EE728
Προχωρημένα Θέματα Θεωρίας Πληροφορίας
5η διάλεξη
(2η έκδοση, 17/3/2013)

Δημήτρης-Αλέξανδρος Τουμπακάρης

Τμήμα ΗΜ&ΤΥ, Πανεπιστήμιο Πατρών

12 Μαρτίου 2013

Περιεχόμενα 5ης διάλεξης

Διακριτά κανάλια – Ορισμοί

- Ορισμός 5.1. Ένα διακριτό κανάλι $(\mathcal{X}, p(y|x), \mathcal{Y})$ αποτελείται από δύο πεπερασμένα σύνολα συμβόλων εισόδου και εξόδου $\mathcal{X}$ και $\mathcal{Y}$, αντιστοίχως, και από ένα σύνολο (μία οικογένεια) δεσμευμένων συναρτήσεων μάζας πιθανότητας $p(y|x)$, μια για κάθε $x \in \mathcal{X}$, ώστε, για κάθε x και y, $p(y|x) \geq 0$ και, για κάθε x, $\sum_y p(y|x) = 1$. Η τ.μ. X είναι η είσοδος του καναλιού και η Y η έξοδός του.

Διακριτά κανάλια – Ορισμοί (2)

- Ορισμός 5.2. Ένα διακριτό κανάλι δεν έχει μνήμη (discrete memoryless channel - DMC) εάν

$$p(y_k|x^k, y^{k-1}, m) = p(y_k|x_k),$$

όπου $m \in \mathcal{M}$ είναι το μήνυμα που θέλουμε να μεταδώσουμε με n χρήσεις του καναλιού

- Παρατηρήστε ότι, από το Θεώρημα Ολικής Πιθανότητας, ο ορισμός αυτός συνεπάγεται και ότι

$$p(y_k|x^k, y^{k-1}) = p(y_k|x_k).$$

- Ορισμός 5.3. Έστω ότι χρησιμοποιούμε ένα διακριτό κανάλι n φορές. Ορίζουμε τη n-οστή επέκταση του διακριτού καναλιού χωρίς μνήμη ως $(\mathcal{X}^n, p(y^n|x^n), \mathcal{Y}^n)$, όπου

$$p(y_k|x^k, y^{k-1}) = p(y_k|x_k), \qquad k = 1, 2, \ldots, n.$$

Μετάδοση σε διακριτά κανάλια χωρίς ανάδραση

- Μπορούμε να γράψουμε

$$p(y^n|x^n, m) = \prod_{i=1}^{n} p(y_i|x^n, y^{i-1}, m).$$

- Εάν το κανάλι *χωρίς μνήμη* χρησιμοποιείται χωρίς ανάδραση, δηλαδή η είσοδος x^n στο κανάλι δεν εξαρτάται από τις εξόδους σε προηγούμενες χρονικές στιγμές αλλά μόνο από το μήνυμα m, $p(y_i|x^n, y^{i-1}, m) = p(y_i|x^i, y^{i-1}, m) = p(y_i|x_i)$ και

$$p(y^n|x^n) = \prod_{i=1}^{n} p(y_i|x_i).$$

($p(y_i|x^n, y^{i-1}, m) = p(y_i|y^{i-1}, m) = p(y_i|x^i, y^{i-1}, m)$ επειδή η αντιστοίχιση $m \leftrightarrow x^n$ είναι ένα-προς-ένα λόγω απουσίας ανάδρασης).

Χωρητικότητα Διακριτού Καναλιού Χωρίς Μνήμη

- Ορισμός 5.4. "Πληροφοριακή" Χωρητικότητα Διακριτού Καναλιού Χωρίς Μνήμη

``Information'' Channel Capacity of a DMC

$$C \triangleq \max_{p(x)} I(X;Y)$$

Παραδείγματα Διακριτών Καναλιών Χωρίς Μνήμη

(Επανάληψη από το μάθημα "Θεωρία Πληροφορίας")

- Δυαδικό Συμμετρικό Κανάλι (Binary Symmetric Channel -- BSC): $C = 1 - H(p)$ bits, επιτυγχάνεται με ομοιομορφη $p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$.
- Δυαδικό Κανάλι με Διαγραφή (Binary Erasure Channel): $C = 1 - \alpha$, όπου α η πιθανότητα διαγραφής. Επιτυγχάνεται με ομοιομορφη $p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$.
- Η χωρητικότητα του δυαδικού καναλιού με διαγραφή παραμένει η ίδια εάν χρησιμοποιήσουμε ανάδραση.
- Θα δούμε ότι το αποτέλεσμα αυτό, δηλαδή ότι η χρήση ανάδρασης δεν αυξάνει τη χωρητικότητα, ισχύει γενικά για όλα τα διακριτά κανάλια χωρίς μνήμη.

Παράδειγμα 5.1. Product DMC

(A. El Gamal & Y.-H. Kim, Example 3.3).

- Θεωρούμε δύο διακριτά κανάλια χωρίς μνήμη $(\mathcal{X}_1, p(y_1|x_1), \mathcal{Y}_1)$ και $(\mathcal{X}_2, p(y_2|x_2), \mathcal{Y}_2)$ με χωρητικότητες C_1 και C_2, αντίστοιχα.
- Έστω, τώρα, το κανάλι $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1|x_1)p(y_2|x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ στο οποίο τα σύμβολα $x_1 \in \mathcal{X}_1$ και $x_2 \in \mathcal{X}_2$ στέλνονται ταυτόχρονα και παράλληλα και τα ληφθέντα σύμβολα ακολουθούν κατανομή $p(y_1, y_2|x_1, x_2) = p(y_1|x_1)p(y_2|x_2)$.

Παράδειγμα 5.1. Product DMC (2)

- Η χωρητικότητα του καναλιού-γινομένου ισούται με

$$\begin{aligned} C &= \max_{p(x_1,x_2)} I(X_1,X_2;Y_1;Y_2) \\ &= \max_{p(x_1,x_2)} \{I(X_1,X_2;Y_1) + I(X_1,X_2;Y_2|Y_1)\} \\ &= \max_{p(x_1,x_2)} \{I(X_1;Y_1) + I(X_2;Y_1|X_1) + \\ &\qquad I(X_2;Y_2|Y_1) + I(X_1;Y_2|X_2,Y_1)\} \\ &\overset{(a),(b)}{=} \max_{p(x_1,x_2)} \{I(X_1;Y_1) + I(X_2;Y_2)\}\,. \end{aligned}$$

(a) Οι X_1 και X_2 είναι ανεξάρτητες και η Y_1 είναι ανεξάρτητη της X_2. Επομένως, $X_2 \to X_1 \to Y_1$ και
$I(X_2;Y_1|X_1) = H(Y_1|X_1) - H(Y_1|X_1,X_2) = 0$.
(b) Με την ίδια συλλογιστική, $(X_1,Y_1) \to X_2 \to Y_2$ και
$I(X_1;Y_2|X_2,Y_1) = H(Y_2|X_2,Y_1) - H(Y_2|X_1,X_2,Y_1) = 0$. Επίσης, λόγω ανεξαρτησίας, $I(X_2;Y_2|Y_1) = I(X_2;Y_2)$.

Παράδειγμα 5.1. Product DMC (3)

- Συνεπώς,

$$\begin{aligned} C &= \max_{p(x_1,x_2)} \{I(X_1;Y_1) + I(X_2;Y_2)\} \\ &= \max_{p(x_1,x_2)} I(X_1;Y_1) + \max_{p(x_1,x_2)} I(X_2;Y_2) \\ &= \max_{p(x_1)} I(X_1;Y_1) + \max_{p(x_2)} I(X_2;Y_2) = C_1 + C_2. \end{aligned}$$

- Το αποτέλεσμα μπορεί να γενικευτεί για $K > 2$ ανεξάρτητα κανάλια.

Χωρητικότητα Συμμετρικού Καναλιού

- Πίνακας μετάβασης $[p(y|x)]_{i,j}$. Σύμβολο στην είσοδο: x_i. Σύμβολο στην έξοδο: y_j.
- Ορισμός 5.5. Ένα διακριτό κανάλι χωρίς μνήμη ονομάζεται συμμετρικό όταν κάθε γραμμή του πίνακα μετάβασης $p(y|x)$ προκύπτει από αναδιάταξη κάθε άλλης γραμμής και το ίδιο ισχύει και για κάθε στήλη του πίνακα. Ένα διακριτό κανάλι χωρίς μνήμη ονομάζεται ασθενώς συμμετρικό όταν κάθε γραμμή του πίνακα μετάβασης $p(y|x)$ προκύπτει από αναδιάταξη κάθε άλλης γραμμής και τα αθροίσματα των στοιχείων κάθε στήλης $\sum_x p(y|x)$ ισούνται μεταξύ τους.

Χωρητικότητα Συμμετρικού Καναλιού (2)

- Θεώρημα 5.6. Για τη χωρητικότητα ασθενώς συμμετρικού καναλιού (και, επομένως, και συμμετρικού καναλιού), ισχύει

$$C = \log|\mathcal{Y}| - H(\text{οποιασδήποτε γραμμής } \mathbf{r} \text{ πίνακα μετάβασης}).$$

- Απόδειξη:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &\overset{(a)}{=} H(Y) - H(\mathbf{r}) \\ &\leq \log|\mathcal{Y}| - H(\mathbf{r}). \end{aligned}$$

- Για το (a) χρησιμοποιήθηκε το γεγονός ότι κάθε γραμμή του πίνακα μετάβασης προκύπτει από αναδιάταξη κάθε άλλης γραμμής.

Χωρητικότητα Συμμετρικού Καναλιού (3)

- Η ισότητα ισχύει όταν η Y ακολουθεί ομοιόμορφη κατανομή.
- Ομοιόμορφη κατανομή για την Y επιτυγχάνεται με χρήση ομοιόμορφα κατανεμημένης εισόδου X.

$$p(y) = \sum_{x \in \mathcal{X}} p(y|x)p(x) = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} p(y|x) \overset{(a)}{=} c\frac{1}{|\mathcal{X}|} = \frac{1}{|\mathcal{Y}|}.$$

  Στο (a) χρησιμοποιήθηκε το γεγονός ότι, για (ασθενώς) συμμετρικά κανάλια, τα αθροίσματα των στοιχείων κάθε στήλης ισούνται μεταξύ τους.
- Παρόλο που για συμμετρικά (και ασθενώς συμμετρικά) κανάλια η χωρητικότητα επιτυγχάνεται πάντοτε με χρήση ομοιόμορφης κατανομής εισόδου, αυτό δε σημαίνει, κατ' ανάγκη, ότι μόνο η ομοιόμορφη κατανομή επιτυγχάνει τη χωρητικότητα.
  - Παράδειγμα: Ενθόρυβη γραφομηχανή με άρτιο αριθμό πλήκτρων.

Η Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP)

Εισαγωγή

- Θα αρχίσουμε, και πάλι, από την ασθενή από κοινού τυπικότητα και, στη συνέχεια, θα αναφερθούμε στην ισχυρή από κοινού τυπικότητα.

Από κοινού τυπικές ακολουθίες (Jointly Typical sequences)

- Ορισμός 5.7. Το σύνολο $A_\epsilon^{(n)}$ από κοινού (ασθενώς) τυπικών ακολουθιών ζευγών (x, y) ως προς την κατανομή $p(x, y)$, ορίζεται ως

$$A_\epsilon^{(n)} = \{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : \left| -\frac{1}{n} \log p(x^n) - H(X) \right| < \epsilon, \\ \left| -\frac{1}{n} \log p(y^n) - H(Y) \right| < \epsilon, \\ \left| -\frac{1}{n} \log p(x^n, y^n) - H(X, Y) \right| < \epsilon \Big\},$$

περιέχει, δηλαδή, τις ακολουθίες ζευγών (ή τα ζεύγη ακολουθιών) $\{(x^n, y^n)\}$ μήκους n οι εμπειρικές εντροπίες των οποίων βρίσκονται σε απόσταση από την πραγματική τους εντροπία που δεν υπερβαίνει το ϵ.

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP)

- Έστω (X^n, Y^n) ακολουθίες μήκους n οι οποίες δημιουργούνται με χρήση ανεξάρτητων και ομοίως κατανεμημένων (i.i.d.) ζευγών (X_i, Y_i), σύμφωνα με την κατανομή $p(x^n, y^n) = \prod_{i=1}^{n} p(x_i, y_i)$. Ισχύουν οι ιδιότητες:
  1. $\Pr\left\{(X^n, Y^n) \in A_\epsilon^{(n)}\right\} \to 1$, για $n \to \infty$.
  2. $\left|A_\epsilon^{(n)}\right| \leq 2^{n(H(X,Y)+\epsilon)}$.
  3. Εάν $(\tilde{X}^n, \tilde{Y}^n) \sim p(x^n)p(y^n)$, δηλαδή οι $\tilde{X}^n$ και $\tilde{Y}^n$ είναι ανεξάρτητες και οι κατανομές τους είναι ίδιες με τις περιθώριες κατανομές της $p(x^n, y^n)$,

$$\Pr\left\{(\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\right\} \leq 2^{-n(I(X;Y)-3\epsilon)}.$$

Επίσης, υπάρχει n_0 τέτοιο ώστε, για $n > n_0$,

$$\Pr\left\{(\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\right\} \geq (1-\epsilon)2^{-n(I(X;Y)+3\epsilon)}.$$

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης – Αποδείξεις

1. $\Pr\left\{(X^n, Y^n) \in A_\epsilon^{(n)}\right\} \to 1$, για $n \to \infty$.
   Από τον ασθενή νόμο των μεγάλων αριθμών, $-\frac{1}{n}\log p(X^n) \to -\mathbb{E}[\log p(X)] = H(X)$ κατά πιθανότητα. Επομένως, για δεδομένο $\epsilon > 0$, υπάρχει n_1 τέτοιο ώστε, για όλα τα $n > n_1$, $\Pr\left\{\left|-\frac{1}{n}\log p(X^n) - H(X)\right| \geq \epsilon\right\} < \frac{\epsilon}{3}$. Παρομοίως, υπάρχουν n_2 και n_3 τέτοια ωστε, $\Pr\left\{\left|-\frac{1}{n}\log p(Y^n) - H(Y)\right| \geq \epsilon\right\} < \frac{\epsilon}{3}$ και $\Pr\left\{\left|-\frac{1}{n}\log p(X^n, Y^n) - H(X, Y)\right| \geq \epsilon\right\} < \frac{\epsilon}{3}$, αντιστοίχως. Επομένως, για $n > \max\{n_1, n_2, n_3\}$, η πιθανότητα το (X^n, Y^n) να μην είναι τυπικό είναι μικρότερη από ϵ, και, συνεπώς, $\Pr\left\{(X^n, Y^n) \in A_\epsilon^{(n)}\right\} > 1 - \epsilon$, για $n > \max\{n_1, n_2, n_3\}$.

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης – Αποδείξεις (2)

2. $\left|A_\epsilon^{(n)}\right| \leq 2^{n(H(X,Y)+\epsilon)}$.

   Παρόμοια με την αντίστοιχη απόδειξη για το AEP,

$$1 = \sum p(x^n, y^n) \geq \sum_{(x^n,y^n)\in A_\epsilon^{(n)}} p(x^n, y^n) \geq \left|A_\epsilon^{(n)}\right| 2^{-n(H(X,Y)+\epsilon)}.$$

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης – Αποδείξεις (3)

3. Έστω *ανεξάρτητες* ακολουθίες τ.μ. $\tilde{X}^n$ και $\tilde{Y}^n$ που έχουν προκύψει από κατανομές $p(\tilde{x}^n)$ και $p(\tilde{y}^n)$ που είναι ίδιες με τις περιθώριες κατανομές της $p(x^n, y^n)$, $p(x^n)$ και $p(y^n)$, αντιστοίχως. Επομένως,

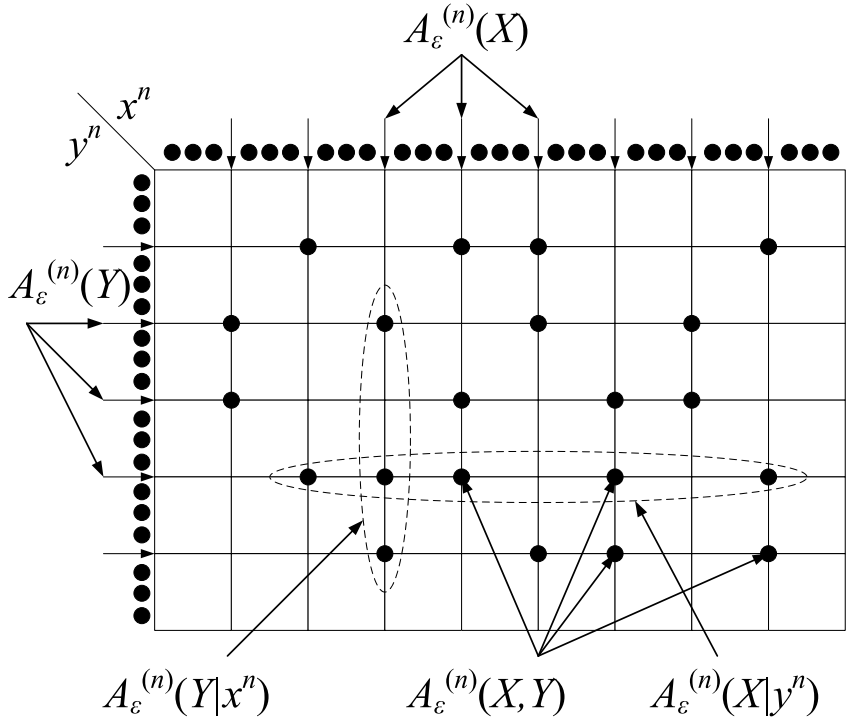
$$\begin{aligned}\Pr\left\{(\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\right\} &= \sum_{(x^n,y^n)\in A_\epsilon^{(n)}} p(x^n)p(y^n) \\ &\leq 2^{n(H(X,Y)+\epsilon)}2^{-n(H(X)-\epsilon)}2^{-n(H(Y)-\epsilon)} \\ &= 2^{-n(I(X;Y)-3\epsilon)}.\end{aligned}$$

Με παρόμοιο τρόπο (βλ. π.χ. Cover Theorem 7.6.1) μπορεί να αποδειχτεί ότι

$$\Pr\left\{(\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\right\} \geq (1-\epsilon)2^{-n(I(X;Y)+3\epsilon)}$$

για $n > n_0$.

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (2)



Στο σχήμα δίνεται ένα παράδειγμα από κοινού τυπικού συνόλου. Υπάρχουν περίπου $2^{nH(X)}$ τυπικές ακολουθίες τ.μ. X και περίπου $2^{nH(Y)}$ τυπικές ακολουθίες τ.μ. Y. Ωστόσο, οι από κοινού τυπικές ακολουθίες είναι περίπου $2^{nH(X,Y)}$, δηλαδή, υπάρχουν ζεύγη τυπικών X^n με τυπικά Y^n τα οποία *δεν* είναι από κοινού τυπικά.

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (3)

- Από την 3η ιδιότητα, η πιθανότητα ένα ζεύγος ακολουθιών (X^n, Y^n) το οποίο επιλέγεται τυχαία και του οποίου οι συνιστώσες είναι (με-μονωμένως) τυπικές να είναι και από κοινού τυπικό, ισούται περίπου με $2^{-nI(X;Y)}$.
- Επομένως, στο σχήμα της προηγούμενης διαφάνειας, κατά μέσο όρο πρέπει να θεωρήσουμε περίπου $2^{nI(X;Y)}$ ζεύγη μεμονωμένως τυπικών X^n και Y^n έως ότου εμφανιστεί ένα τυπικό ζεύγος.
- Ισοδύναμα, εάν θεωρήσουμε μια ακολουθία Y^n η οποία αποτελεί την έξοδο καναλιού με είσοδο X^n, υπάρχουν περίπου $2^{nH(X|Y)}$ υπό συνθήκη τυπικές ακολουθίες X^n. Η πιθανότητα να διαλέξουμε μια ακολουθία X'^n η οποία είναι τυπική με την Y^n αλλά δεν είναι η ακολουθία X^n η οποία μεταδόθηκε ισούται, περίπου, με $2^{nH(X|Y)}/2^{nH(X)} = 2^{-nI(X;Y)}$. Επομένως, και πάλι, κατά μέσο όρο πρέπει να θεωρήσουμε περίπου $2^{nI(X;Y)}$ ακολουθίες X^n έως ότου εμφανιστεί ακολουθία που αποτελεί τυπικό ζεύγος με την Y^n.

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (4)

- Συνεπώς, διαισθητικά, αν έχουμε ένα κανάλι με $p(y|x)$ μπορούμε να μεταδίδουμε περίπου $2^{nI(X;Y)}$ διακριτές ακολουθίες στο κανάλι χωρίς στο δέκτη να υπάρχει σύγχυση της (τυπικής) ακολουθίας y^n που αντιστοιχεί στη μεταδοθείσα τυπική ακολουθία x^n με μια άλλη τυπική ακολουθία $\tilde{y}^n$ η οποία είναι ανεξάρτητη από τη μεταδοθείσα x^n.
- Θα αποδείξουμε ότι είναι εφικτή η μετάδοση έως και $2^{nI(X;Y)}$ διακριτών ακολουθιών με αυθαίρετα μικρή πιθανότητα σφάλματος για $n \to \infty$. Θα δούμε, επίσης, ότι εάν προσπαθήσουμε να μεταδώσουμε περισσότερες από $2^{nI(X;Y)}$ διακριτές ακολουθίες, η πιθανότητα σφάλματος τείνει στο 1.