EE728
Προχωρημένα Θέματα Θεωρίας Πληροφορίας
11η εβδομάδα

Δημήτρης-Αλέξανδρος Τουμπακάρης

Τμήμα ΗΜ&ΤΥ, Πανεπιστήμιο Πατρών

24 Μαΐου 2015

Περιεχόμενα 11ης εβδομάδας

Αντιστοιχία 11ης εβδομάδας με βιβλία Cover & Thomas και El Gamal & Kim

- Cover & Thomas Κεφ. 8, 9.1–9.2
- El Gamal & Kim 2.2, 3.3 – 3.4

Διαφορική Εντροπία – Εισαγωγή

- Έως τώρα θεωρούσαμε διακριτές τ.μ. με τιμές με πεπερασμένο και διακριτό αλφάβητο.
- Τα αποτελέσματα της Θεωρίας Πληροφορίας επεκτείνονται σε συνεχείς τ.μ., με κατάλληλες τροποποιήσεις και με χρήση της διαφορικής εντροπίας (differential entropy).
- Γενικά, όσα ισχύουν για διακριτές τ.μ. ισχύουν (με κατάλληλες τροποποιήσεις) και για συνεχείς τ.μ. Ωστόσο, η διαφορική εντροπία είναι πιο "προβληματικό" μέγεθος σε σχέση με την εντροπία και υπάρχουν κάποιες διαφορές που θα πρέπει να προσεχτούν.
- Θα αναφερθούμε στις συνεχείς τ.μ. πιο επιγραμματικά, φροντίζοντας, όμως, να επισημαίνουμε τις διαφορές, όπου υπάρχουν.

Διαφορική Εντροπία – Ορισμός

- **Ορισμός 11.1.** Η Διαφορική Εντροπία $h(X)$ συνεχούς τ.μ X με συνάρτηση πυκνότητας πιθανότητας $f(x)$, *εάν η f υπάρχει,* ορίζεται ως

$$h(X) = -\int_S f(x) \log f(x) dx,$$

όπου S είναι το πεδίο ορισμού της τ.μ.

- Υποθέτουμε ότι η $f(x) \log f(x)$ είναι ολοκληρώσιμη κατά Riemann.

Παράδειγμα 11.1. – Δεν ισχύει, κατ' ανάγκη, $h(X) \geq 0$!

- Έστω συνεχής τ.μ. X, ομοιόμορφα κατανεμημένη στο διάστημα $[0, a]$.

$$h(X) = -\int_S f(x) \log f(x) dx = -\int_0^a \frac{1}{a} \log \frac{1}{a} dx = \log a.$$

- Για $a < 1$, $h(X) < 0$.
- Ωστόσο, η ποσότητα $2^{h(X)}$ είναι πάντοτε μη αρνητική.
- Η διαφορική εντροπία διακριτής τ.μ. ισούται με $-\infty$ ($2^{-\infty} = 0$).

Παράδειγμα 11.2. – Εντροπία Γκαουσιανής τ.μ.

- Έστω συνεχής τ.μ. X η οποία ακολουθεί Γκαουσιανή κατανομή με μέση τιμή 0 και διασπορά σ^2.

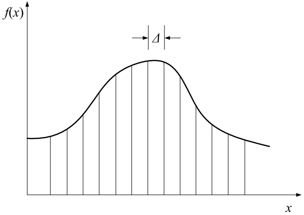
$$X \sim \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{x^2}{2\sigma^2}}.$$

- Με χρήση του ορισμού της διαφορικής εντροπίας,

$$\begin{aligned}
h(X) &= -\int_S f(x) \ln f(x) dx = -\int_{-\infty}^{\infty} f(x) \ln f(x) dx \\
&= -\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{x^2}{2\sigma^2}} \left[-\frac{x^2}{2\sigma^2} - \ln\left(\sqrt{2\pi\sigma}\right)\right] dx \\
&= \frac{\mathbb{E}X^2}{2\sigma^2} + \frac{1}{2}\ln\left(2\pi\sigma^2\right) = \frac{1}{2} + \frac{1}{2}\ln\left(2\pi\sigma^2\right) = \frac{1}{2}\ln e + \frac{1}{2}\ln\left(2\pi\sigma^2\right) \\
&= \frac{1}{2}\ln\left(2\pi e\sigma^2\right) \text{ nats} = \frac{1}{2}\log\left(2\pi e\sigma^2\right) \text{ bits}
\end{aligned}$$

Παράδειγμα 11.3. – Εντροπία διακριτής αναπαράστασης συνεχούς τ.μ.

- Έστω συνεχής τ.μ. X με συνάρτηση πυκνότητας πιθανότητας $f(x)$. Χωρίζουμε την $f(X)$ σε διαστήματα πλάτους Δ, όπως φαίνεται στο Σχήμα.



- Για κάθε διάστημα πλάτους Δ υπάρχει x_i τέτοιο ώστε $f(x_i)\Delta = \int_{i\Delta}^{(i+1)\Delta} f(x)dx$.
- Θεωρούμε τη διακριτή αναπαράσταση, X^{Δ}, της συνεχούς τ.μ. X:

$$X^{\Delta} = x_i, \quad \text{όταν } i\Delta \leq X < (i+1)\Delta.$$

Παράδειγμα 11.3. – Εντροπία διακριτής αναπαράστασης συνεχούς τ.μ. (2)

- $p_i \triangleq \Pr\left\{X^\Delta = x_i\right\} = \int_{i\Delta}^{(i+1)\Delta} f(x)dx = f(x_i)\Delta.$
- Επομένως, για την εντροπία της (διακριτής) X^Δ ισχύει

$$
\begin{aligned}
H(X^\Delta) &= -\sum_{-\infty}^{\infty} p_i \log p_i = -\sum_{-\infty}^{\infty} (f(x_i)\Delta)\log\left(f(x_i)\Delta\right) = \\
&= -\sum_{-\infty}^{\infty} f(x_i)\Delta \log f(x_i) - \sum_{-\infty}^{\infty} f(x_i)\Delta \log \Delta \\
&= -\sum_{-\infty}^{\infty} f(x_i)\Delta \log f(x_i) - \log \Delta.
\end{aligned}
$$

Παράδειγμα 11.3. – Εντροπία διακριτής αναπαράστασης συνεχούς τ.μ. (3)

$$H\left(X^{\Delta}\right) = -\sum_{-\infty}^{\infty} f(x_i)\Delta \log f(x_i) - \log \Delta.$$

- Όταν $\Delta \to 0$, $H\left(X^{\Delta}\right) \to h(X) - \log \Delta$, εάν η $f(x)$ είναι ολοκληρώσιμη κατά Riemann.
- Παρατηρούμε ότι η ποσότητα $\log \Delta$ είναι ανάλογη του αριθμού n των bits που χρησιμοποιούνται για τη διακριτοποίηση (κβάντιση) της συνεχούς τ.μ. X. Επομένως, $H\left(X^{\Delta}\right) \approx h(X) + n$.
- Η ακριβής (μη κβαντισμένη) τιμή συνεχούς τ.μ. απαιτεί άπειρα bits για την περιγραφή της (διαισθητικά λογικό).

Από κοινού και υπό συνθήκη Διαφορική Εντροπία

Οι ορισμοί είναι παρόμοιοι με τους αντίστοιχους ορισμούς για διακριτές τ.μ.

- **Ορισμός 11.2.** Από κοινού διαφορική εντροπία: $h(X_1, X_2, \ldots, X_n) = -\int f(x^n) \log f(x^n) dx^n$ (εάν υπάρχει), όπου $f(x^n) = f(x_1, x_2, \ldots, x_n)$.
- **Ορισμός 11.3.** Υπό συνθήκη διαφορική εντροπία: $h(X|Y) = -\int f(x, y) \log f(x|y) dxdy$ (εάν υπάρχει).

- Όπως και στην περίπτωση διακριτών τ.μ., εάν όλες οι ποσότητες είναι πεπερασμένες,

$$h(X|Y) = h(X, Y) - h(Y).$$

Παράδειγμα 11.4. – Διαφορική Εντροπία πολυμεταβλητής Γκαουσιανής τ.μ.

- Έστω τ.μ. που ακολουθεί πολυμεταβλητή Γκαουσιανή κατανομή:

$$f(\mathbf{x}) = f(x_1, x_2, \ldots, x_n) = \frac{1}{\left(\sqrt{2\pi}\right)^n |K|^{1/2}} e^{-\frac{1}{2}(\mathbf{x}-\mathbf{m})^T K^{-1}(\mathbf{x}-\mathbf{m})},$$

όπου $(\cdot)^T$ υποδηλώνει αναστροφή (διανύσματος ή πίνακα), K είναι ο πίνακας συσχέτισης και $|K|$ η ορίζουσα του K.

- Αποδεικνύεται (με χρήση του ορισμού και πράξεις – Cover & Thomas Theorem 8.4.1) ότι

$$h(X_1, X_2, \ldots, X_n) = h\left(\mathcal{N}_n(\mathbf{m}, K)\right) = \frac{1}{2}\log(2\pi e)^n |K| \text{ bits.}$$

- Για πραγματική τ.μ. $X \sim \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mathbf{m})^2}{2\sigma^2}}$, $h(X) = \frac{1}{2}\log\left(2\pi e\sigma^2\right)$ bits.

Σχετική Εντροπία και Αμοιβαία Πληροφορία για συνεχείς τ.μ.

- **Ορισμός 11.4.** Σχετική Εντροπία (Απόσταση Kullback-Leibler): $D(f||g) = \int f \log \frac{f}{g}$. Πεπερασμένη μόνο εφόσον το πεδίο ορισμού της f περιέχεται στο πεδίο ορισμού της g.
- **Ορισμός 11.5.** Εάν ορίζεται από κοινού συνάρτηση πυκνότητας πιθανότητας για τις τ.μ. X και Y, η Αμοιβαία Πληροφορία ορίζεται ως

$$I(X;Y) = D(f(x,y)||f(x)f(y)) = \int f(x,y) \log \frac{f(x,y)}{f(x)f(y)} dxdy.$$

- Όπως και για τις διακριτές τ.μ., $I(X;Y) = h(X) - h(X|Y) = h(Y) - h(Y|X) = h(X) + h(Y) - h(X,Y)$.

Σχετική Εντροπία και Αμοιβαία Πληροφορία για συνεχείς τ.μ. (2)

- Εάν δεν ορίζεται $f(x, y)$, μπορεί να χρησιμοποιηθεί ο πλέον γενικός ορισμός της Αμοιβαίας Πληροφορίας

$$I(X;Y) = \sup_{\text{όλες οι } \mathcal{P}, \mathcal{Q}} I\left([X]_{\mathcal{P}}; [Y]_{\mathcal{Q}}\right),$$

όπου $\mathcal{P}$ και $\mathcal{Q}$ πεπερασμένες διαμερίσεις (partitions) των $\mathcal{X}$ και $\mathcal{Y}$ και $[X]_{\mathcal{P}}$, $[Y]_{\mathcal{Q}}$ οι κβαντίσεις των X και Y ως προς τις διαμερίσεις $\mathcal{P}$ και $\mathcal{Q}$, αντίστοιχα (περισσότερες λεπτομέρειες στο βιβλίο των Cover & Thomas).

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

- Θεώρημα 11.6. 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 τη διαφορική 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)

- Πόρισμα 11.7. 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 ισχύ (=$\sum_i \mathbb{E}|X_i|^2 = \mathbb{E}\left[\mathbf{X}^T\mathbf{X}\right] =$ tr$\{\mathbb{E}\left[\mathbf{X}\mathbf{X}^T\right]\} =$ tr$\{K\}$), 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 $\mathbb{E}_{g(\mathbf{x})}[X_i X_j] = \int g(\mathbf{x}) x_i x_j d\mathbf{x} = K_{ij}$ για όλα τα i, j. Έστω, επίσης $\phi_K(\mathbf{x})$ 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,

$$0 \leq D(g||\phi_K) = \int g \log \left(\frac{g}{\phi_K}\right) = -h(g) - \int g \log \phi_K$$

$$\overset{(a)}{=} -h(g) - \int \phi_K \log \phi_K = -h(g) + h(\phi_K).$$

(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 αποδειχτεί 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), $\mathrm{Vol}\left(A_\epsilon^{(n)}\right) \approx 2^{nh(X)}$. Επομένως, ο "χώρος" στον οποίο περιέχονται οι τυπικές ακολουθίες έχει πλευρά μήκους $\approx 2^{h(X)}$ *ανά διάσταση*.

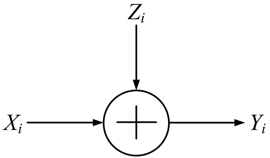
Το Γκαουσιανό Κανάλι. Θεώρημα Κωδικοποίησης

Το Γκαουσιανό Κανάλι – Εισαγωγή

- Κανάλι διακριτού χρόνου με συνεχές αλφάβητο.
- Σχέση Εισόδου-Εξόδου

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

  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

- **Ορισμός 11.8.** 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

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

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

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

Χωρητικότητα Γκαουσιανού Καναλιού με περιορισμό ισχύος (3)

- $Y = X + N$. 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.
- Προκειμένου να έχουμε $Var(X) = P$ πρέπει $\mathbb{E}[X] = 0$ ούτως ώστε $Var(X) = \mathbb{E}[X^2] = P$. Διαισθητικά, αν $\mathbb{E}[X] \neq 0$ χάνουμε ισχύ για να "πολώσουμε" τη X σε μη μηδενική μέση τιμή.
- Άρα, η πληροφοριακή χωρητικότητα του Γκαουσιανού καναλιού επιτυγχάνεται με χρήση Γκαουσιανής εισόδου $X \sim \mathcal{N}(0, P)$ και $C = \frac{1}{2} \log \left(1 + \frac{P}{N}\right)$.
- Απομένει να αποδείξουμε ότι η "πληροφοριακή" χωρητικότητα του Γκαουσιανού καναλιού ισούται με τη "λειτουργική" του χωρητικότητα.

Θεώρημα κωδικοποίησης (ευθύ)

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 βιβλίου των Cover & Thomas. 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 (από το Νόμο των Μεγάλων Αριθμών). Συνεπώς, και η συνολική πιθανότητα σφάλματος μπορεί να γίνει αυθαίρετα μικρή, όπως και στην περίπτωση του διακριτού καναλιού χωρίς μνήμη.

Θεώρημα κωδικοποίησης (αντίστροφο)

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)

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

- Επομένως, μπορούμε να γράψουμε

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

(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, $\mathbb{E}\left[Y_i^2\right] = P_i + N$ και $h(Y_i) \leq \frac{1}{2} \log 2\pi e(P_i + N)$.
- Συνεπώς,

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

Θεώρημα Κωδικοποίησης για το Γκαουσιανό κανάλι (αντίστροφο) (5)

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

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

$$\overset{(b)}{\leq} \frac{1}{2}\log\left(1+\frac{P}{N}\right).$$

(a) από την ανισότητα Jensen. (b) δεδομένου ότι οι κωδικές λέξεις ικανοποιούν τον περιορισμό ισχύος, $\frac{1}{n}\sum_i P_i \leq P$.

- 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 $R > C$.

Κωδικοποίηση καναλιού με κόστος

- Η μετάδοση στο Γκαουσιανό κανάλι με περιορισμό ισχύος είναι ειδική περίπτωση της κωδικοποίησης με κόστος.
- Στην κωδικοποίηση με κόστος, σε κάθε σύμβολο $x \in \mathcal{X}$ της πηγής αντιστοιχεί μία τιμή κόστους $b(x) \geq 0$ και επιβάλλεται ο περιορισμός $\sum_{i=1}^{n} b(x_i(m)) \leq nB$ για κάθε κωδική λέξη $x^n(m)$.
- Αποδεικνύεται (δείτε π.χ. El Gamal & Kim, *Network Information Theory*) ότι η χωρητικότητα Διακριτού Καναλιού Χωρίς Μνήμη με περιορισμό κόστους B ισούται με

$$C(B) = \max_{p(x):\mathbb{E}[b(X)] \leq B} I(X;Y).$$

- Αποδεικνύεται, επίσης, ότι η $C(B)$ (η οποία ονομάζεται συνάρτηση χωρητικότητας-κόστους (cost-capacity function)) είναι αύξουσα, κοίλη $\cap$ και συνεχής συνάρτηση του κόστους B.

Sphere packing

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 $\epsilon \to 0$).

Γεωμετρικό Επιχείρημα (Sphere Packing Argument) (2)

- Μάλιστα, με πιθανότητα που τείνει στο 1, το διάνυσμα βρίσκεται στο φλοιό της σφαίρας (δείτε και Φυλλάδιο 8).
- Έστω σφαίρα n διαστάσεων. Ο όγκος της δίνεται από τη σχέση $C_n r^n$. Επομένως, ο λόγος του όγκου του φλοιού πάχους $\epsilon > 0$ προς τον όγκο της σφαίρας ισούται με

$$\frac{r^n - (r-\epsilon)^n}{r^n} = 1 - \left(1 - \frac{\epsilon}{r}\right)^n \to 1 \text{ για } n \to \infty.$$

- Με χρήση του νόμου των μεγάλων αριθμών, υπάρχει n_0 τέτοιο ώστε, για $n > n_0$ και ακολουθία $\mathbf{x} = x^n$, το διάνυσμα $\mathbf{x} + \mathbf{z}$ να βρίσκεται στο φλοιό σφαίρας n διαστάσεων πάχους ϵ με κέντρο $\mathbf{x}$ και ακτίνα $\sqrt{n\mathbb{E}[||\mathbf{z}||^2]}$ με πιθανότητα αυθαίρετα κοντά στο 1.

Γεωμετρικό Επιχείρημα (Sphere Packing Argument) (3)

- 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) (4)