EE728

Προχωρημένα Θέματα Θεωρίας Πληροφορίας

Δημήτρης - Αλέξανδρος Τουμπακάρης

6ο Μάθημα – 7 Απριλίου 2008

Ανακεφαλαίωση προηγούμενου μαθήματος

- Σύμφωνα με το Θεώρημα Κωδικοποίησης Καναλιού, ο μέγιστος ρυθμός μετάδοσης σε Διακριτά Κανάλια Χωρίς Μνήμη για τον οποίο η μέγιστη πιθανότητα σφάλματος μπορεί να περιοριστεί αυθαίρετα κοντά στο 0 ισούται με $C = \max_{p(x)} I(X;Y)$.
- Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP).
  - Επέκταση της Ιδιότητας Ασυμπτωτικής Ισοδιαμέρισης.
  - Για $n \to \infty$ ο αριθμός ακολουθιών Y^n που "σχετίζονται" με μια ακολουθία X^n όταν οι $(X,Y) \sim p(X,Y)$, τείνει στο $2^{nH(Y|X)}$. Επομένως, μπορούμε να βρούμε περίπου $2^{nH(Y)}/2^{nH(Y|X)} = 2^{nI(X;Y)}$ ακολουθίες X^n που θα απεικονιστούν σε διαφορετικές περιοχές στο σύνολο $\mathcal{Y}^n$.

Περιεχόμενα σημερινού μαθήματος

- Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού
  - Ευθύ

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.
- 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 Τυπικότητας (Cover). Για άλλες αποδείξεις δείτε π.χ. το βιβλίο του Ash.
- Στο μάθημα θα εξετάσουμε την απόδειξη με χρήση Από Κοινού Τυπικότητας η οποία είναι σχετικά απλή, διαισθητική και ίσως η πιο "δημοφιλής" σήμερα.
- Το αντίστροφο του Θεωρήματος Κωδικοποίησης Καναλιού θα αποδειχθεί με χρήση της ανισότητας Fano.

Θεώρημα Κωδικοποίησης Καναλιού – εισαγωγή

- 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.

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.
- Υπό συνθήκη πιθανότητα σφάλματος 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).

Θεώρημα Κωδικοποίησης Καναλιού – Ορισμοί (συνέχεια)

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

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

- 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 (συνέχεια)

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

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

- Ένας ρυθμός R είναι (ασυμπτωτικά) εφικτός (**asymptotically 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 "λειτουργική" χωρητικότητα (**operational capacity**) ενός καναλιού ισούται με το μέγιστο ρυθμό μετάδοσης ο οποίος είναι εφικτός στο κανάλι.
- Το Θεώρημα Κωδικοποίησης Καναλιού αποδεικνύει ότι η λειτουργική χωρητικότητα $\max_{R \text{ εφικτός}} R$ ισούται με την πληροφοριακή χωρητικότητα $\max_{p(x)} I(X;Y)$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού – Εισαγωγή

- Όπως προαναφέρθηκε, θα παρουσιαστεί η απόδειξη η οποία χρησιμοποιεί την Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP).
- Βασική υπόθεση: Ο πομπός και ο δέκτης γνωρίζουν το βιβλίο κωδίκων και τον πίνακα μετάβασης του καναλιού $p(y|x)$.
- Η ιδέα:
  - Στέλνουμε στο κανάλι ακολουθία $X^n = x^n(W)$ μήκους n η οποία εξαρτάται από το μήνυμα W (τ.μ.). 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 $x^n(W)$ ή να είναι από κοινού τυπική με άλλη ακολουθία από αυτή που μεταδόθηκε. Στην περίπτωση αυτή εμφανίζεται σφάλμα μετάδοσης. Θα δείξουμε ότι, καθώς το n τείνει στο άπειρο, η πιθανότητα σφάλματος τείνει στο 0.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού

- Θεώρημα Κωδικοποίησης Καναλιού:
  - (Ευθύ) Σε ένα Διακριτό Κανάλι Χωρίς Μνήμη, όλοι οι ρυθμοί οι οποίοι είναι μικρότεροι από την πληροφοριακή χωρητικότητα είναι (ασυμπτωτικά) εφικτοί. Δηλαδή, για κάθε ρυθμό $R < C$ υπάρχει ακολουθία κωδίκων $\left(\lceil 2^{nR} \rceil, n\right)$ με μέγιστη πιθανότητα σφάλματος $\lambda^{(n)} \rightarrow 0$ όταν $n \rightarrow \infty$.
  - Αντίστροφα, για οποιαδήποτε ακολουθία από κώδικες $\left(\lceil 2^{nR} \rceil, n\right)$ με $\lambda^{(n)} \rightarrow 0$ πρέπει να ισχύει $R \leq C$.
- Απόδειξη (ευθέος).

  Για απλοποίηση, και χωρίς απώλεια γενικότητας, υποθέτουμε ότι ο αριθμός κωδικών λέξεων $\lceil 2^{nR} \rceil$ είναι ακέραιος.

  Θεωρούμε δεδομένη πιθανότητα συμβόλων εισόδου $p(x)$ και δημιουργούμε 2^{nR} τυχαίες κωδικές λέξεις x^n μήκους n θεωρώντας ανεξάρτητες όμοια κατανεμημένες (i.i.d.) τ.μ. x_i. Η πιθανότητα να δημιουργήσουμε μια συγκεκριμένη κωδική λέξη ισούται με $p(x^n) = \prod_{i=1}^{n} p(x_i)$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (2)

- Οι 2^{nR} κωδικές λέξεις χρησιμοποιούνται ως γραμμές του πίνακα

$$\mathcal{C} = \begin{bmatrix} x_1(1) & x_2(1) & \ldots & x_n(1) \\ x_1(2) & x_2(2) & \ldots & x_n(2) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(2^{nR}) & x_2(2^{nR}) & \ldots & x_n(2^{nR}) \end{bmatrix}$$

- Η πιθανότητα να δημιουργηθεί ένας συγκεκριμένος κώδικας (πίνακας) $\mathcal{C}$ ισούται με $\Pr(\mathcal{C}) = \prod_{w=1}^{2^{nR}} \prod_{i=1}^{n} p(x_i(w))$.
- Θεωρούμε την παρακάτω ακολουθία βημάτων
  1. Δημιουργείται ένας <u>τυχαίος</u> κώδικας $\mathcal{C}$ σύμφωνα με την κατανομή $p(x)$ όπως περιγράφτηκε παραπάνω.
  2. Ο κώδικας αποκαλύπτεται στον πομπό και στο δέκτη. Επίσης, τόσο ο πομπός όσο και ο δέκτης γνωρίζουν τον πίνακα μετάβασης του καναλιού $p(y|x)$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (3)

3. Ο πομπός επιλέγει ένα μήνυμα W σύμφωνα με <u>ομοιόμορφη</u> κατανομή $\Pr\{W = w\} = 2^{-nR}$, $w = 1, 2, \ldots, 2^{nR}$.
4. Στέλνεται στο κανάλι η $w-$οστή κωδική λέξη $x^n(w)$ η οποία αντιστοιχεί στη w-οστή γραμμή του πίνακα $\mathcal{C}$.
5. Ο δέκτης λαμβάνει ακολουθία y^n με δεσμευμένη κατανομή $p(y^n|x^n(w)) = \prod_{i=1}^{n} p(y_i|x_i(w))$.
6. Ο δέκτης εκτιμά ποιο μήνυμα w έχει σταλεί. Ο βέλτιστος δέκτης χρησιμοποιεί ανίχνευση Μέγιστης Πιθανοφάνειας (δεδομένου ότι θεωρούμε ομοιόμορφη κατανομή μηνυμάτων). Ωστόσο, όπως αναφέρθηκε, για την απόδειξη θα θεωρήσουμε ανίχνευση με βάση την από κοινού τυπικότητα. Παρόλο που ο δέκτης αυτός δεν είναι βέλτιστος, θα αποδείξουμε ότι, και σε αυτήν την περίπτωση, $\lambda^{(n)} \to 0$ για $n \to \infty$ (ο δέκτης, δηλαδή, που χρησιμοποιεί από κοινού τυπικότητα είναι ασυμπτωτικά βέλτιστος).

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (4)

(συνέχεια 6.) Ο δέκτης αποφασίζει (εκτιμά) ότι εστάλη το μήνυμα $\hat{W}$ εάν ικανοποιούνται και οι δύο συνθήκες ταυτόχρονα:

α. Το ζεύγος ακολουθιών $(X^n(\hat{W}), Y^n)$ είναι από κοινού τυπικό.

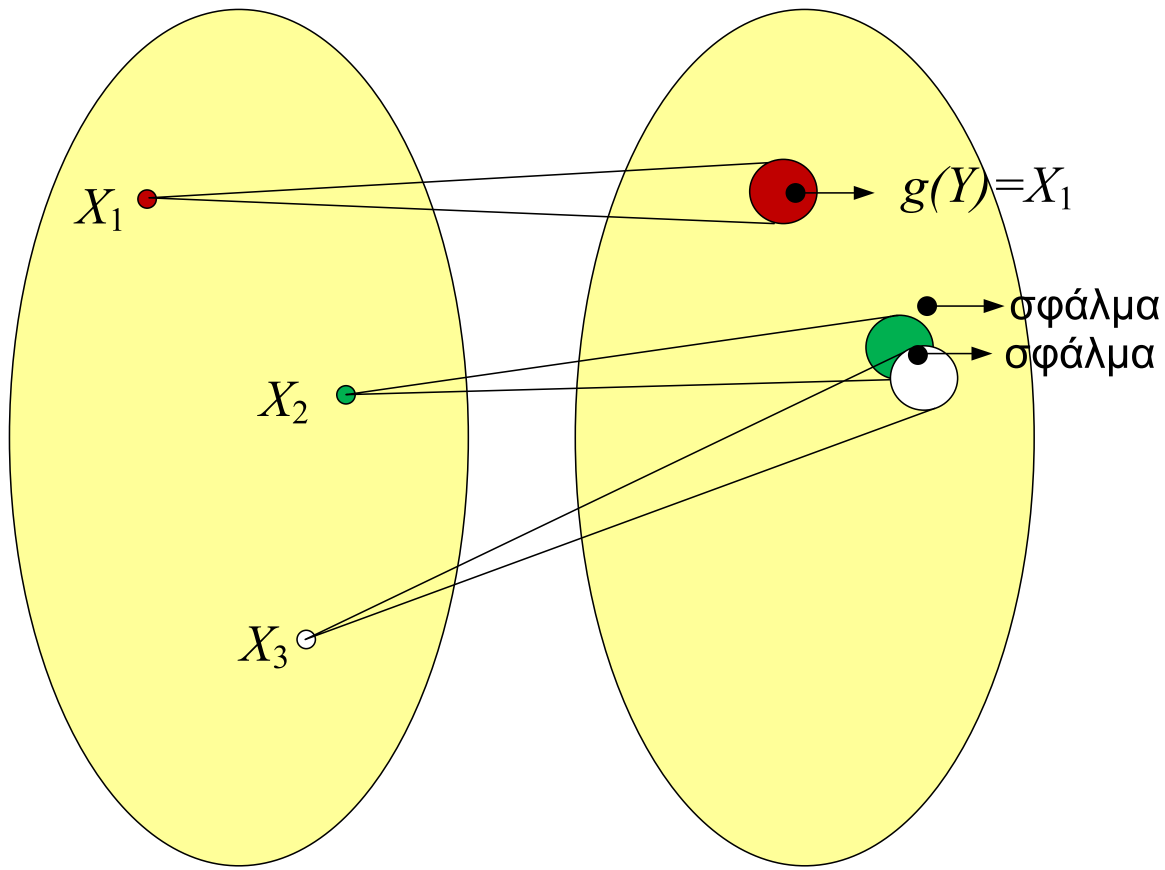
β. Δεν υπάρχει άλλος δείκτης μηνύματος $W' \neq \hat{W}$ για τον οποίο να ισχύει $(X^n(W'), Y^n) \in A_\epsilon^{(n)}$. Δηλαδή, δεν υπάρχει άλλη ακολουθία $X^n(W')$ που αντιστοιχεί σε μήνυμα $W' \neq \hat{W}$ η οποία να είναι από κοινού τυπική με την Y^n.

7. Εάν $\hat{W} \neq W$, εμφανίζεται σφάλμα ανίχνευσης. Έστω $\mathcal{E}$ το ενδεχόμενο $\{\hat{W} \neq W\}$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (5)
Ανάλυση της πιθανότητας σφάλματος – Εισαγωγή

- Η ιδέα: Αντί να υπολογίσουμε την πιθανότητα σφάλματος για ένα συγκεκριμένο κώδικα, θα υπολογίσουμε τη μέση πιθανότητα σφάλματος για τυχαία δημιουργία κωδίκων.
- Όταν χρησιμοποιείται αποκωδικοποίηση με χρήση από κοινού τυπικότητας, υπάρχουν δύο πηγές σφάλματος: Είτε η έξοδος Y^n δεν είναι από κοινού τυπική με την ακολουθία που εκπέμπει ο πομπός ή υπάρχει τουλάχιστον μια ακόμα κωδική λέξη η οποία είναι από κοινού τυπική με την Y^n.
- Από την Από Κοινού Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης, η πιθανότητα η ληφθείσα ακολουθία να είναι από κοινού τυπική με την εκπεμφθείσα τείνει στο 1 για $n \to \infty$. Επίσης, η πιθανότητα η ληφθείσα ακολουθία να είναι από κοινού τυπική με ακολουθία διαφορετική από την εκπεμφθείσα ισούται περίπου με $2^{-nI(X;Y)}$. Επομένως, μπορούμε να χρησιμοποιήσουμε περίπου 2^{nI} κωδικές λέξεις και, ταυτόχρονα, να διασφαλίσουμε μικρή πιθανότητα σφάλματος.
- Στη συνέχεια θα αποδείξουμε τα παραπάνω και με την απαραίτητη μαθηματική αυστηρότητα.

Αποκωδικοποίηση με χρήση από κοινού τυπικότητας



Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (6) Υπολογισμός Πιθανότητας Σφάλματος (I)

- Έστω ότι το μήνυμα W που εκπέμπεται επιλέγεται με ομοιόμορφη κατανομή από τα 2^{nR} πιθανά μηνύματα. $\mathcal{E} \triangleq \{\hat{W}(Y^n) \neq W\}$ είναι το ενδεχόμενο σφάλματος.
- Θα υπολογίσουμε τη μέση πιθανότητα σφάλματος για όλα τα πιθανά βιβλία κωδίκων.

$$\Pr\{\mathcal{E}\} = \sum_{\mathcal{C}} \Pr(\mathcal{C}) P_e^{(n)}(\mathcal{C}) =$$

$$= \sum_{\mathcal{C}} \Pr(\mathcal{C}) \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} \lambda_w(\mathcal{C}) = \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} \sum_{\mathcal{C}} \Pr(\mathcal{C}) \lambda_w(\mathcal{C}).$$

- Δεδομένου ότι η αντιστοίχιση μηνυμάτων σε κωδικές λέξεις γίνεται τυχαία, και επειδή για όλους τους πιθανούς κώδικες το μήνυμα W θα αντιστοιχίζεται κάθε φορά σε διαφορετική κωδική λέξη, η ποσότητα $\sum_{\mathcal{C}} \Pr(\mathcal{C}) \lambda_w(\mathcal{C})$ είναι ανεξάρτητη του μηνύματος w. Επομένως, μπορούμε να υποθέσουμε, χωρίς απώλεια γενικότητας, ότι εστάλη η κωδική λέξη με δείκτη $w = 1$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (7) Υπολογισμός Πιθανότητας Σφάλματος (II)

- Επομένως, η $\Pr(\mathcal{E})$ ισούται με

$$\Pr\{\mathcal{E}\} = \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} \sum_{\mathcal{C}} \Pr(\mathcal{C})\lambda_w(\mathcal{C}) = \sum_{\mathcal{C}} \Pr(\mathcal{C})\lambda_1(\mathcal{C}) \triangleq \Pr(\mathcal{E}).$$

- Ορίζουμε τα ενδεχόμενα $E_i = \{(X^n(i), Y^n) \in A_\epsilon^{(n)}\},\ i \in \{1, 2, \ldots, 2^{nR}\}$, δηλαδή τα ενδεχόμενα η κωδική λέξη i να είναι από κοινού τυπική με τη ληφθείσα ακολουθία Y^n η οποία προήλθε από μετάδοση της κωδικής λέξης $X^n(1)$.
- Συνεπώς,

$$\begin{aligned}\Pr(\mathcal{E}) &= P(E_1^c \cup E_2 \cup E_3 \cup \ldots \cup E_{2^{nR}}|W = 1) \\ &\leq P(E_1^c|W = 1) + \sum_{i=2}^{2^{nR}} P(E_i|W = 1).\end{aligned}$$

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (8) Υπολογισμός Πιθανότητας Σφάλματος (III)

$$\Pr(\mathcal{E}) \leq P(E_1^c|W=1) + \sum_{i=2}^{2^{nR}} P(E_i|W=1).$$

- Από την ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης, η πιθανότητα η Y^n να μην είναι από κοινού τυπική με τη $X^n(1)$ τείνει στο 0 για $n \to \infty$: Επομένως, για κάθε $\epsilon > 0$ υπάρχει n_0 τέτοιο ώστε $P(E_1^c|W=1) \leq \epsilon$, για $n > n_0$.
- Επίσης, από τον τυχαίο τρόπο δημιουργίας του κώδικα, οι κωδικές λέξεις $X^n(1)$ και $X^n(i)$ είναι ανεξάρτητες μεταξύ τους για $i \neq 1$, με αποτέλεσμα η Y^n να είναι ανεξάρτητη από τις $X^n(i)$ για $i \neq 1$. Από την Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης, η πιθανότητα οι $X^n(i)$ και Y^n να είναι από κοινού τυπικές ενώ επιλέχθηκαν ανεξάρτητα είναι $\leq 2^{-n(I(X;Y)-3\epsilon)}$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (9) Υπολογισμός Πιθανότητας Σφάλματος (IV)

- Συνδυάζοντας όλα τα παραπάνω,

$$\Pr(\mathcal{E}) \leq P(E_1^c|W=1) + \sum_{i=2}^{2^{nR}} P(E_i|W=1) \leq \epsilon + \sum_{i=2}^{2^{nR}} 2^{-n(I(X;Y)-3\epsilon)}$$

$$= \epsilon + \left(2^{nR}-1\right) 2^{-n(I(X;Y)-3\epsilon)} \leq \epsilon + 2^{-n(I(X;Y)-3\epsilon-R)} \leq 2\epsilon.$$

  Η τελευταία ανισότητα ισχύει εφόσον $n > n_1$ και $R < I(X;Y) - 3\epsilon$.

- Επομένως, εάν $R < I(X;Y)$ μπορούμε να επιλέξουμε n τέτοιο ώστε η μέση πιθανότητα σφάλματος για όλους τους πιθανούς κώδικες και για όλες τις πιθανές κωδικές λέξεις να μην υπερβαίνει το 2ϵ, για οποιοδήποτε $\epsilon > 0$.

- Δεν τελειώσαμε ακόμα... Πρέπει να δείξουμε ότι η μέγιστη πιθανότητα σφάλματος $\lambda^{(n)} \to 0$.

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (10)
Επιλογή βιβλίου κωδίκων

- Εάν οι κώδικες δημιουργηθούν με βάση την κατανομή $p^*(x)$ η οποία μεγιστοποιεί την αμοιβαία πληροφορία, $I_{p^*}(X;Y) = C$, και, επομένως, μπορούμε να μεταδώσουμε με $R < C$.
- Δεδομένου ότι η μέση πιθανότητα σφάλματος για όλους τους τυχαίους κώδικες δεν υπερβαίνει το 2ϵ, υπάρχει τουλάχιστον ένα βιβλίο κωδίκων (κώδικας) $\mathcal{C}^*$ για το οποίο η πιθανότητα σφάλματος δεν υπερβαίνει το 2ϵ: $\Pr(\mathcal{E}|\mathcal{C}^*) \leq 2\epsilon$. Ο $\mathcal{C}^*$ μπορεί να βρεθεί με αναζήτηση μέσα σε όλους τους 2^{nR} κώδικες. Επομένως,

$$\Pr(\mathcal{E}|\mathcal{C}^*) \leq \frac{1}{2^{nR}} \sum \lambda_i(\mathcal{C}^*) \leq 2\epsilon.$$

Απόδειξη Θεωρήματος Κωδικοποίησης Καναλιού (11) Επιλογή βιβλίου κωδίκων (συνέχεια)

- Το γεγονός ότι η μέση πιθανότητα σφάλματος του κώδικα $\mathcal{C}^*$ είναι $\leq 2\epsilon$, δεν εγγυάται ότι η πιθανότητα σφάλματος που αντιστοιχεί στη μετάδοση ενός συγκεκριμένου μηνύματος W (και, επομένως, μιας συγκεκριμένης κωδικής λέξης $X^n(W)$) θα είναι $\leq 2\epsilon$.
- Εάν θέλουμε να διασφαλίσουμε μικρή πιθανότητα σφάλματος για <u>κάθε</u> κωδική λέξη (και, άρα, για κάθε μήνυμα) μπορούμε να αφαιρέσουμε τις μισές χειρότερες κωδικές λέξεις του κώδικα (δηλαδή τις 2^{nR-1} κωδικές λέξεις με τη μεγαλύτερη πιθανότητα σφάλματος).
- Δεδομένου ότι η μέση πιθανότητα σφάλματος είναι $\leq 2\epsilon$, η <u>μέγιστη</u> πιθανότητα σφάλματος των μισών "καλύτερων" λέξεων που απομένουν δε θα υπερβαίνει το 4ϵ.
- Ο νέος κώδικας έχει 2^{nR-1} κωδικές λέξεις και, άρα, ρυθμό $R' = R - \frac{1}{n}$. Για μεγάλα n, η απώλεια ρυθμού μετάδοσης είναι αμελητέα.
- Επομένως, δείξαμε ότι μπορούμε να επιτύχουμε οποιοδήποτε ρυθμό μετάδοσης που δεν υπερβαίνει τη χωρητικότητα, και, ταυτόχρονα, η <u>μέγιστη</u> πιθανότητα σφάλματος $\lambda^{(n)} \leq 4\epsilon$.

Θεώρημα Κωδικοποίησης Καναλιού (Ευθύ) – Ανακεφαλαίωση

Για να αποδείξουμε το Θεώρημα Κωδικοποίησης Καναλιού

- Δημιουργήσαμε πολλούς τυχαίους κώδικες (βιβλία κωδίκων) με κωδικές λέξεις μεγάλου μήκους n.
- Η δημιουργία των κωδικών λέξεων έγινε με βάση την κατανομή $p^*(x)$ που επιτυγχάνει τη χωρητικότητα καναλιού.
- Κρατήσαμε τον καλύτερο από τους τυχαίους κώδικες $\mathcal{C}^*$ (τον κώδικα στον οποίο αντιστοιχεί η μικρότερη πιθανότητα σφάλματος).
- Δείξαμε ότι, για αρκούντως μεγάλα μήκη κωδικών λέξεων n, εφόσον $R < I(X;Y)$, η πιθανότητα η ακολουθία εξόδου να μην είναι τυπική με τη μεταδοθείσα κωδική λέξη ή να είναι τυπική με κωδική λέξη διαφορετική από αυτή που μεταδόθηκε τείνει στο 0. Επομένως, η μέση πιθανότητα σφάλματος μπορεί να περιοριστεί αυθαίρετα κοντά στο 0.
- Με τροποποίηση του κώδικα δείξαμε ότι όχι μόνο η μέση, αλλά και η μέγιστη πιθανότητα σφάλματος μπορεί να περιοριστεί αυθαίρετα κοντά στο 0.

Θεώρημα Κωδικοποίησης Καναλιού (Ευθύ) – Σχόλια

- Η δημιουργία τυχαίων κωδίκων οδηγεί μεν σε (μια) απόδειξη του Θεωρήματος Κωδικοποίησης Καναλιού, αλλά δεν αποτελεί πρακτικό τρόπο μετάδοσης.
- Η δημιουργία του κώδικα, αν και πολύπλοκη, μπορεί να γίνει μια φορά υποθέτοντας ότι ο πίνακας μετάβασης του καναλιού $p(y|x)$ δεν αλλάζει. Παρατηρήστε ότι ο βέλτιστος κώδικας μπορεί να βρεθεί από τον πομπό και το δέκτη ανεξάρτητα χωρίς συνεννόηση εάν γνωρίζουν και οι δύο τον πίνακα μετάβασης καναλιού και αν δημιουργήσουν όλους τους πιθανούς κώδικες (και κρατήσουν τον καλύτερο από άποψη ελάχιστης πιθανότητας σφάλματος).
- Το σημαντικότερο πρόβλημα βρίσκεται στην αποκωδικοποίηση καθώς ο αριθμός των κωδικών λέξεων των οποίων η από κοινού τυπικότητα με την Y^n θα πρέπει να ελεγχθεί αυξάνει εκθετικά με το n.
- Το πρόβλημα αυτό παραμένει ακόμα και όταν η αποκωδικοποίηση γίνεται με χρήση άλλων κριτηρίων (π.χ. ανίχνευση Μέγιστης Πιθανοφάνειας).
- Η επίτευξη ρυθμών μετάδοσης κοντά στη χωρητικότητα του καναλιού με υλοποιήσιμους τρόπους αποτελεί αντικείμενο της Θεωρίας Κωδικοποίησης. Η μετάδοση κοντά στη χωρητικότητα είναι σήμερα εφικτή με πολυπλοκότητα που δεν είναι απαγορευτική για την υλοποίηση των αποκωδικοποιητών.

Προεπισκόπηση επόμενου μαθήματος

- Θα ολοκληρώσουμε την απόδειξη του Θεωρήματος Κωδικοποίησης Καναλιού με απόδειξη του αντιστρόφου. Θα δείξουμε, δηλαδή, ότι δεν υπάρχει κώδικας με $P_e^{(n)} \to 0$ που να επιτυγχάνει $R > C$.
- Χωρητικότητα Διακριτών Καναλιών Χωρίς Μνήμη με Ανάδραση.
- Βέλτιστη μέθοδος αποκωδικοποίησης (με χρήση Μέγιστης Πιθανοφάνειας – Maximum Likelihood).
- Εκθέτης Σφάλματος (Error Exponent): Παρέχει ένα άνω φράγμα για το σφάλμα αποκωδικοποίησης με χρήση ML για δεδομένο μήκος κώδικα n.
- 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.