EE728
Προχωρημένα Θέματα Θεωρίας Πληροφορίας

Δημήτρης-Αλέξανδρος Τουμπακάρης

Τμήμα ΗΜ&ΤΥ, Πανεπιστήμιο Πάτρας

17 Φεβρουαρίου 2010

Γενικές Πληροφορίες

- Διδάσκων: Δημήτρης - Αλέξανδρος Τουμπακάρης. `dtouba@upatras.gr`
- Γραφείο: 2ος όροφος Νέας Πτέρυγας. Τηλ: 2610-99-6468.
- Σκοπός του μαθήματος: Εμβάθυνση σε θέματα Θεωρίας Πληροφορίας, μεγαλύτερη μαθηματική αυστηρότητα, εισαγωγή στη Θεωρία Πληροφορίας Δικτύων.
- Ειδικότερα, στόχοι του μαθήματος είναι:
  - Να εμβαθύνει σε έννοιες/αποτελέσματα της Θεωρίας Πληροφορίας που παρουσιάστηκαν στο μάθημα "Θεωρία Πληροφορίας".
  - Να παρουσιάσει τις αποδείξεις κάποιων από αυτά τα αποτελέσματα.
  - Να επεκταθεί στα κανάλια πολλών χρηστών (Network Information Theory) και, εάν ο χρόνος το επιτρέψει, σε Θεωρία Ρυθμού-Παραμόρφωσης (Rate Distortion Theory) ή/και Πολυπλοκότητα κατά Kolmogorov.

Γενικές Πληροφορίες (συνέχεια)

- Προαπαιτούμενες γνώσεις:
  - Θεωρία Πιθανοτήτων και Αρχές Συνδυαστικής
  - Γνώση της ύλης του μαθήματος "Θεωρία Πληροφορίας" (πλην της Θεωρίας Κωδικοποίησης) ή διάθεση για εκμάθησή της κατά τη διάρκεια των πρώτων εβδομάδων διδασκαλίας.

Θέματα προς συζήτηση

- Παραδόσεις: Τετάρτη 3:15 - 6 μ.μ., ΕΕΤ. 3 45λεπτα παραδόσεων και 2 15λεπτα διαλείμματα.
- Ώρες γραφείου: Τακτικές (ποια ημέρα;) ή κατόπιν συνεννόησης.
- Παρακαλώ γραφτείτε στο eclass (EE728) για να λαμβάνετε τις ανακοινώσεις σχετικά με το μάθημα.
- Τρόπος εξέτασης:
  - Ίδιος τρόπος εξέτασης για προπτυχιακούς και μεταπτυχιακούς φοιτητές.
  - Γραπτή τελική εξέταση, ανοιχτά βιβλία και σημειώσεις.
  - Προαιρετική Εργασία (project).
  - Βαθμός = $\max\{(\text{Τελικό διαγώνισμα}\times 0.5+\text{project}\times 0.5), \text{Τελικό διαγώνισμα}\}$, εφόσον ο βαθμός τελικού διαγωνίσματος ισούται τουλάχιστον με 5. Αλλιώς, Βαθμός = Τελικό Διαγώνισμα.

Βιβλία/Συγγράμματα

- Το μάθημα θα βασιστεί σε μεγάλο βαθμό στο βιβλίο των T. Cover & J. Thomas: Elements of Information Theory, 2nd Ed., Wiley 2006.
- Ένα αντίτυπο της 1ης έκδοσης και ένα αντίτυπο της 2ης έκδοσης θα παραμένει στη βιβλιοθήκη (δε δανείζεται). Επίσης, το βιβλίο θα διατίθεται για ολιγόωρο δανεισμό από το διδάσκοντα.
- Στις διαλέξεις θα χρησιμοποιηθούν διαφάνειες.
- Επειδή ο διδάσκων δεν έχει εντοπίσει κάποιο βιβλίο στην Ελληνική γλώσσα το οποίο να καλύπτει σε ικανοποιητικό βαθμό το αντικείμενο του μαθήματος έχει ζητηθεί να δοθεί στους φοιτητές ένα από τα βιβλία
    - Elements of Information Theory, 2nd ed. των T. M. Cover και J. A. Thomas.
    - Information Theory and Reliable Communication, του R. G. Gallager.

Βιβλία/Συγγράμματα (2)

- Πριν από λίγες ημέρες ο εκδοτικός οίκος Wiley αποφάσισε να μη διαθέτει, πλέον, βιβλία στα Πανεπιστήμια σε έντυπη μορφή.
  - Γίνονται προσπάθειες να σας δοθεί Ηλεκτρονικό Σύγγραμμα. Θα σας ενημερώνω κατά τη διάρκεια του Εξαμήνου.
  - Ωστόσο, το βιβλίο του Gallager δε διατίθεται σε Ηλεκτρονική μορφή. Επομένως, πιθανότατα δε θα σας δοθεί, ακόμα και αν το επιλέξετε.
- Αντιστοιχία μαθήματος – βιβλίου Cover & Thomas (2η έκδοση).
  - Εντροπία και Κωδικοποίηση Πηγής. Κεφάλαια 2, 3, 4 και 5.
  - Χωρητικότητα και Κωδικοποίηση Καναλιού. Κεφάλαια 7, 8 και 9.
  - Θεωρία Πληροφορίας Δικτύων. Κεφάλαιο 15.
  - Θεωρία Ρυθμού-Παραμόρφωσης. Κεφάλαιο 10.
  - Πολυπλοκότητα κατά Kolmogorov. Κεφάλαιο 14.

Βιβλία/Συγγράμματα (3)

- R. G. Gallager, Information Theory and Reliable Communication. Ιστορικό βιβλίο. Καλύπτει λιγότερες πλευρές της Θεωρίας Πληροφορίας σε σχέση με το βιβλίο των Cover & Thomas, αλλά υπεισέρχεται σε μεγαλύτερο βάθος. Έπίσης, καλύπτει και μέρος της Θεωρίας Κωδικοποίησης. Απαραίτητο σε όσους επιθυμούν να εμβαθύνουν.
- D. McKay, Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003. Διατίθεται δωρεάν στο Διαδίκτυο αρκεί να μην το τυπώσετε. Δίνει αρκετά παραδείγματα. Επίσης, επικεντρώνεται αρκετά στη Θεωρία Κωδικοποίησης, καθώς και στην εξαγωγή συμπερασμάτων (inference).
- D. Tse & P. Viswanath, Fundamentals of Wireless Communication, Cambridge University Press, 2005. Δεν είναι βιβλίο Θεωρίας Πληροφορίας. Ωστόσο, αναφέρεται συχνά σε αποτελέσματα της Θεωρίας Πληροφορίας και περιέχει ενδιαφέρουσες συζητήσεις για θέματα που άπτονται των Ασύρματων Συστημάτων Τηλεπικοινωνιών. Διατίθεται και αυτό δωρεάν στο Διαδίκτυο (σε μη εκτυπώσιμο αρχείο).
- Ένας πιο πλήρης κατάλογος βιβλιογραφίας δίνεται στο Φυλλάδιο 2.

Σύνδεσμοι σε παρόμοια μαθήματα άλλων πανεπιστημίων

- Stanford University: EE 376A/B/Stat 376A/B: Information Theory. `www.stanford.edu/class/ee376a` και `ee376b`.
- Stanford University: EE 478: Network Information Theory `http://eeclass.stanford.edu/ee478/`
- University of Minnesota: EE5581: Information Theory and Coding `http://www.ece.umn.edu/users/nihar/ee5581_fall05/index.html`
- UIUC: ECE 563, Information Theory `http://courses.ece.uiuc.edu/ece563/`
- Hebrew University, Information Theory of Wideband Communication Systems (67891) `http://www.cs.huji.ac.il/~dporrat/WidebandCourse.html`
- Brown University, AM 193/272/IT3: Information Theory I/II/III `http://www.dam.brown.edu/people/yiannis/IT1/index.html` `yiannis/272/index.html`, `yiannis/IT3/index.html`
- Πολυτεχνείο Κρήτης, ΤΗΛ 412, Θεωρία Πληρηφορίας και Κωδίκων, `http://www.telecom.tuc.gr/courses/tel412/`.

Ύλη Μαθήματος

- Επανάληψη Βασικών Εννοιών/Αποτελεσμάτων του μαθήματος "Θεωρία Πληροφορίας" (7ου εξαμήνου).
- Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (AEP). Η εντροπία είναι ο βέλτιστος ρυθμός συμπίεσης. Κωδικοποίηση σταθερού και μεταβλητού μήκους (περιληπτικά, θεωρώντας γνωστά τα περί κωδίκων που αναφέρθηκαν στη "Θεωρία Πληροφορίας").
- Χωρητικότητα Καναλιού. Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP). Θεώρημα Χωρητικότητας Καναλιού για Διακριτά Κανάλια Χωρίς Μνήμη (απόδειξη).
- Συνεχείς τ.μ. Διαφορική Εντροπία. Χωρητικότητα Γκαουσιανού Καναλιού. Παράλληλα Γκαουσιανά Κανάλια. Γκαουσιανό κανάλι με ανάδραση.
- Κανάλια Πολλών Χρηστών: Κανάλι Πολλαπλής Πρόσβασης (MAC), Κανάλι Ευρυεκπομπής (BC), Κανάλι Μεταγωγής (Relay), Κανάλι Παρεμβολών (Interference). Κατανεμημένη συμπίεση και Θεώρημα Slepian-Wolf.
- Εάν προλάβουμε: Θεωρία Ρυθμού–Παραμόρφωσης (Rate Distortion Theory) ή/και Πολυπλοκότητα κατά Kolmogorov.

Περιεχόμενα σημερινού μαθήματος

1. Εισαγωγή στη Θεωρία Πληροφορίας
2. Προεπισκόπηση Μαθήματος
   - Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (AEP)
   - Χωρητικότητα Καναλιού και Από Κοινού (Joint) AEP
   - Θεωρία Πληροφορίας Δικτύων (Network Information Theory)
3. Επανάληψη Βασικών Μεγεθών Θεωρίας Πληροφορίας
   - Εντροπία, Δεσμευμένη και Σχετική Εντροπία, Αμοιβαία Πληροφορία

Αντιστοιχία σημερινής διάλεξης με βιβλία Cover & Thomas και Gallager

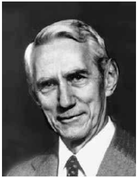
- Βιβλίο Cover & Thomas (2η έκδοση): Κεφ. 1, Κεφ. 2.1 – 2.5.
- Βιβλίο Gallager: Κεφ. 1, Κεφ. 2.1 – 2.3

Εισαγωγή στη Θεωρία Πληροφορίας

- Θεωρία Πληροφορίας: Μια γενική και κατ' εξοχήν *μαθηματική* θεωρία.
- Θεμελιωτής της θεωρείται ο Claude Shannon.
- Ξεκίνησε με σκοπό να κατανοήσει τα Συστήματα Επικοινωνιών (Claude Shannon, ``*A mathematical theory of communication,*'' The Bell System Technical Journal, 1948).
- Ωστόσο, είναι μια αρκετά γενική θεωρία με ευρύ πεδίο εφαρμογής
    - Τηλεπικοινωνίες
    - Θεωρία Πιθανοτήτων (Εκτίμηση/έλεγχος υποθέσεων)
    - Στατιστική (διεξαγωγή συμπερασμάτων)
    - Οικονομικά/Χρηματιστήριο/Τζόγος
    - Επιστήμη Υπολογιστών (Αλγοριθμική Πολυπλοκότητα)
    - Στατιστική Φυσική (Θερμοδυναμική)
    - κ.α.

Εισαγωγή στη Θεωρία Πληροφορίας (2)

- Η Θεωρία Πληροφορίας απαντά σε 2 βασικά ερωτήματα της Θεωρίας Επικοινωνιών:
  1. Ποια είναι η μέγιστη δυνατή συμπίεση των δεδομένων μιας πηγής; $\rightarrow$ Η εντροπία (entropy) H.
  2. Ποιος είναι ο μέγιστος ρυθμός επικοινωνίας (rate of communication) δια μέσου ενός καναλιού; $\rightarrow$ Η χωρητικότητα (capacity) C.
- Ωστόσο, έχει σημαντική συνεισφορά σε πολλά άλλα προβλήματα και αντικείμενα, όπως προαναφέρθηκε.



Claude Shannon, 1916-2001

Προεπισκόπηση μαθήματος

1. Εισαγωγή στη Θεωρία Πληροφορίας

2. Προεπισκόπηση Μαθήματος
   - Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (AEP)
   - Χωρητικότητα Καναλιού και Από Κοινού (Joint) AEP
   - Θεωρία Πληροφορίας Δικτύων (Network Information Theory)

3. Επανάληψη Βασικών Μεγεθών Θεωρίας Πληροφορίας
   - Εντροπία, Δεσμευμένη και Σχετική Εντροπία, Αμοιβαία Πληροφορία

Εντροπία, Αμοιβαία Πληροφορία, Συμπίεση

- Μια τυχαία μεταβλητή ή, γενικότερα, μια τυχαία διαδικασία (στοχαστική ανέλιξη – random process) χαρακτηρίζεται από ένα όριο πολυπλοκότητας (εντροπία) κάτω από το οποίο δεν είναι δυνατόν να συμπιεστεί.
- Ιδιότητες εντροπίας, σχετικής εντροπίας, αμοιβαίας πληροφορίας (επανάληψη από το μάθημα "Θεωρία Πληροφορίας")
- Ανισότητα Fano: Χρήσιμη στην απόδειξη του Θεωρήματος Κωδικοποίησης Καναλιού (2ο Θεώρημα Shannon). Συνδέει την πιθανότητα σφάλματος στην εκτίμηση μιας τ.μ. X με βάση παρατήρηση τ.μ. Y με τη δεσμευμένη εντροπία $H(X|Y)$.
- Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (Asymptotic Equipartition Property -- AEP). Αναφέρθηκε στο μάθημα "Θεωρία Πληροφορίας"· θα την εξετάσουμε με μεγαλύτερη λεπτομέρεια στα Προχωρημένα Θέματα.
- Θεώρημα Κωδικοποίησης Πηγής: Μπορούμε να συμπιέσουμε τα σύμβολα εργοδικής πηγής με απόσταση το πολύ 1 bit από την εντροπία και σε καμία περίπτωση με λιγότερα bits από την εντροπία (εκτός αν δεχτούμε απώλεια πληροφορίας). Θα το αποδείξουμε (για πηγές χωρίς μνήμη).

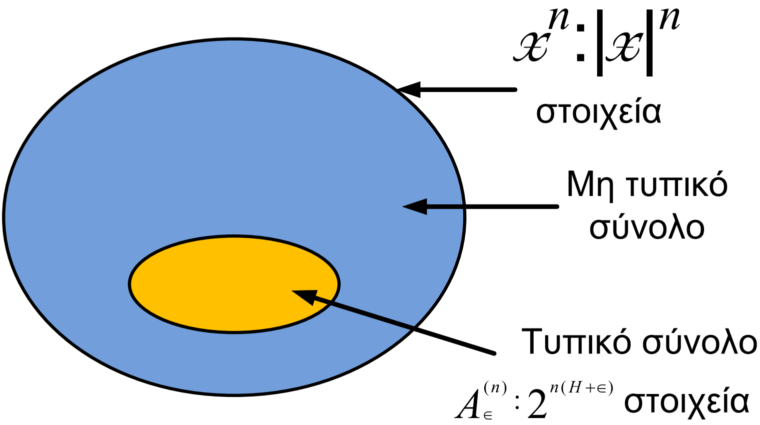
Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (AEP)

- Ο Νόμος των Μεγάλων Αριθμών στη Θεωρία Πληροφορίας, του οποίου αποτελεί επαναδιατύπωση.
- AEP (για ανεξάρτητες, ομοίως κατανεμημένες (i.i.d.) τ.μ.): Καθώς το n τείνει στο άπειρο, η ποσότητα $\frac{1}{n}\log\frac{1}{p(X_1,X_2,\ldots,X_n)}$ τείνει στην εντροπία H. Επομένως, $p(X_1, X_2, \ldots, X_n) \to 2^{-nH}$.
- Χωρισμός ακολουθιών μήκους n σε δύο σύνολα: Τυπικό (κάθε ακολουθία του οποίου έχει πιθανότητα $\sim 2^{-nH}$) και μη τυπικό (όλες οι υπόλοιπες ακολουθίες).

Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (AEP) (2)

- Θα αποδείξουμε ότι το άθροισμα των πιθανοτήτων των τυπικών ακολουθιών τείνει στο 1 καθώς το n τείνει στο άπειρο και ότι το τυπικό σύνολο περιέχει $\sim 2^{nH}$ τυπικές ακολουθίες.
- Επομένως, μπορούμε να ασχοληθούμε μόνο με τις τυπικές ακολουθίες. Καθώς το μήκος τους, n, μεγαλώνει, η πιθανότητα να εμφανιστεί μη τυπική ακολουθία τείνει στο 0.
- Θα αποδείξουμε ότι με τον τρόπο αυτό μπορούμε να περιγράψουμε τις τ.μ. X_i με μέσο μήκος που τείνει στην εντροπία H.

Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (AEP) (3)



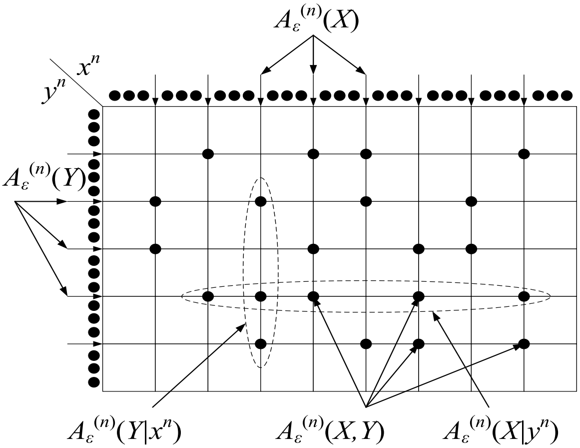
Χωρητικότητα Καναλιού

- "Πληροφοριακός" Ορισμός Χωρητικότητας (information capacity), συμμετρικά κανάλια, παραδείγματα (επανάληψη).
- Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP).
- "Λειτουργικός" Ορισμός Χωρητικότητας. Θεώρημα Κωδικοποίησης Καναλιού Shannon και απόδειξη (για διακριτά κανάλια χωρίς μνήμη).
- Χωρητικότητα καναλιού με ανάδραση.
- Θεώρημα διαχωρισμού καναλιού-πηγής.
- Συνεχείς τ.μ. και Διαφορική Εντροπία.
- Χωρητικότητα Γκαουσιανού Καναλιού.
- Χωρητικότητα Παράλληλων Γκαουσιανών Καναλιών και ``waterfilling''.
- Χωρητικότητα Γκαουσιανού Καναλιού με ανάδραση.

Joint AEP

- Joint AEP: Έστω n ανεξάρτητα, ομοίως κατανεμημένα ζεύγη (X_i, Y_i) (οι X_i και Y_i δεν είναι, κατ' ανάγκη, ανεξάρτητες μεταξύ τους).
    - Καθώς το n τείνει στο άπειρο, $p((X_1, Y_1), (X_2, Y_2) \ldots, (X_n, Y_n)) \to 2^{-nH(X,Y)}$.
- Εάν οι $\tilde{X}_i$ και $\tilde{Y}_i$ είναι ανεξάρτητες με τις ίδιες περιθώριες κατανομές με αυτές των X_i και Y_i, αντίστοιχα, τότε η πιθανότητα η ακολουθία $(\tilde{X}_1, \tilde{Y}_1), (\tilde{X}_2, \tilde{Y}_2) \ldots, (\tilde{X}_n, \tilde{Y}_n)$ να είναι τυπική τείνει στην τιμή $2^{-nI(X;Y)}$.
- Επομένως, η πιθανότητα μια ακολουθία $(\tilde{X}_1, \tilde{Y}_1), (\tilde{X}_2, \tilde{Y}_2) \ldots, (\tilde{X}_n, \tilde{Y}_n)$ της οποίας οι $\tilde{X}_i$ και $\tilde{Y}_i$ είναι, στην πραγματικότητα, ανεξάρτητες να ανήκει στο τυπικό σύνολο ακολουθιών που δημιουργούνται επιλέγοντας τις τ.μ. με βάση την από κοινού συνάρτηση μάζας πιθανότητας $p(X, Y)$ (όχι, απαραίτητα, ίση με $p(X)p(Y)$), ισούται, κατά προσέγγιση, με $2^{-nI(X;Y)}$.
- Θα χρησιμοποιήσουμε την Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης στην απόδειξη του Θεωρήματος Κωδικοποίησης Καναλιού του Shannon.

Joint AEP (2)



Από Κοινού Τυπικές Ακολουθίες

Προεπισκόπηση Μαθήματος
Συνεχείς τ.μ. και Γκαουσιανό Κανάλι

- Προκειμένου να χαρακτηρίσουμε την πληροφορία, να συμπιέσουμε και να μεταδώσουμε συνεχείς τ.μ. (ή διακριτές τ.μ. σε κανάλια με συνεχείς τιμές) ορίζουμε τη Διαφορική Εντροπία.
- Γενικά, τα αποτελέσματα είναι παρόμοια με την περίπτωση διακριτών τ.μ., αλλά και με κάποιες διαφορές.
- Το Γκαουσιανό Κανάλι αποτελεί ένα πολύ καλό μοντέλο για κανάλια που απαντούν στη φύση. Η έκφραση για τη χωρητικότητα του Γκαουσιανού καναλιού αποτελεί ένα από τα πιο διάσημα αποτελέσματα της Θεωρίας Πληροφορίας.
- Θα εξετάσουμε το Γκαουσιανό Κανάλι με μεγαλύτερη λεπτομέρεια απ' ό,τι στο μάθημα "Θεωρία Πληροφορίας"
- Θα αποδείξουμε το Θεώρημα Κωδικοποίησης Καναλιού για Γκαουσιανά Κανάλια με πηγές που υπόκεινται σε περιορισμό ισχύος.

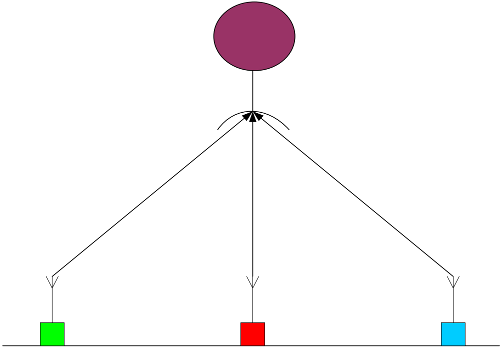
Συνεχείς τ.μ. και Γκαουσιανό Κανάλι (συνέχεια)

- Θα εξετάσουμε την περίπτωση όπου ένας πομπός έχει στη διάθεσή του περισσότερα από ένα ανεξάρτητα Γκαουσιανά κανάλια με διαφορετικό λόγο ισχύος σήματος προς ισχύ θορύβου (SNR) και δεδομένη διαθέσιμη ισχύ με την οποία μπορεί να μεταδώσει.
- Θα αποδείξουμε ότι είναι βέλτιστο να χρησιμοποιήσουμε μεγαλύτερο μέρος της διαθέσιμης ισχύος στα κανάλια με μεγάλο SNR. Δηλαδή, πρέπει να μεταδώσουμε με μεγαλύτερο ρυθμό στα "καλά" κανάλια και με μικρότερο (σε κάποιες περιπτώσεις ακόμα και μηδενικό) στα "κακά".
- Η κατανομή, αυτή, της ισχύος (``waterfilling'') βρίσκει σημαντικές εφαρμογές στα συστήματα DSL, καθώς και σε ασύρματα συστήματα που μεταδίδουν σε κανάλια με διαλείψεις (fading).
- Θα εξετάσουμε, επίσης, την περίπτωση Γκαουσιανών καναλιών με έγχρωμο θόρυβο και τη χωρητικότητά τους, καθώς και Γκαουσιανά κανάλια με ανάδραση.

Θεωρία Πληροφορίας Δικτύων (Network Info Theory)

- Συστήματα με περισσότερους από έναν πομπούς ή/και περισσότερους από έναν δέκτες.
- Νέα στοιχεία: Παρεμβολή (interference), συνεργασία (cooperation) και ανάδραση (feedback).
- Το γενικό πρόβλημα είναι εύκολο να μοντελοποιηθεί, αλλά πολύ δύσκολο να επιλυθεί. Η γενική λύση του προβλήματος δεν έχει βρεθεί έως σήμερα.
- Στη γενική περίπτωση αναφερόμαστε, πλέον, σε περιοχές χωρητικότητας (capacity regions) και σε περιοχές ρυθμών μετάδοσης (rate regions), δεδομένου ότι, λόγω παρεμβολών και συνεργασίας, ο μέγιστος ρυθμός μετάδοσης κάθε χρήστη εξαρτάται από τους ρυθμούς μετάδοσης των άλλων χρηστών (στη γενική περίπτωση).

Κανάλι Πολλαπλής Πρόσβασης (Multiple Access Channel)



- Πολλοί χρήστες που επιθυμούν να επικοινωνήσουν με ένα κεντρικό σταθμό. Παράδειγμα: Κινητά τερματικά προς σταθμό βάσης.
- Το κανάλι πολλών χρηστών που έχει κατανοηθεί καλύτερα από τα άλλα.

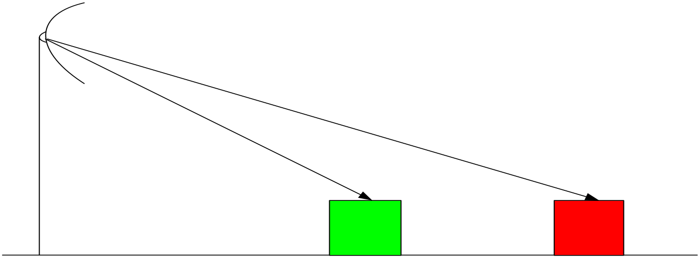
Γκαουσιανό Κανάλι Πολλαπλής Πρόσβασης

- Για το Γκαουσιανό MAC 2 χρηστών (δηλαδή MAC με Γκαουσιανό θόρυβο στο δέκτη) με περιορισμούς ισχύος P_1 και P_2 και διασπορά θορύβου N στο δέκτη η περιοχή χωρητικότητας δίνεται από τη λύση του παρακάτω συνόλου ανισοτήτων:

$R_1 < C\left(\frac{P_1}{N}\right)$, $R_2 < C\left(\frac{P_2}{N}\right)$ και $R_1 + R_2 < C\left(\frac{P_1+P_2}{N}\right)$,
όπου $C(x) = \frac{1}{2}\log(1+x)$.

- Η πολυπλεξία στο χρόνο (TDM) δεν είναι βέλτιστη στη γενική περίπτωση! Το βέλτιστο είναι όλοι οι χρήστες να εκπέμπουν ταυτόχρονα.
- Θα δούμε, επίσης, ότι, καθώς ο αριθμός των χρηστών αυξάνει, το άθροισμα των ρυθμών μετάδοσής τους τείνει στο άπειρο.
    - Παρόλο που η είσοδος νέων χρηστών δημιουργεί επιπρόσθετη παρεμβολή, η ισχύς που "φέρνει" κάθε νέος χρήστης οδηγεί σε αύξηση της συνολικής χωρητικότητας (στο Γκαουσιανό κανάλι).

Κανάλι Ευρυεκπομπής (Broadcast Channel)



- Ένας κεντρικός σταθμός που επιθυμεί να στείλει (διαφορετική) πληροφορία σε περισσότερους από έναν χρήστες.
- Δεν έχει κατανοηθεί πλήρως, εκτός από ειδικές περιπτώσεις (π.χ. Γκαουσιανός θόρυβος στους δέκτες).

Γκαουσιανό Κανάλι Ευρυεκπομής

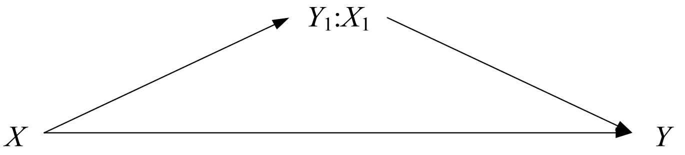
- Έστω Γκαουσιανό BC 2 χρηστών. Ο δέκτης εκπέμπει με ισχύ P και στέλνει διαφορετικά (και ανεξάρτητα) μηνύματα στους χρήστες. Έστω, επίσης, ότι για τις ισχείς (διασπορές) θορύβου των χρηστών, $N_1 < N_2$.
- Η περιοχή χωρητικότητας του Γκαουσιανού BC δίνεται από τη λύση των ανισοτήτων

$$R_1 < C\left(\frac{\alpha P}{N_1}\right) \text{ και } R_2 < C\left(\frac{(1-\alpha)P}{\alpha P + N_2}\right),$$

όπου $0 \leq \alpha \leq 1$, ανάλογα με την επιθυμητή αναλογία ρυθμών μετάδοσης.

- Θα δούμε ότι ο (αδύναμος) χρήστης 2 αποκωδικοποιεί μόνο το μήνυμα που προορίζεται για αυτόν, ενώ ο (ισχυρός) χρήστης 1 αποκωδικοποιεί και τα δύο μηνύματα.
- Όπως και για το MAC, η πολυπλεξία στο χρόνο *δεν* είναι πάντοτε η βέλτιστη στρατηγική χρήσης του καναλιού.

Κανάλι Μεταγωγής (Relay Channel)



- Ένας πομπός και ένας δέκτης, με ενδιάμεσους μεταγωγούς οι οποίοι υποβοηθούν την επικοινωνία (και δε στέλνουν/λαμβάνουν δικά τους μηνύματα).
- Στη γενική περίπτωση, οι μεταγωγοί *δεν* εκπέμπουν το ίδιο σήμα με αυτό που λαμβάνουν.

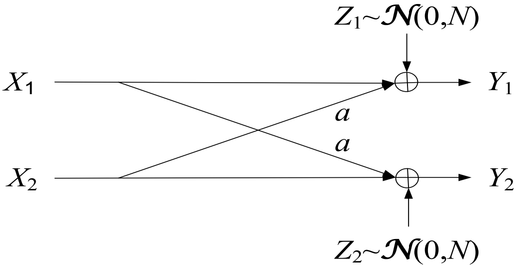
Γκαουσιανό Κανάλι Μεταγωγής

- Έστω ότι ο πομπός εκπέμπει με ισχύ P, ενώ ο μεταγωγός εκπέμπει με ισχύ P_1. Η ισχύς θορύβου στο δέκτη του μεταγωγού ισούται με N_1, ενώ στον τελικό δέκτη με N_2.
- Αποδεικνύεται ότι η χωρητικότητα δίνεται από τη σχέση

$$C = \max_{0 \leq \alpha \leq 1} \min \left\{ C\left(\frac{P + P_1 + 2\sqrt{(1-\alpha)PP_1}}{N_1 + N_2} \right), C\left(\frac{\alpha P}{N_1} \right) \right\}.$$

- Εάν $P_1/N_2 \geq P/N_1$, δηλαδή ο λόγος σήματος προς θόρυβο στον τελικό δέκτη είναι μεγαλύτερος από το λόγο σήματος προς θόρυβο στο δέκτη του μεταγωγού, αποδεικνύεται ότι $\alpha = 1$ και $C = C(P/N_1)$. Επομένως, το κανάλι μετά το μεταγωγό "φαίνεται" αθόρυβο. Προσοχή: ο μεταγωγός δε στέλνει το ίδιο σήμα με αυτό που λαμβάνει.
- Ο τρόπος μετάδοσης δεν είναι προφανής, αλλά είναι πολύ ενδιαφέρων. Περισσότερες λεπτομέρειες σε μεταγενέστερη διάλεξη.

Κανάλι Παρεμβολής (Interference Channel)

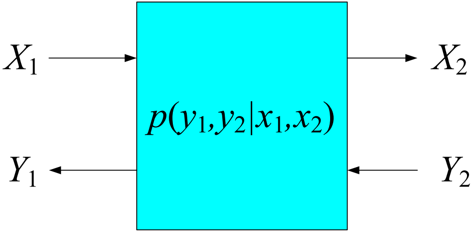


- K πομποί και K δέκτες με διαφωνία (crosstalk). Ο κάθε πομπός θέλει να στείλει πληροφορία στον αντίστοιχο δέκτη χωρίς να ενδιαφέρεται για την επικοινωνία των άλλων ζευγών. Στο σχήμα, $K = 2$.
- Παράδειγμα: Συνεστραμμένα ζεύγη χαλκού (twisted pairs) που βρίσκονται στο ίδιο πλέγμα (bundle) καλωδίων.

Γκαουσιανό Κανάλι Παρεμβολής

- Η περιοχή χωρητικότητας για το Κανάλι Παρεμβολής δεν έχει βρεθεί έως σήμερα, ακόμα και όταν ο θόρυβος είναι Γκαουσιανός.
- Για την περίπτωση ισχυρής παρεμβολής αποδεικνύεται ότι η χωρητικότητα ισούται με την περίπτωση όπου δεν υπάρχει παρεμβολή.
- Η ιδέα: Εάν $C(a^2P/(P+N)) \geq C(P/N)$, όπου a ο συντελεστής παρεμβολής, ο δέκτης 2 μπορεί να αποκωδικοποιήσει το μήνυμα του πομπού 1, εφόσον, βέβαια, γνωρίζει το βιβλίο κωδίκων (codebook) που χρησιμοποιεί ο 1.
- Επομένως, μπορεί να αφαιρέσει την παρεμβολή από το λαμβανόμενο σήμα και, στη συνέχεια, να αποκωδικοποιήσει το μήνυμα του πομπού 2 που προορίζεται για αυτόν.
- Ακριβώς τα ίδια ισχύουν και για το δέκτη 1.

Κανάλι Διπλής Κατεύθυνσης (Two-way Channel)

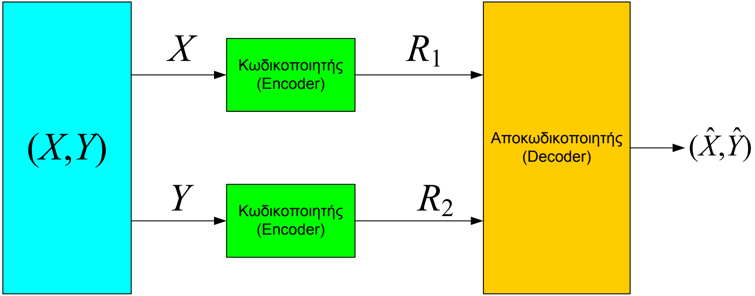


- Δύο σταθμοί οι οποίοι επικοινωνούν μέσω δύο διαύλων.
- Παρόμοιο με το Κανάλι Παρεμβολής, με τη διαφορά ότι ο πομπός 1 συνδέεται με το δέκτη 1 (και ο πομπός 2 συνδέεται με το δέκτη 2).
- Επομένως, ο πομπός 1 μπορεί να χρησιμοποιήσει πληροφορία από σύμβολα που έχουν ληφθεί από το δέκτη 1 πριν εκπέμψει $\rightarrow$ ανάδραση (feedback).
- Η περιοχή χωρητικότητας του Καναλιού Διπλής Κατεύθυνσης δεν είναι γνωστή στη γενική περίπτωση.

Γκαουσιανό Κανάλι Διπλής Κατεύθυνσης

- Η περιοχή χωρητικότητας στην περίπτωση Γκαουσιανού θορύβου είναι γνωστή.
- Έστω ότι ο πομπός 1 και ο πομπός 2 μεταδίδουν με ρυθμό $R_1 < C(P_1/N_1)$ και $R_2 < C(P_2/N_2)$, αντίστοιχα, όπου N_1 (N_2) ο θόρυβος που προστίθεται στο σήμα του πομπού 1 (2).
- Ο δέκτης 2 γνωρίζει το σήμα που εξέπεμψε ο πομπός 2 και, επομένως, μπορεί να το αφαιρέσει από το σήμα που λαμβάνει. Συνεπώς, απομένει να αποκωδικοποιήσει το μήνυμα του πομπού 1 παρουσία Γκαουσιανού θορύβου.
- Ακριβώς τα ίδια ισχύουν και για το δέκτη 1.
- Επομένως, το Γκαουσιανό Κανάλι Διπλής Κατεύθυνσης διαχωρίζεται σε δύο ανεξάρτητα Γκαουσιανά Κανάλια.
- Στη γενική περίπτωση (μη Γκαουσιανού Θορύβου) οι ρυθμοί μετάδοσης των δύο χρηστών δεν είναι ανεξάρτητοι.

Κατανεμημένη Συμπίεση (Distributed Data Compression)



Έστω ότι η X και η Y συμπιέζονται ξεχωριστά (π.χ. σε διαφορετικά σημεία) με σκοπό ένας χρήστης να μπορεί να αποκωδικοποιήσει και τις δύο. Ποιος είναι ο ελάχιστος συνολικός ρυθμός, $R = R_x + R_y$, που απαιτείται για να μεταδοθεί η πληροφορία και των 2 πηγών;

Κατανεμημένη Συμπίεση (2)

- Γνωρίζουμε ότι για να μεταδώσουμε μια πηγή X (χωρίς απώλειες) χρειαζόμαστε ρυθμό τουλάχιστον $H(X)$.
- Για να μεταδώσουμε από κοινού 2 πηγές X και Y (με χρήση κοινού κωδικοποιητή), απαιτείται ρυθμός $R > H(X, Y)$.
- Θεώρημα Κωδικοποίησης Πηγής (Slepian-Wolf): Ακόμα και όταν η συμπίεση των X και Y γίνεται σε διαφορετικά σημεία, αρκεί $R > H(X, Y)$! (καθώς, επίσης, και $R_x > H(X|Y)$ και $R_y > H(Y|X)$).
- Όπως θα δούμε, μόνο ο δέκτης (και όχι οι πομποί) χρειάζεται να γνωρίζει τις τυπικές ακολουθίες.

Θεωρία Ρυθμού-Παραμόρφωσης (Rate Distortion Theory)

- Σε μερικές περιπτώσεις (π.χ. συνεχείς τ.μ.) δεν είναι δυνατόν να επιτευχθεί τέλεια συμπίεση με περιγραφή πεπερασμένου μήκους.
- Σε κάποιες άλλες περιπτώσεις, θέλουμε να συμπιέσουμε τ.μ. περισσότερο από την εντροπία (συμπίεση με απώλειες – lossy compression).
- Μέτρο παραμόρφωσης: Η απόσταση μιας τ.μ. από την αναπαράστασή της.
- Η Θεωρία Ρυθμού-Παραμόρφωσης απαντά στο ερώτημα:
  - Δεδομένων της κατανομής μιας τ.μ. και ενός μέτρου παραμόρφωσης, ποια είναι η ελάχιστη μέση παραμόρφωση για δεδομένο ρυθμό συμπίεσης; Ή, ισοδύναμα,
  - Δεδομένων της κατανομής μιας τ.μ. και ενός μέτρου παραμόρφωσης, ποιο είναι το ελάχιστο μήκος περιγραφής που απαιτείται προκειμένου η παραμόρφωση να μην υπερβεί μια δεδομένη τιμή;

Θεωρία Ρυθμού-Παραμόρφωσης (2)

- Ενδιαφέρον αποτέλεσμα: Είναι καλύτερα να περιγράφουμε τ.μ. από κοινού παρά ξεχωριστά, ακόμα και όταν είναι ανεξάρτητες!
- Γεωμετρική ερμηνεία: Είναι πιο αποδοτικό να κατανέμουμε δεδομένα σημεία σε χώρους μεγαλύτερων διαστάσεων.
  - Αναλογία στη συμπίεση: Πετυχαίνουμε καλύτερη συμπίεση για μεγάλα μήκη ακολουθιών, ακόμα και όταν η πηγή δεν έχει μνήμη.
  - Αναλογία στη μετάδοση: Στη γενική περίπτωση, για να μεταδώσουμε με ρυθμούς κοντά στη χωρητικότητα, χρειαζόμαστε κώδικες μεγάλου μήκους (ακόμα και όταν το κανάλι δεν έχει μνήμη).
- Η Θεωρία Ρυθμού-Παραμόρφωσης μπορεί να εφαρμοστεί τόσο σε συνεχείς όσο και σε διακριτές τ.μ.

Πολυπλοκότητα κατά Kolmogorov

- Είδαμε ότι η εντροπία των ακολουθιών που παράγει μια πηγή εξαρτάται από την κατανομή τους.
- Kolmogorov: Αλγοριθμική πολυπλοκότητα (ή πολυπλοκότητα περιγραφής) ενός αντικειμένου: Το μήκος του συντομότερου προγράμματος υπολογιστή το οποίο περιγράφει το αντικείμενο.
- Δεν απαιτείται η χρήση της κατανομής του αντικειμένου!
- Αποδεικνύεται ότι η μέση πολυπλοκότητα κατά Kolmogorov των ακολουθιών που παράγει μια πηγή ισούται, κατά προσέγγιση, με την εντροπία της.
- Σημαντική παρατήρηση (Kolmogorov): Η αλγοριθμική πολυπλοκότητα δεν εξαρτάται από το συγκεκριμένο υπολογιστή στον οποίο τρέχει το πρόγραμμα.

Επανάληψη Βασικών Ποσοτήτων Θεωρίας Πληροφορίας

1. Εισαγωγή στη Θεωρία Πληροφορίας
2. Προεπισκόπηση Μαθήματος
   - Ιδιότητα Ασυμπτωτικής Ισοδιαμέρισης (AEP)
   - Χωρητικότητα Καναλιού και Από Κοινού (Joint) AEP
   - Θεωρία Πληροφορίας Δικτύων (Network Information Theory)
3. Επανάληψη Βασικών Μεγεθών Θεωρίας Πληροφορίας
   - Εντροπία, Δεσμευμένη και Σχετική Εντροπία, Αμοιβαία Πληροφορία

Τι εννοούμε με τον όρο "κωδικοποίηση";

- Η αναπαράσταση ενός σήματος/μηνύματος από κάποιο άλλο.
- Μια απεικόνιση από ένα σήμα/μήνυμα σε ένα άλλο.
- Ενδέχεται να μην είναι αντιστρέψιμη (κωδικοποίηση με απώλειες – lossy compression).
- Σε τι χρησιμεύει η κωδικοποίηση;
  1. Συμπίεση (Κωδικοποίηση πηγής)
  2. Μετάδοση μέσω καναλιού (Κωδικοποίηση καναλιού)
  3. Μετατροπή σήματος/μηνύματος σε μορφή την οποία μπορούμε να επεξεργαστούμε. Παράδειγμα: Κβαντισμός συνεχούς σήματος, μετατροπή σήματος σε δυαδική μορφή.
  4. Προστασία δεδομένων και πνευματικής ιδιοκτησίας (Κρυπτογραφία, Υδατογράφηση).

Εντροπία διακριτής τ.μ.

Έστω διακριτή τ.μ. X με συνάρτηση μάζας πιθανότητας (pmf) $p(x)$.

$$H(X) = E_p\left[\log \frac{1}{p(X)}\right] = \sum_x p(x) \log \frac{1}{p(x)} = -\sum_x p(x) \log p(x).$$

- $\log \frac{1}{p(x)}$: Η πληροφορία που περιέχεται στο ενδεχόμενο $X = x$.
- Η $H(X)$ δεν εξαρτάται από τις τιμές της X, παρά μόνο από την κατανομή της.
- $H(X)$: Το όριο συμπίεσης.
  - Το μέσο μήκος της συντομότερης περιγραφής της X
  - Η μέση πληροφορία που περιέχεται στη X.
  - Η μέση αβεβαιότητα που έχουμε για τη X (πριν μας αποκαλυφθεί η τιμή της).
- Μονάδα μέτρησης: bit ($\log \to \log_2$). Σπανιότερα, nat ($\log \to \ln$).
- $H_b(X) = \log_b a \cdot H_a(X)$.
- Από εδώ και στο εξής $\log$ υπονοεί $\log_2$ (αν και δεν έχει ιδιαίτερη σημασία ποια μονάδα χρησιμοποιούμε).

Από κοινού και υπό συνθήκη εντροπία

- Από κοινού (συνδυασμένη) εντροπία (joint entropy) 2 τ.μ. με από κοινού pmf $p(x, y)$:

$$H(X, Y) = E_p\left[\log \frac{1}{p(X, Y)}\right] = \sum_x \sum_y p(x, y) \log \frac{1}{p(x, y)} = -\sum_x \sum_y p(x, y) \log p(x, y).$$

- Δεσμευμένη εντροπία (conditional entropy) της τ.μ. X δεδομένης της τ.μ. Y:

$$H(X|Y) = E_p\left[\log \frac{1}{p(X|Y)}\right] = \sum_x \sum_y p(x, y) \log \frac{1}{p(x|y)}$$
$$= -\sum_x \sum_y p(x, y) \log p(x|y) = -\sum_x \sum_y p(y) p(x|y) \log p(x|y)$$
$$= -\sum_y p(y) \sum_x p(x|y) \log p(x|y) = \sum_y H(X|Y = y).$$

Ιδιότητες Εντροπίας διακριτής τ.μ.

- $H(X) \geq 0$.
- Η εντροπία είναι κοίλη ($\cap$) συνάρτηση της συνάρτησης μάζας πιθανότητας $p(x)$. Θα το αποδείξουμε.
- $H(X) \leq \log |\mathcal{X}|$, όπου $|\mathcal{X}|$ το μέγεθος του αλφαβήτου της X. Το μέγιστο επιτυγχάνεται από την ομοιόμορφη κατανομή: $p(X_i) = \frac{1}{|\mathcal{X}|}$ για όλα τα $X_i \in \mathcal{X}$. Αποδείχθηκε στη "Θεωρία Πληροφορίας".
- $H(X,Y) = H(Y,X)$ (εύκολο, π.χ. με χρήση του ορισμού, δεδομένου ότι $p(x,y) = p(y,x)$).
- Κανόνας αλυσίδας: $H(X_1, X_2, \ldots, X_n) = H(X_1) + H(X_2|X_1) + \ldots + H(X_n|X_1, X_2, \ldots, X_{n-1})$. Απόδειξη με χρήση ορισμού και κανόνα Bayes.
- Για <u>ανεξάρτητες</u> τ.μ., $H(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} H(X_i)$.
- Επίσης, εάν οι τ.μ. X και Y είναι ανεξάρτητες, $H(X|Y) = H(X)$ και $H(Y|X) = H(Y)$.
- Γενικά, $H(X|Y) \neq H(Y|X)$.

Ρυθμός Εντροπίας διακριτής πηγής

- Ρυθμός εντροπίας διακριτής πηγής (τυχαίας διαδικασίας):

$$H(\mathcal{X}) = \lim_{n\to\infty} \frac{1}{n} H(X_1, X_2, \ldots, X_n) \text{ bits/σύμβολο},$$

εφόσον το όριο συγκλίνει.

- Το όριο συγκλίνει πάντα όταν η πηγή είναι στάσιμη. Στην περίπτωση αυτή, συγκλίνει και η ποσότητα

$$H'(\mathcal{X}) = \lim_{n\to\infty} H(X_n | X_1, X_2, \ldots, X_{n-1})$$

και $H(\mathcal{X}) = H'(\mathcal{X})$.

Ρυθμός Εντροπίας διακριτής πηγής (συνέχεια)

- Εάν οι τ.μ. είναι ανεξάρτητες,
  $H(\mathcal{X}) = H'(\mathcal{X}) = \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} H(X_i)$.
- Εάν, επιπλέον, οι τ.μ. είναι και ομοίως κατανεμημένες,
  $H(\mathcal{X}) = H'(\mathcal{X}) = \lim_{n\to\infty} \frac{1}{n} nH(X_i) = H(X_i) = H(X_1)$.
- Για στάσιμες πηγές, ο ρυθμός εντροπίας ποσοτικοποιεί το μέσο ποσό νέας πληροφορίας κάθε φορά που παίρνουμε ένα νέο δείγμα (το ποσό πληροφορίας των innovations για όσους έχουν ασχοληθεί με Θεωρία Εκτίμησης).

Παράδειγμα 1.1 (Cover σελ. 74)

- Έστω ακολουθία δυαδικών τ.μ. Bernoulli με $p_i = \Pr\{X_i = 1\}$ που δεν είναι σταθερή, αλλά εξαρτάται από το i ως εξής:

$$p_i = \begin{cases} 0.5 & \text{εάν} \quad 2k < \log\log i \leq 2k+1 \\ 0 & \text{εάν} \quad 2k+1 < \log\log i \leq 2k+2, \end{cases}$$

για $k = 0, 1, 2, \ldots$.

- Επομένως, κομμάτια όπου $H(X_i) = 1$ ακολουθούνται από εκθετικώς αυξανόμενα κομμάτια όπου $H(X_i) = 0$ κ.ο.κ. Συνεπώς, ο μέσος όρος της $H(X_i)$ μεταβάλλεται συνεχώς και δε συγκλίνει.
- Στη συγκεκριμένη περίπτωση δεν είναι δυνατό να οριστεί ρυθμός εντροπίας $H(\mathcal{X})$.

Σχετική Εντροπία $D(p||q)$

- Η σχετική εντροπία (relative entropy) ή απόσταση Kullback-Leibler μεταξύ δύο κατανομών p και q που ορίζονται στο ίδιο αλφάβητο $\mathcal{A}$ ισούται με

$$D(p||q) = \sum_{x} p(x) \log \frac{p(x)}{q(x)} = E_p \left[\log \frac{p(X)}{q(X)} \right].$$

- Προσοχή: Η μέση τιμή είναι ως προς την κατανομή p.
- Από πού πηγάζει αυτός ο ορισμός; ΄Οπως είδαμε στη "Θεωρία Πληροφορίας", η $D(p||q)$ ποσοτικοποιεί τα επιπλέον bits που χρειαζόμαστε για να συμπιέσουμε μια τ.μ. με πραγματική κατανομή p όταν για τη συμπίεση χρησιμοποιείται η κατανομή q.

Σχετική Εντροπία $D(p||q)$ (συνέχεια)

- $H(X) + D(p||q) \leq E[l^*] < H(X) + D(p||q) + 1$, όπου $E[l^*]$ είναι το μέσο μήκος του βέλτιστου κώδικα πηγής για την κατανομή q, ενώ η πραγματική κατανομή της X είναι η p.
- $D(p||q) \geq 0$. Αποδείχθηκε στη "Θεωρία Πληροφορίας" με χρήση της ανισότητας Jensen και του γεγονότος ότι η $\log$ είναι κοίλη ($\cap$). Θα επαναλάβουμε την απόδειξη στο μάθημα.
- Ωστόσο, η $D(p||q)$ δεν είναι απόσταση κατά την αυστηρή έννοια:
  - $D(p||q) \neq D(q||p)$.
  - Επίσης, δεν ισχύει η τριγωνική ανισότητα.

Δεσμευμένη Σχετική Εντροπία και Κανόνας Αλυσίδας

- Δεσμευμένη σχετική εντροπία (conditional relative entropy):

$$D(p(y|x)||q(y|x)) = E_p\left[\log \frac{p(Y|X)}{q(Y|X)}\right] = \sum_x \sum_y p(x,y) \log \frac{p(y|x)}{q(y|x)}.$$

- Προσοχή: Μέση τιμή ως προς την $p(x,y)$.
- Κανόνας αλυσίδας για τη σχετική εντροπία

$$D(p(x,y)||q(x,y)) = D(p(x)||q(x)) + D(p(y|x)||q(y|x)).$$

- Απόδειξη: Απλή, με χρήση ορισμού (Cover Theorem 2.5.3).

Αμοιβαία Πληροφορία $I(X;Y)$

- Έστω μια τ.μ. $X \sim p(X)$. Εάν μας γνωστοποιηθεί η τιμή της τ.μ. Y, η κατανομή πιθανότητας της X αλλάζει σε $p(X|Y)$. Επομένως, κατά μέσο όρο, γνώση της Y αλλάζει την αβεβαιότητα που έχουμε για τη X κατά $E_p\left[\frac{p(X|Y)}{p(X)}\right]$ (η μέση τιμή υπολογίζεται για όλες τις τιμές των X και Y).
- Συνεπώς,

$$I(X;Y) \triangleq E_p\left[\log\frac{p(X|Y)}{p(X)}\right] = \sum_x\sum_y p(x,y)\log\frac{p(x|y)}{p(x)}$$
$$= \sum_x\sum_y p(x,y)\log\frac{p(x|y)p(y)}{p(x)p(y)} = \sum_x\sum_y p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$$
$$= D(p(x,y)||p(x)p(y)) = E_p\left[\log\frac{p(X,Y)}{p(X)p(Y)}\right].$$

Αμοιβαία Πληροφορία $I(X;Y)$ (2)

- Προφανώς (από την προηγούμενη σχέση), $I(X;Y) = I(Y;X)$. Άρα, αποκάλυψη της X οδηγεί στην ίδια μεταβολή της αβεβαιότητας για την Y κατά μέσο όρο.
- Η ποσότητα $I(X;Y)$ ονομάζεται αμοιβαία πληροφορία. Έχουμε δει (και θα το αποδείξουμε, και πάλι, αργότερα) ότι $I(X;Y) \geq 0$. Επομένως, αποκάλυψη της τιμής της Y ελαττώνει την αβεβαιότητα για τη X κατά μέσο όρο.
- Προσοχή: Για κάποιες τιμές της Y, ενδέχεται $I(X;Y=y) < 0$. Ωστόσο, ισχύει πάντα $I(X;Y) = E_{p(Y)}[I(X;Y=y)] \geq 0$.

Αμοιβαία Πληροφορία $I(X;Y)$ (3)

- Μια διαφορετική ερμηνεία της αμοιβαίας πληροφορίας με βάση τη σχετική εντροπία: Η πληροφορία που "χάνουμε" εάν θεωρήσουμε ότι οι X και Y είναι ανεξάρτητες, ενώ, στην πραγματικότητα, δεν είναι.
- $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$. Προκύπτει από τον ορισμό (αποδείχθηκε στη "Θεωρία Πληροφορίας").

Αμοιβαία Πληροφορία $I(X;Y)$ (4)

- $I(X;X) = H(X) - H(X|X) = H(X)$. Η X περιέχει όλη την πληροφορία για τον εαυτό της.
- Κανόνας αλυσίδας για την αμοιβαία πληροφορία:

$$I(X_1, X_2, \ldots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y | X_1, X_2, \ldots, X_{i-1}).$$

- Απόδειξη: Εύκολα, από κανόνα αλυσίδας εντροπίας και χρήση $I(X_1, X_2, \ldots, X_n; Y) = H(X_1, X_2, \ldots, X_n) - H(X_1, X_2, \ldots, X_n | Y)$.
- Υπό συνθήκη αμοιβαία πληροφορία: $I(X;Y|Z) = H(X|Z) - H(X|Y,Z)$.

Διάγραμμα Venn

Η σχέση μεταξύ εντροπίας, δεσμευμένης εντροπίας και αμοιβαίας πληροφορίας μπορεί να αναπαρασταθεί και με χρήση διαγράμματος Venn.