EE728 Προχωρημένα Θέματα Θεωρίας Πληροφορίας 9η διάλεξη

Δημήτρης-Αλέξανδρος Τουμπακάρης

Τμήμα ΗΜ&ΤΥ, Πανεπιστήμιο Πατρών

28 Απριλίου 2010

Περιεχόμενα σημερινού μαθήματος

1. Συνεχείς τ.μ. και Διαφορική Εντροπία
   - Ιδιότητες
   - Μεγιστοποίηση Διαφορικής Εντροπίας
2. AEP για συνεχείς τ.μ.
3. Το Γκαουσιανό Κανάλι. Θεώρημα Κωδικοποίησης
   - Υπολογισμός Χωρητικότητας
   - Θεώρημα κωδικοποίησης (ευθύ)
   - Θεώρημα κωδικοποίησης (αντίστροφο)
   - Shpere packing

Αντιστοιχία με συγγράμματα

- Cover & Thomas: 8.2, 8.6, 9.1, 9.2
- Gallager: 7.3, 7.4

Συνεχείς τ.μ. και Διαφορική Εντροπία

Ιδιότητες Σχετικής Εντροπίας και Αμοιβαίας Πληροφορίας για συνεχείς τ.μ.

- $D(f||g) \geq 0$, με ισότητα όταν $f = g$ σχεδόν παντού.
  Απόδειξη: Εάν S είναι το πεδίο ορισμού της f,

$$-D(f||g) = \int_S f \log \frac{g}{f} \overset{(a)}{\leq} \log \int_S f \frac{g}{f} = \log \int_S g \overset{(b)}{\leq} \log 1 = 0.$$

  (a) γιατί; (b) S υποσύνολο του πεδίου ορισμού της g.
- $I(X;Y) \geq 0$ με $=$ εάν και μόνο εάν X και Y ανεξάρτητες. Γιατί;

Ιδιότητες Σχετικής Εντροπίας και Αμοιβαίας Πληροφορίας για συνεχείς τ.μ. (2)

- $h(X|Y) \leq h(X)$ με $=$ εάν και μόνο εάν X και Y ανεξάρτητες.
- Κανόνας αλυσίδας για τη Διαφορική Εντροπία: $h(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} h(X_i|X_1, X_2, \ldots, X_{i-1})$. Αποδεικνύεται εύκολα από τον ορισμό της Από Κοινού Διαφορικής Εντροπίας.
- $h(X_1, X_2, \ldots, X_n) \leq \sum h(X_i)$, με $=$ εάν και μόνο εάν οι $X_1, X_2, \ldots, X_n$ είναι ανεξάρτητες.

Άλλες Ιδιότητες Διαφορικής Εντροπίας

- $h(X+c) = h(X)$. Προκύπτει απευθείας από τον ορισμό.
  - Η διαφορική εντροπία είναι αναλλοίωτη σε μετάθεση.
  - Αντίστοιχη ιδιότητα για διακριτές τ.μ.: η εντροπία διακριτών τ.μ. εξαρτάται μόνο από την κατανομή τους και όχι από τις τιμές τους.
- $h(aX) = h(X) + \log|a|$. Για την απόδειξη δείτε π.χ. Cover & Thomas Theorem 8.6.4.
  - Διαισθητικά λογικό: Η τ.μ. παίρνει, πλέον, τιμές, σε διάστημα διαφορετικού μήκους.
- $h(A\mathbf{X}) = h(\mathbf{X}) + \log|\det(A)|$, όπου $\det(A)$ η ορίζουσα του A.

Μεγιστοποίηση Διαφορικής Εντροπίας

- Έστω τυχαίο διάνυσμα $\mathbf{X} \in \mathbf{R}^n$ με μέση τιμή $\mathbf{m} = 0$ και πίνακα συσχέτισης $K = \mathbb{E}\left[\mathbf{X}\mathbf{X}^T\right]$ (δηλαδή $K_{ij} = \mathbb{E}\left[X_i X_j\right], \ 1 \leq i, j \leq n$). Για την εντροπία της $\mathbf{X}$ ισχύει $h(\mathbf{X}) \leq \frac{1}{2} \log(2\pi e)^n |K|$, με $=$ εάν και μόνο εάν $\mathbf{X} \sim \mathcal{N}(0, K)$.
- Επομένως, για δεδομένο πίνακα συσχέτισης K, η συνεχής κατανομή που μεγιστοποιεί την εντροπία είναι η Γκαουσιανή!
- Θα μας χρησιμεύσει στον υπολογισμό της χωρητικότητας του Γκαουσιανού Καναλιού.

Μεγιστοποίηση Διαφορικής Εντροπίας (2)

- Για βαθμωτή συνεχή τ.μ. X με μέση τιμή $m = 0$ και διασπορά σ^2, η κατανομή που μεγιστοποιεί την $h(X)$ είναι η $\mathcal{N}(0, \sigma^2)$.
- Δεδομένου ότι $h(X + c) = h(X)$, μπορούμε να επεκτείνουμε το αποτέλεσμα και σε τ.μ. με μη μηδενική μέση τιμή.
- Μεταξύ συνεχών τ.μ. με την ίδια <u>ισχύ</u> (=$\sum_i \mathbb{E}|X_i|^2 = \mathbb{E}\left[\mathbf{X}^T\mathbf{X}\right] = trace\{\mathbb{E}\left[\mathbf{X}\mathbf{X}^T\right]\} = trace\{K\}$), οι πιο "αβέβαιες" είναι αυτές που ακολουθούν Γκαουσιανή κατανομή $\mathcal{N}(\mathbf{m}, K)$.

Μεγιστοποίηση Διαφορικής Εντροπίας – Απόδειξη

- Έστω $g(\mathbf{x})$ οποιαδήποτε συνάρτηση πυκνότητας πιθανότητας που ικανοποιεί τον περιορισμό συσχέτισης $\int g(\mathbf{x}) x_i x_j d\mathbf{x} = K_{ij}$ για όλα τα i, j. Έστω, επίσης ϕ_K η συνάρτηση πυκνότητας πιθανότητας διανύσματος που ακολουθεί Γκαουσιανή κατανομή $\mathcal{N}(0, K)$:

$$\phi_K(\mathbf{x}) = \frac{1}{\left(\sqrt{2\pi}\right)^n |K|^{1/2}} e^{-\frac{1}{2}\mathbf{x}^T K^{-1}\mathbf{x}} \Rightarrow \log \phi_K(\mathbf{x}) = A - \frac{1}{2} \log_2 e \cdot \mathbf{x}^T K^{-1} \mathbf{x}$$

- Επίσης, $\int \phi_K(\mathbf{x}) x_i x_j d\mathbf{x} = K_{ij}$. Επομένως,

$$0 \le D(g||\phi_K) = \int g \log\left(\frac{g}{\phi_K}\right) = -h(g) - \int g \log \phi_K$$
$$\stackrel{(a)}{=} -h(g) - \int \phi_K \log \phi_K = -h(g) + h(\phi_K).$$

(a) Προκύπτει από την παρατήρηση ότι η $\log \phi_K(\mathbf{x})$ είναι τετραγωνική μορφή (άθροισμα όρων της μορφής $a_{ij} x_i x_j$), και από την υπόθεση ότι $\int g(\mathbf{x}) x_i x_j d\mathbf{x} = \int \phi_K(\mathbf{x}) x_i x_j d\mathbf{x}$.

ΑΕΡ για συνεχείς τ.μ.

AEP για συνεχείς τ.μ.

- Για την περίπτωση συνεχών τ.μ. το AEP μπορεί να αποδειχθεί με παρόμοιο τρόπο όπως στην περίπτωση διακριτών τυχαίων μεταβλητών. Πιο συγκεκριμένα,
  1. $\Pr\left\{A_\epsilon^{(n)}\right\} > 1 - \epsilon$ για $n > n_0$.
  2. $\text{Vol}\left(A_\epsilon^{(n)}\right) \leq 2^{n(h(X)+\epsilon)}$ για όλα τα n.
  3. $\text{Vol}\left(A_\epsilon^{(n)}\right) \geq (1-\epsilon)2^{n(h(X)-\epsilon)}$ για $n > n_0$.
- Παρατηρήστε ότι, για συνεχείς τ.μ., η ποσότητα που αντιστοιχεί στον αριθμό στοιχείων του τυπικού συνόλου $\left|A_\epsilon^{(n)}\right|$ είναι ο όγκος $\text{Vol}(A)$ του συνόλου A:

$$\text{Vol}(A) = \int_A dx_1 dx_2 \ldots dx_n.$$

AEP για συνεχείς τ.μ. (συνέχεια)

- Όσο μικρότερη είναι η εντροπία μιας συνεχούς τ.μ., τόσο μικρότερος είναι ο μέσος όγκος που καταλαμβάνει το σύνολο που περιέχει σχεδόν όλη την πιθανότητα (για δεδομένο n).
- Για n σύμβολα (διαστάσεις), Vol$\left(A_\epsilon^{(n)}\right) \approx 2^{nh(X)}$. Επομένως, ανά διάσταση, ο "χώρος" στον οποίο περιέχονται οι τυπικές ακολουθίες έχει πλευρά μήκους $\approx 2^{h(X)}$.

Το Γκαουσιανό Κανάλι. Θεώρημα Κωδικοποίησης για το Γκαουσιανό Κανάλι

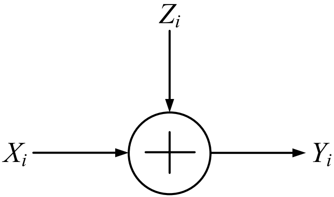
Το Γκαουσιανό Κανάλι – Εισαγωγή

- Κανάλι διακριτού χρόνου με συνεχές αλφάβητο.
- Δίνεται από τη σχέση

$$Y_i = X_i + Z_i, \quad Z_i \sim \mathcal{N}(0, N),$$

όπου οι τ.μ. Z_i είναι ανεξάρτητες μεταξύ τους και ανεξάρτητες από τις X_i.

- Αποτελεί πολύ καλό και ευρέως χρησιμοποιούμενο μοντέλο για συστήματα επικοινωνιών.



Το Γκαουσιανό Κανάλι – Εισαγωγή (2)

- Ποια είναι η χωρητικότητα του Γκαουσιανού Καναλιού; Εξαρτάται από τις υποθέσεις!
- Εάν η διασπορά του θορύβου ισούται με 0, η έξοδος του καναλιού ισούται με την είσοδό του. Επομένως, μπορούμε να μεταδώσουμε με άπειρο ρυθμό (χρησιμοποιώντας συνεχές η άπειρο διακριτό αλφάβητο για τη X).
- Το ίδιο ισχύει εάν ο θόρυβος έχει πεπερασμένη διασπορά, αλλά δεν υπάρχει περιορισμός πλάτους ή ισχύος της εισόδου. Μπορούμε πάντα να χρησιμοποιήσουμε είσοδο τέτοιου πλάτους ώστε να μπορούμε να ανακτήσουμε το μεταδοθέν σήμα στην έξοδο με πιθανότητα σφάλματος που τείνει στο 0.
- Στην πράξη, ο θόρυβος Z έχει μη μηδενική διασπορά (ισχύ). Επίσης, υπάρχει περιορισμός ως προς τη διαθέσιμη ισχύ της X.

Το Γκαουσιανό Κανάλι – Εισαγωγή (3)

- Στο μάθημα "Θεωρία Πληροφορίας" είδαμε ότι, για την περίπτωση πεπερασμένης ισχύος εισόδου $\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P$, η χωρητικότητα του Γκαουσιανού καναλιού ισούται με

Χωρητικότητα Γκαουσιανού Καναλιού

$$C = \frac{1}{2}\log\left(1+\frac{P}{N}\right) \text{ bits/χρήση καναλιού.}$$

Χωρητικότητα Γκαουσιανού Καναλιού με περιορισμό ισχύος

- Η "πληροφοριακή" χωρητικότητα του Γκαουσιανού Καναλιού με περιορισμό ισχύος (power contraint) P ορίζεται ως

$$C = \max_{f_X(x):\mathbb{E}X^2 \leq P} I(X;Y).$$

- Θα επαναλάβουμε τον υπολογισμό της πληροφοριακής χωρητικότητας Γκαουσιανού καναλιού που παρουσιάστηκε στο μάθημα "Θεωρία Πληροφορίας".

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) = h(Y) - h(X+Z|X) \\ &= h(Y) - h(Z|X) \stackrel{(a)}{=} h(Y) - h(Z) = h(Y) - \frac{1}{2}\log 2\pi e N. \end{aligned}$$

(a) η Z (θόρυβος) είναι ανεξάρτητη της X.

Χωρητικότητα Γκαουσιανού Καναλιού με περιορισμό ισχύος (2)

- Για τη διασπορά της Y, και δεδομένου ότι $\mathbb{E}Z = 0$, ισχύει

$$\mathbb{E}Y^2 = \mathbb{E}(X+Z)^2 = \mathbb{E}X^2 + 2\mathbb{E}X\mathbb{E}Z + \mathbb{E}Z^2 = P + N.$$

- Επομένως, $h(Y) \leq \frac{1}{2}\log 2\pi e(P+N)$, με $=$ όταν η Y ακολουθεί Γκαουσιανή κατανομή. Συνεπώς,

$$\begin{aligned} I(X;Y) &= h(Y) - \frac{1}{2}\log 2\pi e N \\ &\leq \frac{1}{2}\log 2\pi e(P+N) - \frac{1}{2}\log 2\pi e N \Rightarrow \end{aligned}$$

$$C = \frac{1}{2}\log\left(1 + \frac{P}{N}\right).$$

Χωρητικότητα Γκαουσιανού Καναλιού με περιορισμό ισχύος (3)

- $X = Y - N$. Από τη Θεωρία Πιθανοτήτων, ο γραμμικός συνδυασμός δύο Γκαουσιανών τ.μ. ακολουθεί Γκαουσιανή κατανομή. Συνεπώς, όταν η Y ακολουθεί Γκαουσιανή κατανομή, το ίδιο ισχύει και για τη X.
- Άρα, η πληροφοριακή χωρητικότητα του Γκαουσιανού καναλιού επιτυγχάνεται με χρήση Γκαουσιανής εισόδου.
- Απομένει να αποδείξουμε ότι η "πληροφοριακή" χωρητικότητα του Γκαουσιανού καναλιού ισούται με τη "λειτουργική" του χωρητικότητα.

Θεώρημα Κωδικοποίησης για το Γκαουσιανό κανάλι

- Σημείωση: Η απόδειξη του ευθέος είναι παρόμοια με αυτή για το διακριτό κανάλι χωρίς μνήμη και δίνεται στο Κεφάλαιο 9.1 του Cover. Θα επισημάνουμε μόνο τις διαφορές.
- Όπως και για το διακριτό κανάλι χωρίς μνήμη, κατασκευάζονται κωδικές λέξεις μήκους n. Η μόνη διαφορά είναι ότι πρέπει να ικανοποιούν τον περιορισμό ισχύος: $\sum_{i=1}^{n} x_i^2(w) \leq nP$, $w = 1, 2, \ldots, M$, όπου M ο αριθμός των μηνυμάτων (και ίσος με 2^{nR}).
- Εάν κατασκευάσουμε τα σύμβολα των κωδικών λέξεων με βάση Γκαουσιανή κατανομή $\mathcal{N}(0, P-\epsilon)$, για μεγάλο n, $\frac{1}{n}\sum X_i^2 \to P - \epsilon$ και, επομένως, ο περιορισμός ικανοποιείται με πιθανότητα που τείνει στο 1.

Θεώρημα Κωδικοποίησης για το Γκαουσιανό κανάλι (2)

- Μετά την κατασκευή του τυχαίου κώδικα, αυτός αποκαλύπτεται τόσο στον πομπό όσο και στο δέκτη. Θεωρούμε ότι η αποκωδικοποίηση στο δέκτη γίνεται με χρήση από κοινού τυπικότητας.
- Σε σύγκριση με τα διακριτά κανάλια χωρίς μνήμη, υπάρχει ένα επιπλέον ενδεχόμενο που συμβάλλει στην πιθανότητα σφάλματος: Το ενδεχόμενο η κωδική λέξη που έχει αποσταλεί να μην ικανοποιεί τον περιορισμό ισχύος. Ωστόσο, για μεγάλα n η πιθανότητα αυτή μπορεί να γίνει αυθαίρετα μικρή. Συνεπώς, και η συνολική πιθανότητα σφάλματος μπορεί να γίνει αυθαίρετα μικρή, όπως και στην περίπτωση του διακριτού καναλιού χωρίς μνήμη.

Θεώρημα Κωδικοποίησης για το Γκαουσιανό κανάλι (αντίστροφο)

- Και για το αντίστροφο, η απόδειξη είναι παρόμοια με αυτή για το αντίστροφο του Θεωρήματος Κωδικοποίησης για διακριτά κανάλια χωρίς μνήμη.
- Θεωρούμε ότι οι κωδικές λέξεις ικανοποιούν τον περιορισμό ισχύος, δηλαδή ότι $\frac{1}{n}\sum_{i=1}^{n} x_i^2(w) \leq P$.
- Επιπλέον, θεωρούμε ότι η κατανομή των 2^{nR} μηνυμάτων είναι ομοιόμορφη και χρησιμοποιούμε την ανισότητα Fano.

$$
\begin{aligned}
H(W|\hat{W}) &\leq H\left(P_e^{(n)}\right) + P_e^{(n)} \log|\mathcal{X}| \\
&= 1 + nP_e^{(n)}R = n\left(\frac{1}{n} + P_e^{(n)}R\right) = n\epsilon_n,
\end{aligned}
$$

όπου $\epsilon_n \to 0$ καθώς $P_e^{(n)} \to 0$.

Θεώρημα Κωδικοποίησης για το Γκαουσιανό κανάλι (αντίστροφο) (2)

- Όπως και στην περίπτωση διακριτού καναλιού χωρίς μνήμη, $I(X^n;Y^n) \leq \sum_{i=1}^{n} I(X_i;Y_i)$.

$$
\begin{aligned}
I(X^n;Y^n) &= h(Y^n) - h(Y^n|X^n) = h(Y^n) - h(Z^n) \\
&\leq \sum_{i=1}^{n} h(Y_i) - h(Z^n) \\
&= \sum_{i=1}^{n} h(Y_i) - \sum_{i=1}^{n} h(Z_i) = \sum_{i=1}^{n} I(X_i,Y_i).
\end{aligned}
$$

Θεώρημα Κωδικοποίησης για το Γκαουσιανό κανάλι (αντίστροφο) (3)

$$H(W|\hat{W}) \leq H\left(P_e^{(n)}\right) + P_e^{(n)} \log|\mathcal{X}| = 1 + nP_e^{(n)} R$$
$$= n\left(\frac{1}{n} + P_e^{(n)} R\right) = n\epsilon_n,$$

- Επομένως, μπορούμε να γράψουμε

$$nR = H(W) = I(W;\hat{W}) + H(W|\hat{W}) \overset{(a)}{\leq} I(W;\hat{W}) + n\epsilon_n$$
$$\overset{(b)}{\leq} I(X^n;Y^n) + n\epsilon_n \leq \sum_{i=1}^{n} I(X_i,Y_i) + n\epsilon_n.$$

(a) Ανισότητα Fano, (b) Ανισότητα Επεξεργασίας Δεδομένων

Θεώρημα Κωδικοποίησης για το Γκαουσιανό κανάλι (αντίστροφο) (4)

- Ορίζουμε $P_i = \frac{1}{2^{nR}} \sum_w x_i^2(w)$, δηλαδή τη μέση ισχύ του $i-$οστού συμβόλου των κωδικών λέξεων. Επομένως, $\mathbb{E}Y_i^2 = P_i + N$ και $h(Y) \leq \frac{1}{2}\log 2\pi e(P_i + N)$.
- Δεδομένου ότι οι κωδικές λέξεις ικανοποιούν τον περιορισμό ισχύος, $\frac{1}{n}\sum_i P_i \leq P$.
  Επομένως,

$$nR \leq \sum_i I(X_i; Y_i) + n\epsilon_n \leq \sum_i \frac{1}{2}\log\left(1 + \frac{P_i}{N}\right) + n\epsilon_n \Rightarrow$$

$$R \leq \sum_i \frac{1}{n} I(X_i; Y_i) + \epsilon_n \overset{(a)}{\leq} \frac{1}{2}\log\left(1 + \frac{1}{n}\sum_{i=1}^{n}\frac{P_i}{N}\right) \leq \frac{1}{2}\log\left(1 + \frac{P}{N}\right).$$

  (a) από την ανισότητα Jensen.
- Συνεπώς, για $P_e^{(n)} \to 0, R \leq \frac{1}{2}\log\left(1 + \frac{P}{N}\right)$ και δεν υπάρχει κώδικας που να ικανοποιεί τον περιορισμό ισχύος και να επιτυγχάνει $R > C$.

Γεωμετρικό Επιχείρημα (Sphere Packing Argument)

- Διαισθητικά, το Θεώρημα Κωδικοποίησης Καναλιού για Γκαουσιανά κανάλια μπορεί περιγραφεί με το ακόλουθο γεωμετρικό επιχείρημα.
- Μια κωδική λέξη x^n αποτελεί ένα διάνυσμα στο $n-$διάστατο χώρο. Επομένως, η ακολουθία y^n που λαμβάνεται στο δέκτη και αντιστοιχεί στο x^n βρίσκεται μέσα σε μια $n-$διάστατη σφαίρα με κέντρο x^n και ακτίνα $\approx \sqrt{n(N+\epsilon)}$. Καθώς το n αυξάνει, η y^n βρίσκεται μέσα στη σφαίρα με ολοένα αυξανόμενη πιθανότητα (και με $\epsilon \to 0$).
- Αποδεικνύεται, μάλιστα, ότι με πιθανότητα που τείνει στο 1, το διάνυσμα βρίσκεται στο φλοιό της σφαίρας (δείτε Φυλλάδιο 10).

Γεωμετρικό Επιχείρημα (Sphere Packing Argument) (2)

- Για μεγάλο n, ο χώρος όλων των πιθανών ακολουθιών στο δέκτη έχει ακτίνα περίπου ίση με $\sqrt{n(P+N)}$. Δεδομένου ότι σε κάθε x^n αντιστοιχεί μια σφαίρα ακτίνας περίπου $\sqrt{nN}$ και ότι ο όγκος μιας $n-$διάστατης σφαίρας ισούται με $C_n r^n$, ο αριθμός "σφαιρών" που αντιστοιχούν σε μηνύματα και τις οποίες μπορούμε να χωρέσουμε στο χώρο όλων των y^n προκειμένου αυτές να μην επικαλύπτονται (και, επομένως, να μη γίνονται σφάλματα εκτίμησης στο δέκτη) δεν μπορεί να υπερβεί τις

$$\frac{C_n\left(\sqrt{n(P+N)}\right)^n}{C_n\left(\sqrt{nN}\right)^n} \Rightarrow \log\left(\frac{C_n\left(\sqrt{n(P+N)}\right)^n}{C_n\left(\sqrt{nN}\right)^n}\right)$$

$$= \frac{n}{2}\log\left(1+\frac{P}{N}\right).$$

Γεωμετρικό Επιχείρημα (Sphere Packing Argument) (3)