβαθρο

- Ένα σύνολο διανυσμάτων S = {z1, z2,…, zk} είναι ***Γραμμικώς Ανεξάρτητο*** αν ∄ βαθμωτές ποσότητες α1, α2,…, αk, με τουλάχιστον μία εξ αυτών ≠ 0, έτσι ώστε: α1 · z1 + … + αk · zk. = 0. Διαφορετικά, S = γραμμικώς εξαρτημένο.
  - Ένα σύνολο, S που περιέχει τη μηδενική λέξη = γραμμικώς εξαρτημένο.
  - Αν S≠{0}, περιέχει ένα μέγιστης διάστασης γραμ. ανεξάρτητο υποσύνολο
- **<u>Παράδειγμα</u>**: Το S = {110, 011, 101, 111} =γραμμικώς εξαρτημένο
  - Ισχύει α1 · 110 + α2 · 011 + α3 · 101 + α4 · 111 = 000 ⇒ α1 α1 0 + 0 α2 α2 +α3 0 α3 + α4 α4 α4 = 000, ⇒ α1 + α3 + α4 = 0, α1 + α2 + α4 = 0 και α2 + α3+ α4 = 0. Προσθέτοντάς τες ⇒ α4 = 0. Έτσι, α1 + α3 = 0, α1 + α2 = 0 και α2 + α3 = 0, ⇒ α1 = α2 = α3. Μπορούμε να επιλέξουμε λοιπόν α1 = α2 = α3 = 1 και επομένως το S=γραμμικώς εξαρτημένο
- <u>Για την εύρεση ενός από τα μέγιστης διάστασης, γραμ. ανεξάρτητου, υποσυνόλου του S, αφαιρούμε από το S το πρώτο διάνυσμα που βρίσκουμε να είναι γραμμ. συνδυασμός των άλλων</u> δηλ. το 110 (110= 011+101) και εξετάζομε αν το S' = {011,101, 111} = γραμ. ανεξάρτητο.
  - Από την 0 α1 α1 +α2 0 α2 + α3 α3 α3 = 000, ⇒α2 + α3 = 0 **(1),** α1 + α3 = 0 **(2)**, α1 + α2 + α3 =0 **(3)**. Από τις **(2)**, **(3)** ⇒ α1 = 0 άρα α3 = 0 και α2 = 0. ⇒ ∄ βαθμωτές ποσότητες, ≠ 0, που ικανοποιούν την (1) ⇒ S' = ένα, μέγιστης διάστασης, γραμμ. ανεξάρτητο υποσύνολο του S.

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες-Μαθηματικό Υπόβαθρο

- Ένα μη κενό υποσύνολο διανυσμάτων B ενός διανυσματικού υποχώρου V είναι μία ***Βάση για τον υποχώρο V***, αν <B> = V και το B είναι γραμμικώς ανεξάρτητο σύνολο.
  - Ένα γραμμικώς ανεξάρτητο υποσύνολο διανυσμάτων S είναι μία βάση για τον διανυσματικό υποχώρο <S>.
  - Κάθε ένα από τα μέγιστης διάστασης γραμμικώς ανεξάρτητα υποσύνολα ενός γραμμικώς εξαρτημένου συνόλου S είναι βάση του υποχώρου <S>..
- **<u>Παράδειγμα</u>**: Εδείχθη ότι ένα από τα μέγιστης διάστασης, γραμμ.ανεξάρτητα υποσύνολα του S = {110, 011, 101,111}, (S= γραμ. εξαρτημένο) είναι το B = {011, 101, 111} $\Rightarrow$ B= βάση του <S> = {000,011,101,111,110,100,010, 001}.
- Ένας διανυσματικός (υπο)χώρος έχει πολλές βάσεις με ίδιο πλήθος διανυσμάτων k με ***k=καλείται διάσταση του (υπο)χώρου***
  - π.χ διάσταση του <S> στο ως άνω παράδειγμα=3 Επίσης η διάσταση του διανυσματικού χώρου K^n είναι n, επειδή το σύνολο των λέξεων μήκους n και βάρους 1, δηλαδή το σύνολο U={0…01, 0…10,…, 1…00}, είναι μια βάση του διανυσματικού χώρου K^n (με <U>= K^n).
- Αν η διάσταση ενός γραμμικού κώδικα (ή διανυσμ. (υπο)χώρου) C είναι k και μια βάση του X = {x1, x2,…, xk}, τότε $\forall$ c $\in$ C ισχύει c = α1 $\cdot$x1+… + αk$\cdot$xk για ***κάποια μοναδική*** επιλογή των α1,…, αk. Επειδή αi = 0 ή 1, οι δυνατοί συνδυασμοί των α1,…, αk είναι 2^k = πλήθος κωδικών λέξεων του C.

©2006, Σπύρος Δενάζης

Εύρεση Βάσης Γραμμικού Κώδικα C

- **<u>Τεχνική για εύρεση μίας βάσης ενός κώδικα C</u>**
- Ισχύει ότι για να βρούμε μια βάση ενός γραμμικού κώδικα C αρκεί να μεταφέρουμε σε μία ειδική μορφή (ΚΔΓ ή ΠΚΔΓ) τον πίνακα οι γραμμές του οποίου αποτελούνται από τις λέξεις του συνόλου S (ή και από όλες τις λέξεις του C), με C = <S>
- Ένας πίνακας βρίσκεται σε μορφή ***Κλιμακωτής Διάταξης Γραμμών (ΚΔΓ ή 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. Μια στήλη που περιέχει έναν «οδηγό» 1 καλείται στήλη «οδηγός»
- Ένας πίνακας βρίσκεται σε μορφή **Περιορισμένης Κλιμακωτής Διάταξης Γραμμών (ΠΚΔΓ ή Reduced Row Echelon Form)**, εάν είναι σε μορφή ΚΔΓ και επιπλέον ισχύει ότι σε κάθε στήλη οδηγό του πίνακα (δηλαδή στήλη που περιέχεται ο οδηγός «1» μιας γραμμής) δεν περιέχονται άλλα ψηφία «1» αλλά μόνο ψηφία «0»
  - Κάθε πίνακας με 0 και 1 μπορεί να τεθεί τόσο σε μορφή ΚΔΓ όσο και ΠΚΔΓ.
  - Ένας πίνακας (με 0 και 1) μπορεί να έχει πολλές μορφές ΚΔΓ αλλά μόνον μία μορφή ΠΚΔΓ

©2006, Σπύρος Δενάζης

Εύρεση Βάσης Γραμμικού Κώδικα C

- Ένας πίνακας τίθεται σε μορφή ΚΔΓ ή ΠΚΔΓ με τον μετ/σμό του σε διαδοχικούς ισοδύναμους πίνακες μέσω των ακολούθων δύο τύπων στοιχειωδών πράξεων που εφαρμόζονται στις γραμμές του:
  - Ανταλλαγή δύο γραμμών και
  - Αντικατάσταση μίας γραμμής από το άθροισμα του εαυτού της με κάποια άλλη
- **<u>Παράδειγμα</u>**
  - Έστω ο κώδικας C = {0000, 1110, 0111, 1001}, του οποίου οι λέξεις αποτελούν τις γραμμές του πίνακα P. Τον μετ/ζομε σε μορφή ΚΔΓ χρησιμοποιώντας τις ως άνω πράξεις ως εξής:

©2006, Σπύρος Δενάζης

Εύρεση Βάσης Γραμμικού Κώδικα C

- **<u>Παράδειγμα (Συνέχεια)</u>**
- Από τον αρχικό πίνακα P οδηγούμαστε στο 2ο πίνακα μόνο με ανταλλαγή γραμμών. Από το 2ο πίνακα στον 3ο με την αντικατάσταση της 3ης γραμμής με το άθροισμα του εαυτού της και της 1ης γραμμής. Τέλος, αντικαθιστώντας την 3ηγραμμή του 3ου πίνακα με το άθροισμα του εαυτού της και της 2ης γραμμής καταλήγουμε στον 4ο πίνακα

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

©2006, Σπύρος Δενάζης

Εύρεση Βάσης Γραμμικού Κώδικα C

- **<u>Παράδειγμα (Συνέχεια)</u>**
- Για τον μετ/σμό του Πίνακα P σε ΠΚΔΓ λαμβάνεται υπόψη ο επιπρόσθετος περιορισμός, η στήλη που περιέχει τον οδηγό «1» μιας γραμμής να μην περιέχει άλλα ψηφία «1».
- Από τον αρχικό πίνακα P οδηγούμαστε στο 2ο πίνακα με ανταλλαγή της 1ης με την 4η γραμμή και της 2ης με την 3η.
- Από το 2ο πίνακα στον 3ο με την αντικατάσταση της 3ης γραμμής με το άθροισμα του εαυτού της και της 1ης γραμμής.
- Τέλος, αντικαθιστώντας την 3η γραμμή του 3ου πίνακα με το άθροισμα του εαυτού της και της 2ης γραμμής καταλήγουμε στον 4ο πίνακα
- Πράγματι, ο 4ος πίνακας είναι σε μορφή ΠΚΔΓ, αφού οι δύο πρώτες του στήλες που περιέχουν τους οδηγούς «1» των δύο μη μηδενικών γραμμών περιέχουν μόνο ψηφία «0» στις υπόλοιπες θέσεις

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

©2000, Σπύρος Δενάζης

Εύρεση Βάσης Γραμμικού Κώδικα C

- **Ανακεφαλαιωτικά Σχόλια**
- Σύμφωνα με τον ορισμό της βάσης ενός διανυσματικού χώρου, οποιοδήποτε από τα μέγιστης διάστασης γραμμικώς ανεξάρτητα υποσύνολα του διανυσματικού (υπο) χώρου C (ή του συνόλου S, όπου C = <S>) είναι βάση του.
- Επίσης, όπως προαναφέρθηκε, οι μη μηδενικές γραμμές ενός πίνακα σε μορφή ΚΔΓ ή ΠΚΔΓ που σχηματίζεται από τις λέξεις του συνόλου S (ή από τις λέξεις του C, όπου C = <S>), είναι οι λέξεις ενός μέγιστης διάστασης γραμμικώς ανεξάρτητου υποσυνόλου του C και, επομένως, μία βάση του.
- Συμπερασματικά, για να βρούμε μία βάση του κώδικα C αρκεί να μεταφέρουμε σε μορφή ΚΔΓ ή ΠΚΔΓ τον πίνακα που σχηματίζεται από τις λέξεις του συνόλου S (ή και από όλες τις λέξεις του C, C = <S>).
- π.χ. στο προηγούμενο Παράδειγμα, το υποσύνολο {1110, 0111} είναι μια βάση του κώδικα C = {0000, 1110, 0111, 1001}, από την οποία προκύπτουν, με γραμμικούς συνδυασμούς, όλες οι λέξεις του C.
- Ομοίως μπορεί να βρεθεί και μία βάση του δυϊκού κώδικα $C^{\perp}$, χρησιμοποιώντας τις λέξεις που τον απαρτίζουν ως ανωτέρω.
  - Εναλλακτικά μπορεί να εφαρμοστεί ένας πιο απλός αλγόριθμος βασισμένος στην γνώση των λέξεων του συνόλου S ή του C, C = <S> ο οποίος περιγράφεται στη συνέχεια.

©2006, Σπύρος Δενάζης

Εύρεση Βάσης Δυϊκού κώδικα $C^{\perp}$

- Η διαδικασία εύρεσης μιας βάσης του δυϊκού κώδικα $C^{\perp}$($C = \langle S \rangle$) με k=διάσταση C, n=μήκος λέξεων C 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 k x n
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 τότε η διάσταση του πίνακα M είναι k x (n-k)
4. Σχηματισμός του πίνακα , $H= [M \;\; I]^T$ διάστασης n x (n – k), από τον πίνακα M (k x (n – k)) και τον πίνακα ταυτότητας I ((n – k) x (n – k)).
5. Ο πίνακας H (n x (n – k)) σχηματίζεται ως εξής:
   - Στις πρώτες k γραμμές του H τοποθετούνται με τη σειρά οι γραμμές του M.
   - Στις υπόλοιπες (n– k) γραμμές του H τοποθετούνται οι γραμμές του πίνακα ταυτότητας I διάστασης (n – k) x (n –k).
6. Μια βάση του δυϊκού κώδικα $C^{\perp}$ αποτελείται από τις στήλες του πίνακα H (ή τις γραμμές του ανάστροφου πίνακα H^T) και είναι διάστασης n-k.

©2006, Σπύρος Δενάζης

Εύρεση Βάσης Δυϊκού κώδικα $C^{\perp}$

- **<u>Παράδειγμα</u>**: Ζητείται μία βάση του $C^{\perp}$ με S = {11101, 10110, 01011, 11010} και C= <S>
- Σχηματίζεται ο πίνακας P με γραμμές της λέξης του S ο οποίος μετ/ζεται σε ΠΚΔΓ χρησιμοποιώντας ανταλλαγή ή και αντικατάσταση γραμμής από το άθροισμά της με άλλη

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

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

G

M

©2006, Σπύρος Δενάζης

Εύρεση Βάσης Δυϊκού κώδικα $C^{\perp}$

- **<u>Παράδειγμα (συνέχεια)</u>**:

Βάση

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

- Επομένως, μια βάση του δυϊκού κώδικα $C^{\perp}$ είναι το σύνολο {01110, 11101}.
- **<u>Παρατήρηση</u>**: Παρατηρήστε ότι ο ΠΚΔΓ, G = της μορφής G= [I M] που είναι σύνηθες για γραμμικούς κώδικες

©2006, Σπύρος Δενάζης

Γεννήτορας Πίνακας Γραμμικού Κώδικα C

- **<u>Ορισμός:</u>** Κάθε πίνακας, του οποίου οι γραμμές αποτελούν μία βάση του κώδικα C, ονομάζεται γεννήτορας πίνακας G για τον C.
  - Το πλήθος των γραμμών k του G = με τη διάσταση του C, δηλαδή = με το πλήθος των λέξεων που απαρτίζουν μία βάση του.
  - Αν η διάσταση ενός κώδικα C = k, το μήκος των κωδικών λέξεων = n και η απόστασή του d, τότε ο C συμβολίζεται ως (n, k, d) γραμμικός κώδικας.
- Αν G είναι ένας γεννήτορας πίνακας για έναν κώδικα C, τότε κάθε πίνακας ισοδύναμος του G, ως προς τις γραμμές, είναι γεννήτορας πίνακας για τον C.
- Για την εύρεση του G ενός κώδικα C, αρκεί να βρούμε μια βάση του $\Rightarrow$ τις μη μηδενικές λέξεις του πίνακα σε μορφή ΠΚΔΓ, που σχηματίζεται από τις λέξεις του C (ή του S, όπου C = <S>), όπως εδείχθη προηγουμένως

©2006, Σπύρος Δενάζης

Γεννήτορας Πίνακας Γραμμικού Κώδικα C

- **<u>Κωδικοποίηση</u>**:Ένας γεννήτορας πίνακας G για ένα γραμμικό κώδικα (n, k, d), C, μπορεί να αξιοποιηθεί για την κωδικοποίηση λέξεων (μηνυμάτων) u μήκους k ψηφίων ως εξής:
- C=u.G= [a1,a2,…ak] $[g1,g2,...gk]^T$ = a1.g1+ a2.g2+…+ak.gk = [b1,b2,..., bn],
  - u= [a1,a2,…ak] η μη κωδική λέξη του μηνύματος και c=[b1,b2,..., bn] η κωδική λέξη μήκους n ψηφίων και $[g1,g2,...gk]^T$ τα διανύσματα λέξεις (πλήθους n) που αποτελούν την βάση του C και απαρτίζουν τον G
  - Το αποτέλεσμα c είναι κωδική λέξη του C (εφόσον u.G = γραμ. συνδυασμός των γραμμών του G, που σχηματίζεται από τις λέξεις gi που απαρτίζουν μία βάση του κώδικα C).
- Ένας γεννήτορας πίνακας G, (kxn), του οποίου οι πρώτες k στήλες σχηματίζουν τον πίνακα ταυτότητας $\mathbf{I_k}$, (kxk), δηλαδή G = [I_k , M], λέγεται ότι βρίσκεται σε **τυπική μορφή (standard form).**
  - π.χ Ο γεννήτορας πίνακας G, ο οποίος προκύπτει στο βήμα 2 του σε προηγούμενο <u>παράδειγμα</u> είναι σε τυπική μορφή.
  - Ο κώδικας C, ο οποίος έχει γεννήτορα πίνακα G σε τυπική μορφή, χαρακτηρίζεται **συστηματικός κώδικας**

©2006, Σπύρος Δενάζης

Γεννήτορας Πίνακας Γραμμικού Κώδικα C

- Σε ένα τέτοιο συστηματικό κώδικα το μήνυμα u αποτελείται από τα πρώτα k ψηφία του c, αφού c = u.G = u.[I, M] = [uI, uM] = [u, uM]. Τα πρώτα k ψηφία των κωδικών λέξεων λέγονται ψηφία πληροφορίας και τα υπόλοιπα n – k, πλεονασμός ή ψηφία ελέγχου ισοτιμίας.
- Δεν έχουν όλοι οι γραμμικοί κώδικες γεννήτορες πίνακες σε τυπική μορφή [I, M]
  - Σε αυτή την περίπτωση και πάλι k από τα ψηφία των κωδικών λέξεων αποτελούνται από τα αρχικά ψηφία του μηνύματος δεν είναι όμως συνεχόμενα αλλά εντοπίζονται σε k προκαθορισμένες θέσεις της κωδικής λέξης που ορίζονται από τις αντίστοιχες θέσεις των στηλών-οδηγών του G
  - *Και σε αυτή την περίπτωση ο G μπορεί να μετασχηματισθεί σε τυπική μορφή με κατάλληλη εναλλαγή στηλών του.*
- **Παράδειγμα:** Οι κωδικές λέξεις που προκύπτουν εάν το μήνυμα u=[0 0 1] για Γεννήτορες Πίνακες G1, G2 είναι:

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \qquad G_2 = \begin{bmatrix} \underline{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \underline{1} & 0 & 1 \\ 0 & 0 & 0 & \underline{1} & 1 \end{bmatrix}$$

- c1= u.G1= 0 (10001) + 0 (01011) + 1(00111)= 00111$\Rightarrow$ [u1,u2,u3] $\rightarrow$[u1,u2,u3,u2+u3,u1+u2+u3] και 001 ψηφία πληροφορίας,11 ισοτιμίας
- c2= u.G2 = 0 (11001) + 0 (00101) +1(00011)= <u>0</u>0<u>0</u> <u>1</u>1 $\Rightarrow$ [u1,u2,u3] $\rightarrow$[u1,u1,u2,u3,u1+u2+u3] και <u>001</u> ψηφία πληροφορίας και 01 ισοτιμίας

©2006, Σπύρος Δενάζης

Πίνακας Ισοτιμίας Γραμμικού Κώδικα C

- ***Πίνακας Ελέγχου Ισοτιμίας*** ενός κώδικα C καλείται ένας πίνακας H του οποίου οι στήλες σχηματίζουν μια βάση του δυϊκού κώδικα $C^{\perp}$, και **μπορεί να χρησιμοποιηθεί για την αποκωδικοποίηση κωδικοποιημένων μηνυμάτων**.
  - Όπως είδαμε υπάρχει αλγόριθμος, ώστε δοθέντος του C να μπορούμε πάντα να προσδιορίσουμε τον πίνακα H
- Αν η διάσταση του C είναι k, τότε η διάσταση του $C^{\perp}$, είναι n – k = με πλήθος των στηλών του H, ενώ το πλήθος των γραμμών του είναι n=ίσο με το μήκος των κωδικών λέξεων του κώδικα C.
  - Σύμφωνα με τα προλεχθέντα, ο γεννήτορας πίνακας G και ο πίνακας ισοτιμίας H ενός κώδικα C είναι γραμμ. ανεξάρτητοι ως προς τις γραμμές και τις στήλες, αντίστοιχα, αφού είναι βάσεις των κωδίκων C, $C^{\perp}$
- Το γινόμενο των πινάκων G και H ισούται με 0, δηλαδή $G \cdot H = 0$. (μια και $C^{\perp}$ άρα και μία βάση του H = ορθογ. συμπλήρωμα του S άρα και μίας βάσης του G , όπου C = <S> και $C^{\perp} = S^{\perp}$)
  - Εύκολα επίσης φαίνεται αυτό από το εάν ληφθεί υπ'όψη ότι $G=[I, M]$, $H= [M, I]^T$ $\Rightarrow G \cdot H= [I, M] \cdot [M, I]^T = M+M=0$
  - $\forall x \in C \Rightarrow x \cdot H= (u \cdot G) \cdot H= u (G H)= 0$

©2006, Σπύρος Δενάζης

Πίνακας Ισοτιμίας Γραμμικού Κώδικα C

- **<u>Θεώρημα:</u>** Η απόσταση d ενός γραμμικού κώδικα = με τον ελάχιστο αριθμό γραμμών του Πίνακα Ισοτιμίας Η των οποίων το άθροισμα ισούται με 0 (ή ισοδύναμα ο ελάχιστος αριθμός γραμμών που είναι γραμμικά εξαρτημένες).
- **<u>Απόδειξη:</u>** $\forall\ x \in C \Rightarrow x \cdot H = 0 \Rightarrow [x1,x2,\ldots,xn] \cdot [h1,h2,\ldots,hn]^T = 0 \Rightarrow [x1\ h1+x2\ h2+\ldots+xn\ hn] = [0,0,\ldots 0]$, hi= i γραμμή του Η. Λαμβάνοντας υπόψη ότι xi =1 ή 0 και wt(x) =∑ 1's ⇒ x H = με το άθροισμα wt(x) γραμμών του Η. Άρα εάν x_{min}=η x με το ελάχιστο wt(x) = d =απόσταση του κώδικα C, τότε $x_{min} \cdot H$ = με τον ελάχιστο αριθμό γραμμών d του Η που ισούνται με 0.
- **<u>Παράδειγμα:</u>** Έστω ο Η προηγούμενου παραδείγματος με

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

- Τότε μια και ισχύει ότι ή 2η + 3η γραμμή = (1 1) + (1 1) (ή ισοδύναμα η 1η +4η = (0 1) + (0 1)) του Η = (0 0) ⇒ η απόσταση του κώδικα είναι d=2

©2006, Σπύρος Δενάζης

Συνομάδες Γραμμικού Κώδικα C

- **Συνομάδα (coset)** = απαραίτητη έννοια για **αποκωδικοποίηση ενός κώδικα C**
- **<u>Ορισμός:</u>** Μια συνομάδα του C ***προσδιορισμένη*** από τη λέξη $x \in K^n$ n=μήκος κωδικής λέξης, συμβολίζεται ως C + x και ορίζεται ως το σύνολο όλων των λέξεων της μορφής c + x, όπου $c \in C$ (το x είναι σταθερό και το c κυμαίνεται σε όλο το εύρος του C). Δηλαδή, $C + x = \{c + x \mid c \in C\}$.
- **<u>Παράδειγμα:</u>** Ζητούνται όλες οι συνομάδες του κώδικα **C = {000, 111}**, k=1, n=3, n-k=2.
  - Για x = 001 έχουμε C + 001 = {000 + 001 = 001, 111 + 001 = 110}.
  - C + 010 = {010, 101},
  - C + 100 = {100, 011},
  - C + 011 = {011, 100},
  - C + 101 = {101, 010},
  - C + 110 = {110, 001},
  - **C + 111 = C + 000 = {000, 111}**.
  - Παρατηρούμε ότι ο αριθμός των όλων των συνομάδων είναι $2^{n-k}=2^2=4$ και κάθε συνομάδα αποτελείται από $2^k=21=2$ λέξεις όσες ακριβώς και το πλήθος των κωδικών λέξεων του κώδικα C
  - Επίσης παρατηρείστε ότι εάν $x,y \in C+x$ (ή ισοδύναμα στο C+y) τότε $x+y \in C$

©2006, Σπύρος Δενάζης

Συνομάδες Γραμμικού Κώδικα C

- Δεν υπάρχουν 2^n διαφορετικές συνομάδες όσες και οι λέξεις μήκους n του K^n καθώς είναι δυνατό δύο συνομάδες C + x = C + y να ταυτίζονται, ακόμα και αν x ≠ y όπως π.χ ισχύει στο προηγούμενο παράδειγμα.
- ***Ιδιότητες Συνομάδων***: Αν C είναι ένας συστηματικός γραμμικός κώδικας (n,k,d) και x και y δύο λέξεις επίσης μήκους n ψηφίων, τότε ισχύουν αναφορικά με τις συνομάδες τα ακόλουθα:
  1. Κάθε λέξη x περιέχεται στη συνομάδα C + x (λόγω ύπαρξης μηδενικής κωδικής λέξης σε γραμμικούς κώδικες)
  2. Το πλήθος των λέξεων σε μια συνομάδα είναι ίσο με το πλήθος των λέξεων του κώδικα C, δηλαδή $|C + x| = |C| = 2^k$.
  3. Αν μια λέξη x περιέχεται στη συνομάδα C + y, τότε ισχύει C + x = C + y, δηλαδή κάθε λέξη της συνομάδας την προσδιορίζει.
  4. Το πλήθος των διαφορετικών συνομάδων του κώδικα C, διάστασης k, ισούται με 2^{n-k}. (Από ιδιότητα 5 ⇒ πλήθος στοιχείων όλων των συνομάδων= 2^n ⇒ εφόσον από ιδιότητα 2, $|C + x| = 2^k$ τότε πλήθος συνομάδων= $2^n / 2^k = 2^{n-k}$)

©2006, Σπύρος Δενάζης

Συνομάδες Γραμμικού Κώδικα C

- ***Ιδιότητες Συνομάδων (συνέχεια)***

5. Οι λέξεις όλων των συνομάδων είναι διαφορετικές, ή ισοδύναμα, κάθε λέξη $x \in K^n$ περιέχεται μόνο σε μία συνομάδα του C, δηλαδή δύο συνομάδες C + x και C + y είτε ταυτίζονται είτε δεν έχουν κανένα στοιχείο κοινό.
   - Απόδειξη: Έστω ότι υπάρχουν δύο λέξεις ίδιες σε όλα τα σύνολα των συνομάδων $\Rightarrow$ δύο περιπτώσεις: α) Να βρίσκονται στην ίδια συνομάδα έστω του C+x. Τότε πρέπει $x + ci = x + cj$ ($ci, cj \in C$, $ci \neq cj$) $\Rightarrow ci = cj$ άτοπο.
   - β) Να βρίσκονται σε διαφορετικές συνομάδες έστω των C+ x, C+y. Τότε θα ίσχυε: $x + ci = y + cj \Rightarrow y = x + (ci + cj)$, με $(ci+cj) \in C \Rightarrow$ Οι x, y πρέπει να ανήκουν στην ίδια συνομάδα, άτοπο μιάς και η υπόθεσή μας είναι ότι x, y ανήκουν σε διαφορετικές συνομάδες, των C+ x και C+y.
6. Αν το άθροισμα $x + y \in C$, τότε οι x,y περιέχονται στην ίδια συνομάδα. Αν το άθροισμα $x + y \notin C$, τότε οι x,y περιέχονται σε διαφορετικές συνομάδες.
   - Απόδειξη: Α' σκέλος. Έστω ότι x, y $\in$ στην ίδια συνομάδα έστω του z+C και ας υποτεθεί ότι $x+y \notin C$ Τότε ισχύει $x=z+c1$, $y=z+c2 \Rightarrow x+y = (z+z) + (c1+c2) = 0 + c3 \Rightarrow x+y=c3$, $c3 \in C \Rightarrow x+y \in C$, άτοπο.
   - Ομοίως για Β' σκέλος έστω ότι $x+y \notin C$ και ας υποτεθεί ότι x, y $\in$ στην ίδια συνομάδα έστω του z+C. $\Rightarrow$ καταλήγομε πάλι στην $x+y=c3$, $c3 \in C \Rightarrow x+y \in C$, άτοπο

Αποκωδικοποίηση με Συνομάδες

- Έστω ο γραμμικός κώδικας C και ότι έχομε μετάδοση της κωδικής λέξης x, που οδηγεί στη λήψη της λέξης y. Τότε έχουμε το πρότυπο σφάλματος ε = x + y. Άρα ισχύει και x = ε + y και συνεπώς (Ιδιότητα 6) **οι λέξεις ε (πρότυπο σφάλματος) και y (ληφθείσα λέξη) περιέχονται στην ίδια συνομάδα του C**!
- Για την επιλογή του κατάλληλου ε δεδομένου ότι από y εντοπίσθηκε η κατάλληλη συνομάδα, λαμβάνεται υπόψη ότι πρότυπα σφάλματος μικρού βάρους λαμβάνουν χώρα με τη μεγαλύτερη πιθανότητα - αποκωδικοποίηση μέγιστης πιθανότητας (ΑΜΠ).
- ***Αλγόριθμος αποκωδικοποίησης με τη βοήθεια των Συνομάδων***

1. Λήψη της λέξης y και υπολογισμός της συνομάδας C + y.
2. Επιλογή της λέξης ε, ελάχιστου βάρους, που περιέχεται στη συνομάδα C + y.
   - Αν υπάρχουν περισσότερες λέξεις της συνομάδας C + y, με ελάχιστο βάρος, τότε στην (ΠΑΜΠ) περίπτωση αποκωδικοποίησης μέγιστης πιθανότητας επιλέγεται αυθαίρετα μία εξ αυτών, ενώ στην περίπτωση της (ΑΑΜΠ) αποκωδικοποίησης ζητείται επανάληψη της μετάδοσης.
3. Υπολογισμός της κωδικής λέξης x που μεταδόθηκε προσθέτοντας τη ληφθείσα λέξη y με το πρότυπο σφάλματος ελάχιστου βάρους ε, δηλαδή, x = y + ε.

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Συνομάδες

- ***Σχηματισμός Τυπικής Διάταξης Αποκωδικοποίησης***
  - Για επίτευξη της αποκωδικοποίησης με συνομάδες είναι αναγκαίο να υπάρχει μεθοδικός τρόπος σχηματισμού όλων των συνομάδων του C καλούμενος και ως ***Τυπική Διάταξη Αποκωδικοποίησης*** (Standard Decoding Array)
- ***<u>Αλγόριθμος Δόμησης Τυπικής Διάταξης Αποκωδικοποίησης (ΤΔΑ)</u>***
- Έστω c1,c2,…,cM οι κωδικές λέξεις του C (n,k,d) μήκους n, $M=2^k$ και c1= μηδενική λέξη. Η διάταξη δε αυτή είναι 2^{n-k} x 2^k με τις 2^{n-k} γραμμές να αποτελούν τις συνομάδες του C. Τα βήματα για τον σχηματισμό της είναι:

1. Οι 2^k κωδικές λέξεις του C τοποθετούνται στην 1η γραμμή με το πρώτο στοιχείο της γραμμής (από αριστερά) να αποτελεί η c1.
2. Ως πρώτο στοιχείο της 2ης γραμμής επιλέγεται το πρότυπο σφάλματος ε2 με το ελάχιστο βάρος και το οποίο δεν υπάρχει ήδη ως λέξη στις <u>*προηγούμενες γραμμές*</u> της διάταξης (στη 1η γραμμή στην συγκεκριμένη περίπτωση) και τοποθετείται ακριβώς κάτω από την c1. Η υπόλοιπη 2η γραμμή σχηματίζεται προσθέτοντας το ε2 σε κάθε ένα από τα αντίστοιχα στοιχεία της προηγούμενης γραμμής (στις κωδικές λέξεις της 1ης γραμμής).
3. Το βήμα 2 επαναλαμβάνεται με τον ίδιο τρόπο έως ότου εξαντληθούν όλες οι διαφορετικές λέξεις μήκους n , κάτι που πρακτικά συμβαίνει όταν σχηματισθεί και η 2^{n-k} γραμμή της διάταξης

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Συνομάδες

$$\begin{vmatrix} c_1 = 0 & c_2 & c_3 & \cdots & c_M \\ \varepsilon_2 & c_2 + \varepsilon_2 & c_3 + \varepsilon_2 & \cdots & c_M + \varepsilon_2 \\ \varepsilon_3 & c_2 + \varepsilon_3 & c_3 + \varepsilon_3 & \cdots & c_M + \varepsilon_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \varepsilon_{2^{n-k}} & c_2 + \varepsilon_{2^{n-k}} & c_2 + \varepsilon_{2^{n-k}} & \cdots & c_M + \varepsilon_{2^{n-k}} \end{vmatrix}$$

- Στην παραπάνω διάταξη κάθε γραμμή αποτελεί και συνομάδα του C. Το πρώτο στοιχείο κάθε γραμμής ονομάζεται Οδηγός Συνομάδας (coset leader)
- **<u>Παράδειγμα:</u>** Για τον κώδικα C = {0000, 1010, 1101, 0111} με n=4, k=2 ζητούνται οι διάφορες $2^{n-k}=2 = 4$ συνομάδες του. Η Τυπική Διάταξη Αποκωδικοποίησης έχει ως εξής:
  - c1=0000 1010 1101 0111
  - ε2=0001 ε2+1010=1011 ε2+1101=1100 ε2+0111=0110
  - ε3=0010 ε3+1010=1000 ε3+1101=1111 ε3+0111=0101
  - ε4=0100 ε4+1010=1110 ε4+1101=1001 ε4+0111=0011

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Συνομάδες

- **<u>Παράδειγμα (συνέχεια)</u>**
- Από την παραπάνω Τυπική Διάταξη Αποκωδικοποίησης προκύπτει ότι οι τέσσερις συνομάδες του C= {0000, 1010, 1101, 0111}, {0001, 1011, 1100, 0110}, {0010, 1000, 1111, 0101} και {0100, 1110, 1001, 0011}.
- Εάν τώρα ο δέκτης λάβει τις λέξεις 1110 και 1111, οι οποίες δεν είναι κωδικές λέξεις τότε σύμφωνα με τις ΠΑΜΠ και ΑΑΜΠ έχομε:
- Αν ληφθεί η λέξη 1110, τότε αφού εντοπιστεί η συνομάδα στην οποία περιέχεται, δηλαδή η τέταρτη, επιλέγεται το πρότυπο βάρους με το μικρότερο βάρος, δηλαδή το 0100. Επομένως, σύμφωνα με τις ΠΑΜΠ και ΑΑΜΠ συμπεραίνεται ότι μεταδόθηκε η λέξη 1110 + 0100 = 1010 $\in$ C.
- Στην περίπτωση λήψης της λέξης 1111, αφού διαπιστωθεί ότι περιέχεται στην 3η συνομάδα, παρατηρείται ότι σε αυτή υπάρχουν δύο πρότυπα σφάλματος με το ελάχιστο βάρος, τα 0010 και 1000.
  - Αν έχουμε εφαρμογή της ΑΑΜΠ, ζητείται επαναμετάδοση του μηνύματος.
  - Αν εφαρμόζεται όμως η ΠΑΜΠ, ο δέκτης επιλέγει αυθαίρετα ένα από τα πρότυπα σφάλματος με το ελάχιστο βάρος, έστω το 1000 και συμπεραίνει επομένως ότι μεταδόθηκε η λέξη 1111 + 1000 = 0111.

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Σύνδρομα

- **<u>Ορισμός:</u>** ***Σύνδρομο, s,*** μίας λέξης y ορίζεται η λέξη $s=y \cdot H$, $s \in K^{n-k}$, (έχει δηλ. μήκος n-k όσο ο αριθμός των πλεοναζόντων ψηφίων), όπου H είναι ο πίνακας ελέγχου ισοτιμίας ενός κώδικα C μήκους n και διάστασης k και y = η ληφθείσα λέξη.
- ***<u>Ιδιότητες Συνδρόμου</u>***
- Αν x, y και $\varepsilon \in K^n$, ισχύουν :
  1. Αν και μόνο αν $x \in C$, τότε $x \cdot H = 0$.
     - Απόδειξη: $\forall x \in C \Rightarrow x \cdot H = (u \cdot G) \cdot H = u\,(G\,H) = u \cdot 0 = 0$
  2. Αν και μόνο αν x και y $\in$ στην ίδια συνομάδα, τότε $x \cdot H = y \cdot H$. ***Έχουν δηλαδή το ίδιο σύνδρομο!***
     - *<u>Απόδειξη</u>*: Εφόσον x, y $\in$ στην ίδια συνομάδα έστω στην $\varepsilon 1 + C \Rightarrow x = \varepsilon 1 + c1$, $y = \varepsilon 1 + c2$, όπου $c1, c2 \in C \Rightarrow x \cdot H = \varepsilon 1 \cdot H + c1 \cdot H$, $y \cdot H = \varepsilon 1 \cdot H + c2 \cdot H$. Από ιδιότητα 1 $\Rightarrow c1 \cdot H = c2 \cdot H = 0$ Άρα $x \cdot H = y \cdot H = \varepsilon 1 \cdot H$
  3. Αν ε είναι το πρότυπο σφάλματος μίας ληφθείσας λέξη y, τότε **$\varepsilon \cdot H$ = με το άθροισμα των γραμμών του πίνακα H που αντιστοιχούν στις θέσεις στις οποίες προκλήθηκαν σφάλματα κατά τη μετάδοση**.
     - *<u>Απόδειξη:</u>* Εάν h_i= i γραμμή του H τότε ισχύει $\varepsilon \cdot H = [\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n] \cdot [h_1, h_2, \ldots, h_n]^T = \varepsilon_1 \cdot h_1 + \varepsilon_2 \cdot h_2 + \ldots + \varepsilon_n \cdot h_n$. (1) Λαμβάνοντας υπόψη ότι οι ε_i με $\varepsilon_i=1$ καθορίζουν την θέση του σφάλματος στο ε τότε από την (1) είναι φανερό ότι οι θέσεις σφάλματος στο ε καθορίζουν και τις αντίστοιχες γραμμές του ε που εμπλέκονται στο άθροισμα της (1)

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Σύνδρομα

- **Αποκωδικοποίηση με την βοήθεια Συνδρόμων**
  - Ο αλγόριθμος με εκτεταμένη Τυπική Διάταξη συνομάδων έχει δύο δυσκολίες, την αναζήτηση της συνομάδας στην οποία περιέχεται η ληφθείσα λέξη και την αναζήτηση στη συνέχεια του πρότυπου σφάλματος με το ελάχιστο βάρος.
  - Ανάγκη για απλούστερο τρόπο αποκωδικοποίησης με μικρότερη ανάγκη για αποθηκευτικό χώρο
- **Η Ιδιότητα 1 Συνδρόμων μπορεί να χρησιμοποιηθεί για ανίχνευση σφαλμάτων:**
  - Αν δεν υπεισέλθουν σφάλματα κατά τη μετάδοση, η ληφθείσα λέξη y θα ανήκει στον κώδικα C και τότε $s=y \cdot H = 0$ ειδάλλως $s= y \cdot H =\varepsilon \cdot H$
- **Από Ιδιότητα 2 Συνδρόμων**
  - Επειδή όλες οι λέξεις μιας συνομάδας έχουν το ίδιο σύνδρομο, το σύνδρομο αυτό μπορεί να χρησιμοποιηθεί αντί της συνομάδας για τον προσδιορισμό της. Έτσι, αρκεί να έχουμε από κάθε συνομάδα μόνο το σύνδρομό της και τη λέξη με το ελάχιστο βάρος (οδηγό της συνομάδας) για αποκωδικοποίηση μιας ληφθείσας λέξης Άρα:
  - Η εκτεταμένη Τυπική Διάταξη Αποκωδικοποίησης (με συνομάδες) μπορεί να απλοποιηθεί σε πίνακα που περιέχει μόνον τα σύνδρομα και τους οδηγούς όλων των συνομάδων).

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Σύνδρομα

- ***Αλγόριθμος Αποκωδικοποίησης με την βοήθεια Συνδρόμων***

1. Λήψη της λέξης y και υπολογισμός του συνδρόμου $s=y \cdot H$.
2. Εύρεση από την τροποποιημένη Τυπική Διάταξη Αποκωδικοποίησης- (δηλ. τον Πίνακα Συνδρόμων και Οδηγών Συνομάδων) του οδηγού ε που αντιστοιχεί στη συνομάδα με σύνδρομο $s=y \cdot H$. Αν δεν υπάρχει αντίστοιχος οδηγός της συνομάδας, τότε ζητείται αναμετάδοση.
   - Αν μια συνομάδα έχει περισσότερες από μία λέξεις ελάχιστου βάρους, τότε είτε επιλέγεται μία από αυτές αυθαίρετα και τοποθετείται ως αντίστοιχος οδηγός συνομάδας στον πίνακα αν εφαρμόζεται ΠΑΜΠ, είτε δεν επιλέγεται καμία αν εφαρμόζεται ΑΑΜΠ και μένη κενή η αντίστοιχη θέση στον Πίνακα Συνδρόμων και Οδηγών Συνομάδων
3. Υπολογισμός από το δέκτη της κωδικής λέξης x που μεταδόθηκε, προσθέτοντας τη ληφθείσα λέξη y με τον οδηγό της συνομάδας (το πρότυπο σφάλματος) ε, δηλαδή $x = y + \varepsilon$.

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Σύνδρομα

- **Παράδειγμα**
- Για τον γραμμικό κώδικα C του προηγούμενου Παραδείγματος με τις 4 συνομάδες του {0000, 1010, 1101, 0111}, {0001, 1011, 1100, 0110}, {0010, 1000, 1111, 0101} και {0011, 1001, 1110, 0100}. ζητούνται οι τροποποιημένες ΤΔΑ (Πίνακες Συνδρόμων και Οδηγών Συνομάδων) στις περιπτώσεις εφαρμογής των ΠΑΜΠ και ΑΑΜΠ.
- **Απάντηση:** Για τον υπολογισμό του συνδρόμου μιας συνομάδας, αρκεί να επιλεγεί μια οποιαδήποτε λέξη της, y και να υπολογιστεί το γινόμενο y·H. Συνεπώς, αφού υπολογιστεί ο H όπως δίδεται παρακάτω και επιλεγεί ο οδηγός κάθε συνομάδας, υπολογίζεται το σύνδρομο κάθε συνομάδας, μπορούν να σχηματισθούν οι αντίστοιχοι Πίνακες Συνδρόμων και Οδηγών Συνομάδων για τις περιπτώσεις εφαρμογής των ΠΑΜΠ και ΑΑΜΠ, όπως φαίνεται στην επόμενη σελίδα

©2006, Σπύρος Δενάζης

Αποκωδικοποίηση με Σύνδρομα

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

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

- Ακολουθώντας την μεθοδολογία που προαναφέρθηκε, Σχηματίζουμε τις απλοποιημένες ΤΔΑ (που περιέχουν μόνον σύνδρομα και οδηγούς συνομάδων) για τις περιπτώσεις ΠΑΜΠ και ΑΑΜΠ

ΤΔΑ για ΠΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
0000	$y \cdot H = 00$
0001	$(0001) \cdot H = 01$
1000, 0010	$(0010) \cdot H = 10$
0100	$(0100) \cdot H = 11$

ΤΔΑ για ΑΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
0000	00
0001	01
———	10
0100	11

Αποκωδικοποίηση με Σύνδρομα

- **<u>Παράδειγμα (συνέχεια)</u>**
- Με δεδομένους τους Πίνακες Συνδρόμων και Οδηγών Συνομάδων του C εάν ληφθούν από τον δέκτη οι λέξεις y= 0110 και 1111, η αποκωδικοποίησή τους κατά ΠΑΜΠ και ΑΑΜΠ έχει ως εξής:.
- Υπολογίζονται τα σύνδρομα των λέξεων που ελήφθησαν και ελέγχονται με βάση τους αντίστοιχους οδηγούς των συνομάδων των Πινάκων.
- Συγκεκριμένα, τα σύνδρομα των λέξεων που ελήφθησαν είναι $0110 \cdot H = 01$ και $1111 \cdot H = 10$.
- Στην περίπτωση της ΠΑΜΠ, εντοπίζονται από τον αντίστοιχο πίνακα οι οδηγοί συνομάδων 0001 (για s=01) και 0010 (s=10) και άρα οι μεταδοθείσες κωδικές λέξεις είναι 0110 + 0001 = 0111και 1111 + 0010 = 1101, αντίστοιχα.
- Στην περίπτωση της ΑΑΜΠ, η ληφθείσα λέξη 0110 (s=01) ομοίως με παραπάνω οδηγεί στην κωδική λέξη 0111, ενώ από τη ληφθείσα λέξη 1111 δεν οδηγούμεθα σε κάποιο συμπέρασμα, εφόσον δεν υπάρχει αντίστοιχος οδηγός και ζητείται αναμετάδοση.

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

- **Δίδεται ο συστηματικός γραμμικός κώδικας C = {000000, 001111, 010011, 011100, 100110, 101001, 110101, 111010}.**

1. Ζητείται να βρεθεί ο Γεννήτορας Πίνακας G του κώδικα.

- Απάντηση: Αρκεί να βρεθεί μία βάση του κώδικα C, κάτι που επιτυγχάνεται εάν μεταφέρουμε σε μορφή ΚΔΓ(Κλιμακωτής Διάταξης Γραμμών) ή ΠΚΔΓ (Περιορισμένης ΚΔΓ) τον πίνακα που σχηματίζεται από όλες τις λέξεις του C ή κάποιου υποσυνόλου του S για το οποίο ισχύει ότι το γραμμικό ανάπτυγμά του(δηλ. το σύνολο όλων των γραμμικών συνδυασμών των λέξεών του) δίδει τον C (C = <S>). Ο αριθμός των διανυσμάτων που απαρτίζουν την βάση αποτελούν και την διάσταση k του κώδικα
  - Ένας πίνακας βρίσκεται σε μορφή ΚΔΓ 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 «1» των προηγούμενων γραμμών. Μια στήλη που περιέχει έναν «οδηγό» 1 καλείται στήλη «οδηγός»
  - Ένας πίνακας βρίσκεται σε μορφή ΠΚΔΓ εάν είναι σε μορφή ΚΔΓ και επιπλέον ισχύει ότι σε κάθε στήλη οδηγό του πίνακα δεν περιέχονται άλλα ψηφία «1» αλλά μόνο ψηφία «0»
  - Ένας πίνακας τίθεται σε μορφή ΚΔΓ ή ΠΚΔΓ με τον μετ/σμό του σε διαδοχικούς ισοδύναμους πίνακες μέσω ανταλλαγής δύο γραμμών ή/και αντικατάσταση μίας γραμμής από το άθροισμα του εαυτού της με κάποια άλλη
- Με βάση τα ανωτέρω ο Γεννήτορας Πίνακας G του κώδικα C θα έχει ως εξής:

Άσκηση Γραμμικών Κωδίκων

- Η βάση του κώδικα C έχει ως εξής-όπως δε φαίνεται η διάσταση k του C ισούται με k=3:

$$\begin{bmatrix} 1&0&0&1&1&0\\ 0&1&0&0&1&1\\ 0&0&1&1&1&1\\ 1&1&0&1&0&1\\ 1&0&1&0&0&1\\ 1&1&1&0&1&0\\ 0&1&1&1&0&0\\ 0&0&0&0&0&0 \end{bmatrix} \rightarrow \begin{pmatrix} (6+1\rightarrow 6)\\ (1+5\rightarrow 5)\\ (1+4\rightarrow 4)\\ (7+2\rightarrow 7) \end{pmatrix} \rightarrow \begin{bmatrix} 1&0&0&1&1&0\\ 0&1&0&0&1&1\\ 0&0&1&1&1&1\\ 0&1&0&0&1&1\\ 0&0&1&1&1&1\\ 0&1&1&1&0&0\\ 0&0&1&1&1&1\\ 0&0&0&0&0&0 \end{bmatrix} \rightarrow \begin{pmatrix} (5+3\rightarrow 5)\\ (4+2\rightarrow 4)\\ (7+3\rightarrow 7) \end{pmatrix} \rightarrow \begin{bmatrix} 1&0&0&1&1&0\\ 0&1&0&0&1&1\\ 0&0&1&1&1&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&1&1&1&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix} \rightarrow$$

$$\rightarrow \left((6+2\rightarrow 6)\right) \rightarrow \begin{bmatrix} 1&0&0&1&1&0\\ 0&1&0&0&1&1\\ 0&0&1&1&1&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&1&1&1&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix} \rightarrow \left((6+3\rightarrow 6)\right) \rightarrow \begin{bmatrix} 1&0&0&1&1&0\\ 0&1&0&0&1&1\\ 0&0&1&1&1&1\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&0&0&0 \end{bmatrix} \Rightarrow G = \begin{bmatrix} 1&0&0&1&1&0\\ 0&1&0&0&1&1\\ 0&0&1&1&1&1 \end{bmatrix}$$

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

2. Ζητείται ο πίνακας ισοτιμίας H του C βασιζόμενοι στην γνώση του G.

- **Απάντηση:** Για την εύρεση του H (ισοδύναμα μίας βάσης του δυικού κώδικα του C) αρκεί να σχηματισθεί ο πίνακας M, ο οποίος αποτελείται μόνον από εκείνες τις στήλες του πίνακα G που δεν περιέχουν οδηγούς «1». (M = kx(n-k), k=διάσταση C και n=μήκος κωδικών λέξεων)
- Ο σχηματισμός του πίνακα , H= $[M \;\; I]^T$ (nx(n – k)), επιτυγχάνεται από τον πίνακα M(kx(n – k)) και τον πίνακα ταυτότητας I ((n – k)x(n – k)). Πιο συγκεκριμένα, ο πίνακας H (nx(n – k)) σχ ως εξής:
  - Στις πρώτες k γραμμές του H τοποθετούνται με τη σειρά οι γραμμές του M.
  - Στις υπόλοιπες (n– k) γραμμές του H τοποθετούνται οι γραμμές του πίνακα ταυτότητας I διάστασης (n – k)x(n –k).
- Σημείωση: Μια βάση του δυϊκού κώδικα του C αποτελείται από τις στήλες του πίνακα H (ή τις γραμμές του ανάστροφου πίνακα H^T).
- Με βάση τα ανωτέρω ο σχηματισμός του πίνακας ισοτιμίας του C έχει ως εξής:

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

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

3. Ζητείται η εύρεση της απόστασης του κώδικα C με χρήση του H καθώς και ο αριθμός των σφαλμάτων t που μπορεί ο κώδικας να διορθώσει:

- **Απάντηση:** Χρησιμοποιούμε το Θεώρημα πού αναφέρει ότι η απόσταση d ενός γραμμικού κώδικα = με τον ελάχιστο αριθμό γραμμών του Πίνακα Ισοτιμίας H των οποίων το άθροισμα ισούται με 0 (ή ισοδύναμα ο ελάχιστος αριθμός γραμμών που είναι γραμμικά εξαρτημένες).
- Ειδικότερα παρατηρούμε ότι δεν υπάρχει συνδυασμός ανά 2 των γραμμών του H των οποίων το άθροισμα =0. Αντίθετα παρατηρείται ότι υπάρχει τουλάχιστον ένας συνδυασμός 3 γραμμών του πίνακα H των οποίων το άθροισμα =0 δηλ : (011) +(111) + (100)= (100) + (100) = (000) Άρα σύμφωνα με το Θεώρημα d=3 και t= (d-1)/2 =1 και άρα ο κώδικας C μπορεί να διορθώσει το πολύ ένα σφάλμα

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

4. Ζητείται η εύρεση του συνόλου των συνομάδων του κώδικα C.

- **Απάντηση:** Σύμφωνα με τον ορισμό μία συνομάδα του C προσδιορισμένη από τη λέξη x μήκους n, (n=μήκος κωδικής λέξης), συμβολίζεται ως C + x και ορίζεται ως το σύνολο όλων των λέξεων της μορφής c + x, όπου $c \in C$ (το x είναι σταθερό και το c κυμαίνεται σε όλο το εύρος του C).

Σχηματισμός Τυπικής Διάταξης Συνομάδων

- Πρακτικά υπάρχει μεθοδικός τρόπος σχηματισμού όλων των συνομάδων του C ⇒ Τυπική Διάταξη Συνομάδων (Standard Decoding Array)
- **Αλγόριθμος Δόμησης Τυπικής Διάταξης Συνομάδων ς (ΤΔΑ)**
- Έστω $c_1, c_2, \ldots, c_M$ οι κωδικές λέξεις του C (n,k,d) μήκους n, $M=2^k$ και c_1= (0…0). Η διάταξη δε αυτή είναι 2^{n-k} x 2^k με τις 2^{n-k} γραμμές να αποτελούν τις συνομάδες του C. Τα βήματα για τον σχηματισμό της είναι:

1. Οι 2^k κωδικές λέξεις του C τοποθετούνται στην 1η γραμμή με το πρώτο στοιχείο της γραμμής (από αριστερά) να αποτελεί η c_1.
2. Ως πρώτο στοιχείο της 2ης γραμμής επιλέγεται η λέξη ε_2 (το πρότυπο σφάλματος) με το ελάχιστο βάρος και το οποίο δεν υπάρχει ήδη ως λέξη στις προηγούμενες γραμμές της διάταξης (στη 1η γραμμή στην συγκεκριμένη περίπτωση) και τοποθετείται ακριβώς κάτω από την c_1. Η υπόλοιπη 2η γραμμή σχηματίζεται προσθέτοντας το ε_2 σε κάθε ένα από τα αντίστοιχα στοιχεία της προηγούμενης γραμμής (στις κωδικές λέξεις της 1ης γραμμής).
3. Το βήμα 2 επαναλαμβάνεται με τον ίδιο τρόπο έως ότου εξαντληθούν όλες οι διαφορετικές λέξεις μήκους n , κάτι που πρακτικά συμβαίνει όταν σχηματισθεί και η 2^{n-k} γραμμή της διάταξης

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

- Με βάση την προηγούμενη μεθοδολογία οι δυνατές συνομάδες του C είναι $2^{n-k}= 2^{6-3}=2^3=8$ και η Τυπική Διάταξη πού τις περιέχει έχει ως ακολούθως:
- Ειδικότερα η πρώτη συνομάδα ταυτίζεται με τις κωδικές λέξεις του C.

1. C = {000000=c_1, 001111= c_2, 010011 = c_3, 011100 = c_4, 100110 = c_5, 101001 = c_6, 110101 = c_7, 111010 = c_8},

- Για την 2η συνομάδα επιλέγομε ως πρώτο στοιχείο της (οδηγό) ε_1 μία από τις λέξεις με την ελάχιστη βαρύτητα, δηλ. με βάρος 1, έστω την 000001,⇒ τα υπόλοιπα στοιχεία της προκύπτουν ως $\varepsilon_1 + c_i, i=2 \ldots 8$

2. {000001=ε_1, 001110= $\varepsilon_1 + c_2$, 010011 = $\varepsilon_1 + c_3$, 011101 = $\varepsilon_1 + c_4$, 100111 = $\varepsilon_1 + c_5$, 101000 = $\varepsilon_1 + c_6$, 110100 = $\varepsilon_1 + c_7$, 111011 = $\varepsilon_1 + c_8$},

Ομοίως εργαζόμενοι και για τις υπόλοιπες συνομάδες παιρνομε:

3. {000010, 001101, 010001, 011100, 100100, 101011, 110111, 111000},
4. {000100, 001011, 010111, 011000, 100010, 101101, 110001, 111110},
5. {001000, 000111, 011011, 010100, 101110, 100001, 111101, 110010}.
6. {010000, 011111, 000011, 001100, 110110, 111001, 100101, 101010,},
7. {100000, 101111, 110011, 111100, 000110, 001001, 010101, 011010},
8. {000101, 001010, 010110, 011001, 100011, 101100, 110000, 111111},

- Όπως φαίνεται από τα παραπάνω σημαντικότατο στοιχείο για τον σχηματισμό των συνομάδων αποτελεί η επιλογή των «οδηγών» τους. Ειδικότερα για τις συνομάδες 2-7 επιλέγονται ως οδηγοί όλες οι δυνατές λέξεις βαρύτητας 1, ενώ για την 8η συνομάδα επιλέγεται μία λέξη αμέσως μεγαλύτερης βαρύτητας, δηλ. βάρους 2, που να μην περιέχεται σε άλλες συνομάδες, η 000101 στην συγκεκριμένη περίπτωση

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

5. **Ζητείται με την βοήθεια της Τυπικής Διάταξης του C (δηλ. του συνόλου των συνομάδων), η αποκωδικοποίηση των ληφθέντων λέξεων 111011 και 111111, στη βάση των ΠΑΜΠ (Πλήρους Αποκωδικοποίησης Μεγίστης Πιθανότητας) και Ατελούς ΑΜΠ.**

- **Απάντηση:** Έστω ότι έχομε μετάδοση της κωδικής λέξης x. που οδηγεί στη λήψη της λέξης y $\Rightarrow$ τότε έχομε y= x + ε. $\Rightarrow$ ισχύει και x = ε + y και συνεπώς (από ιδιότητα συνομάδων που αναφέρει ότι εφόσον το άθροισμα 2 λέξεων=κωδική λέξη, οι λέξεις αυτές περιέχονται στην ίδια συνομάδα)$\Rightarrow$οι λέξεις ε (πρότυπο σφάλματος) και y περιέχονται στην ίδια συνομάδα του C
- Για την επιλογή του κατάλληλου ε λαμβάνεται υπόψη ότι πρότυπα σφάλματος μικρού βάρους λαμβάνουν χώρα με τη μεγαλύτερη πιθανότητα -αποκωδικοποίηση μέγιστης πιθανότητας (ΑΜΠ). Συνεπώς, για την αποκωδικοποίηση μίας λέξης αρκεί να εφαρμοσθεί ο κάτωθι αλγόριθμος
- **Αλγόριθμος αποκωδικοποίησης με τη βοήθεια των Συνομάδων**

α. Λήψη της λέξης y και υπολογισμός της συνομάδας C + y όπου περιέχεται.

β. Επιλογή της λέξης ε, ελάχιστου βάρους, που περιέχεται στη συνομάδα C + y. Αν $\in$ περισσότερες λέξεις της συνομάδας C + y, με ελάχιστο βάρος, τότε στην (ΠΑΜΠ) αποκωδικοποίηση επιλέγεται αυθαίρετα μία εξ αυτών, ενώ στην ΑΑΜΠ αποκωδικοποίηση ζητείται επανάληψη της μετάδοσης.

γ. Υπολογισμός της κωδικής λέξης x που μεταδόθηκε ως x = y + ε.

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

- Με βάση τα προηγούμενα, εφαρμόζοντας τον αλγόριθμο αποκωδικοποίησης για τις λέξεις 111011 και 111111 έχομε:
- Για την 111011 εφαρμόζομε το βήμα α και βρίσκομε ότι αυτή περιέχεται στη 2η συνομάδα, στην οποία η λέξη με το μικρότερο βάρος είναι η 000001. Επομένως, σύμφωνα με τον αλγόριθμο αποκωδικοποίησης και για την ΠΑΜΠ και για την ΑΑΜΠ περίπτωση, συμπεραίνομε ότι μεταδόθηκε η κωδική λέξη 111011 + 000001 = 111010.
- Στην περίπτωση λήψης της λέξης 111111, παρατηρούμε ότι αυτή περιέχεται στην 8η συνομάδα του C, όπου διαπιστώνει ότι υπάρχουν τρεις λέξεις (ή τρία πρότυπα σφάλματος) με το ελάχιστο βάρος, οι 000101, 001010 και 110000. Η επιλογή μας εξαρτάται από το αν βασιζόμαστε στην ΠΑΜΠ ή την ΑΑΜΠ. Αν έχουμε εφαρμογή της ΑΑΜΠ, τότε ζητάμε αναμετάδοση του μηνύματος. Αν εφαρμόζεται η ΠΑΜΠ, επιλέγομε αυθαίρετα ένα από τα πρότυπα σφάλματος με το ελάχιστο βάρος, έστω το 000101 και συμπεραίνομε ότι μεταδόθηκε η κωδική λέξη 111111 + 000101 = 111010.
- Αν είχαμε επιλέξει το πρότυπο σφάλματος 110000, θα είχαμε συμπεράνει τη μετάδοση της κωδικής λέξης 001111 και αν είχαμε επιλέξει το πρότυπο σφάλματος 001010, θα είχαμε οδηγηθεί στην κωδική λέξη 110101.

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

6. **Ζητείται τώρα η αποκωδικοποίηση των λέξεων 011111 και 101111, για τις περιπτώσεις ΠΑΜΠ και της ΑΑΜΠ με την χρήση συνδρόμων τους**

- **Απάντηση:** Σύμφωνα με τις ιδότητες των συνδρόμων αν δεν υπάρξουν σφάλματα στη μετάδοση, η ληφθείσα λέξη y θα ανήκει στον κώδικα C και τότε το σύνδρομό της $s=y \cdot H = 0$ ειδάλλως $s= y \cdot H =\varepsilon \cdot H$
- Από Ιδιότητα Συνδρόμων ⇒επειδή όλες οι λέξεις μιας συνομάδας έχουν το ίδιο σύνδρομο, το σύνδρομο αυτό μπορεί να χρησιμοποιηθεί αντί της συνομάδας για τον προσδιορισμό της. Έτσι, αρκεί να έχουμε από κάθε συνομάδα μόνο το σύνδρομό της και τη λέξη με το ελάχιστο βάρος (οδηγό της συνομάδας) για αποκωδικοποίηση μιας ληφθείσας λέξης
- Άρα η εκτεταμένη Τυπική Διάταξη Αποκωδικοποίησης (με όλες δηλ. τις συνομάδες) μπορεί να απλοποιηθεί σε πίνακα που περιέχει μόνον τα σύνδρομα και τους οδηγούς κάθε συνομάδας.

Με βάση τα προλεχθέντα προκύπτει ο κάτωθι αλγόριθμο αποκωδικοποίησης

Αλγόριθμος Αποκωδικοποίησης με την βοήθεια Συνδρόμων

α. Λήψη της λέξης y και **υπολογισμός του συνδρόμου $s=y \cdot H$**.

β. **Εύρεση** από την τροποποιημένη Τυπική Διάταξη Αποκωδικοποίησης- (δηλ. τον Πίνακα Συνδρόμων και Οδηγών Συνομάδων) **του οδηγού ε που αντιστοιχεί στη συνομάδα με σύνδρομο $s=y \cdot H$**. Αν δεν υπάρχει αντίστοιχος οδηγός της συνομάδας, τότε ζητείται αναμετάδοση.

  – Αν μια συνομάδα έχει περισσότερες από 1 λέξεις ελάχιστου βάρους, στην ΠΑΜΠ επιλέγεται μία από αυτές αυθαίρετα ως οδηγός συνομάδας στον πίνακα, ενώ στην ΑΑΜΠ δεν επιλέγεται καμία και μένη κενή η αντίστοιχη θέση στον Πίνακα.

γ. Υπολογισμός της κωδικής λέξης x που μεταδόθηκε, ως $x = y + \varepsilon$.

©2006, Σπύρος Δενάζης

Άσκηση Γραμμικών Κωδίκων

- Σύμφωνα με τα προηγούμενα υπολογίζομε κατά πρώτον τον) Πίνακα Οδηγών Συνομάδων και Συνδρόμων για ΠΑΜΠ και ΑΑΜΠ με κάθε γραμμή του Πίνακα να περιέχει μόνον τον οδηγό συνομάδας και το σύνδρομό της. Ειδικότερα για την ΑΑΜΠ αφήνομε κενή την θέση του οδηγού της 6ης (στον Πίνακα) συνομάδας καθώς όπως φαίνεται από την Τυπική Διάταξη συνομάδων περιέχει πάνω από 1 λέξεις ελάχιστης βαρύτητας (τις βάρους 2, 000101, 001010, 110000 στην συγκεκριμένη περίπτωση)

ΤΔΑ για ΠΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
000000	$y.H = 000$
000001	$(000001).H = 001$
000100	$(000100).H = 100$
000010	$(000010).H = 010$
010000	$(010000).H = 011$
000101	$(000101).H = 101$
100000	$(100000).H = 110$
001000	$(001000).H = 111$

ΤΔΑ για ΑΑΜΠ	
Οδηγός συνομάδας	Σύνδρομο συνομάδας
000000	000
000001	001
000100	100
000010	010
010000	011
———	101
100000	110
001000	111

©2006, Σπύρος Δενάζης

ΓΡΑΜΜΙΚΟΙ ΚΩΔΙΚΕΣ (ΚΩΔΙΚΕΣ HAMMING)

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες (Κώδικες Hamming)

- **<u>Ορισμός:</u>** Ένας κώδικας μήκους $n = 2^r - 1$ ($r \geq 2$) και πίνακα ελέγχου ισοτιμίας H, του οποίου (H) οι γραμμές απαρτίζονται από όλες τις δυνατές μη μηδενικές λέξεις μήκους r, ονομάζεται ***κώδικας Hamming μήκους $2^r - 1$***.
  - Η διάσταση k του κώδικα = $n-r = 2^r - 1 - r$ και μπορεί να δειχθεί ότι d=3. Άρα μπορούν να διορθώσουν $t=\lfloor (d-1)/2 \rfloor = 1$ λάθος και να ανιχνεύσουν d-1= 2 λάθη
  - r= αριθμός (πλεοναζόντων) bits ισοτιμίας και αριθμός κωδικών λέξεων (και μηνυμάτων) $|C| = 2^\kappa = 2^{2^r - r - 1}$
  - Ο ρυθμός πληροφορίας ενός δυαδικού κώδικα C μήκους n είναι ίσος με $(1/n)\log_2|C| = [\log_2 (2^{2^r - r - 1})]/(2^r - 1) = (2^r - r - 1)/(2^r - 1)$ Εύκολα φαίνεται από τη σχέση ότι ο ρυθμός πληροφορίας πλησιάζει στο 1 για υψηλές τιμές του r
- π.χ. Οι παρακάτω Κώδικες (n,k,r) είναι κώδικες Hamming
- (7,4,3), (15,11,4), (31,26,5) …
- Συμπερασματικά οι κώδικες Hamming είναι κώδικες με υψηλούς ρυθμούς πληροφορίας και σχετικά μικρή απόσταση d. Επιπλέον όπως θα δειχθεί πληρούν τα κριτήρια των τέλειων κωδίκων ενώ τόσο ο σχηματισμός της ΤΔΑ όσο και η διαδικασία αποκωδικοποίησης μπορεί να απλοποιηθεί κατά πολύ

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες (Κώδικες Hamming)

- **<u>Παράδειγμα</u>**: Κώδικας Hamming (7,4,3)
- Σύμφωνα με τον ορισμό, ένας πίνακας ελέγχου ισοτιμίας ενός κώδικα Hamming μήκους 7 (r = 3) θα μπορούσε να έχει σαν γραμμές όλες τις μη μηδενικές λέξεις μήκους r=3, δηλ:

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

- Από τον Πίνακα Η μπορεί εύκολα να δειχθεί ότι d=3 μια και αυτός είναι ο ελάχιστος αριθμός γραμμών του Η το άθροισμα των οποίων ισούται με μηδέν.
  - π.χ 1η +2η +3η γραμμή = [101]+[011]+[111] =[111]+[111]=[000]
- Επιπλέον ισχύει k= n-r=4 και $|C| = 2^k = 16$

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες (Κώδικες Hamming)

- **<u>Παράδειγμα (συνέχεια)</u>**: Από τον πίνακα Η μπορούμε, ακολουθώντας με αντίστροφη σειρά τα βήματα της διαδικασίας σχηματισμού του Η από το γεννήτορα πίνακα G σε μορφή ΠΚΔΓ να σχηματίσουμε τον G του κώδικα. Παρακάτω, εκτός από τον γεννήτορα πίνακα του κώδικα απεικονίζονται επίσης και οι κωδικές λέξεις που προκύπτουν από τον G μετά τον πολ/σμό του με κάθε ένα από τα 2^4 =16 μηνύματα (λέξεις μήκους 4 bits)

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

s	t	s	t	s	t	s	t
0000	0000000	0100	0100110	1000	1000101	1100	1100011
0001	0001011	0101	0101101	1001	1001110	1101	1101000
0010	0010111	0110	0110001	1010	1010010	1110	1110100
0011	0011100	0111	0111010	1011	1011001	1111	1111111

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες (Κώδικες Hamming)

- ***<u>Αποκωδικοποίηση Hamming κωδίκων</u>***
- Ο σχηματισμός του Πίνακα Συνδρόμων και Οδηγών Συνομάδων ενός κώδικα Hamming είναι πολύ εύκολος. Αφού ο κώδικας διορθώνει κάθε απλό σφάλμα, όλα τα δυνατά πρότυπα σφάλματος βάρους 1 θα περιέχονται ως οδηγοί των συνομάδων .
- Επίσης (από την ιδιότητα 3 των συνδρόμων, ε.Η) προκύπτει ότι το αντίστοιχο σύνδρομο είναι η γραμμή του h_i του H= $[h_1, h_2,\ldots h_i\ldots,h_n]^T$ που πολλαπλασιάζεται με το μοναδικό «1» του οδηγού (ή πρότυπου σφάλματος) ε_i=[0,0,…,1, …,0]

Οδηγός Συνομάδας	***Σύνδρομο (λέξη μήκους r)***
00…. 0	00…0
00…. 1	h_n
00…10	h_{n-1}
……	……..
10…. 0	h_{2^r-1}

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες (Κώδικες Hamming)

- ***<u>Αποκωδικοποίηση Hamming κωδίκων (συνέχεια)</u>***
- Επαναδιατυπώνοντας την ιδιαιτερότητα του συνδρόμου ενός Hamming κώδικα που περιγράφηκε προηγουμένως έχομε: Το σύνδρομο μίας ληφθείσας λέξης y ταυτίζεται με μία γραμμή h_i του H η θέση της οποίας ταυτίζεται με την θέση στο ε, άρα και στο y όπου υπήρξε σφάλμα
- Με βάση την ανωτέρω διαπίστωση καθίσταται φανερό ότι για αποκωδικοποίηση Hamming κωδίκων δεν χρειάζεται πλέον ο Πίνακας Συνδρόμων και Οδηγών συνομάδων και η όλη διαδικασία απλοποιείται στον παρακάτω αλγόριθμο
- **<u>Αλγόριθμος Αποκωδικοποίησης Hamming Κωδίκων</u>**
- Εάν x=μεταδοθείσα λέξη, y=ληφθείσα λέξη, (αμφότερες μήκους n) και H=πίνακας ισοτιμίας ενός Hamming κώδικα τότε για υπολογισμό της x έχομε:

1. Υπολογισμός του συνδρόμου $s= y \cdot H$
2. Εάν $s=0 \Rightarrow$ η y ταυτίζεται με την μεταδοθείσα λέξη x
3. Εάν $s\neq 0$ τότε το s ταυτίζεται με μία μοναδική γραμμή του H, έστω την h_i. Τότε απλώς προστίθεται ένα 1 (mod2) στην i συντεταγμένη του y και το αποτέλεσμα μας δίνει την μεταδοθείσα λέξη x

©2006, Σπύρος Δενάζης

Γραμμικοί Κώδικες (Κώδικες Hamming)

- **Παράδειγμα:** Εφαρμογή Αποκωδικοποίησης στον Hamming κώδικα (7,4,3)
- Εάν έχει ληφθεί η λέξη y=0000001 τότε για την εύρεση της κωδικής (κατά Hamming (7,4,3)) λέξης x που εστάλη έχομε:
  - Το σύνδρομο s που αντιστοιχεί στην λέξη y $\Rightarrow$ s= (0000001) H = (001) . Όπως φαίνεται από τον Πίνακα H (αλλά και από τον παρακάτω πίνακα συνδρόμων-οδηγών συνομάδων) το s ταυτίζεται με την 7η γραμμή του H. Άρα αρκεί να αλλάξουμε το 7ο bit της y από 0 σε 1 (ισοδύναμα να προσθέσομε 1 $\Rightarrow$ 0+1=1) και συνεπώς x=0000000

Οδηγός Συνομάδας	**Σύνδρομο (λέξη μήκους 3)**
0000000	000
0000001	(001)= h_7
0000010	(010)= h_6
0000100	(100)= h_5
0001000	(110)= h_4
0010000	(111)= h_3
0100000	(011)= h_2
1000000	(101)= h_1

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

©2006, Σπύρος Δενάζης

ΚΥΚΛΙΚΟΙ ΚΩΔΙΚΕΣ

(Cyclic Codes)

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες

- **<u>Εισαγωγή:</u>**
- Για να έχουμε απόδοση κοντά στο όριο Shannon οδηγούμαστε αναπόφευκτα στη χρήση γραμμικών κωδίκων μεγάλων διαστάσεων (k>>20)
  - Τέτοιοι κώδικες είναι πολύ δύσκολο να υλοποιηθούν σε υλικό
- Για πρακτικούς λοιπόν λόγους κάνουμε σχεδόν αποκλειστική χρήση ενός μικρού υποσυνόλου των γραμμικών κωδίκων, των καλά δομημένων κυκλικών κωδίκων
  - Εύκολος και κομψός αλγεβρικός χειρισμός κυκλικών κωδίκων μέσω πράξεων πολυωνύμων
  - Σχετικά εύκολη υλοποίηση μέσω άμεσης αντιστοίχισης πολυωνυμικών πράξεων με δομές καταχωρητών ολίσθησης για κωδικοποίηση/αποκωδικοποίηση
- Υπάρχουν μεν αρκετοί κυκλικοί κώδικες αλλά συγκρινόμενοι με τους γραμμικούς είναι πραγματικά ελάχιστοι
  - Για παράδειγμα αν και υπάρχουν περίπου 11 811 γραμμικοί (7,3) δυαδικοί κώδικες μόνον δύο από αυτούς είναι κυκλικοί

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες

- Έστω c μια κωδική λέξη ενός γραμμικού κώδικα C όπου $c=(c_0,c_1,\ldots,c_{n-1})$
  - *Αριστερή Κυκλική Μετατόπιση* (Left Cyclic Shift) μιας κωδικής λέξης c είναι αυτή κατά την οποία κάθε ψηφίο της κωδικής λέξης μετατίθεται προς τα αριστερά
    - Π.χ μετακίνηση της c κατά μια θέση, $\kappa_L(c)=c'=(c_1,c_2,\ldots,c_{n-1}, c_0)$
  - *Δεξιά Κυκλική Μετατόπιση* (Right Cyclic Shift) μιας κωδικής λέξης c είναι αυτή κατά την οποία κάθε ψηφίο της κωδικής λέξης μετατίθεται προς τα δεξιά
    - Π.χ μετακίνηση της c΄ κατά 4 θέσεις $\kappa_R^4(c')= c''=(c_{n-3},c_{n-2},c_{n-1},c_0, c_1,\ldots, \ldots,c_{n-5}, c_{n-4})$
- **<u>Ορισμός:</u>** Ένας (n,k) **<u>γραμμικός</u>** κώδικας C καλείται **<u>κυκλικός</u>** αν η κυκλική μετατόπιση κάθε κωδικής λέξης είναι και αυτή κωδική λέξη.
- ***<u>Παρατηρήσεις</u>***
  - Προσοχή!! Αυτό που λέει ο ορισμός είναι ότι η κυκλική μετατόπιση παράγει λέξη η οποία και αυτή $\in$ C. ΔΕΝ λέει ότι όλος ο κώδικας μπορεί να παραχθεί από κυκλικές μετατοπίσεις μιας κωδικής λέξης.
    - Π.χ. Το μηδενικό στοιχείο ενός κώδικα δεν είναι αποτέλεσμα κυκλικής μετατόπισης
  - Ο συνδυασμός της γραμμικότητας και της κυκλικότητας μπορεί να παράξει όλο τον κώδικα.
  - Αναφορικά με τη συνάρτηση κυκλικής μετατόπισης κ(.), ισχύει κ(x + y) = κ(x) + κ(y) και κ(αx) = ακ(x), όπου x, y λέξεις και $\alpha \in K = \{0,1\}$. *Επομένως για να δείξουμε ότι ένας κώδικας είναι κυκλικός αρκεί να δείξουμε ότι κ(x)$\in$C, $\forall x \in$ Βάση του C*

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες

- **<u>Παραδείγματα</u>**
- Μερικοί τετριμμένοι κυκλικοί κώδικες σύμφωνα με τον ως άνω ορισμό είναι:
  - Ο (n,1) κώδικας επανάληψης με κωδικές λέξεις της μορφής (α,α,…, α), $\alpha \in \{0,1\}$
  - Ο (n, n-1) κώδικας απλής ισοτιμίας , δηλ. $\sum c_i=0$, $\forall$ x= $(c_0,c_1,\ldots,c_{n-1})$, x $\in$ C
- Να εξετασθεί εάν ο C = {000, 110, 101, 011} είναι κυκλικός κώδικας
  - Πρώτα ελέγχεται αν είναι γραμμικός κώδικας, δηλ. αν το άθροισμα οποιονδήποτε δύο ή περισσότερων κωδικών λέξεων είναι επίσης κωδική λέξη του C, που στην περίπτωσή μας ισχύει
  - Κατόπιν εξετάζονται οι κυκλικές μετατοπίσεις όλων των κωδικών λέξεων ήτοι: κ(000) = 000, κ(110) = 011, κ(101) = 110, κ(011) = 101. Εφόσον όλες καταλήγουν σε κωδικές λέξεις, ο κώδικας είναι κυκλικός.
- Να εξετασθεί εάν ο γραμμικός κώδικας (5,2) με C = $\{c_0=00000, c_1=01101, c_2=10111, c_3=11010\}$ είναι κυκλικός
  - $\kappa_L(c_1)= \kappa_L(01101)=11010=c_3$
  - $\kappa_L(c_3)= \kappa_L(11010)=10101 \notin C$
  - Άρα ο γραμμικός κώδικας δεν είναι κυκλικός

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες

- **<u>Παραδείγματα (συνέχεια)</u>**
- Κατασκευή γραμμικού κώδικα Hamming (7,4) από την κωδική λέξη 0001011

1.	Μηδενικό στοιχείο	0000000
2.	Κωδική λέξη	**0001011**
3.	1η Αριστερή μετατόπιση	**0010110**
4.	2η Αριστερή μετατόπιση	0101100
5.	3η Αριστερή μετατόπιση	1011000
6.	4η Αριστερή μετατόπιση	0110001
7.	5η Αριστερή μετατόπιση	1100010
8.	6η Αριστερή μετατόπιση	**1000101**
9.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,3)	0011101
10.	1η Αριστερή μετατόπιση κωδικής λέξης 0011101 (βήμα 9)	0111010
11.	2η Αριστερή μετατόπιση	1110100
12.	3η Αριστερή μετατόπιση	1101001
13.	4η Αριστερή μετατόπιση	1010011
14.	5η Αριστερή μετατόπιση	**0100111**
15.	6η Αριστερή μετατόπιση	1001110
16.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,11)	1111111

ΒΑΣΗ

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες - Μαθηματικό Υπόβαθρο

- Για κατάλληλο αλγεβρικό χειρισμό κυκλικών κωδίκων (λ.χ. των κυκλικών μετατοπίσεων) υιοθετείται η πολυωνυμική μορφή των κωδικών λέξεων:
- Ειδικότερα, μία λέξη a μήκους n, αποτελούμενη από τα bits $a_0\ a_1 \ldots\ a_{n-1}$, παριστάνεται ως ένα πολυώνυμο βαθμού (n – 1) με συντελεστές στο σύνολο K = {0, 1}: $a_0 + a_1x + a_2\ x^2 + \ldots + a_{n-1}\ x^{n-1}$. Το σύνολο όλων των πολυωνύμων με συντελεστές στο K συμβολίζεται με **K[x]**.
- Οι πράξεις του *πολλαπλασιασμού* και της *πρόσθεσης* μεταξύ πολυωνύμων του **K[x]** συντελούνται όπως και με συντελεστές στο σύνολο των ακεραίων ή πραγματικών αριθμών,
  - Η διαφορά έγκειται στο ότι το άθροισμα δύο συντελεστών ίσων με 1 δίνει 0, δηλαδή 1 + 1 = 0 και επομένως $x^n + x^n = (1 + 1)\ x^n = 0$.
- Για την *διαίρεση* πολυωνύμων ισχύει:
  - Αν f(x), g(x) $\in$ K[x], με g(x) ≠0, τότε υπάρχουν τα μοναδικά πολυώνυμα q(x), r(x) $\in$ K[x], τέτοια ώστε f(x) = q(x) $\cdot$ g(x) + r(x), όπου r(x) είναι το υπόλοιπο και είτε r(x)=0 είτε ο βαθμός του είναι μικρότερος του βαθμού του g(x) (deg r(x)< deg g(x)) και q(x) είναι το πηλίκο της διαίρεσης.
  - Η διαίρεση πολυωνύμων στο K[x] γίνεται ως συνήθως, εκτός από την ανωτέρω διαφορά στην πρόσθεση των συντελεστών.

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες - Μαθηματικό Υπόβαθρο

- **<u>Παράδειγμα:</u>** Η παράσταση του κώδικα C = {000000, 100100, 010010, 001001, 110110, 101101, 011011, 111111}. με πολυώνυμα, περιέχεται στον ακόλουθο πίνακα:

Κωδική λέξη	Πολυώνυμο
000000	0
100100	$1+x^3$
010010	$x+x^4$
001001	x^2+x^5
110110	$1+x+x^3+x^4$
101101	$1+x^2+x^3+x^5$
011011	$x+x^2+x^4+x^5$
111111	$1+x+x^2+x^3+x^4+x^5$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες - Μαθηματικό Υπόβαθρο

- **<u>Παράδειγμα διαίρεσης πολυωνύμων</u>**
- Η διαδικασία διαίρεσης των πολυωνύμων $(1 + x + x^2 + x^5)/(1 + x^2)$ έχει ως εξής:

$$
\begin{array}{l|l}
 & x^3 + x + 1 \text{ (=πηλίκο)} \\
 & \text{----------} \\
x^2 + 1 & x^5 + x^2 + x + 1 \\
 & x^5 + x^3 \\
 & \text{----------} \\
 & x^3 + x^2 + x + 1 \\
 & x^3 + x \\
 & \text{----------} \\
 & x^2 + 1 \\
 & x^2 + 1 \\
 & \text{--------} \\
 & 0
\end{array}
$$

- Συνεπώς το πολυώνυμο $1 + x^2$ διαιρεί ακριβώς το πολυώνυμο $1 + x + x^2 + x^5$ (δηλ. υπόλοιπο=0) και το αποτέλεσμα (πηλίκο) είναι $1 + x + x^3$.

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες - Μαθηματικό Υπόβαθρο

- ***<u>Modulo αριθμητική στα πολυώνυμα</u>***
- Αν f(x) , g(x) = πολυώνυμα, τότε το f(x) mod g(x)= με το υπόλοιπο της διαίρεσης του f(x) με το g(x), δηλ εάν f(x) = q(x) · g(x) + r(x), τότε f(x) mod g(x) = r(x) ή f(x) ≡ r(x) (mod g(x)), δηλαδή το πολυώνυμο f(x) είναι ισότιμο (ή ισοδύναμο) με το r(x) (mod g(x)).
- Ισοδύναμα το f(x) mod g(x) ισούται με το μοναδικό πολυώνυμο r(x) τέτοιο ώστε το f(x) - r(x) (f(x)+ r(x) στην περίπτωσή μας μια και οι συντελεστές των πολυωνύμων=0 ή 1) να διαιρείται από το g(x) και deg r(x)< deg g(x)
- Δύο πολυώνυμα f(x), h(x), τα οποία διαιρούμενα με το ίδιο πολυώνυμο g(x) έχουν το ίδιο υπόλοιπο r(x), χαρακτηρίζονται ισοδύναμα mod g(x) και η σχέση ισοτιμίας ή ισοδυναμίας συμβολίζεται με f(x)≡ h(x) (mod g(x)).
- **<u>Παραδείγματα</u>**:
- x^7 mod (x^7 +1) =1 διότι x^7 = 1(x^7 +1) +1,
- x^3 mod x^2 = 0 διότι x^3 = x · x^2 + 0,
- x^2 mod x^3 = x^2 διότι x^2 = 0 · x^3 + x^2

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες - Μαθηματικό Υπόβαθρο

- ***<u>Ιδιότητες του modulo τελεστή</u>***

1. Εάν deg P(x)<deg M(x), τότε P(x) mod M(x)= P(x)
   - π.χ. x^2 mod x^3 = x^2
2. Εάν το M(x) διαιρεί το P(x), τότε P(x) mod M(x)= 0
   - π.χ. x^3 mod x^2 = 0
3. (P(x) + Q(x)) mod M(x) = P(x) mod M(x) + Q(x) mod M(x)
   - π.χ. (x^7 +1) mod x^7 = x^7 mod x^7 + 1 mod x^7 = 0+1=1
4. (P(x) · Q(x)) mod M(x) = (P(x) · (Q(x) mod M(x))) mod M(x)
   - π.χ. (x^3 +x) mod (x^2 +1) = (x(x^2 +1)) mod (x^2 +1)=(x · ((x^2 +1) mod (x^2 +1))) mod (x^2 +1) =(x · 0) mod (x^2 +1) = 0 mod (x^2 +1) =0
5. Εάν το M(x) διαιρεί το N(x), τότε (P(x) mod N(x)) mod M(x) = P(x) mod M(x)
   - π.χ. ((x^2 +x+1) mod x^2) mod x = (x^2 +x+1) mod x =1
6. Η σχέση (modulo) ισοτιμίας μεταξύ δύο πολυωνύμων διατηρείται και μετά την πρόσθεση ή τον πολλαπλασιασμό με ένα τρίτο πολυώνυμο, δηλαδή αν f(x)≡ h(x) (mod g(x)) τότε f(x) + p(x)≡ h(x) + p(x) (mod g(x)) και f(x) · p(x)≡ h(x) · p(x) (mod g(x)).

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Ιδιότητες κυκλικής μετατόπισης)

- ***Θεώρημα:*** Έάν **c**= (c_0 ,c_1, … , c_{n-1}) είναι μία κωδική λέξη ενός κυκλικού κώδικα C με πολυωνυμική συνάρτηση $c(x)= c_0 + c_1x + c_2 x^2 +\ldots + c_{n-1} x^{n-1}$ τότε η κυκλική μετατόπιση (προς τα δεξιά) του **c**, κ(c), αναπαριστάται από το πολυώνυμο $c^R(x)$ που δίδεται από την συνάρτηση: $\mathbf{c^R(x) = x\, c(x) \bmod (x^n+1)}$
- ***Απόδειξη:*** Εφόσον $c(x) = c_0 + c_1x +\ldots + c_{n-1} x^{n-1} \Rightarrow x\cdot c(x)= c_0x + c_1x^2 +\ldots + c_{n-2} x^{n-1} + c_{n-1} x^n$ ενώ $c^R(x) = c_{n-1} + c_0x +\ldots + c_{n-2} x^{n-1}$
- Τότε $x\cdot c(x) + c^R(x) = c_{n-1} (x^n +1)$. Εφόσον deg $c^R(x) <$ deg $(x^n +1)$ και $x\cdot c(x) + c^R(x)$ = πολλαπλάσιο του $(x^n +1)$ τότε $c^R(x) = x\, c(x) \bmod (x^n +1)$ από τον ορισμό του modulo
- Από το ως άνω θεώρημα μπορεί να διατυπωθεί το εξής: Ένας κυκλικός κώδικας είναι ένας γραμμικός κώδικας τέτοιος ώστε εάν c(x) είναι κωδική λέξη, τότε και η $x\cdot c(x) \bmod(x^n +1)$ είναι επίσης κωδική λέξη.
  - Εφαρμόζοντας επαναλαμβανόμενα κυκλικές μετατοπίσεις $c^R(x)$ όπως ορίζει το θεώρημα, εύκολα μπορεί να δειχθεί ότι $x^i\, c(x) \bmod (x^n +1)$ είναι επίσης κωδική λέξη για όλα τα $i\geq 0$ (για $i=n \Rightarrow c^R(x) = c(x)$)
  - Στο εξής η $\mathbf{P(x) \bmod (x^n +1)}$ θα συμβολίζεται και ως $\mathbf{[P(x)]_n}$
- **Παράδειγμα**: Θεωρούμε την κωδική λέξη c = 1101000 μήκους n = 7. Τότε $c(x) = 1 + x + x^3$ και $x\cdot c(x) = x + x^2 + x^4$ αναπαριστά τη λέξη 0110100 =κ(c), $x^2\cdot c(x) = x^2 + x^3 + x^5$ αναπαριστά τη λέξη 0011010=κ(0110100), $x^3\cdot c(x) = x^3 + x^4 + x^6$ αναπαριστά τη λέξη 0001101=κ(0011010), κοκ

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο Γεννήτορας)

- **Θεώρημα:** Αν C είναι ένας κυκλικός κώδικας και $u \in C$, τότε για κάθε πολυώνυμο α(x), η λέξη c που αντιστοιχεί στο πολυώνυμο $c(x) = a(x)u(x) \bmod (1 + x^n)$ ανήκει στον κώδικα C.
- **Απόδειξη:** Αν $a(x) = (a_0 + a_1x + a_2 x^2 + \ldots + a_{n-1} x^{n-1})$, τότε $c(x) = a(x)\, u(x) \bmod (1 + x^n) = (a_0 + a_1x + a_2 x_2 + \ldots + a_{n-1} x^{n-1})u(x) \bmod (1 + x^n) = (a_0\, u(x) + a_1xu(x) + a_2 x^2\, u(x) + \ldots + a_{n-1} x^{n-1}\, u(x)) \bmod (1 + x^n)$. Από ιδιότητα 3 του modulo $\Rightarrow c(x)= a_0 [u(x)]_n + a_1 [xu(x)]_n + \ldots + a_{n-1} [x^{n-1} u(x)]_n$. Εφόσον το c(x) είναι γραμμικός συνδυασμός του u(x) και των (n – 1) κυκλικών μετατοπίσεών του που όλες τους $\in C$, τότε η αντίστοιχη λέξη c περιέχεται στον κώδικα C.
- **Πολυώνυμο-Γεννήτορας:** Σε ένα κυκλικό κώδικα C υπάρχει μία μοναδική λέξη g, της οποίας το αντίστοιχο πολυώνυμο g(x) έχει το μικρότερο βαθμό σε σύγκριση με τα αντίστοιχα πολυώνυμα όλων των άλλων μη μηδενικών λέξεων. ***Το πολυώνυμο ελάχιστου βαθμού που αντιστοιχεί σε αυτή τη μοναδική, μη μηδενική, λέξη του C καλείται πολυώνυμο – γεννήτορας***. Ονομάζεται γεννήτορας γιατί για κάθε πολυώνυμο (λέξη) $c(x) \in C$, υπάρχει πολυώνυμο a(x), τέτοιο ώστε $c(x) = a(x)g(x) \bmod (1 + x^n)$. Το πολυώνυμο γεννήτορας **διαιρεί** όλες τις κωδικές λέξεις $c(x) \in C$
- **Παράδειγμα:** Για τον κυκλ. κώδικα C = {000, 110, 101, 011} η λέξη ≠ 0 που αντιστοιχεί στον μικρότερο πολυωνυμικό βαθμό είναι η 110 με αναπαράσταση 1+x = ο γεννήτορας πολυώνυμο g(x). Πράγματι, όλες οι κωδικές λέξεις μπορούν να προκύψουν ως πολ/σια του g(x) καθώς: (000) = 0g(x), $101 \rightarrow 1+ x^2 = (1+x)(1+x)=g(x)(1+x)$, $011 \rightarrow x+ x^2 = x\,(x+1)=xg(x)$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο Γεννήτορας)

- **<u>Παράδειγμα</u>**
- Κατασκευή γραμμικού κώδικα Hamming (7,4) από την κωδική λέξη 0001011

1.	Μηδενικό στοιχείο	0000000
2.	Κωδική λέξη	0001011
3.	1η Αριστερή μετατόπιση	0010110
4.	2η Αριστερή μετατόπιση	0101100
5.	3η Αριστερή μετατόπιση	1011000
6.	4η Αριστερή μετατόπιση	0110001
7.	5η Αριστερή μετατόπιση	1100010
8.	6η Αριστερή μετατόπιση	1000101
9.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,3)	0011101
10.	1η Αριστερή μετατόπιση κωδικής λέξης 0011101 (βήμα 9)	0111010
11.	2η Αριστερή μετατόπιση	1110100
12.	3η Αριστερή μετατόπιση	1101001
13.	4η Αριστερή μετατόπιση	1010011
14.	5η Αριστερή μετατόπιση	0100111
15.	6η Αριστερή μετατόπιση	1001110
16.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,11)	1111111

Πολυώνυμο γεννήτορας
$1+x^2+x^3$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο-Γεννήτορας)

- ***Ιδιότητες Πολυωνύμου Γεννήτορα***
- Αν C είναι ένας κυκλικός κώδικας μήκους n, g(x) = πολυώνυμο – γεννήτορας και n – k ο βαθμός του, τότε ισχύουν τα ακόλουθα:

1. Ο κώδικας C είναι διάστασης k,
   - Η απόδειξη είναι προφανής, καθώς δεδομένου ότι το μήκος κωδικής λέξης = n και deg g(x)= n-k $\Rightarrow$Διάσταση C= n-(n-k)=k
2. Εάν P(x) είναι ένα πολυώνυμο τέτοιο ώστε το $[P(x)]_n$ να αποτελεί κωδική λέξη τότε το πολυώνυμο-γεννήτορας g(x) διαιρεί το P(x)
   - Αντίστροφα, μία λέξη c ανήκει στον C, αν και μόνον αν το αντίστοιχο πολυώνυμο c(x) διαιρείται από το g(x) (είναι πολλαπλάσιο του γεννήτορα g(x))
   - **Απόδειξη**: Έστω $[P(x)]_n \in C$. Τότε ισχύει: P(x) = Q(x)g(x) +R(x), όπου degR<deg g. Εφαρμόζοντας mod $(x^n +1)$ και λαμβάνοντας υπ' όψη ότι degR<deg g≤n-1 $\Rightarrow$ { R(x) mod $(x^n +1)$ } = $[P(x)]_n$ - $[Q(x)g(x)]_n$ $\Rightarrow$ R(x) = $[P(x)]_n$ - $[Q(x)g(x)]_n$ (1).
   - Δεδομένου ότι $[P(x)]_n \in C$ και $[Q(x)g(x)]_n \in C$ (όπως υποδεικνύει το προηγούμενο θεώρημα) $\Rightarrow$ R(x) $\in$ C επίσης. Άρα δεδομένου ότι degR<deg g και g εξ' ορισμού μη μηδενική κωδική λέξη με τον ελάχιστο βαθμό (deg) τότε R=η μηδενική λέξη του C και συνεπώς από (1) $\Rightarrow$ P(x) = Q(x)g(x) $\Rightarrow$ το g(x) διαιρεί το P(x)

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο-Γεννήτορας)

- ***Ιδιότητες Πολυωνύμου Γεννήτορα (συνέχεια)***

3. Το πολυώνυμο g(x) είναι το πολυώνυμο – γεννήτορας ενός κυκλικού κώδικα C μήκους n, αν και μόνον αν διαιρεί το μέτρο ισοτιμίας (x^n + 1), δηλαδή αν (x^n+ 1) =h(x)g(x)
   - **Απόδειξη:** Εφαρμόζοντας την Ιδιότητα 2 με P(x)= x^n +1, έχομε $[P(x)]_n$ =0, όπου βέβαια 0=κωδική λέξη ⇒ από Ιδιότητα 2 ότι το g(x) είναι διαιρέτης του x^n+ 1
4. Από τα προηγούμενα συνάγεται ότι: Εάν κάποιο πολυώνυμο g(x) είναι διαιρέτης του x^n+ 1 τότε υπάρχει ένας (n,k) κυκλικός κώδικας που έχει το g(x) ως πολυώνυμο-γεννήτορα με διάσταση k=n-deg g(x) και με κωδικές λέξεις το σύνολο όλων των διανυσμάτων-λέξεων των οποίων η πολυωνυμική αναπαράσταση είναι διαιρετή από το g(x)
   - Με βάση την παραπάνω πρόταση και έχοντες στην διάθεσή μας τους παράγοντες του x^n+ 1 για διάφορες τιμές του n, μπορεί κανείς με κατάλληλη εξέταση αυτών (των παραγόντων) να επιλέξει εκείνο το g(x) που θα ικανοποιεί τις εκάστοτε προδιαγραφές όπως αριθμός μηνυμάτων (2^k), n , d κλπ.
5. Οι λέξεις που αντιστοιχούν στα πολυώνυμα g(x), xg(x), x^2g(x),…,x^{k-1}g(x) αποτελούν μια βάση του C
   1. Δηλαδή όλες οι κυκλικές μετατοπίσεις

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο Γεννήτορας)

- **<u>Παράδειγμα (Ιδιότητα 5)</u>**
- Κατασκευή γραμμικού κώδικα Hamming (7,4) από την κωδική λέξη 0001011

1.	Μηδενικό στοιχείο	0000000
2.	Κωδική λέξη	0001011
3.	1η Αριστερή μετατόπιση	0010110
4.	2η Αριστερή μετατόπιση	0101100
5.	3η Αριστερή μετατόπιση	1011000
6.	4η Αριστερή μετατόπιση	0110001
7.	5η Αριστερή μετατόπιση	1100010
8.	6η Αριστερή μετατόπιση	1000101
9.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,3)	0011101
10.	1η Αριστερή μετατόπιση κωδικής λέξης 0011101 (βήμα 9)	0111010
11.	2η Αριστερή μετατόπιση	1110100
12.	3η Αριστερή μετατόπιση	1101001
13.	4η Αριστερή μετατόπιση	1010011
14.	5η Αριστερή μετατόπιση	0100111
15.	6η Αριστερή μετατόπιση	1001110
16.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,11)	1111111

Πολυώνυμο γεννήτορας
$1+x^2+x^3$

Άλλη Βάση

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο-Γεννήτορας)

- **<u>Παράδειγμα</u>**: Το πολυώνυμο $x^7 + 1$ παραγοντοποιείται ως εξής: $x^7 + 1 = (x+1)(x^3 + x+1)(x^3 + x^2 +1)$. **Κάθε ένας από τους παράγοντες αυτούς ή και συνδυασμός τους μπορεί εν δυνάμει να αποτελέσει και το πολυώνυμο-γεννήτορα για έναν αντίστοιχο κυκλικό κώδικα μήκους n=7** (όσο δηλ. και ο βαθμός του $x^7 + 1$) Ενδεικτικά:
- Το $g(x)= (x^3 + x+1)$ ορίζει έναν κυκλικό κώδικα με n=7, k=n-deg g(x)= 7-3=4, και αριθμό parity bits =deg g(x)=3, πρόκειται δε για τον Hamming (7,4,3) κυκλικό κώδικα
- Το $g(x)=(x +1)$ ορίζει τον parity-check (7,6,1) κώδικα
- Το $g(x)=(x^3 + x+1)(x^3 + x^2 +1)$ ορίζει τον επαναληπτικό (7,1,6) κώδικα
- Το $g(x)=(x+1)(x^3 + x +1)= x^4 + x^3 + x^2 +1$ ορίζει έναν maximum-length-sequence (7,3,4) κώδικα ο οποίος είναι δυικός του κώδικα που ορίζεται από $g(x)= (x^3+x^2+1)$. Οι $2^3 = 8$ διαφορετικές λέξεις του κώδικα αυτού μπορούν άμεσα να παραχθούν άμεσα από το g(x) ως εξής:
  - $C_0 = 0 \rightarrow (0000000)$
  - $C_1 = 1 \cdot g(x) = x^4 + x^3 + x^2 +1 \rightarrow (1011100)$
  - $C_2 = x \cdot g(x) = x^5 + x^4 + x^3 +x \rightarrow (0101110)$
  - $C_3 = x^2 \cdot g(x) = x^6 + x^5 + x^4 + x^2 \rightarrow (0010111)$
  - $C_4 = (1+x) \cdot g(x) = (1+x) \cdot (x^4 + x^3 + x^2 +1)= x^5 + x^2 +1 +x \rightarrow (1110010)$
  - $C_5 = (1+ x^2) \cdot g(x) = (1+ x^2) \cdot (x^4 + x^3 + x^2 +1) = x^6+ x^5+x^3+1\rightarrow (1001011)$
  - $C_6 = (x+ x^2) \cdot g(x) = x^6 + x^3 + x^2 + x \rightarrow (0111001)$
  - $C_7 = (1+x+ x^2) \cdot g(x)= x^6 + x^4 +x + 1 \rightarrow (1100101)$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- Εξ ίσου σημαντικό με το πολυώνυμο γεννήτορα και στενά σχετιζόμενο με αυτό αποτελεί και το πολυώνυμο – ελέγχου - ισοτιμίας, h(x) που ορίζεται ως:
  - $$h(x) = \frac{x^n+1}{g(x)}$$
- Ισχύει και εδώ παρόμοια ότι εάν $c \in C \Rightarrow [c(x) \cdot h(x)]_n = 0$.
  - Πράγματι $[c(x) \cdot h(x)]_n = (c(x) \cdot h(x)) \bmod (x^n+1) = (c(x) \cdot h(x)) \bmod (g(x) \cdot h(x)) = 0$ γιατί το g(x) ως πολυώνυμο γεννήτορας διαιρεί το $c \in C$. Αυτός είναι και ο λόγος που το h(x) επελέγη ως άνω
- **Πίνακες Γεννήτορες & Ελέγχου Ισοτιμίας- *<u>Μη Συστηματική</u>* Κωδικοποίηση**
- ***<u>Πρόταση 1:</u>*** Εάν C = (n,k) κυκλικός κώδικας με πολυώνυμο γεννήτορα $g(x) = g_0 + g_1x + \ldots + g_r x^r$ (με r=n-k) και πολυώνυμο ελέγχου ισοτιμίας $h(x)=h_0+h_1x+\ldots+h_kx^k$ τότε οι αντίστοιχοι G , H πίνακές τους έχουν ως εξής:

1. Ο πιο απλός γεννήτορας πίνακας G_1 είναι εκείνος που έχει ως γραμμές τις λέξεις που αντιστοιχούν στο πολυώνυμο - γεννήτορα του κώδικα και τις πρώτες k – 1 κυκλικές μετατοπίσεις του, δηλ:

$$G_1 = \begin{bmatrix} g(x) \\ xg(x) \\ \ldots\ldots \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \ldots & \ldots & g_r & 0 & \ldots & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & \ldots & g_r & 0 & \ldots & 0 \\ . & & & & & & & & \\ . & & & & & & & & \\ . & & & & & & & & \\ 0 & \ldots & \ldots & 0 & g_0 & g_1 & \ldots & \ldots & g_r \end{bmatrix}$$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- ***<u>Πρόταση 1 (συνέχεια)</u>***

2. Παρόμοια με τον γεννήτορα πίνακα ο πιο απλός πίνακας ελέγχου ισοτιμίας H_1 είναι εκείνος που ο ανάστροφός του έχει ως γραμμές τις λέξεις που αντιστοιχούν στο αντίστροφο πολυώνυμο ελέγχου ισοτιμίας $\hat{h}(x)$ του $h(x)$
   - (όπου $\hat{h}(x) = h_k+h_{k-1}x+\ldots+h_0x^k =$ και στις πρώτες r – 1 κυκλικές μετατοπίσεις του, δηλ:

$$H_1^T = \begin{bmatrix} \bar{h}(x) \\ x\bar{h}(x) \\ \ldots\ldots \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ x^{r-1}\bar{h}(x) \end{bmatrix} = \begin{bmatrix} h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & \ldots & \ldots & 0 \\ 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ . & & & & & & & & \\ . & & & & & & & & \\ . & & & & & & & & \\ 0 & \ldots & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 \end{bmatrix}$$

3. Επιπλέον εύκολα μπορεί να δειχθεί ότι η κωδικοποίηση $C=I \cdot G_1$ ενός μηνύματος $I= (I_0 ,I_1, \ldots , I_{k-1})$ είναι ισοδύναμη με $c(x) =I(x)\, g(x)$, όπου $c(x) = c_0 + c_1x +\ldots + c_{n-1}\, x_{n-1}$ και $I(x) = I_0 + I_1x +\ldots + I_{\kappa-1}\, x^{\kappa-1}$
   - Εδώ πρέπει να σημειωθεί ότι η ως άνω κωδικοποίηση **δεν είναι συστηματική**, καθώς, όπως μπορεί να φανεί και από το σχετικό παράδειγμα, στη κωδική λέξη C(x) που προκύπτει κατ'αυτόν τον τρόπο δεν περιέχονται αναλοίωτα τα bits του μηνύματος I(x)

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- ***<u>Αποδείξεις:</u>***
- Δεδομένου ότι η i γραμμή του G_1 έχει εξ'ορισμού πολυωνυμική αναπαράσταση $x^i g(x)$, i=0,1…,k-1 κάθε μία από αυτές αποτελεί και μία κωδική λέξη του C αφού είναι πολ/σιο του g(x). Επιπλέον λόγω της ειδικής δομής του G_1 και από το γεγονός ότι κάθε γραμμή είναι διαφορετικής τάξης $\Rightarrow$ εύκολα αποδεικνύεται ότι είναι και γραμμικά ανεξάρτητες και εφόσον η διάσταση του C είναι k $\Rightarrow$ αποτελούν βάση του C
- Για να αποδειχθεί ότι ο H_1 είναι πίνακας ελέγχου ισοτιμίας του C αρκεί να σημειωθεί ότι το εσωτερικό γινόμενο της i γραμμής του G_1 και της j στήλης του H_1 (j γραμμής του H_1^T) είναι ο συντελεστής του x_{k-i+j} στο γινόμενο g(x)h(x). Αλλά το $g(x)h(x)= x^n -1$ και εφόσον ο δείκτης k-i+j κυμαίνεται από 1 (όταν i=k-1 και j=0) έως n-1 (όταν i=0 και j=r-1) $\Rightarrow$ κάθε ένα από τα εσωτερικά γινόμενα =0 $\Rightarrow$ $G \cdot H=0$. Εφόσον επιπλέον η διάσταση του $C^{\perp}$ είναι r και οι r στήλες του είναι γραμ. ανεξάρτητες (εύκολα μπορεί αυτό να δειχθεί καθώς έχουν παρόμοια δομή με γραμμές του G_1) $\Rightarrow$ αποτελούν μία βάση του $C^{\perp}$ και άρα όντως ο H_1 = πίνακας ισοτιμίας
- Το διάνυσμα nx1 που προκύπτει από τη σχέση κωδικοποίησης $C=I \cdot G_1$, όπου $I= (I_0,I_1,\dots ,I_{k-1})$, θα έχει ως εξής: $[I_0 , I_1,\dots ,I_{k-1}] \cdot [g(x),xg(x), \dots, x^{k-1} g(x)]^T = I_0 g(x)+ I_1 x g(x)+\dots+ I_{k-1} x^{k-1} g(x) = I(x)g(x)$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- **Παράδειγμα:**
- Έστω ο κώδικας C = {0000, 1010, 0101, 1111}. Ζητείται ο γεννήτορας πίνακας G_1 του C .
- Κατά πρώτον προσδιορίζεται το πολυώνυμο γεννήτορας =το πολυώνυμο ελάχιστου βαθμού που αντιστοιχεί σε μη μηδενική λέξη του C $\Rightarrow$ το $g(x) = 1 + x^2 \rightarrow (1010)$. Αφού $k = n–deg(g(x)) = 4 – 2 = 2$
- Ο γεννήτορας πίνακας G_1 του C έχει ως γραμμές τις λέξεις που αντιστοιχούν στα πολυώνυμα g(x) και $x \cdot g(x)$, δηλαδή

$$G_1 = \begin{bmatrix} g(x) \\ xg(x) \end{bmatrix} = \begin{bmatrix} 1+x^2 \\ x+x^3 \end{bmatrix} = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}$$

- Για την κωδικοποίηση των ψηφίων πληροφορίας 01 και 10 εφαρμόζομε την αντίστοιχη σχέση c(x) =I(x) g(x). Οι πολυωνυμικές αναπαραστάσεις των ψηφίων πληροφορίας 01 και 10 αντιστοιχούν στα πολυώνυμα 1 και x και το γινόμενό τους με το πολυώνυμο – γεννήτορα $g(x) = 1 + x^2 = 1 + x^2 \rightarrow 1010$ και $x + x^3 \rightarrow 0101$.
- Επιπλέον $h(x)= (1 + x^4)/(1 + x^2)= 1 + x^2$. Το αντίστροφο πολυώνυμο του h(x) ταυτίζεται με το h(x) και είναι ίσο με $1 + x^2 = g(x) \Rightarrow$ είναι προφανές ότι και ο πίνακας ισοτιμίας H_1 ταυτίζεται με τον G_1

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο Γεννήτορας)

- **Παράδειγμα (Κατασκευή γεννήτορα πίνακα, πίνακα ισοτιμίας, κωδικοποίηση)**
- Κατασκευή γραμμικού κώδικα Hamming (7,4) από την κωδική λέξη 0001011

1.	Μηδενικό στοιχείο	0000000
2.	Κωδική λέξη	0001011
3.	1η Αριστερή μετατόπιση	0010110
4.	2η Αριστερή μετατόπιση	0101100
5.	3η Αριστερή μετατόπιση	1011000
6.	4η Αριστερή μετατόπιση	0110001
7.	5η Αριστερή μετατόπιση	1100010
8.	6η Αριστερή μετατόπιση	1000101
9.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,3)	0011101
10.	1η Αριστερή μετατόπιση κωδικής λέξης 0011101 (βήμα 9)	0111010
11.	2η Αριστερή μετατόπιση	1110100
12.	3η Αριστερή μετατόπιση	1101001
13.	4η Αριστερή μετατόπιση	1010011
14.	5η Αριστερή μετατόπιση	0100111
15.	6η Αριστερή μετατόπιση	1001110
16.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,11)	1111111

Πολυώνυμο γεννήτορας
$1+x^2+x^3$

Άλλη Βάση

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο Γεννήτορας)

- **<u>Παράδειγμα (Κατασκευή γεννήτορα πίνακα, πίνακα ισοτιμίας, κωδικοποίηση)</u>**
- Το πολυώνυμο γεννήτορας $g(x) = 1+x^2+x^3 \rightarrow (1011000)$ που αντιστοιχεί σε μη μηδενική λέξη του C $\in$ k = n–deg(g(x)) = 7 – 3 = 4
- Άρα ο G_1 δίνεται από τον παρακάτω γεννήτορα πίνακα

$$G_1 = \begin{bmatrix} g(x) \\ x \cdot g(x) \\ x^2 \cdot g(x) \\ x^3 \cdot g(x) \end{bmatrix} = \begin{bmatrix} 1+x^2+x^3 \\ x+x^3+x^4 \\ x^2+x^4+x^5 \\ x^3+x^5+x^6 \end{bmatrix} = \begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix}$$

- Επιπλέον $h(x)= (1 + x^7)/(1+x^2+x^3)= 1 + x^2 + x^3 + x^4 \rightarrow 10111$. Το αντίστροφο πολυώνυμο του h(x) είναι ίσο με $x^4 + x^2 + x + 1 \Rightarrow$ είναι προφανές ότι και ο πίνακας ισοτιμίας H_1 είναι

$$H_1^{\,T} = \begin{bmatrix} \bar{h}(x) \\ x \cdot \bar{h}(x) \\ x^2 \cdot \bar{h}(x) \end{bmatrix}^T = \begin{bmatrix} 1+x+x^2+x^4 \\ x+x^2+x^3+x^5 \\ x^2+x^3+x^4+x^6 \end{bmatrix}^T = \begin{bmatrix} 1110100 \\ 0111010 \\ 0011101 \end{bmatrix}^T$$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πολυώνυμο Γεννήτορας)

- **<u>Παράδειγμα (Κατασκευή γεννήτορα πίνακα, πίνακα ισοτιμίας, κωδικοποίηση)</u>**
- Για την κωδικοποίηση των ψηφίων πληροφορίας 0011 και 1101 εφαρμόζομε την αντίστοιχη σχέση $c(x) = I(x)\, g(x)$.
- Οι πολυωνυμικές αναπαραστάσεις των ψηφίων πληροφορίας 0011 και 1101 αντιστοιχούν στα πολυώνυμα x^2+x^3 και $1+x+x^3$
- Το γινόμενό τους με το πολυώνυμο – γεννήτορα $g(x) = 1 + x^2 + x^3$ είναι
  - $(0011)\cdot g(x) = x^2 + x^3 + x^4 + x^6 \rightarrow 0011101$
  - $(1101)\cdot g(x) = 1+x+x^2+x^3+x^4+x^5+x^6 \rightarrow 1111111$.
- Παρατηρείστε ότι δεν μπορούμε να βρούμε εύκολα τα bits του μηνύματος (1101) από την κωδική λέξη 1111111.
  - Αυτό συμβαίνει γιατί ο γεννήτορας πίνακας με τον οποίο κωδικοποιούμε δημιουργεί μη-συστηματικό κώδικα

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- ***Πίνακες Γεννήτορες & Ελέγχου Ισοτιμίας- Συστηματική Κωδικοποίηση***
- ***Πρόταση 2***: Έστω ότι C ένας (n,k) κυκλικός κώδικας με g(x) = πολυώνυμο γεννήτορα. Τότε εάν $G_{2,i}$= το διάνυσμα μήκους n με $G_{2,i}(x) = x^{r+i} + x^{r+i} \bmod g(x)$, (r=n-k) τότε ένας γεννήτορας πίνακας G_2 του C δημιουργείται από τον kxn πίνακα με γραμμές $G_{2,i}$, i=0,1,…,κ-1:
- Παρομοίως εάν $H_{2,j}$ = διάνυσμα μήκους r με: $H_{2,j}(x)= x^j \bmod g(x)$ ⇒ πίνακας ισοτιμίας H_2 δημιουργείται από τον nxr πίνακα με γραμμές $H_{2,j}$, j=0,1,…,n-1

$$G_2 = \begin{bmatrix} G_{2,0} \\ G_{2,1} \\ \dots\dots\dots \\ \dots\dots\dots \\ \dots\dots\dots \\ G_{2,k-1} \end{bmatrix} = \begin{bmatrix} x^r + x^r \bmod g(x) \\ x^{r+1} + x^{r+1} \bmod g(x) \\ \dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots \\ x^{r+k-1} + x^{r+k-1} \bmod g(x) \end{bmatrix} \qquad H_2 = \begin{bmatrix} H_{2,0}^T & H_{2,1}^T & \dots & H_{2,n-1}^T \end{bmatrix}^T = \begin{bmatrix} 1 \bmod g(x) \\ x \bmod g(x) \\ \dots\dots \\ \dots\dots \\ \dots\dots \\ x^{n-1} \bmod g(x) \end{bmatrix}^T$$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- ***Πίνακες Γεννήτορες & Ελέγχου Ισοτιμίας- Συστηματική Κωδικοποίηση***
- ***Πρόταση 2 (συνέχεια)***: Επιπλέον εύκολα μπορεί να δειχθεί ότι η κωδικοποίηση $C=I \cdot G_2$ ενός μηνύματος $I= (I_0 ,I_1, \ldots , I_{k-1})$ αντιστοιχεί στην παρακάτω πολυωνυμική αναπαράσταση του C :
  - $$C(x) = x^r I(x) + [x^r I(x) \bmod g(x)]$$
  - Από την σχέση αυτή είναι προφανές ότι ο κώδικας C που προκύπτει είναι συστηματικός καθώς ο παράγων x^r I(x) απεικονίζει αναλλοίωτα τα k bits πληροφορίας στις **k πλέον υψηλόβαθμες θέσεις** του C(x) με τις υπόλοιπες n-k να καταλαμβάνονται από τα bits ισοτιμίας που προκύπτουν από τον [x^r I(x) mod g(x)] παράγοντα

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

Αποδείξεις:

1. Κάθε γραμμή i του G_2 είναι πολ/σιο του g(x) και επομένως κωδική λέξη του C,διότι : $[x^{r+i} + x^{r+i} \bmod g(x)] \bmod g(x) = x^{r+i} \bmod g(x) + x^{r+i} \bmod g(x) = 0$ (όπου έγινε χρήση των ιδοτήτων 3 και 5 του modulo τελεστή. Εύκολα επίσης μπορεί να αποδειχθεί ότι είναι γραμμικά ανεξάρτητες. Άρα εφόσον το G_2 έχει k γραμμικά ανεξάρτητες γραμμές, (πρέπει εδώ να σημειωθεί ότι οι τελευταίες k στήλες του G_2 σχηματίζουν έναν kxk πίνακα ταυτότητας) όσες και η διάσταση του C και είναι επιπλέον κωδικές λέξεις $\Rightarrow$ όντως G_2 = Γεννήτορας Πίνακας του C
2. Για να αποδειχθεί ότι ο H_2 είναι πίνακας ελέγχου ισοτιμίας του C (πρέπει εδώ να σημειωθεί ότι οι πρώτες r γραμμές του H_2 σχηματίζουν έναν rxr πίνακα ταυτότητας) αρκεί να δειχθεί ότι εάν $\mathbf{R} \in \mathbf{C} \Rightarrow \mathbf{R} \cdot \mathbf{H} = 0$. Έστω $\mathbf{R} = (R_0, R_1, \ldots, R_{n-1})$ τότε το $\mathbf{R} \cdot \mathbf{H}$ είναι ένα 1xr διάνυσμα (γραμμής) και ισούται με $[R_0, R_1, \ldots, R_{n-1}] \cdot [1 \bmod g(x), x \bmod g(x), \ldots, x^{r-1} \bmod g(x)]^T = R_0 \bmod g(x) + R_1 x \bmod g(x) + \ldots + R_{r-1} x^{r-1} \bmod g(x) = (R_0 + R_1 x + \ldots + R_{r-1} x^{r-1}) \bmod g(x) = R(x) \bmod g(x) = 0$ εφόσον έχει υποτεθεί ότι $\mathbf{R} \in \mathbf{C}$ και επομένως R(x)=πολ/σιο του g(x)
3. Το διάνυσμα nx1 που προκύπτει από τη σχέση κωδικοποίησης $\mathbf{C} = \mathbf{I} \cdot \mathbf{G_2}$, όπου $\mathbf{I} = (I_0, I_1, \ldots, I_{k-1})$, θα έχει ως εξής: $[I_0, I_1, \ldots, I_{k-1}] \cdot [x^r + x^r \bmod g(x), x^{r+1} + x^{r+1} \bmod g(x), \ldots, x^{r+k+1} + x^{r+k+1} \bmod g(x)]^T = I_0 (x^r + x^r \bmod g(x)) + I_1 (x^{r+1} + x^{r+1} \bmod g(x)) + \ldots + I_{k-1} (x^{r+k+1} + x^{r+k+1} \bmod g(x)) = x^r I(x) + [x^r I(x)] \bmod g(x)$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- **Παράδειγμα (Συστηματική Κωδικοποίηση)**
- Κατασκευή γραμμικού κώδικα Hamming (7,4) από την κωδική λέξη 0001011

1.	Μηδενικό στοιχείο	0000000
2.	Κωδική λέξη	0001011
3.	1η Αριστερή μετατόπιση	0010110
4.	2η Αριστερή μετατόπιση	0101100
5.	3η Αριστερή μετατόπιση	1011000
6.	4η Αριστερή μετατόπιση	0110001
7.	5η Αριστερή μετατόπιση	1100010
8.	6η Αριστερή μετατόπιση	1000101
9.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,3)	0011101
10.	1η Αριστερή μετατόπιση κωδικής λέξης 0011101 (βήμα 9)	0111010
11.	2η Αριστερή μετατόπιση	1110100
12.	3η Αριστερή μετατόπιση	1101001
13.	4η Αριστερή μετατόπιση	1010011
14.	5η Αριστερή μετατόπιση	0100111
15.	6η Αριστερή μετατόπιση	1001110
16.	Άθροισμα κωδικών λέξεων 0001011+0010110 (βήμα 2,11)	1111111

Πολυώνυμο γεννήτορας
$1+x^2+x^3$

Άλλη Βάση

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- **Παράδειγμα (Συστηματική Κωδικοποίηση)**
- Το πολυώνυμο γεννήτορας $g(x) = 1+x^2+x^3 \rightarrow (1011000)$ που αντιστοιχεί σε μη μηδενική λέξη του C $\Rightarrow k = n-\deg(g(x)) = 7 - 3 = 4$
- Άρα ο G_2 δίνεται από τον παρακάτω γεννήτορα πίνακα

$$G_2 = \begin{bmatrix} x^3 + x^3 \bmod g(x) \\ x^4 + x^4 \bmod g(x) \\ x^5 + x^5 \bmod g(x) \\ x^6 + x^6 \bmod g(x) \end{bmatrix} = \begin{bmatrix} 1 + x^2 + x^3 \\ 1 + x + x^2 + x^4 \\ 1 + x + x^5 \\ x + x^2 + x^6 \end{bmatrix} = \begin{bmatrix} 1011000 \\ 1110100 \\ 1100010 \\ 0110001 \end{bmatrix}$$

- Και ο πίνακας ισοτιμίας H_2 είναι

$$H_2^T = \left[1, \quad x, \quad x^2, \quad x^3 \bmod g(x), \quad x^4 \bmod g(x), \quad x^5 \bmod g(x), \quad x^6 \bmod g(x)\right]^T =$$

$$= \left[1, \quad x, \quad x^2, \quad 1+x^2, \quad 1+x+x^2, \quad 1+x, \quad x+x^2\right]^T$$

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

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- **Παράδειγμα (Κατασκευή γεννήτορα πίνακα, πίνακα ισοτιμίας, κωδικοποίηση)**
- Για την κωδικοποίηση των ψηφίων πληροφορίας 0011 και 1101 εφαρμόζομε την αντίστοιχη σχέση $c(x) = x^r I(x) + [x^r I(x)] \bmod g(x)$.
- Οι πολυωνυμικές αναπαραστάσεις των ψηφίων πληροφορίας 0011 και 1101 αντιστοιχούν στα πολυώνυμα x^2+x^3 και $1+x+x^3$
- Το γινόμενό τους με το $x^r I(x)$ είναι
  - 0011 → $(x^2+x^3)\cdot x^3 = x^5 + x^6$
  - 1101 → $(1+x+x^3)\cdot x^3 = x^3+x^4+x^6$.
- Ενώ το $[x^r I(x)] \bmod g(x)$ είναι
  - 0011 → $(x^2+x^3) \bmod (1 + x^2 + x^3) = 1$
  - 1101 → $(x^3+x^4+x^6) \bmod (1 + x^2 + x^3) = x^2$
- Άρα έχουμε
  - $C(0011) = 1 + x^5 + x^6 = 100\underline{0011}$
  - $C(1101) = x^2 + x^3 + x^4 + x^6 = 001\underline{1101}$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

- **Παράδειγμα:** Έστω ο (7,3,4) κυκλικός κώδικας με $g(x)= x^4+x^3+x^2+1$. Το $h(x)= (x^7+1)/(x^4+x^3+x^2+1)=x^3+x^2+1$. Οι (μη συστηματικοί) πίνακες γεννήτορες G_1και ισοτιμίας H_1 σύμφωνα με την πρόταση 1 έχουν ως εξής:

$$G_1 = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \end{bmatrix} = \begin{bmatrix} x^4+x^3+x^2+1 \\ x^5+x^4+x^3+x \\ x^6+x^5+x^4+x^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$H_1^T = \begin{bmatrix} \bar{h}(x) \\ x\bar{h}(x) \\ x^2\bar{h}(x) \\ x^3\bar{h}(x) \end{bmatrix} = \begin{bmatrix} x^3+x+1 \\ x^4+x^2+x \\ x^5+x^3+x^2 \\ x^6+x^5+x^3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- όπου στον H_1 το αντίστροφο (reciprocal) πολυώνυμο του $h(x) = x^3+x+1$.
- Σύμφωνα την πρόταση 2 οι συστηματικοί πίνακες G_2 και H_2 έχουν ως εξής:

$$G_2 = \begin{bmatrix} x^4 + x^4 \bmod g(x) \\ x^5 + x^5 \bmod g(x) \\ x^6 + x^6 \bmod g(x) \end{bmatrix} = \begin{bmatrix} 1+x^2+x^3+x^4 \\ 1+x+x^2+x^5 \\ x+x^2+x^3+x^6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

Παράδειγμα (Συνέχεια): Ο (συστηματικός) πίνακας ισοτιμίας H_2 έχει ως εξής:

$$H_2^T = \left[1, \quad x, \quad x^2, \quad x^3, \quad x^4 \bmod g, \quad x^5 \bmod g, \quad x^6 \bmod g\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- Όσον αφορά την κωδικοποίηση μηνυμάτων, έστω ότι επιθυμούμε να κωδικοποιήσουμε το μήνυμα I= [101] → $1+x^2$. Τότε:
  - Χρησιμοποιώντας τον γεννήτορα πίνακα G_1 και βάσει της σχέσης **c(x) =I(x) g(x)** παίρνομε **c(x)**= $(1+x^2)(1+x^2+x^3+x^4) = 1+x^3+x^5+x^6$ → [1001011].
  - Χρησιμοποιώντας δε τον γεννήτορα πίνακα G_2 και βάσει της σχέσης $c(x)= x^r I(x)+ [x^r I(x)] \bmod g(x)$ και για r=4 παίρνομε: **c(x)**= $x^4(1+x^2) + [x^4 \cdot (1+x^2)] \bmod (1+x^2+x^3+x^4) = x^4 + x^6 + (x^4 + x^6) \bmod (1+x^2+ x^3+x^4) = x^4 + x^6 + x + 1$ → [1100<u>101</u>].
  - Όπως παρατηρείται η κωδική λέξη [1100<u>101</u>] που προκύπτει από τον G_2 περιέχει το αρχικό μήνυμα [101] αναλλοίωτο στα 3 τελευταία ψηφία της και συνεπώς έχομε όντως συστηματική κωδικοποίηση σε αντίθεση με την προηγούμενη περίπτωση όπου κάτι τέτοιο δεν ισχύει

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Πίνακες Γεννήτορες και Ισοτιμίας)

Εναλλακτικός τρόπος Συστηματικής Κωδικοποίησης με χρήση του h(x)

- Τρόπος (συστηματικής κωδικοποίησης) μπορεί να προκύψει και με χρήση της σχέσης που διέπει το πολυώνυμο γεννήτορα h(x) του C με τις κωδικές του λέξεις δηλ.**$c \in C \Rightarrow [c(x) \cdot h(x)]_n = 0$ ($[P(x)]_n = P(x) \bmod (x^n + 1)$)**
- ***<u>Θεώρημα:</u>*** Εκκινώντας από την παραπάνω σχέση **$c(x) \cdot h(x) \bmod (x^n + 1) = 0$** με $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \in C$, $h(x) = h_0 + h_1 x + \ldots + h_k x^k$ και αναλύοντάς την στους παράγοντές της, μπορεί να αποδειχθεί ότι θα πρέπει να ισχύει μεταξύ των c_i's και h_i's η παρακάτω σχέση:

$$\sum_{j=0}^{k} h_j c_{(i-j) \bmod n} = 0, i = 0,1,\ldots n-1$$

  - Εάν μάλιστα ισχύει $h_0 = 1$ τότε η παραπάνω σχέση απλοποιείται στην:

$$c_i = -\sum_{j=1}^{k} h_j c_{(i-j)}, i = k, k+1, \ldots, n-1$$

  - Η σχέση αυτή ουσιαστικά σημαίνει ότι εάν τα πρώτα k bits μίας κωδικής λέξης c_0, $c_1, \ldots, c_{k-1}$ είναι γνωστά τότε τα υπόλοιπα n-k bits c_k, $c_{k+1}, \ldots, c_{n-1}$ μπορούν να υπολογιστούν ως γραμ. συνδυασμός των k πρώτων bits. Χρησιμοποιώντας ως τα πρώτα k bits αυτά του αρχικού μηνύματος είναι φανερό ότι η μέθοδος αυτή οδηγεί σε συστηματική κωδικοποίηση
- **Παράδειγμα:** Έστω ο maximum-length-sequence (7,3,4) κώδικας με $g(x) = (x+1)(x^3 + x + 1) \Rightarrow h(x) = (x^7 + 1)/g(x) = 1 + x + x^2$ Άρα από την προηγούμενη σχέση $\Rightarrow c_i = c_{i-2} + c_{i-3}$, i= 3, …,6

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Σύνδρομα)

- **Σύνδρομο Κυκλικών Κωδίκων - Ιδιότητες**
- Όπως εδείχθη κατά την απόδειξη της πρότασης 2 εάν C(n,k) κυκλικός κώδικας και R διάνυσμα-λέξη μήκους n τότε ισχύει $R \cdot H_2 = R(x) \bmod g(x)$. Συνάγεται συνεπώς ότι το Σύνδρομο S μίας οποιασδήποτε ληφθείσας λέξης R (μήκους n) είναι ένα διάνυσμα μήκους 1xr, η πολυωνυμική αναπαράσταση του οποίου δίδεται από την σχέση:
- $S(x)= R(x) \bmod g(x)$, $\deg S(x)< \deg g(x) = n-k$

1. Για κάθε κωδική λέξη του C ισχύει $S(x) = R(x) \bmod g(x)=0$ (εφόσον $R(x)\in C \Rightarrow R(x)=$πολ/σιο του $g(x)$)
2. Το σύνδρομο μίας ληφθείσας λέξης R εξαρτάται αποκλειστικά από το τυχόν σφάλμα στην μετάδοση. Ειδικότερα εάν ε=πρότυπο σφάλματος, $c(x)\in C$ και $R= c + \varepsilon$ τότε για το σύνδρομο του R ισχύει:

   $$\mathbf{S(x) = \varepsilon(x) \bmod g(x)}$$

   - Πράγματι $S(x) = R(x) \bmod g(x) = (c(x) + \varepsilon(x)) \bmod g(x) = c(x) \bmod g(x) + \varepsilon(x) \bmod g(x) = 0 + \varepsilon(x) \bmod g(x) = \varepsilon(x) \bmod g(x)$
3. Με βάση τα παραπάνω ένα πολύ σημαντικό συμπέρασμα που προκύπτει από την σχέση $S(x) = \varepsilon(x) \bmod g(x)$ είναι πώς εάν
   - **$\deg \varepsilon(x) < \deg g(x) \Rightarrow S(x)=\varepsilon(x)$**
   - Εάν $\deg \varepsilon(x) <\deg g(x) \Rightarrow$ ότι το πλήθος των σφαλμάτων = μικρότερο του n-k

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Αποκωδικοποίηση)

- ***<u>Αποκωδικοποίηση Κυκλικών Κωδίκων</u>***
- ***Συμβατικός Τρόπος***: Χρήση του πίνακα ελέγχου ισοτιμίας H (είτε H_1, είτε H_2) και δημιουργία της ΤΔΑ. Έτσι, η αποκωδικοποίηση = υπολογισμός του συνδρόμου της ληφθείσας λέξης, εύρεση του αντίστοιχου προτύπου σφάλματος από την ΤΔΑ και υπολογισμός της κωδικής λέξης που μεταδόθηκε (άθροισμα της ληφθείσας λέξης με το πρότυπο σφάλματος).
- Απλοποίηση της όλης διαδικασίας χρησιμοποιώντας τις ιδιότητες των κυκλικών κωδίκων, και ειδικότερα αυτές των συνδρόμων για την διόρθωση **συνεχόμενων λαθών (error bursts)**
- ***<u>Αποκωδικοποίηση Συνεχόμενων Λαθών (Burst-error correction)</u>***
- **Ορισμός:** Έστω $c \in C$, C= κυκλικός (n,k) κώδικας ε= πρότυπο σφάλματος και R= c+ε . Τότε το διάνυσμα σφάλματος ε θα ορίζεται ότι αντιπροσωπεύει **Συνεχόμενα λάθη (error bursts) μήκους b** εάν τα μη μηδενικά στοιχεία (bits) του ε (δηλ. το πρώτο – τελευταίο μη μηδενικό στοιχείο του ε) καλύπτουν b διαδοχικά στοιχεία του ε (όχι απαραίτητα όλα μη μηδενικά)
  - π.χ. το ε=(010000110) αντιπροσωπεύει συνεχόμενα λάθη μήκους 7 καθώς το πρώτο -τελευταίο «1» του ε καλύπτει 7 διαδοχικά στοιχεία, δηλ. τα 1000011

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Αποκωδικοποίηση)

- ***<u>Ορισμός Συνεχόμενων Λαθών (συνέχεια)</u>***
- Ο πλήρης καθορισμός συνεχόμενων λαθών μήκους b προσδιορίζεται: Από το πρότυπο σφάλματος P το οποίο ταυτίζεται με τα b διαδοχικά στοιχεία του ε (ή ισοδύναμα με την πολυωνυμική τους αναπαράσταση P(x)), καθώς και από τη θέση i_0 του προτύπου του σφάλματος στο ε η οποία προσδιορίζεται από την θέση στο ε του πρώτου μη μηδενικού στοιχείου από τα b του προτύπου σφάλματος και θα συμβολίζεται με (P,i_0)
  - π.χ. Έστω το ε=(0**1**0000110) που αντιπροσωπεύει συνεχόμενα λάθη μήκους 7. Αυτά προσδιορίζονται: Από το πρότυπο σφάλματος, δηλ το P= (1000011) – ισοδύναμα από το $P(x)= 1+x^5+x^6$ – και την θέση του i_0 στο ε που εδώ $i_0 = 1$ (εάν $i_0 = 0 \Rightarrow \varepsilon(x)=P(x)$)
- **<u>Αρχή αποκωδικοποίησης συνεχόμενων σφαλμάτων</u>**
- Η αρχή της αποκωδικοποίησης για έναν κυκλικό κώδικα C με δυνατότητα διόρθωσης b συνεχόμενων σφαλμάτων στηρίζεται στην Ιδιότητα 3 των συνδρόμων ότι δηλ. εάν $\deg \varepsilon(x) \le \deg g(x) -1 \Rightarrow S(x)=\varepsilon(x)$, όπου $R=c+\varepsilon$, $c\in C$, δηλ. αυτό ισχύει εάν ο αριθμός των λαθών είναι μικρότερος του n-k (ή ≤ n-k-1) . Επειδή στην περίπτωσή μας έχουμε δυνατότητα διόρθωσης b σφαλμάτων η συνθήκη πρέπει να μετατραπεί σε $\deg \varepsilon(x) \le b-1 (\le n-k-1) \Rightarrow$ **$\deg S(x) \le b-1$ (1)** Τότε απλώς $c(x)=R(x) + S(x)$. Η συνθήκη (1) όμως ισχύει μόνον όταν $i_0 = 0$ (δεδομένου επίσης ότι ισχύει και $S(0)\neq 0$ συνθήκη που πρέπει να προστεθεί στην (1)), δηλ. όταν το πρότυπο b σφαλμάτων βρίσκεται στην θέση 0 του διανύσματος ε κάτι που δεν ισχύει στην γενική περίπτωση
  - Π.χ Για ε=(0**1**0000110) $\Rightarrow$ b=7 αλλά στην περίπτωση όπου $S(x)=\varepsilon(x) \Rightarrow$ **$\deg S(x) = \deg(x+x^6+x^7)= 7 > b-1 = 6$,** άρα η (1) δεν ισχύει, θα ίσχυε μόνο εάν ε=(**1**00001100)

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Αποκωδικοποίηση)

- ***<u>Αποκωδικοποίηση Συνεχόμενων Λαθών (Burst-error correction)</u>***
- Λύση= συνεχόμενες κυλήσεις προς τα δεξιά μέχρις ότου το ψηφίο στη θέση i_0 να είναι 1. Αποδεικνύεται ότι κυλήσουμε προς τα δεξιά το R, j_0 φορές $\Rightarrow R_{j0}= c_{j0} + \varepsilon_{j0}$, $\Rightarrow S_{j0}(x)= R_{j0}(x) \bmod g(x) \Rightarrow \varepsilon_{j0} = P(x)=$ με το ψηφίο στη θέση 0 να είναι 1
- Και άρα αρκεί $S_j(x)= R_j(x) \cdot \bmod g(x)=[x^j R]_n$ έως deg $S_j(x) <= b-1$
- Για πιο εύκολο υπολογισμό $S_j(x)$ χρήση ιδιότηταςΣ$S_{j+1}(x)=[x\, S_j(x)] \bmod g(x)$
- Στην γενική περίπτωση (όπου δηλ $i_0 \neq 0$) για ε(x) με b σφάλματα ισχύει ότι το ε(x) προσδιορίζεται από (P(x), i_0) με deg(P) ≤ b-1 και P(0)≠0 $\Rightarrow$ $\varepsilon(x) = [x_{i0}\, P(x)]_n \Rightarrow S(x)= [x_{i0}\, P(x)]_n \bmod g(x)$
- Έστω και εάν $i_0 \neq 0$, η λύση θα συνίστατο στο να εφαρμόσουμε στο ε(x) τον κατάλληλο αριθμό κυκλικών μετατοπίσεων j_0 με $0\leq j_0 \leq n-1$ έτσι ώστε $i_0+ j_0=0 \pmod n$ (δηλ. το πρότυπο σφάλματος P να έλθει στην θέση 0 του ε) οπότε ε(x) κυκλικά μετατοπισμένο κατά j_0 = P(x) , και μπορούν να εφαρμοσθούν τα προηγούμενα.
- **Με βάση τα ως άνω εάν R_{j0} (x) = η j_0-στή κυκλική μετατόπιση του R(x), τότε ισχύει: $R_{j0}(x) = c_{j0}(x) + \varepsilon_{j0}(x)$, $c_{j0}(x) \in C$ επίσης$\Rightarrow S_{j0}(x) = R_{j0}(x) \bmod g(x) = (c_{j0}(x) + \varepsilon_{j0}(x)) \bmod g(x) = c_{j0}(x) \bmod g(x) + P(x) \bmod g(x) = 0+ P(x) = P(x)$**
  - **Αυτό σημαίνει ότι το S_{j0} (x) ικανοποιεί την συνθήκη (1) και έτσι μπορεί άμεσα να υποτεθεί ότι το $c_{j0}(x) = R_{j0}(x) + S_{j0}(x)$ είναι η j_0-στή κυκλική μετατόπιση της πραγματικής μεταδοθείσης κωδικής λέξης C(x)**

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Αποκωδικοποίηση)

- ***Αποκωδικοποίηση Συνεχόμενων Λαθών (Burst-error correction)***
- Συμπερασματικά εάν ένας αποκωδικοποιητής υπολογίσει διαδοχικά τα $S_0(x)$, $S_1(x)$,…. και εξετάζει αυτά κάθε φορά κατά πόσον ικανοποιούν την (1) (**deg S(x) ≤ b-1)** τελικά το πρότυπο σφάλματος P(x) του ε(x) θα παγιδευτεί στην θέση 0 του ε(x) και θα μπορεί να διορθωθεί. Πραγματικά τότε το πρότυπο b σφαλμάτων $P(x) = S_{j0}(x)$ και η θέση του προτύπου σφάλματος, P(x), στο ε(x) θα δίδεται από την σχέση $i_0 + j_0 = 0 \bmod n \Rightarrow j_0 = (-i_0) \bmod n = n - j_0 \bmod n$
- ***Λήμμα του Meggit:*** Για μεγαλύτερη διευκόλυνση στον υπολογισμό των $S_j(x)$'s μπορεί να ληφθεί υπόψη το Λήμμα του Meggit δηλ: $S_{j+1}(x) = [x\, S_j(x)] \bmod g(x)$
- **Απόδειξη**: $S_j(x) = R_{j0}(x) \bmod g(x) = [x^j R(x)]_n = [x^j R(x)] \bmod g(x)$ Τότε $[x\, S_j(x)] \bmod g(x) = [x\, [x^j R(x)] \bmod g(x)\,] \bmod g(x) = [x^{j+1} R(x)] \bmod g(x) = S_{j+1}(x)$
- Με βάση όλα αυτά ο αλγόριθμος αποκωδικοποίησης θα έχει ως εξής:

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Αποκωδικοποίηση)

- ***<u>Αλγόριθμος αποκωδικοποίησης για κυκλικούς κώδικες με δυνατότητα διόρθωσης b (συνεχόμενων) σφαλμάτων</u>***
- Θεωρούμε έναν κυκλικό κώδικα C μήκους n και διάστασης k με δυνατότητα διόρθωσης b (συνεχόμενων) σφαλμάτων και με πολυώνυμο – γεννήτορα του C, g(x), του οποίου ο βαθμός είναι n – k. Και R(x)= ληφθείσα λέξη. Η αποκωδικοποίηση συνίσταται στα ακόλουθα τρία βήματα:

1. Υπολογισμός του συνδρόμου $S(x) = R(x) \bmod g(x)$.
2. Υπολογισμός του $S_i(x) = (x^i S(x)) \bmod g(x)$, για κάθε $i \geq 0$, μέχρι να βρεθεί ένα S_j του οποίου ο βαθμός είναι μικρότερος ή ίσος του b-1 και επιπλέον $S_j(0) \neq 0$. Τότε το πρότυπο σφάλματος είναι $P(x) = S_j(x)$ και η θέση του προτύπου σφάλματος, P(x) , στο ε(x) θα δίδεται από την σχέση $i_0 + j_0 = 0 \bmod n \Rightarrow j_0 = (-i_0) \bmod n = n - j_0 \bmod n$ ή εναλλακτικά $\varepsilon(x) = x^{n-j} S_j(x) \bmod (1 + x^n)$.
3. Υπολογισμός της κωδικής λέξης που μεταδόθηκε
   - $c(x) = R(x) + \varepsilon(x)$.

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Αποκωδικοποίηση)

- **Παράδειγμα:** Θεωρούμε έναν κώδικα *C* μήκους $n = 7$ με πολυώνυμο – γεννήτορα $g(x) = 1 + x^2 + x^3$ και δυνατότητα διόρθωσης $b = 1$. Εάν ελήφθη η λέξη 1111000, ζητείται η κωδική λέξη που μεταδόθηκε.
- **Απάντηση:** Η ληφθείσα λέξη αντιστοιχεί στο πολυώνυμο $R(x) = 1 + x + x^2 + x^3$ και επομένως:
- $S(x) = R(x) \bmod g(x) = (1 + x + x^2 + x^3) \bmod (1 + x^2 + x^3) = x$, του οποίου ο βαθμός είναι $1>b-1=0$ και άρα δεν ικανοποιεί την συνθήκη (1) $\Rightarrow$ πρέπει να υπολογιστούν τα διαδοχικά $S_j(x)$ έως ότου $\deg S_j(x) \leq 0 (=b-1)$. Έτσι έχομε:
- $S_1(x)=x\,S(x)= x^2 \bmod (1 + x^2 + x^3) = x^2$
- $S_2(x)=x\,S_1(x)= x^3 \bmod (1 + x^2 + x^3) = 1 + x^2$
- $S_3(x)=x\,S_2(x)= x(1 + x^2) \bmod (1 + x^2 + x^3)=x^3+x \bmod(1 + x^2 + x^3)=x^2 + x+1$
- $S_4(x)=x\,S_3(x)= x(x^2 + x+1) \bmod (1 + x^2 + x^3)=x^3 + x^2 +x \bmod (1 + x^2+x^3)=x+1$
- $S_5(x)=x\,S_4(x)= x(x+1) \bmod (1 + x^2 + x^3)= x^2 +x \bmod (1 + x^2+x^3)= x^2 +x$
- $S_6(x)=x\,S_5(x)= x(x^2+x) \bmod (1 + x^2 + x^3) = x^3 + x^2 \bmod (1 + x^2 + x^3) =1$
- Εφόσον $\deg S_6(x)=0$ και $S_6(0)=1\neq 0$ ικανοποιείται η (1) και άρα το πρότυπο σφάλματος $P(x)=1$ και $j_0=6$. Η θέση i_0 του $P(x)$ στο $\varepsilon(x)$ θα δίδεται από την σχέση $i_0+ j_0=0 \bmod n \Rightarrow i_0 = n - j_0 \bmod n \Rightarrow 7-6=1$. Συνεπώς $\varepsilon= (0100000)$
- Επομένως, εφόσον το πρότυπο σφάλματος είναι $\varepsilon = 0100000$ η κωδική λέξη που μεταδόθηκε $c= R + \varepsilon= 1111000 + 0100000 = 1011000$.

©2006, Σπύρος Δενάζης

Κυκλικοί Κώδικες (Αποκωδικοποίηση)

Διόρθωση της Άσκησης αυτοξιολόγησης 4.17 (*Θεωρία Πληροφορίας του ΕΑΠ)*

- Θεωρούμε έναν κώδικα C, μήκους n = 7, και δυνατότητα διόρθωσης t=1 λαθών με $g(x) = 1 + x + x^3$ και τη λήψη των λέξεων 1111000 και 1100101. Ζητούνται οι κωδικές λέξεις που μεταδόθηκαν.
- ***Απάντηση***: Χρειάζεται διόρθωση το α'σκέλος της άσκησης που αφορά την αποκωδικοποίηση της λέξης 1111000 *(καθώς παρότι t=1 καταλήγει στην διόρθωση 2 λαθών) δηλ:*
- Η ληφθείσα λέξη R= 1111000 αντιστοιχεί στο πολυώνυμο $R(x) = 1 + x + x^2 + x^3$ και επομένως $S(x) = R(x) \bmod g(x) = 1 + x + x^2 + x^3 \bmod (1 + x + x^3) = x^2$ του οποίου ο βαθμός είναι 2>b-1=0 και άρα δεν ικανοποιεί την συνθήκη (1) $\Rightarrow$ πρέπει να υπολογιστούν τα $S_j(x)$ έως ότου $\deg S_j(x) \leq 0 (=b-1)$:
- $S_1(x) = xS(x) \bmod g(x) = x(x^2) \bmod (1 + x + x^3) = x^3 \bmod (1 + x + x^3) = 1 + x$,
- $S_2(x)=x\, S_1(x)= x\,(1+x) \bmod (1 + x + x^3) = x+x^2 \bmod (1 + x + x^3) = x + x^2$
- $S_3(x)=xS_2(x)= x\,(x + x^2) \bmod (1 + x + x^3) = x^2 + x^3 \bmod (1 + x + x^3) = x^2 + x+1$
- $S_4(x)=xS_3(x)= x\,(x^2 + x+1) \bmod (1 + x + x^3) = x^3 + x^2+x \bmod (1+x+ x^3) = x^2+1$
- $S_5(x)=xS_4(x)= x(x^2+1) \bmod (1 + x + x^3) = x^3 + x \bmod (1 + x + x^3) = 1$
- Εφόσον $\deg S_5(x)=0$ και $S_5(0)=1 \neq 0$ ικανοποιείται η (1) και άρα το πρότυπο σφάλματος P(x)=1 και $j_0=5$. Η θέση i_0 του P(x) στο ε(x) θα δίδεται από την σχέση $i_0 = n - j_0 \bmod n \Rightarrow 7-5=2$. Συνεπώς ε= (0010000) και η κωδική λέξη που μεταδόθηκε c= R + ε = 1111000 + 0010000 = 1101000.

©2006, Σπύρος Δενάζης