EE728
Προχωρημένα Θέματα Θεωρίας Πληροφορίας
11η διάλεξη

Δημήτρης-Αλέξανδρος Τουμπακάρης

Τμήμα ΗΜ&ΤΥ, Πανεπιστήμιο Πατρών

25 Απριλίου 2013

Περιεχόμενα 11ης εβδομάδας

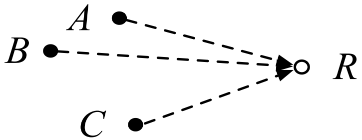
1 Θεωρία Πληροφορίας Δικτύων (Network Information Theory)

2 Κατανεμημένη Κωδικοποίηση
- Μοντέλο και Ορισμοί
- Random binning
- Θεώρημα Slepian-Wolf

Θεωρία Πληροφορίας Δικτύων

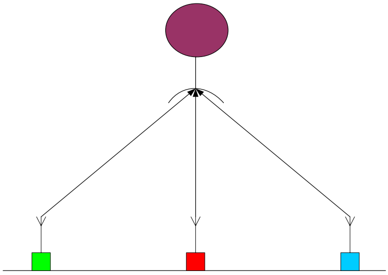
- Έως τώρα αναφερθήκαμε σε συστήματα με έναν αποστολέα και ένα παραλήπτη.
  - Στην κωδικοποίηση πηγής υποθέσαμε ότι, ακόμα και εάν θέλουμε να κωδικοποιήσουμε περισσότερες από μία πηγές, για τη συμπίεση χρησιμοποιείται ένας κωδικοποιητής ο οποίος έχει πρόσβαση σε όλες τις πηγές.
  - Για τη μετάδοση μέσα σε κανάλια υποθέσαμε ότι το σύστημα αποτελείται από έναν πομπό και ένα δέκτη.
- Ωστόσο, πολλά συστήματα αποτελούνται από περισσότερα από ένα τερματικά (πομπούς/κωδικοποιητές ή/και δέκτες/αποκωδικοποιητές).

Κατανεμημένη Συμπίεση



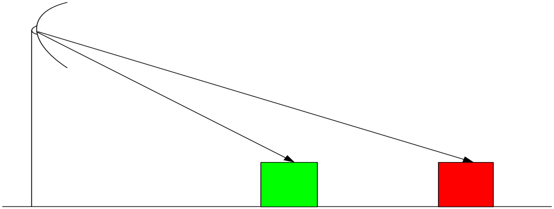
- Στο σχήμα, οι αισθητήρες επιθυμούν να στείλουν στο δέκτη πληροφορία για τις πηγές που μετρούν.
- Οι πηγές ενδέχεται να είναι συσχετισμένες (για παράδειγμα, τιμές της θερμοκρασίας σε διαφορετικές περιοχές μίας πόλης). Ωστόσο, οι αισθητήρες δεν μπορούν να επικοινωνήσουν μεταξύ τους.
- Όπως θα δούμε, στο όριο, μπορούμε να συμπιέσουμε τόσο αποδοτικά όσο και εάν ένας κωδικοποιητής έχει πρόσβαση σε όλες τις πηγές! (Θεώρημα Slepian-Wolf).

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.
- Όπως θα δούμε, στη γενική περίπτωση, για να επιτύχουμε μετάδοση με το μέγιστο δυνατό ρυθμό, οι χρήστες πρέπει να μεταδίδουν *ταυτόχρονα*.

Κανάλι Ευρυεκπομπής (Broadcast Channel)

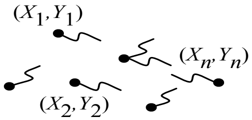


- Ένας κεντρικός σταθμός που επιθυμεί να στείλει (διαφορετική) πληροφορία σε περισσότερους από έναν χρήστες.
- Δεν έχει κατανοηθεί πλήρως, εκτός από ειδικές περιπτώσεις (π.χ. Γκαουσιανός θόρυβος στους δέκτες).
- Όπως θα δούμε, η χωρητικότητα του Γκαουσιανού BC επιτυγχάνεται με ταυτόχρονη μετάδοση όλων των χρηστών (στη γενική περίπτωση).

Άλλα κανάλια

- Άλλα ενδιαφέροντα κανάλια πολλών χρηστών, τα οποία δε θα εξετάσουμε λεπτομερώς στο μάθημα είναι
    - Το κανάλι μεταγωγής (relay channel): Ένας ή περισσότεροι μεταγωγείς βοηθούν έναν πομπό να στείλει πληροφορία σε ένα δέκτη. Δεν έχει λυθεί στη γενική περίπτωση.
    - Το κανάλι παρεμβολών (interference channel): K Ζεύγη πομπού/δέκτη που μεταδίδουν στο ίδιο κανάλι και αλληλοπαρεμβάλλονται. Δεν έχει λυθεί στη γενική περίπτωση.

Το γενικό πρόβλημα της Θεωρίας Πληροφορίας Δικτύων



- Το γενικό πρόβλημα της Θεωρίας Πληροφορίας Δικτύων είναι το εξής:
    - Δοθέντος ενός συστήματος με S πηγές (στη γενική περίπτωση συσχετισμένες) και D προορισμούς, όπου η κάθε πηγή θέλει να στείλει συγκεκριμένη πληροφορία σε ένα υποσύνολο των προορισμών
    - Δοθέντος του τρόπου με τον οποίο οι παρεμβολές και ο θόρυβος επηρεάζουν την επικοινωνία στο δίκτυο
    - Δοθεισών των δυνατοτήτων συνεργασίας μεταξύ των πηγών και των προορισμών
    - Δοθείσης της δυνατότητας (ή μη) ανάδρασης

Να βρεθούν οι ρυθμοί που είναι εφικτοί ή, ισοδύναμα, να βρεθεί αν ένα δεδομένο διάνυσμα ρυθμών μετάδοσης είναι εφικτό.

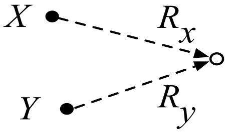
Το γενικό πρόβλημα της Θεωρίας Πληροφορίας Δικτύων (2)

- Το γενικό πρόβλημα δεν έχει ακόμα λυθεί.
- Για μετάδοση σε ένα δίκτυο απαιτείται συνδυασμός
  - Κατανεμημένης Κωδικοποίησης Πηγής
  - Κατανεμημένης Επικοινωνίας
- Οι πρώτες μελέτες στη Θεωρία Πληροφορίας Δικτύων έγιναν από το Shannon.
- Το πεδίο γνώρισε μεγάλη άνθηση στις αρχές της δεκαετίας του 1970 (οπότε και βρέθηκε η περιοχή χωρητικότητας του MAC και του degraded BC).
- Τα τελευταία χρόνια γνωρίζει νέα άνθηση λόγω της ανάπτυξης των συστημάτων επικοινωνιών (ιδιαίτερα των ασύρματων).

Κατανεμημένη Κωδικοποίηση

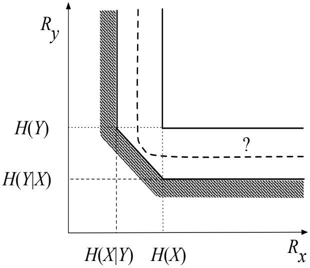
1. Θεωρία Πληροφορίας Δικτύων (Network Information Theory)
2. Κατανεμημένη Κωδικοποίηση
   - Μοντέλο και Ορισμοί
   - Random binning
   - Θεώρημα Slepian-Wolf

Κατανεμημένη Κωδικοποίηση – Εισαγωγή



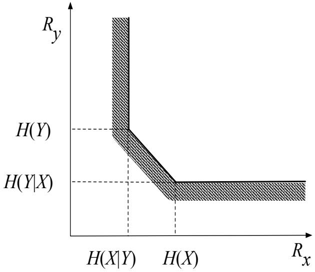
- Θα ξεκινήσουμε από την περίπτωση δύο πηγών που φαίνεται στο σχήμα. Η επέκταση σε K πηγές είναι εύκολη (σε θεωρητικό επίπεδο).
- Έστω ότι θέλουμε να αποστείλουμε τις τιμές των πηγών X και Y στο δέκτη, χρησιμοποιώντας όσο το δυνατόν πιο αποδοτική περιγραφή. Οι συμπιεστές σε κάθε πηγή *δεν* μπορούν να συνεργαστούν για την κωδικοποίηση. Επίσης, το κανάλι δεν έχει θόρυβο.
- Για απλοποίηση θα θεωρήσουμε ότι οι πηγές δεν έχουν μνήμη.
- Ωστόσο, οι τιμές των πηγών για δεδομένη χρονική στιγμή είναι εξαρτημένες!

Κατανεμημένη Κωδικοποίηση – Εισαγωγή (2)



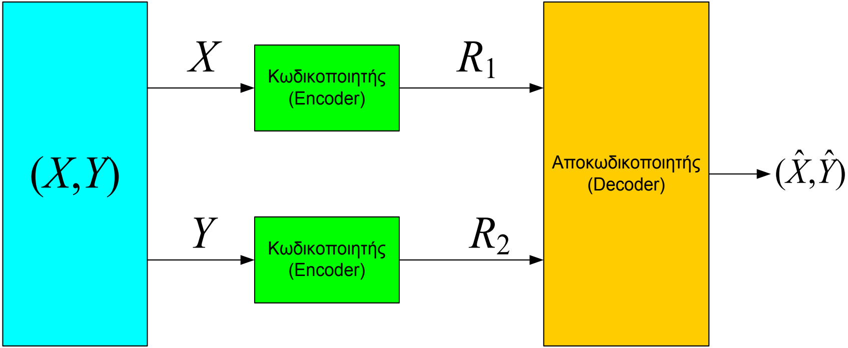
- Γνωρίζουμε ότι υπάρχει τρόπος να μεταδώσουμε την πληροφορία των πηγών με συνολικό ρυθμό $R_x + R_y = H(X) + H(Y)$.
- Εάν είχαμε πρόσβαση και στις δύο πηγές, θα μπορούσαμε να μεταδώσουμε με $R_x + R_y = H(X, Y)$.
- Υπάρχει τρόπος να συμπιέσουμε με συνολικό ρυθμό μεταξύ αυτών των δύο τιμών και αν ναι, με ποιο τρόπο; Ποιος είναι ο συνολικός ρυθμός που απαιτείται;

Κατανεμημένη Κωδικοποίηση – Εισαγωγή (3)



- Θα δείξουμε ότι αρκεί $R_x + R_y > H(X, Y)$ ακόμα και εάν η κωδικοίηση γίνεται ξεχωριστά!
- Το εντυπωσιακό, αυτό, αποτέλεσμα αποδείχτηκε από τους Slepian και Wolf το 1973.
- Η απόδειξη βασίζεται στην ιδέα του random binning στην οποία θα αναφερθούμε στη συνέχεια.
- Ισχύει μόνο για αναπωλειακή (lossless) συμπίεση.

Μοντέλο



- Το μοντέλο του προβλήματος φαίνεται στο σχήμα.

Ορισμοί

- Ορισμός 11.1. Ενας κατανεμημένος κώδικας πηγής (distributed source code) $\left(\left(2^{nR_1}, 2^{nR_2}\right), n\right)$ για το ζεύγος (X, Y) αποτελείται από δύο απεικονίσεις κωδικοποίησης (encoder maps)

$$f_1 : \mathcal{X}^n \to \left\{1, 2, \ldots, 2^{nR_1}\right\} \text{ και}$$
$$f_2 : \mathcal{Y}^n \to \left\{1, 2, \ldots, 2^{nR_2}\right\}$$

και από μία απεικόνιση αποκωδικοποίησης (decoder map)

$$g : \left\{1, 2, \ldots, 2^{nR_1}\right\} \times \left\{1, 2, \ldots, 2^{nR_2}\right\} \to \mathcal{X}^n \times \mathcal{Y}^n.$$

- Ορισμός 11.2. Η πιθανότητα σφάλματος κατανεμημένου κώδικα ορίζεται ως

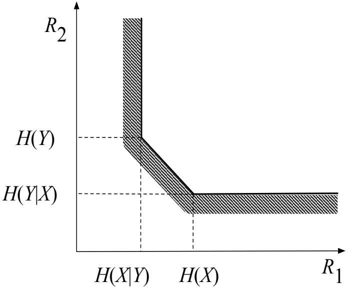
$$P_e^{(n)} = \Pr\left\{g(f_1(X^n), f_2(Y^n)) \neq (X, Y)\right\}.$$

Ορισμοί (συνέχεια)

- Ορισμός 11.3. Ένα ζεύγος ρυθμών (R_1, R_2) ονομάζεται *επιτεύξιμο* (achievable) εάν υπάρχει ακολουθία κατανεμημένων κωδίκων $\left(\left(2^{nR_1}, 2^{nR_2}\right), n\right)$ με $P_e^{(n)} \to 0$.
- Ορισμός 11.4. Η περιοχή επιτεύξιμων ρυθμών (achievable rate region) είναι το περίβλημα (closure) του συνόλου των επιτεύξιμων ρυθμών.
- Θεώρημα 11.5. (Slepian-Wolf) Η περιοχή επιτεύξιμων ρυθμών για την κατανεμημένη συμπίεση του ζεύγους (X, Y) εάν τα (X_i, Y_i) είναι i.i.d. $\sim p(x, y)$, δίνεται από τις σχέσεις

$$\begin{aligned} R_1 &\geq H(X|Y) \\ R_2 &\geq H(Y|X) \\ R_1 + R_2 &\geq H(X, Y). \end{aligned}$$

Περιοχή επιτεύξιμων ρυθμών



$$R_1 \geq H(X|Y)$$
$$R_2 \geq H(Y|X)$$
$$R_1 + R_2 \geq H(X,Y).$$

- Η περιοχή επιτεύξιμων ρυθμών φαίνεται στο σχήμα.

Random binning

1. Θεωρία Πληροφορίας Δικτύων (Network Information Theory)
2. Κατανεμημένη Κωδικοποίηση
   - Μοντέλο και Ορισμοί
   - Random binning
   - Θεώρημα Slepian-Wolf

Random binning

- Η απόδειξη του θεωρήματος των Slepian και Wolf βασίζεται στην τεχνική random binning η οποία είναι ένας τρόπος να επιτύχουμε συμπίεση.
- Στην απόδειξη του ευθέος του Θεωρήματος Κωδικοποίησης Πηγής αγνοήσαμε τις μη τυπικές ακολουθίες και αντιστοιχίσαμε ένα *μοναδικό* δείκτη σε κάθε τυπική ακολουθία.
- Στην τεχνική random binning σε κάθε ακολουθία (ακόμα και στις μη τυπικές) θα αντιστοιχίσουμε ένα δείκτη με *τυχαίο* τρόπο. Επομένως, υπάρχει η πιθανότητα ένας δείκτης να αντιστοιχιστεί σε περισσότερες από μία ακολουθίες.
- Ωστόσο, όπως θα δούμε, όταν $R > H(X)$, η πιθανότητα να συμβεί αυτό (και, επομένως, η πιθανότητα να συμβεί σφάλμα αποκωδικοποίησης) τείνει στο 0 για $n \to \infty$.

Συμπίεση με τη μέθοδο random binning – Κωδικοποίηση

- Προκειμένου να παρουσιάσουμε την τεχνική random binning θεωρούμε, αρχικά, το πρόβλημα κωδικοποίησης *μίας* πηγής, X, *χωρίς μνήμη* (για το οποίο χρησιμοποιήσαμε κωδικοποίηση με χρήση τυπικών ακολουθιών τις πρώτες εβδομάδες του μαθήματος). Θα παρουσιάσουμε μια εναλλακτική απόδειξη επιτευξιμότητας με χρήση random binning.
- Κωδικοποίηση: Σε κάθε ακολουθία $X_1, X_2, \ldots, X_n$ αντιστοιχίζουμε ένα δείκτη από το σύνολο $\left\{1, 2, \ldots, 2^{nR}\right\}$ με *τυχαίο* τρόπο (με *ομοιόμορφη* κατανομή). Η αντιστοίχιση κάθε ακολουθίας γίνεται ανεξάρτητα από τις αντιστοιχίσεις των άλλων ακολουθιών.
- Η αντιστοίχιση γίνεται για όλες τις ακολουθίες (και για τις μη τυπικές).
- Το σύνολο των ακολουθιών που έχουν τον ίδιο δείκτη ονομάζεται bin.
- Δηλαδή, κατανέμουμε με τυχαίο (ομοιόμορφο) τρόπο όλες τις ακολουθίες σε 2^{nR} bins.

Συμπίεση με τη μέθοδο random binning – Αποκωδικοποίηση

- Οι αντιστοιχίσεις ακολουθιών σε bins αποκαλύπτονται σε πομπό και σε δέκτη.
- Ο κωδικοποιητής κωδικοποιεί το bin στο οποίο ανήκει η ακολουθία X^n.
- Στον αποκωδικοποιητή, δεδομένου του δείκτη του bin, ελέγχουμε το περιεχόμενο του bin.
- Εάν το bin περιέχει μόνο μία τυπική ακολουθία, έστω $\hat{X}^n$, η ακολουθία στέλνεται στην έξοδο του αποκωδικοποιητή.
- Αλλιώς, δηλώνεται αδυναμία αποκωδικοποίησης.
- Θα δείξουμε ότι αν $R > H(X)$ το σφάλμα αποκωδικοποίησης τείνει στο 0 για $n \to \infty$.

Συμπίεση με τη μέθοδο random binning – Πιθανότητα σφάλματος

- Έστω $f(X^n)$ το bin που αντιστοιχεί στην ακολουθία X^n.
- Για να συμβεί σφάλμα αποκωδικοποίησης πρέπει
  1. Η X^n να είναι μη τυπική ή
  2. Το bin να περιέχει περισσότερες από μία τυπικές ακολουθίες.
- Επομένως,

$$
\begin{aligned}
P_e^{(n)} &= \Pr\{g(f(\mathbf{X})) \neq \mathbf{X}\} \\
&\overset{(a)}{\leq} \Pr\left\{\mathbf{X} \notin A_\epsilon^{(n)}\right\} + \sum_{\mathbf{x}} \Pr\left\{\exists \mathbf{x}' \neq \mathbf{x} : \mathbf{x}' \in A_\epsilon^{(n)}, f(\mathbf{x}') = f(\mathbf{x})\right\} p(\mathbf{x}) \\
&\overset{(b)}{\leq} \epsilon + \sum_{\mathbf{x}} \sum_{\mathbf{x}' \in A_\epsilon^{(n)}, \mathbf{x}' \neq \mathbf{x}} \Pr\{f(\mathbf{x}') = f(\mathbf{x})\} p(\mathbf{x})
\end{aligned}
$$

(a) από το φράγμα ένωσης (union bound), (b) από το AEP.

Συμπίεση με τη μέθοδο random binning – Πιθανότητα σφάλματος (2)

$$
\begin{aligned}
P_e^{(n)} &\leq \epsilon + \sum_{\mathbf{x}} \sum_{\mathbf{x}' \in A_\epsilon^{(n)}, \mathbf{x}' \neq \mathbf{x}} \Pr\{f(\mathbf{x}') = f(\mathbf{x})\} p(\mathbf{x}) \\
&\overset{(c)}{\leq} \epsilon + \sum_{\mathbf{x}} \sum_{\mathbf{x}' \in A_\epsilon^{(n)}} 2^{-nR} p(\mathbf{x}) \leq \epsilon + \sum_{\mathbf{x}' \in A_\epsilon^{(n)}} 2^{-nR} \sum_{\mathbf{x}} p(\mathbf{x}) \\
&= \epsilon + \sum_{\mathbf{x}' \in A_\epsilon^{(n)}} 2^{-nR} \overset{(d)}{\leq} \epsilon + 2^{n(H(X)+\epsilon)} 2^{-nR} \overset{(e)}{\leq} 2\epsilon.
\end{aligned}
$$

(c) λόγω του τυχαίου τρόπου δημιουργίας των bins, (d) από το AEP, εάν $R > H(X) + \epsilon$, (e) για αρκούντως μεγάλο n.

Συμπίεση με τη μέθοδο random binning – Σχόλια

- Η $P_e^{(n)}$ είναι η μέση πιθανότητα σφάλματος για όλους τους πιθανούς τρόπους δημιουργίας bins (θεωρήσαμε ότι $\Pr\{f(\mathbf{x}') = f(\mathbf{x})\} = 2^{-nR}$).
- Επομένως, υπάρχει τουλάχιστον ένας τρόπος δημιουργίας bins για τον οποίο η πιθανότητα αποτυχίας αποκωδικοποίησης τείνει στο 0.
- Επίσης, όπως και στην περίπτωση κωδικοποίησης καναλιού, από την ανισότητα Markov προκύπτει ότι για αρκούντως μεγάλο n, για οποιοδήποτε τρόπο δημιουργίας bins, $P_e^{(n)} \to 0$.
- Η κωδικοποίηση με χρήση random binning είναι ένας ακόμη τρόπος κωδικοποίησης.
- Παρατηρήστε ότι για να κωδικοποιήσουμε με random binning δεν απαιτείται να ελέγχουμε στον πομπό αν οι ακολουθίες που κωδικοποιούμε είναι τυπικές! (ωστόσο, χρειάζεται να το ελέγξουμε στο δέκτη)

Θεώρημα Slepian-Wolf

1. Θεωρία Πληροφορίας Δικτύων (Network Information Theory)

2. Κατανεμημένη Κωδικοποίηση
   - Μοντέλο και Ορισμοί
   - Random binning
   - Θεώρημα Slepian-Wolf

Θεώρημα Slepian-Wolf – ευθύ

- Θα αποδείξουμε το ευθύ του θεωρήματος Slepian-Wolf με χρήση random binning.
- Δημιουργία κώδικα: Ο κωδικοποιητής 1 αντιστοιχίζει ένα από 2^{nR_1} bins σε κάθε ακολουθία x^n με τυχαίο (ομοιόμορφο) τρόπο. Ο κωδικοποιητής 2 αντιστοιχίζει ένα από 2^{nR_2} bins σε κάθε ακολουθία y^n με τυχαίο (ομοιόμορφο) τρόπο.
- Οι αντιστοιχίσεις, έστω f_1 και f_2, αποκαλύπτονται στον αντίστοιχο κωδικοποιητή και στο (μοναδικό) αποκωδικοποιητή.
- Κωδικοποίηση: Ο πομπός 1 στέλνει το δείκτη του bin στο οποίο ανήκει η X^n (έστω m). Ο πομπός 2 στέλνει το δείκτη του bin στο οποίο ανήκει η Y^n (έστω n).

Θεώρημα Slepian-Wolf – ευθύ (2)

- Αποκωδικοποίηση: Με βάση το ζεύγος δεικτών (m, n), ο δέκτης αποκωδικοποιεί στις ακολουθίες $\hat{x}^n$ και $\hat{y}^n$ αν το ζεύγος ακολουθιών $(\hat{x}^n, \hat{y}^n)$ είναι από κοινού τυπικό και είναι το μοναδικό ζεύγος για το οποίο ισχύει $f_1(\hat{x}^n) = m$ και $f_2(\hat{y}^n) = n$. Αλλιώς, δηλώνει αδυναμία αποκωδικοποίησης.
- Τα ενδεχόμενα που οδηγούν σε σφάλμα είναι τα εξής
  1. $\mathcal{E}_0 \triangleq \left\{(X^n, Y^n) \notin A_\epsilon^{(n)}\right\}$.
  2. $\mathcal{E}_1 \triangleq \left\{\exists \tilde{x}^n \neq X^n : f_1(\tilde{x}^n) = f_1(X^n) \text{ και } (\tilde{x}^n, Y^n) \in A_\epsilon^{(n)}\right\}$.
  3. $\mathcal{E}_2 \triangleq \left\{\exists \tilde{y}^n \neq Y^n : f_2(\tilde{y}^n) = f_2(Y^n) \text{ και } (X^n, \tilde{y}^n) \in A_\epsilon^{(n)}\right\}$.
  4. $$\begin{aligned}\mathcal{E}_{12} \triangleq \{\exists (\tilde{x}^n, \tilde{y}^n) : \tilde{x}^n \neq X^n, \tilde{y}^n \neq Y^n, f_1(\tilde{x}^n) = f_1(X^n),\\ f_2(\tilde{y}^n) = f_2(Y^n) \text{ και } (\tilde{x}^n, \tilde{y}^n) \in A_\epsilon^{(n)}\right\}\end{aligned}$$

Θεώρημα Slepian-Wolf – ευθύ (3)

- Υπολογισμός πιθανότητας σφάλματος: Επομένως,

$$\begin{aligned} P_e^{(n)} &= \Pr\left\{\mathcal{E}_0 \cup \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_{12}\right\} \\ &\leq \Pr\{\mathcal{E}_0\} + \Pr\{\mathcal{E}_1\} + \Pr\{\mathcal{E}_2\} + \Pr\{\mathcal{E}_{12}\}. \end{aligned}$$

- Από το AEP, για αρκούντως μεγάλο n, $\Pr\{\mathcal{E}_0\} < \epsilon$.
- Για το ενδεχόμενο $\mathcal{E}_1$,

$$\begin{aligned} \Pr\{\mathcal{E}_1\} &= \Pr\left\{\exists \tilde{x}^n \neq X^n : f_1(\tilde{x}^n) = f_1(X^n) \text{ και } (\tilde{x}^n, Y^n) \in A_\epsilon^{(n)}\right\} \\ &= \sum_{(x^n, y^n)} p(x^n, y^n) \Pr\left\{\exists \tilde{x}^n \neq x^n : f_1(\tilde{x}^n) = f_1(x^n) \text{ και } (\tilde{x}^n, y^n) \in A_\epsilon^{(n)}\right\} \\ &\leq \sum_{(x^n, y^n)} p(x^n, y^n) \sum_{\tilde{x}^n \neq x^n, (\tilde{x}^n, y^n) \in A_\epsilon^{(n)}} \Pr\left\{f_1(\tilde{x}^n) = f_1(x^n)\right\}. \end{aligned}$$

Θεώρημα Slepian-Wolf – ευθύ (4)

$$\Pr\{\mathcal{E}_1\} \leq \sum_{(x^n,y^n)} p\left(x^n, y^n\right) \sum_{\tilde{x}^n \neq x^n, (\tilde{x}^n, y^n) \in A_\epsilon^{(n)}} \Pr\left\{f_1\left(\tilde{x}^n\right) = f_1\left(x^n\right)\right\}$$

$$\stackrel{(a)}{=} \sum_{(x^n,y^n)} p\left(x^n, y^n\right) 2^{-nR_1} \left|A_\epsilon^{(n)}(X|y^n)\right|$$

$$\stackrel{(b)}{\leq} 2^{-nR_1} 2^{n(H(X|Y)+2\epsilon)} \to 0, \text{ εάν } R_1 > H(X|Y) + 2\epsilon.$$

(a) λόγω του ομοιόμορφου random binning (και επειδή ο μέσος όρος υπολογίζεται για όλους τους τρόπους random binning) (b) Θα αποδείξουμε ότι ο αριθμός των ακολουθιών X^n που είναι από κοινού τυπικές με *συγκεκριμένη* τυπική ακολουθία y^n ικανοποιεί τη σχέση $\left|A_\epsilon^{(n)}(X|y^n)\right| \leq 2^{n(H(X|Y)+2\epsilon)}$.

Θεώρημα Slepian-Wolf – ευθύ (5)

- Με παρόμοιο τρόπο μπορούμε να δείξουμε ότι
  - $\Pr\{\mathcal{E}_2\} \leq \epsilon$ για αρκούντως μεγάλο n εάν $R_2 > H(Y|X)$ και
  - $\Pr\{\mathcal{E}_{12}\} \leq \epsilon$ για αρκούντως μεγάλο n εάν $R_1 + R_2 > H(X, Y)$.
- Συνεπώς, για αρκούντως μεγάλο n, και εάν ικανοποιούνται οι συνθήκες του Θεωρήματος Slepian-Wolf υπάρχουν δύο random binnings f_1^* και f_2^* τέτοια ώστε η πιθανότητα σφάλματος να μην υπερβαίνει το 4ϵ.

Υπό συνθήκη τυπικές ακολουθίες

- Θεώρημα 11.6. (Cover & Thomas, Theorem 15.2.2.) Εάν $A_\epsilon^{(n)}(X|y^n)$ είναι το σύνολο των ακολουθιών X^n που είναι από κοινού (ασθενώς) ϵ-τυπικές με μία συγκεκριμένη τυπική ακολουθία $y^n \in A_\epsilon^{(n)}(Y)$,

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

Επίσης, για αρκούντως μεγάλο n,

$$(1-\epsilon)2^{n(H(X|Y)-2\epsilon)} \leq \sum_{y^n} p(y^n)\left|A_\epsilon^{(n)}(X|y^n)\right|.$$

Υπό συνθήκη τυπικές ακολουθίες (2)

- Λήμμα 11.7. (Cover & Thomas Theorem 15.2.1.4:) Θα αποδείξουμε, πρώτα, το εξής: Αν ένα ζεύγος ακολουθιών (x^n, y^n) είναι από κοινού (ασθενώς) $\epsilon-$τυπικό,

$$2^{-n(H(X|Y)+2\epsilon)} \leq p(x^n|y^n) \leq 2^{-n(H(X|Y)-2\epsilon)}.$$

- Απόδειξη: Επειδή το ζεύγος (x^n, y^n) είναι από κοινού $\epsilon-$τυπικό,

$$2^{-n(H(X,Y)+\epsilon)} \leq p(x^n, y^n) \leq 2^{-n(H(X,Y)-\epsilon)}.$$

Επίσης, επειδή η ακολουθία y^n είναι $\epsilon-$τυπική,

$$2^{-n(H(Y)+\epsilon)} \leq p(y^n) \leq 2^{-n(H(Y)-\epsilon)}.$$

Διαιρώντας, προκύπτει το ζητούμενο.

Υπό συνθήκη τυπικές ακολουθίες (3)

- Απόδειξη Θεωρήματος 11.6: Για την πρώτη ανισότητα,

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

(a) από το Λήμμα 11.7.

- Για τη δεύτερη ανισότητα, αν το n είναι αρκετά μεγάλο,

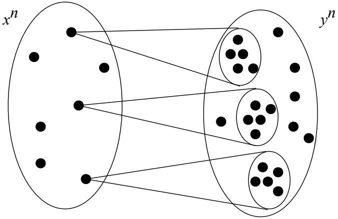
$$1 - \epsilon \leq \sum_{(x^n, y^n) \in A_\epsilon^{(n)}(X,Y)} p(x^n, y^n)$$
$$= \sum_{y^n \in A_\epsilon^{(n)}(Y)} p(y^n) \sum_{x^n \in A_\epsilon^{(n)}(X|y^n)} p(x^n|y^n)$$

Υπό συνθήκη τυπικές ακολουθίες (4)

$$
\begin{aligned}
1-\epsilon &\leq \sum_{y^n \in A_\epsilon^{(n)}(Y)} p(y^n) \sum_{x^n \in A_\epsilon^{(n)}(X|y^n)} p(x^n|y^n) \\
&\leq \sum_{y^n} p(y^n) \sum_{x^n \in A_\epsilon^{(n)}(X|y^n)} p(x^n|y^n) \\
&\overset{(b)}{\leq} \sum_{y^n} p(y^n) \sum_{x^n \in A_\epsilon^{(n)}(X|y^n)} 2^{-n(H(X|Y)-2\epsilon)} \\
&= \sum_{y^n} p(y^n) \left|A_\epsilon^{(n)}(X|y^n)\right| 2^{-n(H(X|Y)-2\epsilon)}.
\end{aligned}
$$

(b) από το Λήμμα 11.7.

Ερμηνεία της κωδικοποίησης Slepian-Wolf

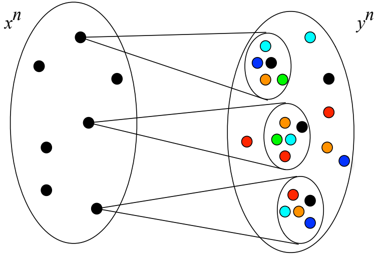


- Όπως είδαμε, σε κάθε τυπική ακολουθία x^n αντιστοιχούν $\left|A_\epsilon^{(n)}(Y|x^n)\right|$ τυπικές ακολουθίες Y^n, όπου

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

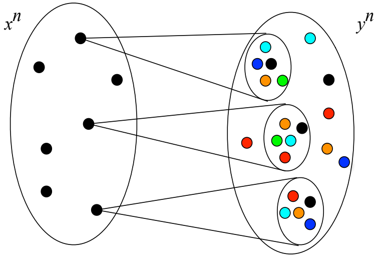
- Αν ο κωδικοποιητής της πηγής Y γνωρίζει την ακολουθία x^n αρκούν $H(Y|X) + 2\epsilon$ bits κατά μέσο όρο για την κωδικοποίηση κάθε συμβόλου της y^n.

Ερμηνεία της κωδικοποίησης Slepian-Wolf (2)



- Αν ο κωδικοποιητής της Y δε γνωρίζει την x^n, "χρωματίζει" τυχαία (και ομοιόμορφα) όλες τις ακολουθίες y^n χρησιμοποιώντας 2^{nR_2} χρώματα.
- Επειδή $R_2 > H(Y|X) + 2\epsilon$, καθώς το $n \to \infty$, η πιθανότητα δύο ακολουθίες με το ίδιο χρώμα να βρεθούν στο ίδιο bin τείνει στο 0.

Ερμηνεία της κωδικοποίησης Slepian-Wolf (3)



- Επομένως, αν ο κωδικοποιητής της X στείλει το bin στο οποίο ανήκει η x^n και ο κωδικοποιητής της Y στείλει το "χρώμα" της y^n, ο αποκωδικοποιητής μπορεί να εκτιμήσει το ζεύγος (x^n, y^n) με $P_e^{(n)} \to 0$ για $n \to \infty$.
- Συνεπώς, αρκεί $R_x + R_y > H(X) + \epsilon + H(Y|X) + 2\epsilon = H(X,Y) + 3\epsilon$.

Ερμηνεία της κωδικοποίησης Slepian-Wolf (4)

- Μπορούμε να επιτύχουμε τον ίδιο συνολικό ρυθμό μετάδοσης αν ο κωδικοποιητής της Y στέλνει το δείκτη του bin της ακολουθίας y^n και ο κωδικοποιητής της X στέλνει το "χρώμα" της x^n.
- Επίσης, μπορούμε να επιτύχουμε οποιαδήποτε R_x και R_y τέτοια ώστε $R_x + R_y > H(X, Y)$ με διαμοιρασμό χρόνου (time sharing):
  - Για α % του χρόνου, $R_x > H(X)$ και $R_y > H(Y|X)$ (αρκεί το n να είναι αρκετά μεγάλο).
  - Για $1 - \alpha$ % του χρόνου, $R_y > H(Y)$ και $R_x > H(X|Y)$ (αρκεί το n να είναι αρκετά μεγάλο).
  - Συνεπώς, $R_x > \alpha H(X) + (1-\alpha)H(X|Y)$, $R_y > \alpha H(Y|X) + (1-\alpha)H(Y)$ και $R_x + R_y > H(X, Y)$.
  - Εάν μεταδίδουμε ακριβώς επάνω στο όριο, η τιμή του α καθορίζει το σημείο της ευθείας $R_x + R_y = H(X, Y)$ πάνω στο οποίο βρίσκονται τα R_x και R_y.

Θεώρημα Slepian-Wolf – αντίστροφο

- Το αντίστροφο του θεωρήματος Slepian-Wolf μπορεί να αποδειχτεί άμεσα με χρήση του ακόλουθου επιχειρήματος:
  - Αν επιτρέψουμε στους δύο κωδικοποιητές πηγής να συνεργαστούν, η συμπίεση θα είναι τουλάχιστον τόσο καλή όσο στην περίπτωση που δε συνεργάζονται (αφού, αν θέλουν, μπορούν να επιλέξουν να μη συνεργαστούν, αν αυτό είναι καλύτερο).
  - Ωστόσο, από το Θεώρημα Κωδικοποίησης Πηγής γνωρίζουμε ότι, προκειμένου $P_e^{(n)} \to 0$, πρέπει $R_x + R_y > H(X,Y)$.
- Για μια απευθείας απόδειξη του αντιστρόφου, χωρίς χρήση του Θεωρήματος Κωδικοποίησης μίας πηγής, δείτε, π.χ. Cover & Thomas.

Κατανεμημένη κωδικοποίηση με μηδενική πιθανότητα αδυναμίας αποκωδικοποίησης

- Όταν αναφερθήκαμε στην κωδικοποίηση μίας πηγής είδαμε ότι, στο όριο, μπορούμε να επιτύχουμε κωδικοποίηση με $P_e^{(n)}$ ακριβώς ίση με 0 για $n \to \infty$ (χρησιμοποιώντας, για παράδειγμα, κώδικα Huffman ή αριθμητική κωδικοποίηση).
- Ωστόσο, στη γενική περίπτωση, αυτό *δεν* ισχύει στην κατανεμημένη κωδικοποίηση. Δηλαδή, δεν μπορούμε να επιτύχουμε $R_x + R_y = H(X, Y)$ και ακριβώς μηδενική πιθανότητα σφάλματος.

Γενίκευση για K πηγές και για πηγές με μνήμη

- Μπορεί να αποδειχτεί (με παρόμοιο τρόπο όπως στην περίπτωση δύο χρηστών) ότι, για το πρόβλημα κατανεμημένης συμπίεσης K πηγών, οι ρυθμοί συμπίεσης πρέπει να ικανοποιούν τις σχέσεις

$$R(S) < H(X(S)|X(S^c)) \text{ για όλα τα } S \subseteq \{1, 2, \ldots, K\},$$

όπου

$$R(S) = \sum_{i \in S} R_i \text{ και}$$
$$X(S) = \{X_i, i \in S\}.$$

- Μπορεί, επίσης, να αποδειχτεί ότι, όταν οι πηγές έχουν μνήμη και είναι από κοινού στάσιμες και εργοδικές, αρκεί να αντικαταστήσουμε εντροπίες με ρυθμούς εντροπίας.