

EE728

Προχωρημένα Θέματα Θεωρίας Πληροφορίας

5η διάλεξη

Δημήτρης-Αλέξανδρος Τουμπακάρης

Τμήμα ΗΜ&ΤΥ, Πανεπιστήμιο Πατρών

22 Μαρτίου 2010

Περιεχόμενα σημερινού μαθήματος

- 1 Διακριτά κανάλια και χωρητικότητα
 - Ορισμοί και Θεωρήματα

- 2 Η Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP)

Αντιστοιχία με συγγράμματα

- Cover & Thomas: 7.1 – 7.4
- Gallager: 4.1 – 4.2

Διακριτά κανάλια – Ορισμοί

Ορισμός Ένα διακριτό κανάλι $(\mathcal{X}, p(y|x), \mathcal{Y})$ αποτελείται από δύο πεπερασμένα σύνολα \mathcal{X} και \mathcal{Y} και ένα σύνολο 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 έξοδος του.

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

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

Μετάδοση σε διακριτά κανάλια χωρίς ανάδραση

- Εάν το κανάλι χωρίς μνήμη χρησιμοποιείται χωρίς ανάδραση, δηλαδή η είσοδος στο κανάλι δεν εξαρτάται από τις εξόδους σε προηγούμενες χρονικές στιγμές, $p(x_k | x^{k-1}, y^{k-1}) = p(x_k | x^{k-1})$, και

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

Χωρητικότητα Διακριτού Καναλιού Χωρίς Μνήμη

Ορισμός “Πληροφοριακή” Χωρητικότητα Διακριτού Καναλιού Χωρίς Μνήμη

“Information” Channel Capacity

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

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 κατανομή εισόδου $p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$.
- Δυαδικό Κανάλι με Διαγραφή (Binary Erasure Channel): $C = 1 - \alpha$, όπου α η πιθανότητα διαγραφής. Επιτυγχάνεται με ομοιομορφη κατανομή εισόδου $p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$.
- 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.

Χωρητικότητα Συμμετρικού Καναλιού

- Πίνακας μετάβασης $[p(y|x)]_{i,j}$. Σύμβολο στην είσοδο: x_i . Σύμβολο στην έξοδο: y_j .

Ορισμός Ένα διακριτό κανάλι 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 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 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:

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

- Για το (a) χρησιμοποιήσαμε 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 κατανομημένης εισόδου X .

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

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)

- 1 Διακριτά κανάλια και χωρητικότητα
 - Ορισμοί και Θεωρήματα
- 2 Η Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης (Joint AEP)

Από κοινού τυπικές ακολουθίες (Jointly Typical sequences)

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

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

περιέχει, δηλαδή, 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 κατανομημένων (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. $\Pr\{(X^n, Y^n) \in A_\epsilon^{(n)}\} \rightarrow 1$, για $n \rightarrow \infty$.
2. $|A_\epsilon^{(n)}| \leq 2^{n(H(X,Y)+\epsilon)}$.
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 ισούνται με τις περιθώριες κατανομές της $p(x^n, y^n)$,

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

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

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

Ιδιότητα Από Κοινού Ασυμπτωτικής Ισοδιαμέρισης – Αποδείξεις

1. $\Pr\{(X^n, Y^n) \in A_\epsilon^{(n)}\} \rightarrow 1$, για $n \rightarrow \infty$.

Από τον ασθενή νόμο των μεγάλων αριθμών, $-\frac{1}{n} \log p(X^n) \rightarrow -\mathbb{E}[\log p(X)] = H(X)$ 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 ώστε, $\Pr\left\{\left|-\frac{1}{n} \log p(Y^n) - H(Y)\right| \geq \epsilon\right\} < \frac{\epsilon}{3}$ και $\Pr\left\{\left|-\frac{1}{n} \log p(X^n, Y^n) - H(X, Y)\right| \geq \epsilon\right\} < \frac{\epsilon}{3}$, αντίστοιχα. 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 και ότι οι από κοινού κατανομές $p(\tilde{x}^n)$ και $p(\tilde{y}^n)$ ισούνται με τις περιθώριες κατανομές της $p(x^n, y^n)$, $p(x^n)$ και $p(y^n)$, αντίστοιχα. Επομένως,

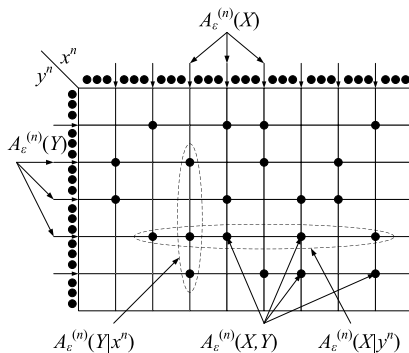
$$\begin{aligned} \Pr \left\{ (\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)} \right\} &= \sum_{(x^n, y^n) \in A_\epsilon^{(n)}} p(x^n) p(y^n) \\ &\leq 2^{n(H(X, Y) + \epsilon)} 2^{-n(H(X) - \epsilon)} 2^{-n(H(Y) - \epsilon)} \\ &= 2^{-n(I(X; Y) - 3\epsilon)}. \end{aligned}$$

Με παρόμοιο τρόπο (βλ. π.χ. Cover Theorem 7.6.1) μπορεί να αποδειχθεί 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 (X^n, Y^n) το οποίο επιλέγεται τυχαία και του οποίου οι συνιστώσες είναι (μεμονωμένα 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 μεμονωμένα 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, μπορούμε να μεταδώσουμε περίπου $2^{nI(X;Y)}$ διακριτές ακολουθίες στο κανάλι χωρίς να υπάρξει σύγχυση.
- Θα αποδείξουμε ότι είναι εφικτή η μετάδοση έως και $2^{nI(X;Y)}$ διακριτών ακολουθιών με αυθαίρετα μικρή πιθανότητα σφάλματος για $n \rightarrow \infty$. Θα αποδείξουμε, επίσης, ότι εάν προσπαθήσουμε να μεταδώσουμε περισσότερες από $2^{nI(X;Y)}$ διακριτές ακολουθίες, η πιθανότητα σφάλματος τείνει στο 1.