Κώδικες διόρθωσης σφαλμάτων

Αθανάσιος Κούτρας

Αναπληρωτής Καθηγητής

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών,
Παν. Πελοποννήσου

24 Ιανουαρίου 2022

Περίγραμμα διάλεξης

Υλικό μελέτης

B.P. Lathi, Zhi Ding, "**Κώδικες διόρθωσης σφαλμάτων**"

Εισαγωγή

- από τις προηγούμενες διαλέξεις προκύπτει το συμπέρασμα ότι για την επίτευξη ψηφιακής επικοινωνίας χωρίς σφάλματα υπό την παρουσία παραμόρφωσης, θορύβου και παρεμβολής είναι απαραίτητη η προσθήκη του κατάλληλου πλεονασμού στα bits των αρχικών δεδομένων.
- ένα παράδειγμα αποτελεί η προσθήκη απλού ψηφίου ελέγχου ισοτιμίας για την ανίχνευση περιττού πλήθους από σφάλματα.
- τεχνικές όπως αυτή ανήκουν στην περιοχή της εμπρόσθιας διόρθωσης σφαλμάτων (forward error correction - FEC).
- υπάρχουν δύο κατηγορίες κωδικών FEC: οι **κώδικες block** και οι **συνελικτικοί κώδικες**.

- στους κώδικες block, κάθε block που αποτελείται από k bits κωδικοποιείται σε μια κωδικολέξη μεγαλύτρου μήκους ίσου με n bits.
- συνπώς κάθε μοναδική ακολουθία μήκους k bits προσδιορίζει πλήρως μια μοναδική κωδικολέξη μήκους n ψηφίων.
- στους συνελικτικούς κώδικες, η κωδικοποιημένη ακολουθία των n ψηφίων εξαρτάται όχι μόνο από τα k ψηφία, αλλά και από τα προηγούμενα $N-1$ ψηφία δεδομένων.
- συνεπώς η κωδικοποιημένη ακολουθία δεν είναι μοναδική, αλλά εξαρτάται και από προηγούμενα ψηφία (κωδικοποιητής με μνήμη).
- στους block κώδικες, τα ψηφία δεδομένων πρώτα συλλέγονται και μετά κωδικοποιούνται σε μια κωδικολέξη.
- στους συνελικτικούς, η κωδικοποίηση πραγματοποιείται σε συνεχή βάση παρά σε ομάδες των k bits.

- η εργασία του Shannon έχει οδηγήσει στο θεώρημα κωδικοποίησης καναλιού με θόρυβο:
  για ένα κανάλι χωρητικότητας C που έχει θόρυβο, υπάρχουν κώδικες με ρυθμό $R < C$, τέτοιο ώστε η αποκωδικοποίηση μέγιστης πιθανοφάνειας να μπορεί να οδηγήσει σε πιθανότητα σφάλματος

$$P_e \leq 2^{-nE_b(R)}$$

  όπου $E_b(R)$ είναι η ενέργεια ανά bit πληροφορίας που ορίζεται ως συνάρτηση του ρυθμού του κώδικα R.
- η σχέση δείχνει ότι μπορούμε να μειώσουμε το σφάλμα, αν αυξήσουμε τα bit κωδικοποίησης, διατηρώντας σταθερό τον ρυθμό μετάδοσης.

- ενώ το προηγούμενο μας λέει ότι υπάρχουν καλοί κώδικες που μειώνουν το σφάλμα, εντούτοις δεν μας λένε τον τρόπο που θα μπορέσουμε να τους βρούμε.
- μεγαλώνοντας το n θα έχουμε ως αποτέλεσμα μεν μικρή πιθανότητα σφάλματος, αλλά με κόστος υψηλότερη πολυπλοκότητα και μεγαλύτερο αποθηκευτικό χώρο.
- οι πιο αποδοτικές τεχνικές είναι οι κωδικοί χαμηλής πυκνότητας ελέγχου ισοτιμίας (low density parity check) και οι κώδικες turbo.

Η επανάληψη για διόρθωση λαθών

- στους κώδικες FEC, κάθε κωδικολέξη αποτελεί ομάδα από n bits τα οποία κωδικοποιούν k ψηφία δεδομένων και μπορεί να αποκωδικοποιηθεί ανεξάρτητα από τις άλλες.
- τα ψηφία ελέγχου είναι $m = n - k$, ενώ ο ρυθμός κώδικα είναι $R = k/n$. Ο κώδικας αυτός συμβολίζεται ως κώδικας (n, k).
- **πόσα στοιχεία ελέγχου απαιτούνται για την ανίχνευση ή την διόρθωση ενός πλήθους t σφαλμάτων σε έναν κώδικα** (n, k);
- μπορούμε να υπολογίσουμε το όριο Hamming το οποίο μας δίνει τον ελάχιστο αριθμό στοιχείων ελέγχου σύμφωνα που θα πρέπει να ικανοποιούν την σχέση

$$2^m \geq \sum_{j=0}^{t} \binom{n}{j}$$

- το παραπάνω όριο Hamming αποτελεί αναγκαία αλλά όχι ικανή συνθήκη. Μόνο για κώδικες διόρθωσης απλού σφάλματος, αποτελεί τόσο ικανή όσο και αναγκαία συνθήκη.
- Δηλαδή αν κάποιο m ικανοποιεί την παραπάνω σχέση ορίου Hamming, αυτό δεν σημαίνει ότι μπορεί να κατασκευαστεί κώδικας διόρθωσης n ψηφίων που να μπορεί να διορθώσει τα t σφάλματα.

	n	k	Κώδικας	Απόδοση κώδικα (ή ρυθμός κώδικα)
Διόρθωση απλού σφάλματος, t=1	3	1	(3,1)	0.33
Ελάχιστη απόσταση κώδικα 3	4	1	(4,1)	0.25
	5	2	(5,2)	0.4
	6	3	(6,3)	0.5
	7	4	(7,4)	0.57
	15	11	(15,11)	0.73
	31	26	(31,26)	0.838
Διόρθωση διπλού σφάλματος, t=2	10	4	(10,4)	0.4
Ελάχιστη απόσταση κώδικα 5	15	8	(15,8)	0.533
Διόρθωση τριπλού σφάλματος, t=3	10	2	(10,2)	0.2
Ελάχιστη απόσταση κώδικα 7	15	5	(15,5)	0.33
	23	12	(23,12)	0.52

Σχήμα: Παραδείγματα κωδικών διόρθωσης σφαλμάτων

- ο κώδικας για τον οποίο ισχύει η ισότητα ονομάζεται βέλτιστος κώδικας.
- αυτοί οι βέλτιστοι κώδικες υπάρχουν σε λίγες συγκριτικά περιπτώσεις. Οι δυαδικοί τέλειοι κώδικες διόρθωσης ενός απλού σφάλματος ονομάζονται κώδικες Hamming.
- για έναν τέτοιο κώδικα, είναι $t = 1$ και $d_{min} = 3$ οπότε από την προηγούμενη εξίσωση θα έχουμε

$$2^m = \sum_{j=0}^{1} \binom{n}{j} = 1 + n$$

$$n = 2^m - 1$$

- γενικά οι κώδικες Hamming είναι κώδικες (n, k) με $n = 2^m - 1$ και $k = 2^m - 1 - m$ και ελάχιστη απόσταση $d_{min} = m$
- ένας από τους πιο γνωστούς κώδικες Hamming είναι ο κώδικας $(7, 4, 3)$

- άλλος τρόπος διόρθωσης σφαλμάτων μπορεί να δημιουργηθεί σχεδιάζοντας κώδικα για την ανίχνευση και όχι την διόρθωση μέχρι t σφάλματα.
- στην περίπτωση ανίχνευσης, ο δέκτης μπορεί να αιτηθεί επαναμετάδοση. Η τεχνική αυτή ονομάζεται αυτόματη αίτηση επανάληψης (automatic repeat request - ARQ)
- το πλεονέκτημα τους είναι ότι λειτουργούν σε υψηλότερο ρυθμό καθώς απαιτούν λιγότερα bits ελέγχου
- η ελάχιστη απόσταση μεταξύ κωδικολέξεων ανίχνευσης t σφαλμάτων πρέπει να είναι

$$d_{min} = t + 1$$

Γραμμικοί κώδικες Block

- έστω η αναπαράσταση με διανύσματα των κωδικολέξεων **c** και δεδομένων **d** ως

$$\mathbf{c} = (c_1, c_2, \ldots, c_n) \qquad \mathbf{d} = (d_1, d_2, \ldots, d_k)$$

- για τους γραμμικούς κώδικες block, όλες οι κωδικολέξεις σχηματίζονται από γραμμικούς συνδυασμούς (προσθέσεις modulo-2) των k ψηφίων των δεδομένων.
- η ειδική περίπτωση για την οποία ισχύει ότι $c_1 = d_1, c_2 = d_2, \ldots, c_k = d_k$ ενώ τα υπόλοιπα ψηφία από c_{k+1} μέχρι c_n είναι γραμμικοί συνδυασμοί των $d_1, d_2, \ldots, d_n$ ονομάζεται **συστηματικός κώδικας**.
- σε αυτόν, τα πρώτα ψηφία είναι τα δεδομένα και τα υπόλοιπα $m = n - k$ είναι ψηφία ελέγχου ισοτιμίας που προκύπτουν από γραμμικούς συνδυασμούς των ψηφίων δεδομένων.

- οι κωδικολέξεις σχηματίζονται σύμφωνα με τις παρακάτω εξισώσεις

$$
\begin{aligned}
c_1 &= d_1 \\
c_2 &= d_2 \\
&\vdots \\
c_k &= d_k \\
c_{k+1} &= h_{11}d_1 \oplus h_{12}d_2 \oplus \ldots h_{1k}d_k \\
c_{k+2} &= h_{21}d_1 \oplus h_{22}d_2 \oplus \ldots h_{2k}d_k \\
&\vdots \\
c_n &= h_{m1}d_1 \oplus h_{m2}d_2 \oplus \ldots h_{mk}d_k
\end{aligned}
$$

ή ισοδύναμα

$$\mathbf{c} = \mathbf{dG}$$

όπου

$$
G = \begin{bmatrix}
1 & 0 & 0 & \cdots & 0 & h_{11} & h_{21} & \cdots & h_{m1} \\
0 & 1 & 0 & \cdots & 0 & h_{12} & h_{22} & \cdots & h_{m2} \\
 & & & \vdots & & & & \vdots & \\
 & & & \vdots & & & & \vdots & 0 \\
0 & 0 & 0 & \cdots & 1 & h_{1k} & h_{2k} & \cdots & h_{mk}
\end{bmatrix}
$$

ο **γεννήτορας πίνακας**

- ο πίνακας $\mathbf{G}$ έχει διαστάσεις $k \times k$. Για τους συστηματικούς κώδικες, ο πίνακας αυτός διαμερίζεται σε έναν ταυτοτικό πίνακα $\mathbf{I}_k$ διαστάσεων $k \times k$ και έναν πίνακα $\mathbf{P}$ διαστάσεων $k \times m$
- τα στοιχεία του πίνακα $\mathbf{P}$ έχουν μια από τις τιμές 0 ή 1.
- η κάθε κωδικολέξη μπορεί να εκφραστεί ως

$$\mathbf{c} = \mathbf{dG} = \mathbf{d}[\mathbf{I}_k\mathbf{P}] = [\mathbf{d} \qquad \mathbf{dP}] = [\mathbf{d} \qquad \mathbf{c}_p]$$

όπου τα ψηφία ελέγχου (που ονομάζονται bits αθροίσματος ελέγχου ή bits ισοτιμίας) είναι

$$\mathbf{c}_p = \mathbf{dP}$$

- συνεπώς η γνώση των ψηφίων δεδομένων μας επιτρέπει να υπολογίσουμε τα ψηφία ελέγχου και κατ' επέκταση και την κωδικολέξη $\mathbf{c}_p$.
- ορίζουμε ως βάρος της κωδικολέξης το πλήθος των **1** στην κωδικολέξη
- απόσταση του Hamming ανάμεσα σε δύο κωδικολέξεις $\mathbf{c}_a$ και $\mathbf{c}_b$ είναι το πλήθος των ψηφίων στα οποία αυτές διαφέρουν.
- δηλαδή ισχύει ότι

$$d(\mathbf{c}_a, \mathbf{c}_b) = \ \textbf{βάρος}\ (\mathbf{c}_a \oplus \mathbf{c}_b)$$

Γραμμικοί Κώδικες

- ένας block κώδικας χαρακτηρίζεται ως **γραμμικός κώδικας block** αν για κάθε ζευγάρι κωδικολέξεων $\mathbf{c}_a$, $\mathbf{c}_b$ από τον κώδικα block, ο συνδυασμός

$$\mathbf{c}_a \oplus \mathbf{c}_b$$

  αποτελεί και αυτός μια κωδικολέξη.
- για αυτό τον λόγο οι γραμμικοί κώδικες θα πρέπει να διαθέτουν μια κωδικολέξη που να περιέχει μόνο μηδενικά σύμβολα της μορφής **000...00**
- για αυτούς τους κώδικες, η ελάχιστη απόσταση είναι ίση με το ελάχιστο βάρος.

Αποκωδικοποίηση

- κάθε κωδικολέξη θα πρέπει να ικανοποιεί τη σχέση

$$\mathbf{c}\mathbf{H}^T = 0$$

όπου ο πίνακας $\mathbf{H}$ ονομάζεται **πίνακας ελέγχου ισοτιμίας** και είναι ίσος με

$$H = [\mathbf{P}^T \qquad \mathbf{I}_m]$$

- θεωρούμε την περίπτωση λήψης μιας λέξης $\mathbf{r}$ η οποία όμως διαφέρει από την μεταδιδόμενη κωδικολέξη $\mathbf{c}$ λόγω θορύβου του καναλιού

$$\mathbf{r} = \mathbf{c} \oplus \mathbf{e}$$

- αν $\mathbf{r}$ =**101101**, $\mathbf{c}$ =**100101** και $\mathbf{e}$ =**001000**, παρατηρούμε ότι ενα στοιχείο **1** στο διάνυσμα $\mathbf{e}$ δείχνει σφάλμα στην αντίστοιχη θέση, ενώ ένα **0** δείχνει ότι δεν υπάρχει σφάλμα.
- η απόσταση Hamming ανάμεσα στα διανύσματα $\mathbf{r}$ και $\mathbf{c}$ είναι απλά ίση με το πλήθος των **1** του διανύσματος $\mathbf{e}$
- σε περίπτωση που δεν είχαμε σφάλματα κατά την μετάδοση, τότε θα ίσχυε $\mathbf{r}\mathbf{H}^T = 0$.
- επειδή όμως έχουμε σφάλματα, η παραπάνω ποσότητα είναι μη μηδενικό διάνυσμα το οποίο ονομάζεται **σύνδρομο**.

- λαμβάνοντας ένα διάνυσμα $\mathbf{r}$, μπορούμε από την προηγούμενη σχέση να υπολογίσουμε το σύνδρομο $\mathbf{s}$ και επειδή

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T = (\mathbf{c}_i \oplus \mathbf{e}_i)H^T = \mathbf{c}_i\mathbf{H}^T \oplus \mathbf{e}_i\mathbf{H}^T = \mathbf{e}_i\mathbf{H}^T$$

  πιθανώς να μπορούμε να υπολογίσουμε και το σφάλμα.
- το παραπάνω δεν ισχύει πάντα καθώς το σύνδρομο δεν μπορεί να ορίσει από μόνο του ένα μοναδικό διάνυσμα σφάλματος αφού η σχέση αυτή ικανοποιείται από 2^k διανύσματα σφάλματος.
- **πως μπορούμε να καταλήξουμε σε μια λύση**; χρησιμοποιώντας το κριτήριο μέγιστης πιθανοφάνειας σύμφωνα με το οποίο αν λάβουμε το $\mathbf{r}$, αποφασίζουμε υπέρ εκείνου του $\mathbf{c}$ για το οποίο το $\mathbf{r}$ χαρακτηρίζεται από την μεγαλύτερη πιθανότητα παραλαβής μεταξύ όλων των διαφορετικών κωδικολέξεων $\mathbf{c}_k$

$$P(\mathbf{r}|\mathbf{c}_i) > P(\mathbf{r}|\mathbf{c}_k) \qquad \text{για όλα τα } k \neq i$$

- σε ένα δυαδικό συμμετρικό κανάλι (BSC) και για απόσταση μεταξύ του r και του $\mathbf{c}_i$ ίση με d, τότε για πιθανότητα σφάλματος ψηφίου του καναλιού ίση με P_e, η πιο πάνω πιθανότητα $P(\mathbf{r}|\mathbf{c}_i)$ είναι ίση με

$$P(\mathbf{r}|\mathbf{c}_i) = P_e^d(1-P_e)^{n-d} = (1-P_e^n)\left(\frac{P_e}{1-P_e}\right)^d$$

- στην προηγούμενη σχέση

$$P(\mathbf{r}|\mathbf{c}_i) = P_e^d(1-P_e)^{n-d} = (1-P_e^n)\left(\frac{P_e}{1-P_e}\right)^d$$

  αν για το κανάλι ισχύει ότι $P_e < 1$, τότε η συνάρτηση $P(\mathbf{r}|\mathbf{c}_i)$ είναι μια μονότονα φθίνουσα συνάρτηση του d.
- για να μεγιστοποιήσουμε αυτή, θα πρέπει να επιλέξουμε εκείνο το $\mathbf{c}_i$ που είναι πιο κοντά στην τιμή του $\mathbf{r}$ δηλαδή το διάνυσμα σφάλματος με τον ελάχιστο αριθμό 1. Αυτό είναι το διάνυσμα ελάχιστου βάρους.
- το διάνυσμα ελάχιστου βάρους θα χρησιμοποιηθεί για να διορθώσει το διάνυσμα $\mathbf{r}$ μέσω της σχέσης

$$\mathbf{c} = \mathbf{r} \oplus \mathbf{e}_{min}$$

- η διαδικασία της αποκωδικοποίησης είναι λίγο ανοργάνωτη. Για να μπορέσει να γίνει πιο οργανωμένη, θα πρέπει να υπολογίσουμε όλα τα δυνατά σύνδρομα και για το κάθε ένα να υπολογίσουμε το διάνυσμα ελάχιστου βάρους.
- σε αυτούς τους υπολογισμούς, μπορεί να καταλήξουμε σε κάποια σύνδρομα τα οποία θα συσχετιστούν με διανύσματα βάρους ίσα με **1**, ενώ μπορεί να προκύψουν και άλλα σύνδρομα που θα συσχετιστούν με διανύσματα βάρους μεγαλύτερου από **1**.
- σε αυτή την περίπτωση μπορούμε να επιλέξουμε οποιαδήποτε από αυτά ως πρότυπο σφάλματος προς διόρθωση.
- για να πετύχουμε συστηματική αποκωδικοποίηση, προετοιμάζουμε έναν πίνακα με όλα τα πρότυπα σφάλματος προς διόρθωση και με τα αντίστοιχα σύνδρομα.
- για την αποκωδικοποίηση υπολογίζουμε την ποσότητα $\mathbf{s} = \mathbf{r}\mathbf{H}^T$ και από τον πίνακα αποκωδικοποίησης υπολογίζουμε το αντίστοιχο $\mathbf{e}$.
- η απόφαση είναι ίση με $\mathbf{c} = \mathbf{r} \oplus \mathbf{e}$.
- το διάνυσμα $\mathbf{s}$ έχει $m = n - k$ ψηφία, και ως εκ τούτου θα υπάρχουν 2^{n-k} σύνδρομα, το καθένα από αυτά να αποτελείται από $n - k$ ψηφία.
- ο αριθμός των διανυσμάτων σφάλματος e είναι ο ίδιος, το καθένα από τα οποία περιέχει n ψηφία.
- ο συνολικός αποθηκευτικός χώρος που χρειαζόμαστε είναι $(2n - k)2^{n-k} = (2n - k)2^m$ bits.

Κατασκευάζοντας κώδικες Hamming

- δυστυχώς δεν υπάρχει ένας γενικός συστηματικός τρόπος για να σχεδιάσουμε κώδικες εκτός από ορισμένες ειδικές περιπτώσεις όπως είναι οι κυκλικοί κώδικες και οι κώδικες Hamming.
- έστω η περίπτωση του κώδικα διόρθωσης απλού σφάλματος $(7, 4)$. Αυτός ικανοποιεί το όριο Hamming και είναι ικανή η δημιουργία ενός κατάλληλου κώδικα.
- επειδή $m = 3$, υπάρχουν 7 μη μηδενικά σύνδρομα. Επειδή $n \neq 7$, θα υπάρχουν ακριβώς 7 πρότυπα απλού σφάλματος.
- κατασκευάζουμε τον πίνακα $\mathbf{H}^T$ θέτοντας την απαίτηση πως και οι επτά γραμμές του να είναι διακριτές και διάφορες του μηδενός (ο πίνακας έχει διαστάσεις $n \times n - k$ δηλαδή 7×3. Η διάταξη αυτών των γραμμών μπορεί να γίνει αυθαίρετα με μόνο περιορισμό οι 3 τελευταίες γραμμές να σχηματίζουν μοναδιαίο πίνακα $\mathbf{I}_m$

$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{P} \\ \mathbf{I}_m \end{bmatrix}$$

- ο αντίστοιχος γεννήτορας πίνακας είναι

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

- συνεπώς αν **d=1011**, η αντίστοιχη κωδικολέξη είναι η **c=1011001**.
- ένας γενικός γραμμικός κώδικας (n, k) χαρακτηρίζεται από διανύσματα συνδρόμων m διαστάσεων $(m = n - k)$. Συνεπώς υπάρχουν $2^m - 1$ διακριτά μη μηδενικά διανύσματα συνδρόμων τα οποία μπορούν να διορθώσουν $2^m - 1$ πρότυπα απλού σφάλματος.
- σε έναν κώδικα (n, k) υπάρχουν ακριβώς n πρότυπα απλού σφάλματος τα οποία μπορούν να διορθωθούν αν ικανοποιείται η

$$2^m - 1 \geq n$$

Χαρακτηριστικά κώδικα Hamming

ένας κώδικας Hamming $(2^m - 1, 2^m - 1 - m, m)$ έχει τις παρακάτω ιδιότητες:

1. Πλήθος bit ισοτιμίας $m \geq 3$
2. Μήκος κώδικα $n = 2^m - 1$
3. Αριθμός bit μηνύματος $k = 2^m - m - 1$
4. ελάχιστη απόσταση $d_{min} = 3$
5. Δυνατότητα διόρθωσης σφάλματος $t = 1$

Κυκλικοί κώδικες

- οι κυκλικοί κώδικες είναι μια υποκατηγορία των γραμμικών κωδικών block
- προτάθηκαν για να επιλύσουν το πρόβλημα της δύσκολης επιλογής γεννητόρων για κώδικες διόρθωσης πιο σύνθετων σφαλμάτων υψηλότερης τάξης.
- η υλοποίηση τους είναι εύκολη καθώς στηρίζονται σε καταχωρητές ολίσθησης. Οι κωδικολέξεις που προκύπτουν αποτελούν απλά πλευρικές κυκλικές ολισθήσεις κάποιων άλλων τέτοιων λέξεων.
- ένα διάνυσμα κώδικα

$$\mathbf{c} = (c_1, c_2, \cdots, c_n)$$

το οποίο μετατοπίζεται κυκλικά κατά i θέσεις προς τα αριστερά συμβολίζεται

$$\mathbf{c}^{(i)} = (c_{i+1}, c_{i+2}, \cdots, c_n, c_1, c_2, \cdots, c_i)$$

- οι κυκλικοί κώδικες μπορούν να περιγραφούν σε μια πολυωνυμική μορφή διευκολύνοντας τις πράξεις

$$c(x) = c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n$$

- με την ίδια λογική που εισάγουμε το πολυώνυμο του κώδικα, μπορούμε να εισάγουμε πολυώνυμο γεννήτορας κώδικα $g(x)$ καθώς και το πολυώνυμο δεδομένων $d(x)$
- με χρήση αυτών, μπορούμε να δημιουργήσουμε το πολυώνυμο κώδικα ως

$$c(x) = d(x)g(x)$$

όπου

$$d(x) = d_1 x^{k-1} + d_2 x^{k-2} + \cdots + d_k$$

Συστηματικοί κώδικες

- σε έναν συστηματικό κώδικα, τα πρώτα k ψηφία είναι τα bits των δεδομένων, ενώ τα υπόλοιπα $m = n - k$ ψηφία είναι τα bits ελέγχου ισοτιμίας.
- για έναν συστηματικό κώδικα, το πολυώνυμο $c(x)$ της κωδικολέξης που αντιστοιχεί στο πολυώνυμο δεδομένων $d(x)$ δίνεται από τη σχέση

$$c(x) = x^{n-k} d(x) + \rho(x)$$

με $\rho(x)$ το υπόλοιπο της διαίρεσης του πολυωνύμου x^{n-k} από το $g(x)$

$$\rho(x) = \text{Rem} \ \frac{x^{n-k} d(x)}{g(x)}$$

- οι κυκλικοί κώδικες μπορούν να περιγραφούν και με τη βοήθια ενός πίνακα γεννήτορα **G**. Ειδικότερα, οι κώδικες Hamming είναι κυκλικοί κώδικες.
- στην περίπτωση που έχουμε δοθεί το πολυώνυμο γεννήτορας, μπορούμε εύκολα να προσδιορίσουμε τον πίνακα γεννήτορα του συστηματικού κώδικα

$$\mathbf{G} = [\mathbf{G} \qquad \mathbf{P}]$$

προσδιορίζοντας τον πίνακα ισοτιμίας P ως

$$1\eta \text{ γραμμή του } \mathbf{P}\text{: } \mathrm{Rem}\frac{x^{n-1}}{g(x)}$$

$$2\eta \text{ γραμμή του } \mathbf{P}\text{: } \mathrm{Rem}\frac{x^{n-2}}{g(x)}$$

$$k\text{-οστή γραμμή του } \mathbf{P}\text{: } \mathrm{Rem}\frac{x^{n-k}}{g(x)}$$

Αποκωδικοποίηση

- κατά την αποκωδικοποίηση ισχύει ότι κάθε έγκυρο πολυώνυμο κώδικα $c(x)$ είναι πολλαπλάσιο του $g(x)$, δηλαδή το $c(x)$ διαιρείται με $g(x)$.
- αν εμφανιστεί κάποιο σφάλμα κατά την μετάδοση, τότε το πολυώνυμο της λέξης $r(x)$ που έχει παραληφθεί, δεν θα αποτελεί πολλαπλάσιο του $g(x)$

$$\frac{r(x)}{g(x)} = m_i(x) + \frac{s(x)}{g(x)}$$

$$s(x) = \text{Rem}\ \frac{r(x)}{g(x)}$$

- αν $e(x)$ είναι το πολυώνυμο σφάλματος, τότε θα είναι

$$r(x) = c(x) + e(x)$$

και επειδή το $c(x)$ είναι πολλαπλάσιο του $g(x)$

$$s(x) = \text{Rem}\ \frac{r(x)}{g(x)} = \text{Rem}\ \frac{c(x) + e(x)}{g(x)} = \text{Rem}\ \frac{e(x)}{g(x)}$$

- για την αποδοτικότερη αποκωδικοποίηση προετοιμάζουμε έναν πίνακα αποκωδικοποίησης καταγράφοντας τα συνδρομα για όλα τα σφάλματα που μπορούν να διορθωθούν.
- για κάθε τιμή του $\mathbf{r}$ υπολογίζουμε το σύνδρομο ως $s(x) = \text{Rem}\ \frac{r(x)}{g(x)}$ και από τον πίνακα προσδιορίζουμε το αντίστοιχο σφάλμα προς διόρθωση $\mathbf{e}$.
- θα είναι τελικά

$$\mathbf{c} = \mathbf{r} \otimes \mathbf{e}$$

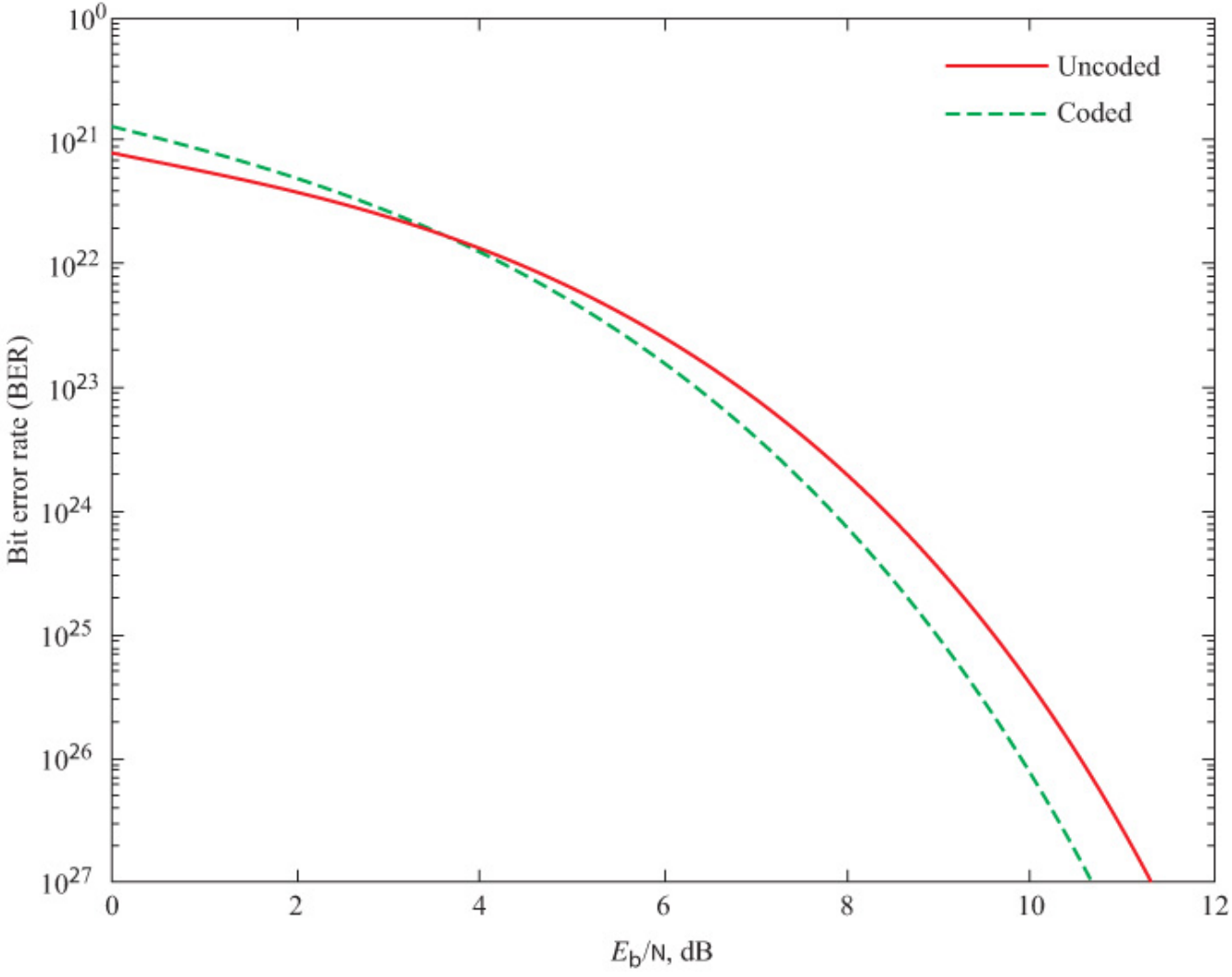
Αποτελέσματα διόρθωσης σφάλματος

- ενδιαφέρον έχει να παρουσιάσουμε και να συγκρίνουμε τις πιθανότητες σφάλματος bit όταν τα κωδικοποιημένα και τα μη κωδικοποιημένα σχήματα χαρακτηρίζονται από παρόνμοιους περιορισμούς και ρυθμούς πληροφορίας.
- για την περίπτωση ενός κώδικα (n, k) διόρθωσης t σφαλμάτων συμβολίζουμε με P_{ec} την πιθανότητα σφάλματος bit δεδομένων, ενώ για την περίπτωση της μη κωδικοποίησης η πιθανότητα συμβολίζεται με P_{eu}
- μετά από υπολογισμούς βρίσκουμε ότι

$$P_{ec} = \binom{n-1}{t} \left[Q\left(\sqrt{\frac{2kE_b}{N}} \right) \right]^{t+1}$$

$$P_{eu} = Q\left(\sqrt{\frac{2E_b}{N}} \right)$$

- η απευθείας σύγκριση δεν είναι εύκολη καθώς θα έπρεπε να χρησιμοποιήσουμε ολόκληρες οικογένειες γραφημάτων για διαφορετικές τιμές των παραμέτρων t, k, n στην περίπτωση της κωδικοποίησης.



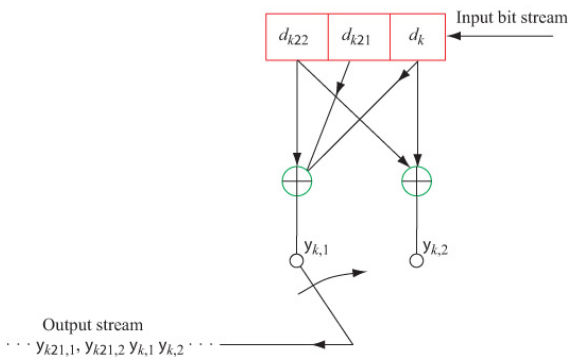
Σχήμα: Σύγκριση επίδοσης κωδικοποιημένων και μη κωδικοποιημένων συστημάτων

Συνελικτικοί Κώδικες

- μέχρι τώρα παρουσιάσαμε κώδικες block στους οποίους μια ομάδα n ψηφίων κώδικα που δημιουργούνται από τον κωδικοποιητή σε κάθε συγκεκριμένη χρονική μονάδα, εξαρτάται μόνο από την ομάδα των k ψηφίων των δεδομένων εισόδου μέσα σε αυτή τη χρονική μονάδα.
- στην περίπτωση του συνελικτικού κώδικα, η ομάδα των n ψηφίων κώδικα που δημιουργούνται δεν εξαρτάται μόνο από την ομάδα των k ψηφίων του μηνύματος, αλλά και από ψηφία δεδομένων που αντιστοιχούν σε έκταση $N-1$ χρονικών μονάδων $(N>1)$
- η μέθοδος αυτή κωδικοποίησης είναι πιο εύκολη και πραγματοποιείται με καταχωρητές ολίσθησης.
- είναι πιο απλοί και επιτρέπουν πιο εύκολη αποκωδικοποίηση.

Παράδειγμα συνελικτικού κωδικοποιητή

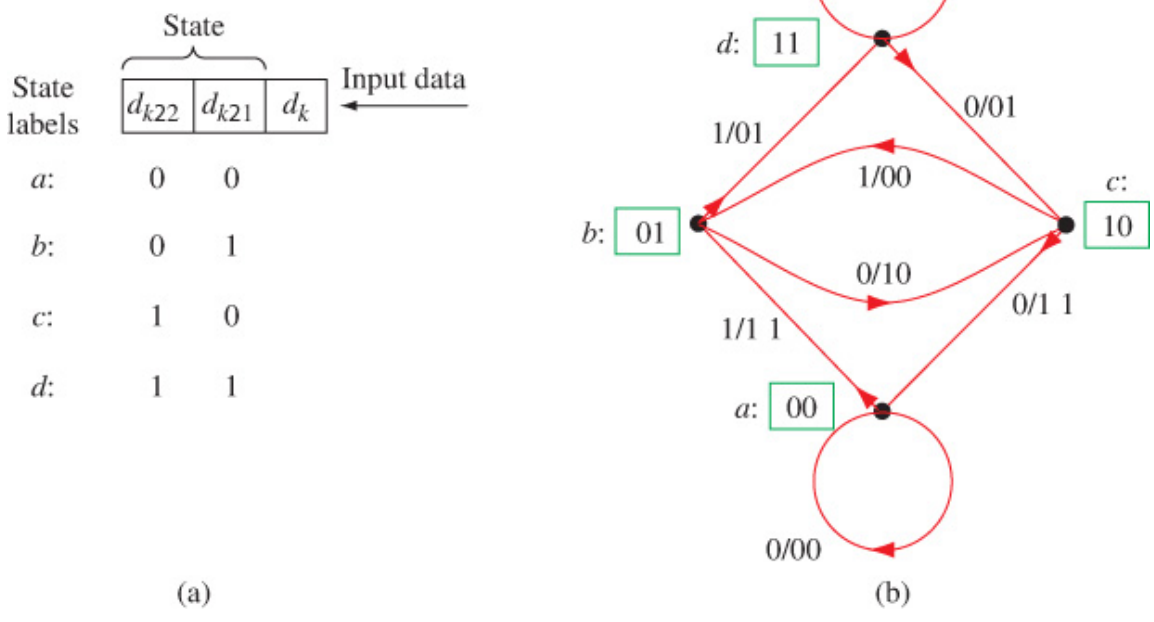
- το παρακάτω σχήμα απεικονίζει συνελικτικό κωδικοποιητή μήκους περιορισμού $N = 3$ που αποτελείται από έναν καταχωρητή ολίσθησης με $N = 3$ βαθμίδες και $l = 2$ αθροιστές που πραγματοποιούν πρόσθεση modulo-2.
- για την περίπτωση που στην είσοδο χρησιμοποιήσουμε τα ψηφία **11010**, η έξοδος του κωδικοποιητή θα είναι ίση με **11010100101100**.
- παρατηρούμε ότι για κάθε ομάδα των k ψηφίων δεδομένων, υπάρχουν τιμές σε όλα τα $n = (N + k - 1)l$ ψηφία στην κωδικοποιημένη έξοδο
- στην πράξη επειδή $k >> N$, υπάρχουν κατά προσέγγιση kl κωδικοποιημένα ψηφία εξόδου, για κάθε k ψηφία δεδομένων.
- ο ρυθμός κωδικοποίησης είναι ίσος με $n \approx 1/l^4$



Σχήμα: Συνελικτικός κωδικοποιητής

Αναπαράσταση με διάγραμμα μετάβασης καταστάσεων

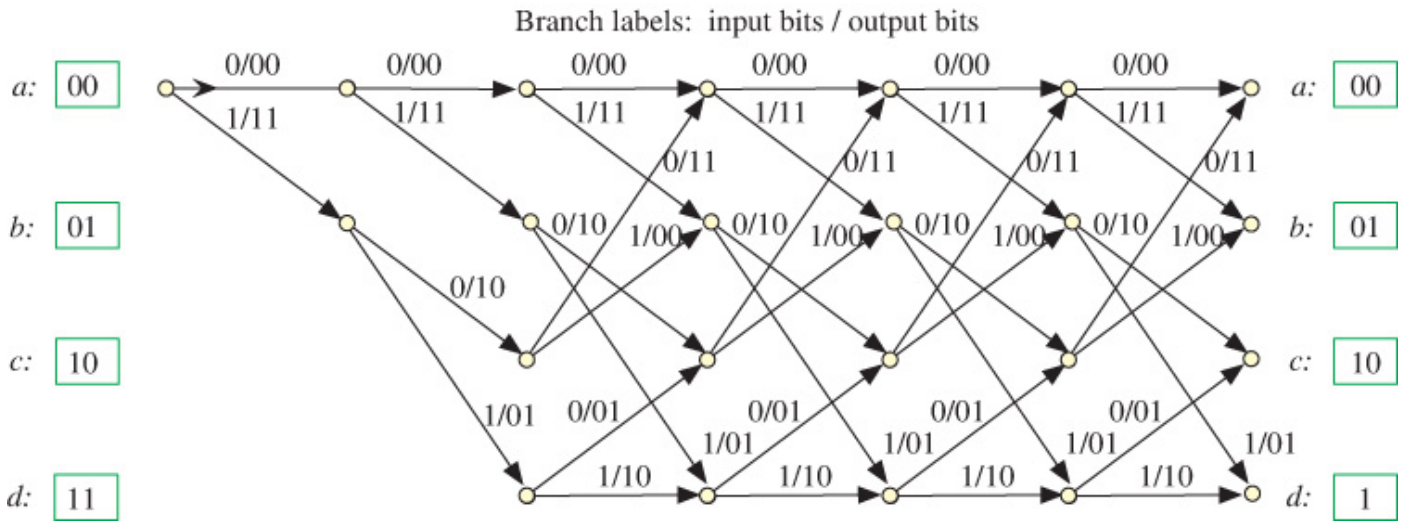
- ο κωδικοποιητής μπορεί να μελετηθεί και από την οπτική γωνία μιας μηχανής πεπερασμένων καταστάσεων χρησιμοποιώντας το διάγραμμα μετάβασης καταστάσεων.



Σχήμα: (α) Καταστάσεις (β) διάγραμμα μετάβασης καταστάσεων για τον κωδικοποιητή του προηγούμενου σχήματος

Διάγραμμα Trellis

- ένας άλλος τρόπος αναπαράστασης του δέντρου κώδικα είναι το διάγραμμα trellis.
- η αρχική κατάσταση του διαγράμματος είναι το **0** δηλαδή βρίσκεται στην κατάσταση (α)



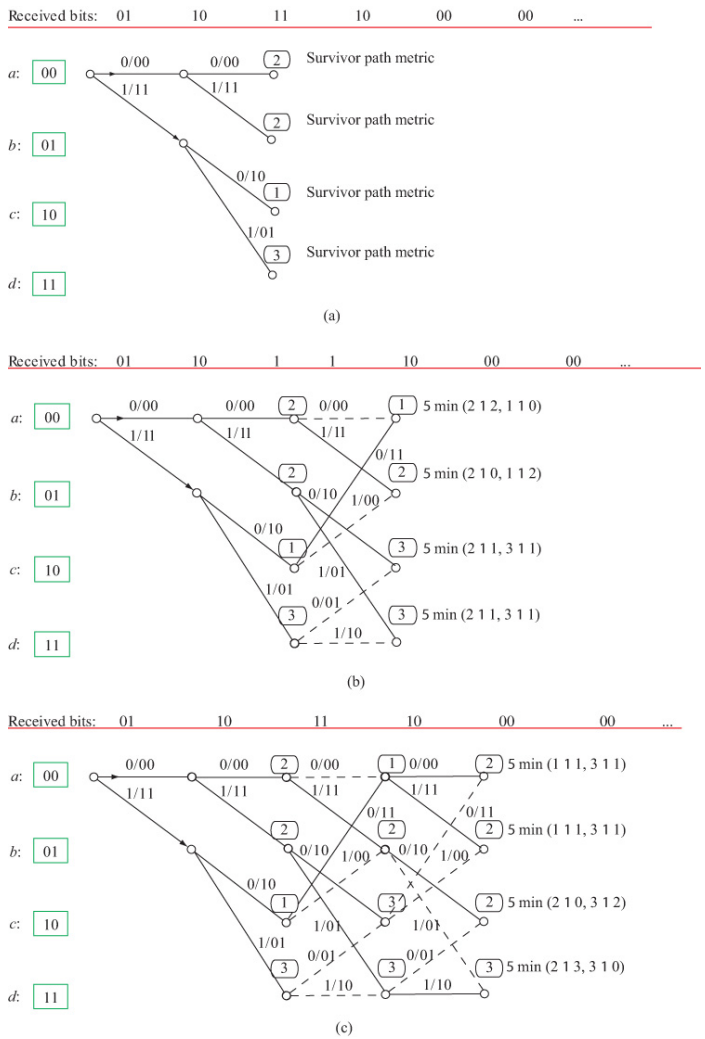
Σχήμα: Διάγραμμα Trellis για τον κωδικοποιητή του προηγούμενου σχήματος

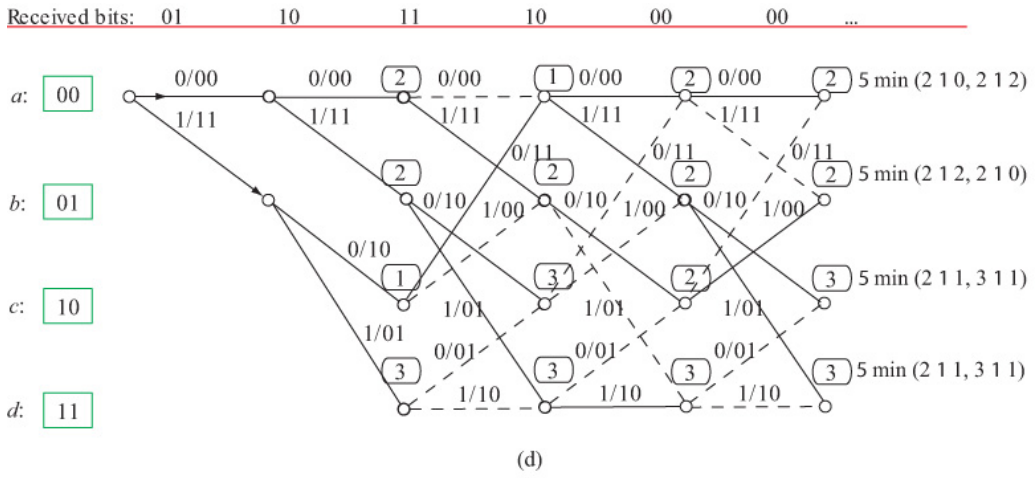
Αποκωδικοποίηση συνελικτικών κωδικών

- για την αποκωδικοποίηση των συνελικτικών κωδικών χρησιμοποιούνται δύο σημαντικές τεχνικές:
  1. **αποκωδικοποίηση μέγιστης πιθανοφάνειας** (αλγόριθμος Viterbi)
  2. **ακολουθιακή αποκωδικοποίηση**
- και οι δύο τεχνικές είναι γνωστές ως αποκωδικοποιητές σκληρής απόφασης, εντούτοις ο Viterbi είναι πιο ευλύγιστος και μπορεί εύκολα να προσαρμοστεί για να επιτρέψει την χρήση ήπιας εισόδου και να δημιουργήσει ήπιες αποφάσεις εξόδου.
- ο αλγόριθμος Viterbi επιτρέπει απλοποιήσεις σε εξοπλισμό για μικρό μήκος περιορισμού N και πετυχαίνει υψηλούς ρυθμούς δεδομένων που φτάνουν μέχρι και 10Gbps

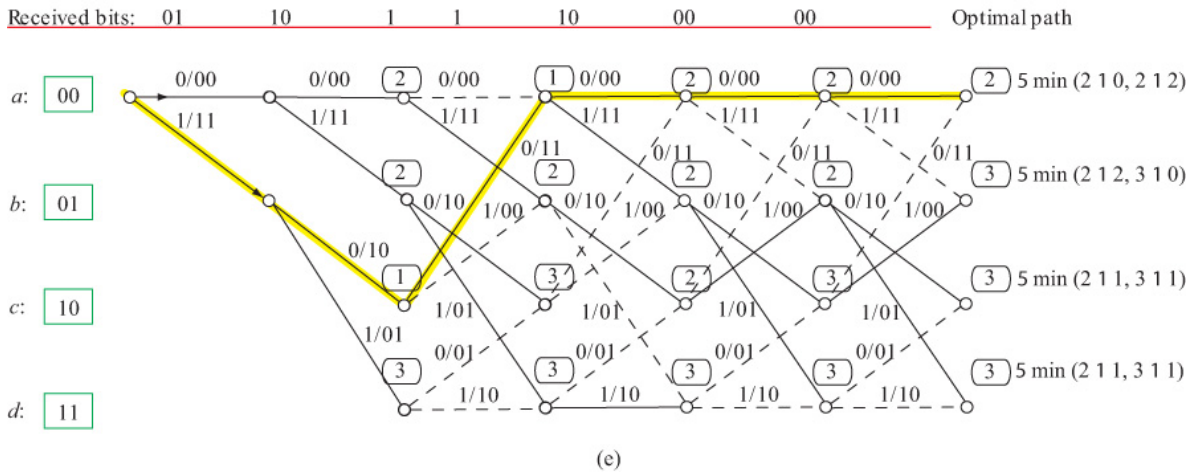
Παράδειγμα αποκωδικοποίησης με Viterbi

- Να αποκωδικοποιηθεί με τον Viterbi η ακολουθία **01**, **10**, **11**, **10**, **00**, **00**




Received bits: 01 10 11 10 00 00 ...
a: 00
b: 01
c: 10
d: 11
5 min (2 1 0, 2 1 2)
5 min (2 1 2, 2 1 0)
5 min (2 1 1, 3 1 1)
5 min (2 1 1, 3 1 1)

(d)


Received bits: 01 10 1 1 10 00 00
Optimal path
a: 00
b: 01
c: 10
d: 11
5 min (2 1 0, 2 1 2)
5 min (2 1 2, 3 1 0)
5 min (2 1 1, 3 1 1)
5 min (2 1 1, 3 1 1)

(e)

Περαιτέρω μελέτη

- Μπορείτε να πειραματιστείτε με τις διαφορετικές τεχνικές που παρουσιάστηκαν στο Κεφάλαιο αυτό, δοκιμάζοντας τα προγράμματα σε MATLAB που βρίσκονται στην ενότητα 14.13

Signal & Image Processing, Pattern Recognition Group (SIPPRE)

www.sippre-group.com