ΕΕ728

Προχωρημένα Θέματα Θεωρίας Πληροφορίας

Δημήτρης - Αλέξανδρος Τουμπακάρης

7ο Μάθημα – 16 Απριλίου 2008

Ανακεφαλαίωση προηγούμενου μαθήματος

- Παρουσιάσαμε την απόδειξη του ευθέος του Θεωρήματος Κωδικοποίησης Καναλιού με χρήση αποκωδικοποίησης από κοινού τυπικότητας (βασιζόμενοι στο Από Κοινού AEP).
  - Κατασκευάσαμε τυχαίο κώδικα $\mathcal{C}$ 2^{nR} κωδικών λέξεων με βάση κατανομή $p(x)$.
  - Αποκωδικοποιούμε με χρήση από κοινού τυπικότητας. Σφάλμα εμφανίζεται όταν δεν υπάρχει κωδική λέξη η οποία είναι από κοινού τυπική με τη ληφθείσα ακολουθία (αδυναμία αποκωδικοποίησης – "διαγραφή") ή όταν μια από τις κωδικές λέξεις που δεν εστάλησαν είναι από κοινού τυπική με τη ληφθείσα ακολουθία Y^n (αποκωδικοποίηση σε εσφαλμένο μήνυμα).
  - Αποδείξαμε ότι, για αρκούντως μεγάλο μήκος κώδικα, η μέση πιθανότητα σφάλματος αποκωδικοποίησης υπολογισμένη σε όλους τους πιθανούς κώδικες τείνει στο 0, αρκεί $R < I(X;Y)$.
  - Κατασκευάζουμε όλα τα πιθανά βιβλία κωδίκων με βάση την κατανομή $p^*(x)$ η οποία μεγιστοποιεί την $I(X;Y)$, κρατάμε το καλύτερο βιβλίο κωδίκων και "σβήνουμε" τις μισές χειρότερες κωδικές λέξεις.
  - Με τον τρόπο αυτό, επιτυγχάνουμε μετάδοση με μέγιστη πιθανότητα σφάλματος $\longrightarrow 0$, αρκεί $R < C$.

Προεπισκόπηση σημερινού μαθήματος

- Θα αποδείξουμε το αντίστροφο του Θεωρήματος Κωδικοποίησης Καναλιού.
- Θα εξετάσουμε τι συμβαίνει όταν μπορούμε να χρησιμοποιήσουμε ανάδραση κατά τη μετάδοση σε Διακριτό Κανάλι Χωρίς Μνήμη.
- Θα αναφερθούμε στη βέλτιστη μέθοδο αποκωδικοποίησης (με χρήση της μεθόδου Μέγιστης Πιθανοφάνειας – Maximum Likelihood) καθώς και στον Εκθέτη Σφάλματος (Error Exponent) ο οποίος παρέχει ένα άνω φράγμα για το σφάλμα αποκωδικοποίησης με χρήση ML για δεδομένο μήκος κώδικα n.

Περιεχόμενα σημερινού μαθήματος

- Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού
  - Αντίστροφο
- Χωρητικότητα Καναλιού με Ανάδραση
- Αποκωδικοποίηση Μέγιστης Πιθανοφάνειας και Εκθέτης Σφάλματος

$I(X^n;Y^n) \leq nC$

- Θα αποδείξουμε, κατ΄ αρχήν, ότι για Διακριτά Κανάλια Χωρίς Μνήμη, η πληροφοριακή χωρητικότητα ανά χρήση του καναλιού δεν αυξάνει εάν το κανάλι χρησιμοποιηθεί πολλές φορές. Δηλαδή, $I(X^n;Y^n) \leq nC$ για οποιαδήποτε $p(x)$, όπου $C = \max_{p(x)} I(X;Y)$.

$$I(X^n;Y^n) = H(Y^n) - H(Y^n|X^n) = H(Y^n) - \sum_{i=1}^{n} H(Y_i|Y_1,\ldots,Y_{i-1},X^n) =$$

$$\stackrel{(a)}{=} H(Y^n) - \sum_{i=1}^{n} H(Y_i|X_i) \stackrel{(b)}{\leq} \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i|X_i)$$

$$= \sum_{i=1}^{n} I(X_i;Y_i) \leq nC.$$

(a) Το κανάλι δεν έχει μνήμη, επομένως η έξοδος τη χρονική στιγμή i εξαρτάται μόνο από την είσοδο τη χρονική στιγμή i. Επίσης, δε χρησιμοποιείται ανάδραση.
(b) Η από κοινού εντροπία δεν υπερβαίνει το άθροισμα των εντροπιών.

Ανισότητα **Fano**

- Για την απόδειξη του αντιστρόφου του Θεωρήματος Κωδικοποίησης Καναλιού θα χρησιμοποιήσουμε την Ανισότητα Fano.
- Είδαμε ότι, για κάθε εκτιμητή $\hat{X} = g(Y)$,

$$H(X|Y) \le H(X|\hat{X}) \le H(P_e) + P_e \log |\mathcal{X}| \Rightarrow H(X|\hat{X}) \le 1 + P_e \log |\mathcal{X}|,$$

  όπου $P_e = \Pr\{\hat{X} \neq X\}$.
- Εάν θεωρήσουμε Διακριτό Κανάλι Χωρίς Μνήμη με βιβλίο κωδίκων $\mathcal{C}$ και ομοιόμορφα κατανεμημένα μηνύματα W,

$$H(W|\hat{W}) \le 1 + P_e^{(n)} nR,$$

  όπου $P_e^{(n)} = \Pr\{W \neq \hat{W}\}$.

Θεώρημα Κωδικοποίησης Καναλιού – Απόδειξη αντιστρόφου

- Θα δείξουμε ότι, για <u>οποιονδήποτε</u> κώδικα $(2^{nR}, n)$ με $\lambda^{(n)} \to 0$, πρέπει να ισχύει $R \leq C$. Δεδομένου ότι $\lambda^{(n)} \to 0$, και η μέση πιθανότητα σφάλματος $P_e^{(n)} \to 0$.
- Έστω ότι ο δέκτης αποφασίζει ποια ακολουθία μεταδόθηκε με βάση κάποια συνάρτηση αποκωδικοποίησης $\hat{W} = g(Y^n)$. Ισχύει $W \to X^n(W) \to Y^n \to \hat{W}$.
- Έστω, επίσης, ότι το μήνυμα που στέλνεται στο κανάλι επιλέγεται με βάση ομοιόμορφη κατανομή στο σύνολο των πιθανών μηνυμάτων $\{1, 2, \ldots, 2^{nR}\}$. Επομένως, $\Pr\{\hat{W} \neq W\} = P_e^{(n)} = \frac{1}{2^{nR}} \sum_i \lambda_i$. Συνεπώς,

$$\begin{aligned} nR &\overset{(a)}{=} H(W) \overset{(b)}{=} H(W|\hat{W}) + I(W;\hat{W}) \overset{(c)}{\leq} 1 + P_e^{(n)} nR + I(W;\hat{W}) \\ &\overset{(d)}{\leq} 1 + P_e^{(n)} nR + I(X^n;Y^n) \overset{(e)}{\leq} 1 + P_e^{(n)} nR + nC. \end{aligned}$$

(a) W ομοιόμορφη τ.μ., (b) σχέση αμοιβαίας πληροφορίας – εντροπίας, (c) ανισότητα Fano, (d) ανισότητα επεξεργασίας δεδομένων, (e) $I(X^n;Y^n) \leq nC$.

Θεώρημα Κωδικοποίησης Καναλιού
Απόδειξη αντιστρόφου (συνέχεια)

$$nR \le 1 + P_e^{(n)} nR + nC \Rightarrow R \le P_e^{(n)} R + \frac{1}{n} + C.$$

- Από την υπόθεση ότι $\lambda^{(n)} \to 0$, $P_e^{(n)} R \to 0$ για $n \to \infty$. Επομένως, για $n \to \infty$,

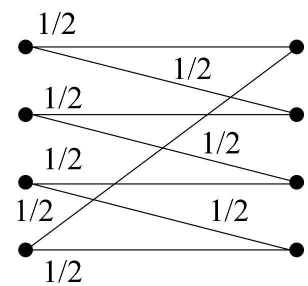
$$R \le C.$$

- Λύνοντας ως προς $P_e^{(n)}$, $P_e^{(n)} \ge 1 - \frac{C}{R} - \frac{1}{nR}$. Συνεπώς, εάν $R > C$, $P_e^{(n)} > 0$ για $n \to \infty$.
- Το αποτέλεσμα αυτό ονομάζεται ασθενές αντίστροφο του Θεωρήματος Κωδικοποίησης Καναλιού. Αποδεικνύεται (ισχυρό αντίστροφο) ότι, εάν $R > C$, $P_e^{(n)} \to 1$ εκθετικά.
- Συνεπώς, η χωρητικότητα καναλιού C αποτελεί μια πολύ σαφή διαχωριστική γραμμή: Όταν $R < C$ η πιθανότητα σφάλματος τείνει εκθετικά στο 0. Αντίθετα, όταν $R > C$, η πιθανότητα σφάλματος τείνει εκθετικά στο 1.

Χωρητικότητα Καναλιού με Ανάδραση

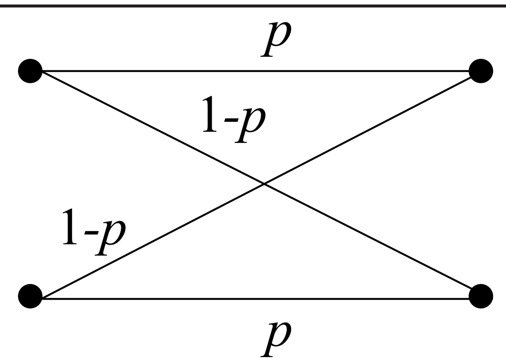
- Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού
  - Αντίστροφο
- Χωρητικότητα Καναλιού με Ανάδραση
- Αποκωδικοποίηση Μέγιστης Πιθανοφάνειας και Εκθέτης Σφάλματος

Παράδειγμα 7.1



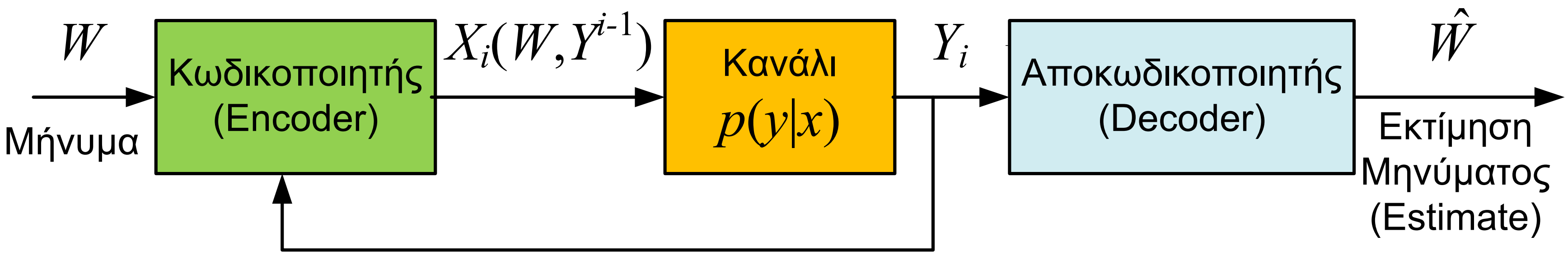
- Θεωρούμε το διακριτό κανάλι χωρίς μνήμη του σχήματος (‵ενθόρυβη γραφομηχανή″).
- Η χωρητικότητα του καναλιού ισούται με $C = \max I(X;Y) = \max H(Y) - H(Y|X) = 2 - 1 = 1$ bit.
- Μπορούμε να επιτύχουμε μετάδοση με ρυθμό ίσο με τη χωρητικότητα και με μηδενική πιθανότητα σφάλματος χρησιμοποιώντας π.χ. τις εισόδους 0 και 2. Προφανώς, $R = 1$ bit $= C$.
- Ό,τι και να συμβεί στο κανάλι είμαστε βέβαιοι ότι δε θα εμφανιστεί σφάλμα αποκωδικοποίησης.
- Εάν μπορούσαμε να χρησιμοποιήσουμε ανάδραση (feedback), η χωρητικότητα θα παρέμενε η ίδια;

Παράδειγμα 7.2



- Ας θεωρήσουμε, τώρα, το δυαδικό συμμετρικό κανάλι.
- Γνωρίζουμε ότι $C = 1 - H(p)$ και ότι η χωρητικότητα επιτυγχάνεται χρησιμοποιώντας και τα δύο μηνύματα με ίση πιθανότητα. Επομένως, κάθε φορά που στέλνουμε ένα από τα δύο μηνύματα στο κανάλι δε γνωρίζουμε εάν το μήνυμα μεταδόθηκε επιτυχώς. Η πιθανότητα σφάλματος ανά μετάδοση είναι μη μηδενική.
- Τι συμβαίνει εάν χρησιμοποιήσουμε ανάδραση; (όπου γνωρίζουμε εάν έχει εμφανιστεί σφάλμα στο δέκτη;)
- Παρόλο που κανείς θα περίμενε το αντίθετο, θα αποδείξουμε ότι, σε διακριτά κανάλια χωρίς μνήμη, η χρήση ανάδρασης δεν αυξάνει τη χωρητικότητα!

Χωρητικότητα καναλιού με ανάδραση – Μοντέλο



- Στο μοντέλο του σχήματος θεωρούμε ότι ο δέκτης στέλνει όλα τα ληφθέντα σύμβολα Y_i στον πομπό <u>άμεσα</u> και <u>χωρίς λάθη</u>. Ο πομπός χρησιμοποιεί την πληροφορία που λαμβάνει από το δέκτη προκειμένου να αποφασίσει πώς θα μεταδώσει.

Χωρητικότητα καναλιού με ανάδραση – Ορισμοί

- Κώδικας ανάδρασης (feedback code) $(2^{nR}, n)$:
  - Μια ακολουθία απεικονίσεων $x_i(W, Y^{i-1})$, όπου κάθε x_i είναι συνάρτηση του τρέχοντος μηνύματος W, καθώς και των σημάτων που ελήφθησαν στο δέκτη έως και τη χρονική στιγμή $i-1$: $Y_1, Y_2, \ldots, Y_{i-1}$, και
  - Μια ακολουθία συναρτήσεων αποκωδικοποίησης $g : \mathcal{Y}^n \to \{1, 2, \ldots, 2^{nR}\}$.
- Θεωρούμε ότι τα μηνύματα W είναι ομοιόμορφα κατανεμημένα. Επομένως, $P_e^{(n)} = \Pr\{g(Y^n) \neq W\}$, όπου $X^n = X^n(W)$.
- Η (λειτουργική) χωρητικότητα με ανάδραση C_{FB} του διακριτού καναλιού χωρίς μνήμη ισούται με το μέγιστο ρυθμό που είναι εφικτός με χρήση κωδίκων ανάδρασης.

Χωρητικότητα καναλιού με ανάδραση

- Θεώρημα (Cover 7.12.1): $C_{FB} = C = \max_{p(x)} I(X;Y)$.
- Απόδειξη. Είναι, κατ' αρχήν, προφανές ότι $C_{FB} \geq C$, δεδομένου ότι το κανάλι χωρίς ανάδραση μπορεί να θεωρηθεί ως ειδική περίπτωση του καναλιού με ανάδραση.
- Θα αποδείξουμε ότι $C \geq C_{FB}$ και, επομένως, $C = C_{FB}$.
- Θα χρησιμοποιήσουμε και πάλι την ανισότητα Fano, όπως και στο αντίστροφο του Θεωρήματος Κωδικοποίησης Καναλιού. Ωστόσο, η απόδειξη διαφέρει γιατί στο κανάλι με ανάδραση δεν ισχύει η σχέση $I(X^n;Y^n) \leq nC$.
- Υπενθυμίζεται ότι θεωρούμε ότι το W είναι ομοιόμορφα κατανεμημένο στο σύνολο $\{1, 2, \ldots, 2^{nR}\}$.

$$nR = H(W) \overset{(a)}{=} H(W|\hat{W}) + I(W;\hat{W}) \overset{(b)}{\leq} 1 + P_e^{(n)} nR + I(W;\hat{W})$$
$$\overset{(c)}{\leq} 1 + P_e^{(n)} nR + I(W;Y^n),$$

(a) Σχέση αμοιβαίας πληροφορίας-εντροπίας, (b) ανισότητα Fano, (c) ανισότητα επεξεργασίας δεδομένων.

Χωρητικότητα καναλιού με ανάδραση (2)

$$nR \leq 1 + P_e^{(n)} nR + I(W; Y^n).$$

Η $I(W; Y^n)$ μπορεί να γραφτεί ως εξής:

$$\begin{aligned} I(W; Y^n) &= H(Y^n) - H(Y^n|W) \stackrel{(a)}{=} H(Y^n) - \sum_{i=1}^{n} H(Y_i|Y_1, Y_2, \ldots, Y_{i-1}, W) \\ &\stackrel{(b)}{=} H(Y^n) - \sum_{i=1}^{n} H(Y_i|Y_1, Y_2, \ldots, Y_{i-1}, W, X_i) \stackrel{(c)}{=} H(Y^n) - \sum_{i=1}^{n} H(Y_i|X_i) \\ &\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i|X_i) = \sum_{i=1}^{n} I(X_i; Y_i) \leq nC. \end{aligned}$$

(a) Κανόνας αλυσίδας εντροπίας, (b) εάν γνωρίζουμε την ακολουθία Y^{i-1} και το μήνυμα W, γνωρίζουμε και το σύμβολο X_i που μεταδίδεται, (c) το κανάλι δεν έχει μνήμη, οπότε η έξοδος τη χρονική στιγμή i εξαρτάται μόνο από την είσοδο X_i.

Χωρητικότητα καναλιού με ανάδραση (3)

- Επομένως, $I(W;Y^n) \leq nC$, και

$$nR \leq P_e^{(n)} nR + 1 + nC.$$

- Διαιρώντας με n, και για $n \to \infty$,

$$R \leq C, \text{ και, επομένως, } C_{FB} \leq C.$$

- Παρόλο που η χρήση ανάδρασης σε διακριτά κανάλια χωρίς μνήμη δεν αυξάνει τη χωρητικότητα, ενδέχεται να διευκολύνει τη μετάδοση. Για παράδειγμα, στο κανάλι διαγραφής, η μετάδοση απλουστεύεται εάν γνωρίζουμε πότε το σήμα εισόδου διαγράφεται.
- Φυσικά, στην πράξη, μπορεί να μην υπάρχει αξιόπιστος δίαυλος ανάδρασης, ή να έχει κόστος (π.χ. σε εύρος ζώνης ή καθυστέρηση).

Αποκωδικοποίηση Μέγιστης Πιθανοφάνειας και Εκθέτης Σφάλματος

- Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού
  - Αντίστροφο
- Χωρητικότητα Καναλιού με Ανάδραση
- Αποκωδικοποίηση Μέγιστης Πιθανοφάνειας και Εκθέτης Σφάλματος

Αποκωδικοποίηση Μέγιστης εκ των Υστέρων Πιθανότητας (**Maximum A Posteriori Probability – MAP**)

- Για την απόδειξη του Θεωρήματος Κωδικοποίησης Καναλιού υποθέσαμε ότι η αποκωδικοποίηση βασίζεται στην Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοκατανομής (Joint AEP).
- Δείξαμε ότι εάν η αποκωδικοποίηση βασίζεται στο Joint AEP μπορούμε να μεταδώσουμε με ρυθμούς αυθαίρετα κοντά στη χωρητικότητα με αυθαίρετα μικρή πιθανότητα σφάλματος.
- Αποδείξαμε ότι δε μπορούμε να υπερβούμε τη χωρητικότητα. Επομένως, η αποκωδικοποίηση με χρήση από κοινού τυπικών ακολουθιών είναι ασυμπτωτικά βέλτιστη.
- Εάν το κριτήριο είναι να ελαχιστοποιηθεί η πιθανότητα σφάλματος στο δέκτη, πρέπει να χρησιμοποιηθεί αποκωδικοποίηση Μέγιστης εκ των Υστέρων Πιθανότητας (Maximum a Posteriori (MAP) probability detection).
- Θεωρούμε την πιθανότητα $p(y^n|x^n(w))$ να ληφθεί η ακολουθία y^n στο δέκτη δεδομένου ότι εστάλη ακολουθία $x^n(w)$ η οποία αντιστοιχεί στο μήνυμα w (η κωδική λέξη του μηνύματος w).

Αποκωδικοποίηση Μέγιστης εκ των Υστέρων Πιθανότητας (2)

- Από τον κανόνα του Bayes,

$$p(\boldsymbol{w}|\boldsymbol{y}^n) = \frac{p(\boldsymbol{y}^n|\boldsymbol{x}^n(\boldsymbol{w}))p(\boldsymbol{w})}{p(\boldsymbol{y}^n)}, \text{ όπου } p(\boldsymbol{y}^n) = \sum_{w=1}^{|\mathcal{W}|} p(\boldsymbol{w})p(\boldsymbol{y}^n|\boldsymbol{x}^n(\boldsymbol{w})).$$

- Εάν ο δέκτης αποκωδικοποιεί την ακολουθία $\boldsymbol{y}^n$ στο μήνυμα $\boldsymbol{w}$, η πιθανότητα σφάλματος δεδομένης της ληφθείσας ακολουθίας $\boldsymbol{y}^n$ ισούται με $1 - p(\boldsymbol{w}|\boldsymbol{y}^n)$.
- Επομένως, για να ελαχιστοποιηθεί η πιθανότητα σφάλματος, πρέπει να επιλεγεί το μήνυμα $\boldsymbol{w}$ το οποίο μεγιστοποιεί την εκ των υστέρων (a posteriori) πιθανότητα του $\boldsymbol{w}$ δεδομένης της ληφθείσας ακολουθίας $\boldsymbol{y}^n$ ($p(\boldsymbol{w}|\boldsymbol{y}^n)$).
- Κανόνας αποκωδικοποίησης MAP: $\boldsymbol{w} = g(\boldsymbol{y}^n)$, τέτοιο ώστε

$$p(\boldsymbol{w}|\boldsymbol{y}^n) \geq p(\boldsymbol{w}'|\boldsymbol{y}^n), \text{ για όλα τα } \boldsymbol{w}' \neq \boldsymbol{w},\ \boldsymbol{w}, \boldsymbol{w}' \in \mathcal{W}.$$

Αποκωδικοποίηση Μέγιστης εκ των Υστέρων Πιθανότητας (3)

- Με χρήση του κανόνα του Bayes,

$$p(w|y^n) \geq p(w'|y^n) \Rightarrow$$

$$\frac{p(y^n|x^n(w))p(w)}{p(y^n)} \geq \frac{p(y^n|x^n(w'))p(w')}{p(y^n)}$$

- Επομένως, ο κανόνας MAP μπορεί να γραφεί ως:

$$\boxed{p(y^n|x^n(w))p(w) \geq p(y^n|x^n(w'))p(w')}$$

- Για κανάλι χωρίς μνήμη,

$$p(y^n|x^n(w)) = \prod_{i=1}^{n} p(y_i|x_i(w)).$$

Αποκωδικοποίηση Μέγιστης Πιθανοφάνειας (**Maximum Likelihood (ML) decoding**)

- Με βάση τον κανόνα MAP επιλέγεται το μήνυμα που ικανοποιεί τη σχέση $p(y^n|x^n(w))p(w) \geq p(y^n|x^n(w'))p(w')$ για όλα τα $w' \neq w$.
- Εάν όλα τα μηνύματα εκπέμπονται με την ίδια πιθανότητα (ομοιόμορφα), ο αποκωδικοποιητής μπορεί να αποκωδικοποιήσει με βάση τη σχέση

$$p(y^n|x^n(w)) \geq p(y^n|x^n(w')) \text{ για όλα τα } w' \neq w.$$

- Η αποκωδικοποίηση με βάση την παραπάνω σχέση ονομάζεται μέγιστης πιθανοφάνειας. Στη γενική περίπτωση (όπου τα μηνύματα δεν ακολουθούν ομοιόμορφη κατανομή) δε μεγιστοποιεί την πιθανότητα να έχει μεταδοθεί το μήνυμα w δεδομένης της ακολουθίας y^n.
- Ωστόσο, μεγιστοποιείται η πιθανότητα να έχει ληφθεί η y^n δεδομένου του w.

Γιατί **ML** και όχι **MAP**;

- Στη γενική περίπτωση (όπου η κατανομή των μηνυμάτων στην είσοδο του καναλιού δεν είναι ομοιόμορφη) η αποκωδικοποίηση ML δεν είναι βέλτιστη.
- Ωστόσο, στην πράξη, η αποκωδικοποίηση ML χρησιμοποιείται συχνότερα από την αποκωδικοποίηση MAP. Κάποιοι από τους λόγους είναι οι εξής:
  - Σε κάποια συστήματα, τα μηνύματα που στέλνονται είναι ισοπίθανα, οπότε η αποκωδικοποίηση ML είναι βέλτιστη.
  - Αποδεικνύεται (βλ. π.χ. Cioffi, http://www.stanford.edu/class/ee379a/course_reader/chap1.pdf) ότι εάν η κατανομή των μηνυμάτων $p(w)$ είναι άγνωστη, η αποκωδικοποίηση ML ελαχιστοποιεί την πιθανότητα σφάλματος.
- Πολλές φορές η αποκωδικοποίηση ML είναι πολύπλοκη, οπότε χρησιμοποιούνται υποβέλτιστες μέθοδοι. Περισσότερα στα μαθήματα Ψηφιακών Επικοινωνιών.

Εκθέτης Σφάλματος (**Error Exponent**) (εισαγωγή)

- Σύμφωνα με το Θεώρημα Κωδικοποίησης Καναλιού, είναι δυνατόν να μεταδώσουμε σε διακριτό κανάλι χωρίς μνήμη με αυθαίρετα μικρή πιθανότητα σφάλματος, εφόσον ο ρυθμός μετάδοσης δεν υπερβαίνει τη χωρητικότητα.
- Αντίστροφα, δεν υπάρχει κώδικας με αυθαίρετα μικρή πιθανότητα σφάλματος ο οποίος επιτυγχάνει μετάδοση με ρυθμό μεγαλύτερο από τη χωρητικότητα καναλιού.
- Αποδείξαμε το Θεώρημα Κωδικοποίησης Καναλιού όταν ο δέκτης αποκωδικοποιεί με βάση την Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης. Το Θεώρημα αποδεικνύεται και για αποκωδικοποίηση μέγιστης πιθανοφάνειας (ML – βλ. π.χ. Gallager).
- Στην απόδειξη, για να επιτύχουμε αυθαίρετα μικρή πιθανότητα σφάλματος, αφήσαμε το n να τείνει στο άπειρο.
- Τι συμβαίνει όταν το n είναι πεπερασμένο; Πώς μεταβάλλεται η πιθανότητα σφάλματος ως συνάρτηση του n;
- Ένας τρόπος να ποσοτικοποιηθεί η εξάρτηση της μέσης πιθανότητας σφάλματος από το n είναι ο εκθέτης σφάλματος (error exponent) ο οποίος παρέχει ένα άνω φράγμα όταν χρησιμοποιειται αποκωδικοποίηση μέγιστης πιθανοφάνειας.

Εκθέτης Σφάλματος (**Error Exponent**)

- Θεώρημα (Gallager 5.6.2 & Corollary 1): Έστω διακριτό κανάλι χωρίς μνήμη με πίνακα μετάβασης $p(y_j|x_k)$, $j = 1, \ldots, J$ και $k = 1, \ldots, K$. Για δεδομένο n και R θεωρούμε το σύνολο των κωδίκων $(2^{nR}, n)$ των οποίων τα σύμβολα επιλέγονται ανεξάρτητα με βάση κατανομή $p(x)$. Εάν ο δέκτης χρησιμοποιεί αποκωδικοποίηση μέγιστης πιθανοφάνειας, για τη μέση τιμή σφάλματος υπολογισμένη για όλους τους τυχαίους κώδικες οι οποίοι παράγονται με βάση κατανομή $p^*(x)$ και για όλα τα πιθανά μηνύματα, ισχύει

$$P_e^{(n)} \leq exp\{-nE_r(R)\},$$

όπου $E_r(R)$ είναι ο εκθέτης τυχαίας κωδικοποίησης ή εκθέτης σφάλματος (random coding/error exponent)

$E_r(R) = \max\limits_{0\leq\rho\leq 1} \max\limits_{p(x)}\{E_0(\rho, p(x)) - \rho R\}$, $p^*(x)$ η κατανομή που επιτυγχάνει τον $E_r(R)$ και

$$E_0(\rho, p(x)) = -\log \sum_{j=1}^{J} \left[\sum_{k=1}^{K} p(x_k) p(y_j|x_k)^{1/(1+\rho)} \right]^{1+\rho}.$$

Εκθέτης Σφάλματος (**Error Exponent**) (συνέχεια)

- Παρόλο που η έκφραση για τον εκθέτη σφάλματος είναι σχετικά πολύπλοκη, βασίζεται σε απλά βήματα (βλ. Gallager 5.6).
- Εάν μπορούμε να υπολογίσουμε τον $E_r(R)$ για δεδομένο διακριτό κανάλι χωρίς μνήμη, αποκτούμε ένα φράγμα για την πιθανότητα σφάλματος για δεδομένο ρυθμό μετάδοσης και δεδομένο μήκος κώδικα n: $P_e^{(n)} \le exp\{-nE_r(R)\}$.
- Αποδεικνύεται ότι, για $0 \le R < C$, $E_r(R) > 0$ και, επομένως, με κατάλληλη κωδικοποίηση, η πιθανότητα σφάλματος μπορεί να κρατηθεί αυθαίρετα κοντά στο μηδέν με χρήση κωδίκων κατάλληλου μήκους n.
- Όπως και στην περίπτωση αποκωδικοποίησης με χρήση από κοινού τυπικότητας, το γεγονός ότι $P_e^{(n)} \le exp\{-nE_r(R)\}$ δε συνεπάγεται ότι η πιθανότητα σφάλματος $P_{e,w}^{(n)}$ που αντιστοιχεί στην κωδική λέξη $x^n(w)$ θα είναι $\le exp\{-nE_r(R)\}$. Ωστόσο, αποδεικνύεται (Gallager 5.6 Corollary 2) ότι υπάρχει κώδικας $(2^{nR}, n)$ τέτοιος ώστε $P_{e,w}^{(n)} \le 4exp\{-nE_r(R)\}$ για όλα τα $w = 1, 2, \ldots, 2^{nR}$.

Ανακεφαλαίωση μαθήματος

- Θεώρημα Κωδικοποίησης Καναλιού (για Διακριτά Κανάλια Χωρίς Μνήμη)
  - Αντίστροφο: Με χρήση της ανισότητας Fano δείξαμε ότι δεν υπάρχει κώδικας με $P_e^{(n)} \to 0$ που να επιτυγχάνει $R > C$.
- Η χρήση ανάδρασης (feedback) δεν αυξάνει τη χωρητικότητα διακριτού καναλιού χωρίς μνήμη! (παρόλο που ενδέχεται να διευκολύνει την κωδικοποίηση/αποκωδικοποίηση). Θα δούμε σε επόμενο μάθημα ότι υπάρχουν περιπτώσεις όπου η χρήση ανάδρασης σε κανάλια με μνήμη οδηγεί σε αύξηση της χωρητικότητας (π.χ. Γκαουσιανά κανάλια με έγχρωμο θόρυβο).
- Ο βέλτιστος αποκωδικοποιητής βασίζεται σε ανίχνευση μέγιστης πιθανοφάνειας (ML). Ένα άνω φράγμα για την πιθανότητα σφάλματος για δεδομένο μήκος κώδικα n μπορεί να προσδιοριστεί με χρήση του Εκθέτη Σφάλματος.

Προεπισκόπηση επόμενου μαθήματος

- Απόδειξη Θεωρήματος Διαχωρισμού Πηγής - Καναλιού. Η κωδικοποίηση πηγής και καναλιού μπορούν να γίνουν ανεξάρτητα χωρίς απώλεια ρυθμού μετάδοσης (για κανάλια μιας εισόδου - μιας εξόδου).
- Συνεχείς τ.μ. και κανάλια διακριτού χρόνου αλλά συνεχών τιμών.
- Ποσότητες Θεωρίας Πληροφορίας για συνεχείς τ.μ.: Διαφορική Εντροπία, Σχετική Εντροπία και Αμοιβαία Πληροφορία για συνεχείς τ.μ.
- Ιδιότητες Διαφορικής Εντροπίας.
- AEP για συνεχείς τ.μ.
- Η (πολυμεταβλητή) Γκαουσιανή κατανομή και η εντροπία της.
- Το Γκαουσιανό κανάλι. Χωρητικότητα και Θεώρημα Κωδικοποίησης.
- Κανάλι Προσθετικού Λευκού Γκαουσιανού Θορύβου (AWGN). Κανάλι συνεχών τιμών και συνεχούς χρόνου με πεπερασμένο εύρος ζώνης. Πώς μπορούμε να το χαρακτηρίσουμε και ποια είναι η χωρητικότητά του;