ΕΕ728

Προχωρημένα Θέματα Θεωρίας Πληροφορίας

Δημήτρης - Αλέξανδρος Τουμπακάρης

6ο Μάθημα – 8 Απριλίου 2008

Ανακεφαλαίωση προηγούμενου μαθήματος

- Συμμετρικά Κανάλια και Χωρητικότητα.
- Από Κοινού Τυπικότητα και Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP).

Προεπισκόπηση σημερινού μαθήματος

- Θεώρημα Κωδικοποίησης Καναλιού για διακριτά κανάλια χωρίς μνήμη. Ορισμοί.

Θεώρημα Κωδικοποίησης Καναλιού – εισαγωγή

- Το Θεώρημα Κωδικοποίησης Καναλιού (Channel Coding Theorem) αποτελεί το πιο βασικό και το πιο διάσημο αποτέλεσμα της Θεωρίας Πληροφορίας.

- Σύμφωνα με το Θεώρημα Κωδικοποίησης Καναλιού, είναι εφικτή η μετάδοση σε κανάλια χωρίς μνήμη με ρυθμό αυθαίρετα κοντά στη χωρητικότητα και με αυθαίρετα μικρή πιθανότητα σφάλματος. Αντίστροφα, δεν είναι εφικτή μετάδοση με αυθαίρετα μικρή πιθανότητα σφάλματος εάν ο ρυθμός μετάδοσης υπερβαίνει τη χωρητικότητα του καναλιού.

Θεώρημα Κωδικοποίησης Καναλιού – εισαγωγή (2)

- Στη συνέχεια, θα διατυπώσουμε με την απαραίτητη λεπτομέρεια και θα αποδείξουμε το Θεώρημα Κωδικοποίησης Καναλιού.

- Υπάρχουν περισσότερες από μία αποδείξεις για το Θεώρημα Κωδικοποίησης Καναλιού (ευθύ). Οι πιο γνωστές είναι η απόδειξη με χρήση αποκωδικοποίησης Μέγιστης Πιθανοφάνειας (Maximum Likelihood decoding – Gallager) και η απόδειξη με χρήση Από Κοινού Τυπικών ακολουθιών (Cover).

- Στο μάθημα θα εξετάσουμε την απόδειξη με χρήση Από Κοινού Τυπικότητας η οποία είναι μάλλον πιο απλή.

- Το αντίστροφο του Θεωρήματος Κωδικοποίησης Καναλιού θα αποδειχθεί με χρήση της ανισότητας Fano.

Θεώρημα Κωδικοποίησης Καναλιού – εισαγωγή (3)

- Το βασικό ερώτημα (και, εκ πρώτης όψεως, παράδοξο) είναι το εξής: Πώς είναι δυνατόν να μεταδώσουμε με αυθαίρετα μικρή πιθανότητα σφάλματος σε ένα κανάλι που εισάγει σφάλματα με μη μηδενική πιθανότητα και με τυχαίο τρόπο;
- Για να απαντήσει στο ερώτημα, ο Shannon χρησιμοποίησε ένα διαφορετικό τρόπο σκέψης:
  - Δεν προσπάθησε να μηδενίσει την πιθανότητα σφάλματος, απλώς να την περιορίσει σε αυθαίρετα μικρές τιμές.
  - Βασίστηκε σε πολλές διαδοχικές χρήσεις του καναλιού ώστε να εκμεταλλευτεί το Νόμο των Μεγάλων Αριθμών.
  - Χρησιμοποίησε κώδικες οι οποίοι δημιουργούνται τυχαία και υπολόγισε τη μέση πιθανότητα σφάλματος.
- Αυτός ο τρόπος σκέψης διέπει τόσο την απόδειξη με χρήση τυπικότητας όσο και την απόδειξη με αποκωδικοποίηση Μέγιστης Πιθανοφάνειας.

Θεώρημα Κωδικοποίησης Καναλιού – Ορισμοί

- Ένας κώδικας (M, n) για το Διακριτό Κανάλι Χωρίς Μνήμη $(\mathcal{X}, p(y|x), \mathcal{Y})$ αποτελείται από

1. Ένα σύνολο δεικτών $\{1, 2, \ldots, M\}$.
2. Μια συνάρτηση κωδικοποίησης $X^n : \{1, 2, \ldots, M\} \to X^n$ η οποία παράγει κωδικές λέξεις (**codewords**) $x^n(1), x^n(2), \ldots, x^n(M)$. Το σύνολο των κωδικών λέξεων ονομάζεται βιβλίο κωδίκων (**codebook**).
3. Μια συνάρτηση αποκωδικοποίησης $g : \mathcal{Y}^n \to \{1, 2, \ldots, M\}$, η οποία αποτελεί ένα νομοτελειακό κανόνα ο οποίος αντιστοιχίζει ένα εκτιμώμενο δείκτη μεταδοθέντος μηνύματος σε κάθε ληφθείσα ακολουθία.

Θεώρημα Κωδικοποίησης Καναλιού – Ορισμοί (2)

- <u>Υπό συνθήκη πιθανότητα σφάλματος</u> δεδομένου ότι εστάλη το μήνυμα με δείκτη i:

$$\lambda_i = \Pr\{g(Y^n) \neq i | X^n = x^n(i)\} = \sum_{y^n} p(y^n | x^n(i)) I(g(y^n) \neq i),$$

όπου $I(\cdot)$ η συνάρτηση δείκτης (ισούται με 1 όταν το όρισμά της αληθεύει, αλλιώς με 0).

- Η <u>Μέγιστη Πιθανότητα Σφάλματος</u> $\lambda^{(n)}$ κώδικα (M, n) ορίζεται ως

$$\lambda^{(n)} = \max_{i \in \{1,2,\ldots,M\}} \lambda_i.$$

Θεώρημα Κωδικοποίησης Καναλιού – Ορισμοί (3)

- Η <u>μέση (αριθμητικά) πιθανότητα σφάλματος</u> $P_e^{(n)}$ κώδικα (M, n) ισούται με

$$P_e^{(n)} = \frac{1}{M} \sum_{i=1}^{M} \lambda_i.$$

- Όταν ο δείκτης μηνύματος W ακολουθεί ομοιόμορφη κατανομή, $P_e^{(n)} = \Pr\{W \neq g(Y^n)\}$, όπου Y^n η ακολουθία που λαμβάνεται στην έξοδο καναλιού όπου έχει μεταδοθεί η ακολουθία $X^n = x^n(W)$.

- Επίσης, $P_e^{(n)} \leq \lambda^{(n)}$.

Θεώρημα Κωδικοποίησης Καναλιού – Ορισμοί (4)

- Ο ρυθμός (rate) R κώδικα (M, n) ισούται με

$$R = \frac{\log M}{n} \text{ bits ανά μετάδοση.}$$

- Ένας ρυθμός R είναι εφικτός (achievable) όταν υπάρχει ακολουθία κωδίκων $\left(\lceil 2^{nR} \rceil, n\right)$ για την οποία η μέγιστη πιθανότητα σφάλματος $\lambda^{(n)}$ τείνει στο 0 καθώς το n τείνει στο άπειρο.
- Η Χωρητικότητα λειτουργίας (operational capacity) ενός καναλιού ισούται με το μέγιστο ρυθμό ο οποίος έιναι εφικτός.
- Το Θεώρημα Κωδικοποίησης Πηγής αποδεικνύει ότι η χωρητικότητα λειτουργίας $\max_{R \text{ εφικτός}} R$ ισούται με την πληροφοριακή χωρητικότητα $\max_{p(x)} I(X;Y)$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού – Εισαγωγή

- Θα αναφερθούμε στην απόδειξη η οποία χρησιμοποιεί την Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP).
- Η ιδέα:
  - Στέλνουμε στο κανάλι ακολουθία $X^n = x^n(W)$ μήκους n.
  - Στην έξοδο του καναλιού λαμβάνουμε ακολουθία Y^n η οποία εξαρτάται από τη X^n, καθώς και από τον πίνακα μετάβασης $p(y|x)$ του καναλιού.
  - Στο δέκτη αναζητούμε ακολουθία $\hat{X}^n$ η οποία να είναι από κοινού τυπική με την Y^n. Εάν υπάρχει, ο δέκτης θεωρεί ότι η $\hat{X}^n$ είναι η ακολουθία που μετέδωσε ο πομπός.
  - Από την Ιδιότητα από κοινού Ασυμπτωτικής Ισοδιαμέρισης, με μεγάλη πιθανότητα η ληφθείσα ακολουθία θα είναι από κοινού τυπική με τη μεταδοθείσα.
  - Ωστόσο, υπάρχει η πιθανότητα η Y^n να μην είναι από κοινού τυπική με καμία από τις πιθανές κωδικές λέξεις X^n ή να είναι από κοινού τυπική με άλλη ακολουθία από αυτή που μεταδόθηκε. Στην περίπτωση αυτή εμφανίζεται σφάλμα μετάδοσης.
  - Θα δείξουμε ότι, εάν $R < C$, καθώς το n τείνει στο άπειρο, η πιθανότητα σφάλματος τείνει στο 0.

Προεπισκόπηση επόμενου μαθήματος

- Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού για Διακριτά Κανάλια χωρίς μνήμη (ευθύ και αντίστροφο).
- Παρατηρήσεις και Θεωρήματα για τη Χωρητικότητα διακριτών καναλιών χωρίς μνήμη.
- Χωρητικότητα καναλιού με ανάδραση (feedback). Αυξάνει η χωρητικότητα εάν χρησιμοποιηθεί ανάδραση;
- Αποκωδικοποίηση Μέγιστης Πιθανοφάνειας (Maximum Likelihood) και Εκθέτης Σφάλματος (error exponent). Ποια είναι η πιθανότητα σφάλματος για δεδομένο μήκος κώδικα n όταν χρησιμοποιείται βέλτιστη αποκωδικοποίηση στο δέκτη (μέγιστης πιθανοφάνειας);