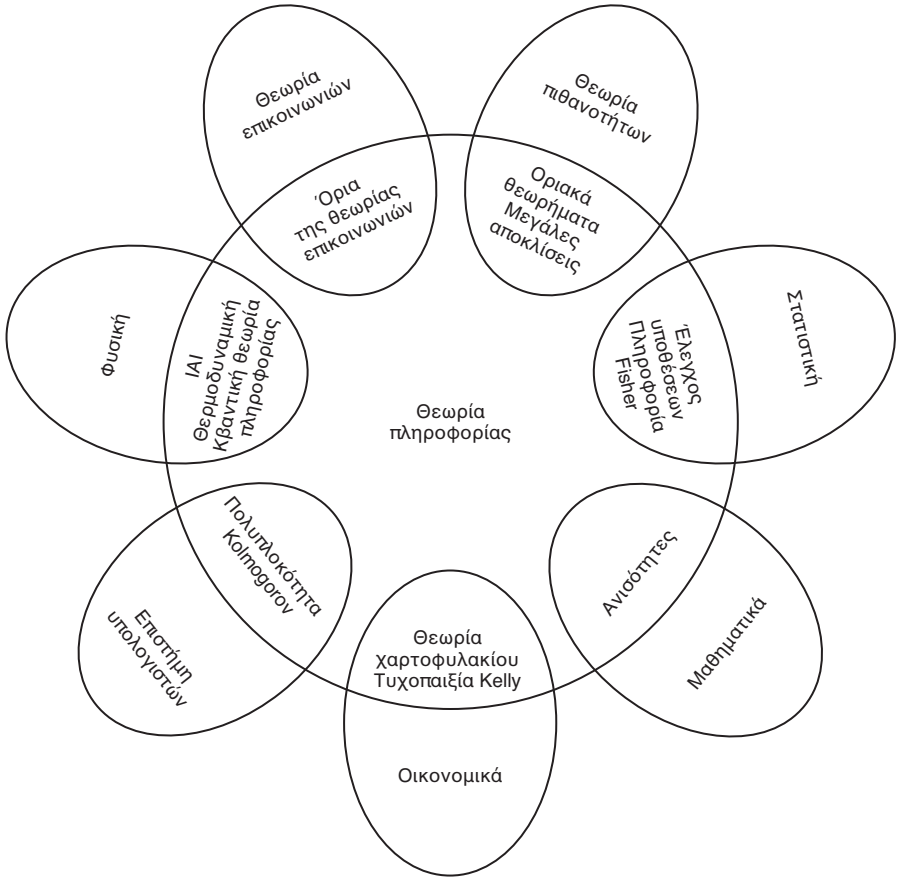
ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ ΚΑΙ ΠΡΟΕΠΙΣΚΟΠΗΣΗ

Η θεωρία πληροφορίας δίνει απαντήσεις σε δύο θεμελιώδη ερωτήματα της θεωρίας επικοινωνιών: Ποια είναι η «υπέρτατη» συμπίεση δεδομένων (απάντηση: η εντροπία H) και ποιος ο υπέρτατος ρυθμός μετάδοσης που μπορεί να επιτευχθεί σε μια επικοινωνία (απάντηση: η χωρητικότητα διαύλου C). Γι' αυτό τον λόγο κάποιοι θεωρούν τη θεωρία πληροφορίας υποσύνολο της θεωρίας επικοινωνιών. Υποστηρίζουμε ότι είναι κάτι πολύ περισσότερο. Πράγματι, οι συνεισφορές της στη στατιστική φυσική (θερμοδυναμική), στην επιστήμη των υπολογιστών (πολυπλοκότητα Kolmogorov ή αλγοριθμική πολυπλοκότητα), στη στατιστική συμπερασματολογία (ξυράφι του Όκκαμ: «η απλούστερη εξήγηση είναι η καλύτερη») και στις πιθανότητες και στη στατιστική (εκθέτες σφάλματος για τον βέλτιστο έλεγχο υποθέσεων και εκτίμηση) είναι θεμελιώδεις.

Σε αυτό το κεφάλαιο, που αποτελεί ένα είδος «πρώτης διάλεξης», θα περιηγηθούμε στη θεωρία πληροφορίας και τις εκ φύσεως σχετιζόμενες με αυτήν έννοιες. Η πλήρης παράθεση των ορισμών και η αναλυτική μελέτη του αντικειμένου ξεκινούν στο Κεφάλαιο 2. Στο Σχήμα 1.1 παρουσιάζεται η σχέση της θεωρίας πληροφορίας με άλλα γνωστικά αντικείμενα. Όπως φαίνεται στο σχήμα, η θεωρία πληροφορίας έχει κοινές περιοχές με τη φυσική (στατιστική μηχανική), τα μαθηματικά (θεωρία πιθανοτήτων), την ηλεκτρομηχανική (θεωρία επικοινωνιών) και την επιστήμη των υπολογιστών (αλγοριθμική πολυπλοκότητα). Ακολούθως θα περιγράψουμε λεπτομερέστερα αυτές τις περιοχές.

Ηλεκτρομηχανική (θεωρία επικοινωνιών). Στις αρχές της δεκαετίας του 1940 εθεωρείτο ότι είναι αδύνατο να σταλεί πληροφορία με θετικό ρυθμό και αμελητέα πιθανότητα σφάλματος. Ο Shannon εξέπληξε τους επιστήμονες που ασχολούνταν με τη θεωρία επικοινωνιών αποδεικνύοντας ότι η πιθανότητα σφάλματος μπορούσε να γίνει σχεδόν μηδενική για κάθε ρυθμό επικοινωνίας μικρότερο από τη χωρητικότητα του διαύλου. Η χωρητικότητα μπορεί να υπολογιστεί με απλό τρόπο από τα χαρακτηριστικά του διαύλου που αφορούν τον θόρυβο. Ο Shannon υποστήριξε επιπλέον ότι τυχαίες διεργασίες όπως η μουσική και η ομιλία έχουν ένα επίπεδο πολυπλοκότητας ανεπίδεκτο περαιτέρω μείωσης και ότι το σήμα δεν μπορεί να συμπιεστεί περισσότερο από όσο επιτρέπει αυτό το επίπεδο. Σε αυτή την ποσότητα έδωσε το όνομα *εντροπία*, έχοντας υπόψη του την παράλ-

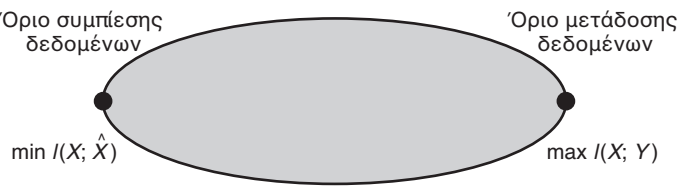


ΣΧΗΜΑ 1.1. Σχέση της θεωρίας πληροφορίας με άλλα γνωστικά αντικείμενα.

ληλη χρήση του όρου στη θερμοδυναμική, και έδειξε ότι αν η εντροπία της πηγής είναι μικρότερη από τη χωρητικότητα του διαύλου, τότε ασυμπτωτικά μπορεί να επιτευχθεί επικοινωνία άνευ σφαλμάτων.

Όπως φαίνεται στο ιδιόρρυθμο Σχήμα 1.2, σήμερα η θεωρία πληροφορίας αντιπροσωπεύει τα ακραία σημεία του συνόλου όλων των δυνατών τεχνικών επικοινωνίας. Στο ένα άκρο του συνόλου των δυνατών τεχνικών επικοινωνίας βρίσκεται το ελάχιστο $I(X;\hat{X})$ της συμπίεσης δεδομένων. Σε όλες τις τεχνικές συμπίεσης δεδομένων ο ρυθμός περιγραφής πρέπει να είναι τουλάχιστον ίσος με αυτό το ελάχιστο. Στο άλλο άκρο βρίσκεται το μέγιστο $I(X;Y)$ της μετάδοσης δεδομένων, που είναι γνωστό ως *χωρητικότητα διαύλου*. Συνεπώς, όλες οι τεχνικές διαμόρφωσης και συμπίεσης δεδομένων βρίσκονται μεταξύ αυτών των ορίων.

Η θεωρία πληροφορίας προτείνει επίσης τρόπους για την επίτευξη αυτών των



ΣΧΗΜΑ 1.2. Η θεωρία πληροφορίας αντιπροσωπεύει τα δύο ακραία σημεία της θεωρίας επικοινωνιών.

έσχατων ορίων που διέπουν την επικοινωνία. Ωστόσο, αυτές οι θεωρητικά βέλτιστες τεχνικές επικοινωνίας, όσο κομψές και αν είναι, πιθανόν να μην είναι καθόλου πρακτικές από υπολογιστικής πλευράς. Το γεγονός ότι χρησιμοποιούμε κάποιες απλές τεχνικές διαμόρφωσης και αποδιαμόρφωσης αντί της τυχαίας κωδικοποίησης και του κανόνα αποκωδικοποίησης βάσει του πλησιέστερου γείτονα που προτείνεται στην απόδειξη του Shannon για το θεώρημα χωρητικότητας διαύλου οφείλεται απλώς και μόνο στην υπολογιστική εφικτότητά τους. Η πρόοδος στα ολοκληρωμένα κυκλώματα και τον σχεδιασμό κωδίκων μάς έχει επιτρέψει να απολαύσουμε κάποια από τα οφέλη που προβλέπει η θεωρία του Shannon. Η υπολογιστική πρακτικότητα τελικά επιτεύχθηκε με την έλευση των κωδίκων turbo. Ένα καλό παράδειγμα εφαρμογής των ιδεών της θεωρίας πληροφορίας είναι η χρήση των κωδίκων διόρθωσης σφαλμάτων στους συμπαγείς δίσκους και στα DVD.

Η πρόσφατη ερευνητική δραστηριότητα πάνω στις πλευρές της θεωρίας πληροφορίας που αφορούν τις επικοινωνίες έχει επικεντρωθεί στη δικτυακή θεωρία πληροφορίας: τη θεωρία των ταυτόχρονων ρυθμών μετάδοσης από πολλούς πομπούς σε πολλούς δέκτες παρουσία παρεμβολής και θορύβου. Κάποιες από τις σχέσεις αλληλεξάρτησης των ρυθμών μεταξύ πομπών και δεκτών είναι μη αναμενόμενες, αλλά όλες τους έχουν μια μαθηματική απλότητα. Ωστόσο, δεν έχει βρεθεί ακόμα κάποια ενιαία θεωρία.

Επιστήμη των υπολογιστών (πολυπλοκότητα Kolmogorov). Οι Kolmogorov, Chaitin και Solomonoff διατύπωσαν την ιδέα ότι η πολυπλοκότητα μιας συμβολοσειράς δεδομένων μπορεί να οριστεί μέσω του μήκους του μικρότερου δυνατού δυαδικού προγράμματος υπολογιστή που υπολογίζει τη συγκεκριμένη συμβολοσειρά. Δηλαδή η πολυπλοκότητα είναι το ελαχιστιαίο μήκος περιγραφής. Όπως αποδεικνύεται, αυτός ο ορισμός της πολυπλοκότητας είναι καθολικός, δηλαδή ανεξάρτητος από τον εκάστοτε υπολογιστή, και θεμελιώδους σημασίας. Επομένως, η πολυπλοκότητα Kolmogorov θέτει τις βάσεις για *τη* θεωρία της περιγραφικής πολυπλοκότητας. Είναι μάλιστα ιδιαίτερα ευχάριστο το γεγονός ότι η πολυπλοκότητα Kolmogorov K είναι προσεγγιστικά ίση με την εντροπία Shannon H

αν η ακολουθία λαμβάνεται τυχαία σύμφωνα με μια κατανομή που έχει εντροπία H. Άρα η σχέση μεταξύ θεωρίας πληροφορίας και πολυπλοκότητας Kolmogorov είναι τέλεια. Πράγματι, η πολυπλοκότητα Kolmogorov θεωρείται πιο θεμελιώδης από την εντροπία Shannon. Είναι η υπέρτατη συμπίεση δεδομένων και οδηγεί σε έναν λογικά συνεπή τρόπο εξαγωγής συμπερασμάτων.

Υπάρχει μια ευχάριστη συμπληρωματική σχέση μεταξύ της αλγοριθμικής και της υπολογιστικής πολυπλοκότητας. Μπορούμε να φανταστούμε την υπολογιστική πολυπλοκότητα (χρονική πολυπλοκότητα) και την πολυπλοκότητα Kolmogorov (μήκος προγράμματος ή περιγραφική πολυπλοκότητα) σαν δύο άξονες που αντιστοιχούν ο πρώτος στον χρόνο εκτέλεσης και ο δεύτερος στο μήκος ενός προγράμματος. Η πολυπλοκότητα Kolmogorov επικεντρώνεται στην ελαχιστοποίηση ως προς τον δεύτερο άξονα, ενώ η υπολογιστική πολυπλοκότητα στην ελαχιστοποίηση ως προς τον πρώτο άξονα. Η ταυτόχρονη ελαχιστοποίηση και των δύο δεν έχει μελετηθεί ακόμη αρκετά.

Φυσική (θερμοδυναμική). Η εντροπία και ο δεύτερος νόμος της θερμοδυναμικής γεννήθηκαν στους κόλπους της στατιστικής μηχανικής. Η εντροπία αυξάνεται πάντα. Μεταξύ άλλων, ο δεύτερος νόμος μάς επιτρέπει να απορρίψουμε κάθε ισχυρισμό περί αεικίνητων μηχανών. Θα αναφερθούμε εν συντομία στον δεύτερο νόμο στο Κεφάλαιο 4.

Μαθηματικά (θεωρία πιθανοτήτων και στατιστική). Οι θεμελιώδεις ποσότητες της θεωρίας πληροφορίας –η εντροπία, η σχετική εντροπία και η αμοιβαία πληροφορία– ορίζονται ως συναρτησιοειδή κατανομών πιθανότητας. Χαρακτηρίζουν τη συμπεριφορά μακρών ακολουθιών τυχαίων μεταβλητών και μας επιτρέπουν να εκτιμούμε τις πιθανότητες σπάνιων ενδεχομένων (θεωρία μεγάλων αποκλίσεων) και να βρίσκουμε τον καλύτερο εκθέτη σφάλματος κατά τον έλεγχο υποθέσεων.

Φιλοσοφία της επιστήμης (ξυράφι του Όκκαμ). Ο Γουλιέλμος του Όκκαμ είχε πει: «Τα αίτια δεν πρέπει να πολλαπλασιάζονται περισσότερο από όσο είναι απαραίτητο», με άλλα λόγια: «Η απλούστερη εξήγηση είναι η καλύτερη». Οι Solomonoff και Chaitin υποστήριξαν ότι αν πάρουμε έναν σταθμισμένο συνδυασμό όλων των προγραμμάτων που εξηγούν κάποια δεδομένα και παρατηρήσουμε την επόμενη έξοδό τους, τότε έχουμε μια καθολικά καλή μέθοδο πρόβλεψης. Επιπλέον, αυτή η διαδικασία εξαγωγής συμπερασμάτων είναι αποτελεσματική σε πολλά προβλήματα που δεν μπορούμε να χειριστούμε μέσω της στατιστικής. Για παράδειγμα, αυτή η μέθοδος θα προβλέψει τελικά τα επόμενα ψηφία του π. Αν την εφαρμόσουμε στις ρίψεις ενός κέρματος που φέρνει γράμματα με πιθανότητα $0{,}7$, θα το συμπεράνουμε και αυτό. Αν την εφαρμόσουμε στη χρηματιστηριακή αγορά,

θα πρέπει ουσιαστικά να βρει όλους τους «νόμους» της χρηματιστηριακής αγοράς και να τους προεκβάλει κατά βέλτιστο τρόπο. Θεωρητικά, χρησιμοποιώντας μια τέτοια μέθοδο θα μπορούσαμε να ανακαλύψουμε και τους νόμους της φυσικής του Νεύτωνα. Ασφαλώς, η συγκεκριμένη μέθοδος εξαγωγής συμπερασμάτων δεν είναι καθόλου πρακτική, διότι για να απορριφθούν όλα τα προγράμματα υπολογιστή που δεν καταφέρνουν να παραγάγουν τα υπάρχοντα δεδομένα απαιτείται απαγορευτικά πολύς χρόνος. Θα προβλέπαμε τι πρόκειται να συμβεί αύριο ύστερα από εκατό χρόνια.

Οικονομικά (επενδύσεις). Οι επαναλαμβανόμενες επενδύσεις σε μια στάσιμη χρηματιστηριακή αγορά έχουν ως αποτέλεσμα την εκθετική μεγέθυνση του πλούτου. Ο ρυθμός μεγέθυνσης του πλούτου είναι μια δυϊκή ποσότητα του ρυθμού εντροπίας της χρηματιστηριακής αγοράς. Οι αντιστοιχίες μεταξύ της θεωρίας βέλτιστων επενδύσεων σε μια χρηματιστηριακή αγορά και της θεωρίας πληροφορίας είναι εντυπωσιακές. Για να μελετήσουμε αυτή τη δυϊκότητα θα αναπτύξουμε τη θεωρία επενδύσεων.

Υπολογισμός και επικοινωνία. Καθώς κατασκευάζουμε ολοένα και μεγαλύτερους υπολογιστές από ολοένα και μικρότερα μέρη, βρισκόμαστε αντιμέτωποι με ένα όριο που αφορά τόσο τις υπολογιστικές όσο και τις επικοινωνιακές δυνατότητες. Οι επικοινωνιακές δυνατότητες επιβάλλουν περιορισμούς στις υπολογιστικές δυνατότητες και οι υπολογιστικές δυνατότητες επιβάλλουν περιορισμούς στις επικοινωνιακές δυνατότητες. Αυτά τα δύο συνυφαίνονται, και έτσι όλες οι ανακαλύψεις της θεωρίας επικοινωνιών μέσω της θεωρίας πληροφορίας έχουν άμεση επίδραση στη θεωρία υπολογισμού.

1.1 ΠΡΟΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΠΕΡΙΕΧΟΜΕΝΩΝ ΤΟΥ ΒΙΒΛΙΟΥ

Τα πρωταρχικά ερωτήματα που πραγματεύεται η θεωρία πληροφορίας εμπίπτουν στις περιοχές της συμπίεσης και της μετάδοσης δεδομένων. Οι απαντήσεις είναι ποσότητες όπως η εντροπία και η αμοιβαία πληροφορία, οι οποίες είναι συναρτήσεις των κατανομών πιθανότητας που διέπουν την εκάστοτε επικοινωνιακή διεργασία. Μερικοί ορισμοί θα διευκολύνουν την αρχική μας ανάλυση. Οι ορισμοί αυτοί επαναλαμβάνονται στο Κεφάλαιο 2.

Η εντροπία μιας τυχαίας μεταβλητής X με συνάρτηση μάζας πιθανότητας $p(x)$ ορίζεται ως εξής:

$$H(X) = -\sum_{x} p(x) \log_2 p(x). \tag{1.1}$$

Χρησιμοποιούμε λογαρίθμους με βάση το 2, οπότε η εντροπία θα μετριέται σε δυφία. Η εντροπία είναι μέτρο της μέσης αβεβαιότητας της τυχαίας μεταβλητής.

Είναι το πλήθος των δυφίων που απαιτούνται κατά μέσο όρο για την περιγραφή της τυχαίας μεταβλητής.

Παράδειγμα 1.1.1 Θεωρήστε μια τυχαία μεταβλητή που είναι ομοιόμορφα κατανεμημένη με 32 δυνατές εκβάσεις. Για να ξεχωρίζουμε μεταξύ τους τις διάφορες εκβάσεις, χρειαζόμαστε μια επιγραφή που μπορεί να πάρει 32 διαφορετικές τιμές. Επομένως, οι 5-δύφιες συμβολοσειρές είναι κατάλληλες για επιγραφές.

Η εντροπία αυτής της τυχαίας μεταβλητής είναι

$$H(X) = -\sum_{i=1}^{32} p(i) \log p(i) = -\sum_{i=1}^{32} \frac{1}{32} \log \frac{1}{32} = \log 32 = 5 \text{ δυφία}, \qquad (1.2)$$

το οποίο συμπίπτει με το πλήθος των δυφίων που απαιτούνται για την περιγραφή της X. Σε αυτή την περίπτωση, όλες οι εκβάσεις έχουν ισομήκεις αναπαραστάσεις.

Ακολούθως εξετάζουμε ένα παράδειγμα όπου η κατανομή είναι μη ομοιόμορφη.

Παράδειγμα 1.1.2 Υποθέστε ότι έχουμε μια ιπποδρομία στην οποία συμμετέχουν οκτώ άλογα και θεωρήστε ότι οι πιθανότητες νίκης καθενός εξ αυτών είναι $\left(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{64}, \frac{1}{64}, \frac{1}{64}, \frac{1}{64}\right)$. Η εντροπία της ιπποδρομίας υπολογίζεται ως εξής:

$$\begin{aligned} H(X) &= -\frac{1}{2} \log \frac{1}{2} - \frac{1}{4} \log \frac{1}{4} - \frac{1}{8} \log \frac{1}{8} - \frac{1}{16} \log \frac{1}{16} - 4 \frac{1}{64} \log \frac{1}{64} \\ &= 2 \text{ δυφία}. \end{aligned} \qquad (1.3)$$

Υποθέστε ότι θέλουμε να στείλουμε ένα μήνυμα που να αναφέρει ποιο άλογο νίκησε στην ιπποδρομία. Μια δυνατή επιλογή είναι να στείλουμε τον αύξοντα αριθμό του αλόγου που νίκησε. Η περιγραφή αυτή απαιτεί 3 δυφία, όποιο και να είναι το άλογο. Δεδομένου όμως ότι οι πιθανότητες νίκης δεν είναι ομοιόμορφες, θα είχε νόημα να χρησιμοποιήσουμε βραχύτερες περιγραφές για τα άλογα που έχουν περισσότερες πιθανότητες να νικήσουν και μεγαλύτερου μήκους περιγραφές για τα άλογα που έχουν λιγότερες πιθανότητες, ώστε να πετύχουμε μικρότερο μέσο μήκος περιγραφής. Για παράδειγμα, θα μπορούσαμε να χρησιμοποιήσουμε το ακόλουθο σύνολο δυφιοσειρών για να αναπαραστήσουμε τα οκτώ άλογα: 0, 10, 110, 1110, 111100, 111101, 111110, 111111. Σε αυτή την περίπτωση το μέσο μήκος περιγραφής είναι 2 δυφία, ενώ στην περίπτωση του ομοιόμορφου κώδικα ήταν 3 δυφία. Παρατηρήστε ότι σε αυτή την περίπτωση το μέσο μήκος περιγραφής ισούται με την εντροπία. Στο Κεφάλαιο 5 θα δείξουμε ότι η εντροπία μιας τυχαίας μεταβλητής είναι ένα κάτω φράγμα του μέσου πλήθους δυφίων που απαιτούνται

για την αναπαράσταση της τυχαίας μεταβλητής, καθώς και του μέσου πλήθους ερωτήσεων που απαιτούνται για τον προσδιορισμό της τιμής της μεταβλητής σε ένα παίγνιο «20 ερωτήσεων». Θα δείξουμε επίσης πώς μπορούμε να κατασκευάσουμε αναπαραστάσεις με μέσο μήκος που να διαφέρει το πολύ κατά 1 δυφίο από την εντροπία.

Η έννοια της εντροπίας στη θεωρία πληροφορίας σχετίζεται με την έννοια της εντροπίας στη στατιστική μηχανική. Αν έχουμε μια ακολουθία n ανεξάρτητων και ταυτόνομων[1] τυχαίων μεταβλητών, θα δείξουμε ότι η πιθανότητα μιας «τυπικής» ακολουθίας είναι περίπου $2^{-nH(X)}$ και ότι υπάρχουν περίπου $2^{nH(X)}$ τέτοιες τυπικές ακολουθίες. Η ιδιότητα αυτή (που είναι γνωστή ως *ιδιότητα της ασυμπτωτικής ισοκατανομής* (ΙΑΙ)) αποτελεί τη βάση πολλών αποδείξεων στη θεωρία πληροφορίας. Στην πορεία θα παρουσιάσουμε και άλλα προβλήματα στα οποία η εντροπία αναδεικνύεται ως φυσική απάντηση (π.χ. το πλήθος των ρίψεων ενός τίμιου κέρματος που απαιτούνται για την παραγωγή μιας τυχαίας μεταβλητής).

Επεκτείνοντας την έννοια της περιγραφικής πολυπλοκότητας μιας τυχαίας μεταβλητής μπορούμε να ορίσουμε την περιγραφική πολυπλοκότητα μιας απλής συμβολοσειράς. Η *πολυπλοκότητα Kolmogorov* μιας δυαδικής συμβολοσειράς ορίζεται ως το μήκος του μικρότερου δυνατού προγράμματος υπολογιστή που τυπώνει τη συγκεκριμένη συμβολοσειρά. Όπως θα αποδειχθεί, αν η συμβολοσειρά είναι πράγματι τυχαία, τότε η πολυπλοκότητα Kolmogorov είναι κοντά στην εντροπία. Η πολυπλοκότητα Kolmogorov αποτελεί ένα φυσικό πλαίσιο για τη μελέτη των προβλημάτων της στατιστικής συμπερασματολογίας και μοντελοποίησης, και μας βοηθά να κατανοήσουμε καλύτερα το *ξυράφι του Όκκαμ*: «Η απλούστερη εξήγηση είναι η καλύτερη». Στο Κεφάλαιο 1 θα περιγράψουμε μερικές απλές ιδιότητες της πολυπλοκότητας Kolmogorov.

Η *εντροπία* είναι η αβεβαιότητα μιας απλής τυχαίας μεταβλητής. Μπορούμε επίσης να ορίσουμε τη δεσμευμένη εντροπία $H(X|Y)$, που είναι η εντροπία μιας τυχαίας μεταβλητής με δεδομένο ότι γνωρίζουμε μια άλλη τυχαία μεταβλητή. Η μείωση που υφίσταται η αβεβαιότητα λόγω μιας άλλης τυχαίας μεταβλητής ονομάζεται *αμοιβαία πληροφορία*. Για δύο τυχαίες μεταβλητές X και Y, η μείωση αυτή είναι η αμοιβαία πληροφορία

$$I(X;Y) = H(X) - H(X|Y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}. \tag{1.4}$$

Η αμοιβαία πληροφορία $I(X;Y)$ είναι ένα μέτρο της εξάρτησης μεταξύ των δύο τυχαίων μεταβλητών. Είναι συμμετρική ως προς τις X και Y, είναι πάντα μη αρνητική και ισούται με μηδέν αν και μόνο αν οι X και Y είναι ανεξάρτητες.

[1] ΣτΜ: Οι ταυτόνομες τυχαίες μεταβλητές έχουν αποδοθεί στα ελληνικά επίσης ως ισόνομες και ομοκατανεμημένες.

Ένας *δίαυλος επικοινωνίας* είναι ένα σύστημα του οποίου η έξοδος εξαρτάται πιθανοκρατικά από την είσοδό του. Περιγράφεται από μια μήτρα πιθανοτήτων μετάβασης $p(y|x)$ που καθορίζει τη δεσμευμένη κατανομή της εξόδου δεδομένης της εισόδου. Για έναν δίαυλο επικοινωνίας με είσοδο X και έξοδο Y μπορούμε να ορίσουμε τη χωρητικότητα C ως εξής:

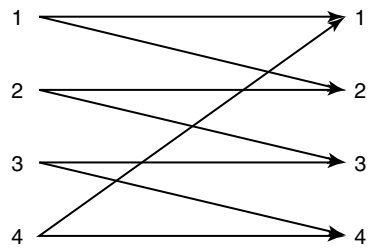
$$C = \max_{p(x)} I(X;Y). \tag{1.5}$$

Στην πορεία θα δείξουμε ότι η χωρητικότητα είναι ο μέγιστος ρυθμός με τον οποίο μπορούμε να στείλουμε πληροφορία διαμέσου του διαύλου και να την ανακτήσουμε στην έξοδο με πιθανότητα σφάλματος που τείνει στο μηδέν. Ακολουθούν μερικά παραδείγματα.

Παράδειγμα 1.1.3 (*Αθόρυβος δυαδικός δίαυλος*) Σε αυτό τον δίαυλο η δυαδική είσοδος αναπαράγεται επακριβώς στην έξοδο. Ο δίαυλος απεικονίζεται στο Σχήμα 1.3. Όλα τα μεταδιδόμενα δυφία λαμβάνονται χωρίς σφάλμα. Επομένως, σε κάθε μετάδοση μπορούμε να στείλουμε αξιόπιστα στον παραλήπτη 1 δυφίο, οπότε η χωρητικότητα είναι 1 δυφίο. Μπορούμε επίσης να υπολογίσουμε την πληροφοριακή χωρητικότητα: $C = \max I(X;Y) = 1$ δυφίο.

Παράδειγμα 1.1.4 (*Θορυβώδης δίαυλος τεσσάρων συμβόλων*) Θεωρήστε τον δίαυλο του Σχήματος 1.4. Σε αυτό τον δίαυλο κάθε γράμμα εισόδου λαμβάνεται είτε ως το ίδιο γράμμα με πιθανότητα $\frac{1}{2}$ είτε ως το επόμενο γράμμα με πιθανότητα $\frac{1}{2}$. Αν χρησιμοποιούμε και τα τέσσερα σύμβολα εισόδου, η εξέταση της εξόδου δεν μας αποκαλύπτει με βεβαιότητα ποιο ήταν το σύμβολο εισόδου που στάλθηκε. Αντιθέτως, αν χρησιμοποιήσουμε μόνο δύο από τα σύμβολα εισόδου (λ.χ. το 1 και το 3), μπορούμε αμέσως να καταλάβουμε από την έξοδο ποιο ήταν το σύμβολο εισόδου που στάλθηκε. Αυτός ο δίαυλος συμπεριφέρεται όπως ο αθόρυβος δίαυλος του Παραδείγματος 1.1.3, οπότε διαμέσου αυτού του διαύλου μπορούμε να στείλουμε χωρίς σφάλματα 1 δυφίο ανά μετάδοση. Αν υπολογίσουμε τη χωρητικότητα $C = \max I(X;Y)$ αυτού του διαύλου, βρίσκουμε ότι ισούται με 1 δυφίο ανά μετάδοση, πράγμα που συμφωνεί με την ανάλυσή μας.

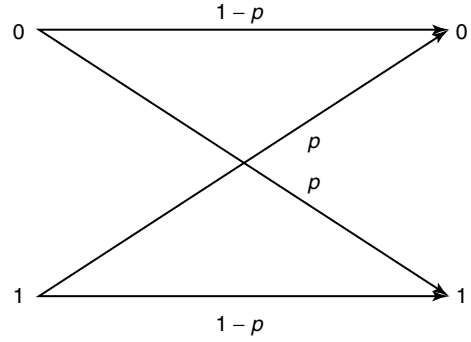
ΣΧΗΜΑ 1.3. Αθόρυβος δυαδικός δίαυλος. $C = 1$ δυφίο.



ΣΧΗΜΑ 1.4. Θορυβώδης δίαυλος.

Γενικά, οι δίαυλοι επικοινωνίας δεν έχουν την απλή δομή αυτού του παραδείγματος, με αποτέλεσμα να μην μπορούμε πάντα να καθορίσουμε ένα υποσύνολο των εισόδων που να μας επιτρέπει να στείλουμε πληροφορία χωρίς σφάλματα. Αν όμως θεωρήσουμε μια ακολουθία μεταδόσεων, όλοι οι δίαυλοι μοιάζουν με αυτό το παράδειγμα, και έτσι μπορούμε να καθορίσουμε ένα υποσύνολο των ακολουθιών εισόδου (τις κωδικολέξεις) που μπορούμε να χρησιμοποιήσουμε για να μεταδώσουμε κάποια πληροφορία διαμέσου του διαύλου με τέτοιο τρόπο ώστε τα σύνολα των δυνατών ακολουθιών εξόδου που αντιστοιχούν σε κάθε κωδικολέξη να είναι κατά προσέγγιση ξένα μεταξύ τους. Κατόπιν, εξετάζοντας την ακολουθία εξόδου, μπορούμε να βρούμε την ακολουθία εισόδου με πιθανότητα σφάλματος που τείνει στο μηδέν.

Παράδειγμα 1.1.5 (*Δυαδικός συμμετρικός δίαυλος*) Αυτό είναι το βασικό παράδειγμα ενός συστήματος επικοινωνίας με θόρυβο. Ο δίαυλος απεικονίζεται στο Σχήμα 1.5. Η είσοδος του διαύλου είναι δυαδική και η έξοδός του ισούται με την



ΣΧΗΜΑ 1.5. Δυαδικός συμμετρικός δίαυλος.

είσοδο με πιθανότητα $1-p$. Από την άλλη, με πιθανότητα p το 0 λαμβάνεται ως 1 και αντιστρόφως. Αν υπολογίσουμε τη χωρητικότητα αυτού του διαύλου βρίσκουμε ότι είναι $C = 1+p\log p+(1-p)\log(1-p)$ δυφία ανά μετάδοση. Ωστόσο, δεν είναι πλέον προφανές πώς μπορούμε να επιτύχουμε αυτή τη χωρητικότητα. Αν όμως χρησιμοποιήσουμε τον δίαυλο πολλές φορές, τότε αρχίζει να μοιάζει με τον θορυβώδη δίαυλο τεσσάρων συμβόλων του Παραδείγματος 1.1.4, οπότε μπορούμε να στείλουμε πληροφορία με ρυθμό C δυφία ανά μετάδοση με αυθαίρετα μικρή πιθανότητα σφάλματος.

Το ανώτατο όριο του ρυθμού μετάδοσης πληροφορίας διαμέσου ενός διαύλου δίνεται από τη χωρητικότητα του διαύλου. Σύμφωνα με το θεώρημα κωδικοποίησης διαύλου, αυτό το όριο μπορεί να επιτευχθεί με τη χρήση κωδίκων μεγάλου μήκους μπλοκ. Στα συστήματα επικοινωνίας που χρησιμοποιούνται στην πράξη υπάρχουν περιορισμοί ως προς την πολυπλοκότητα των κωδίκων που μπορούμε να χρησιμοποιήσουμε, άρα μπορεί να μην είναι δυνατόν να επιτύχουμε τη χωρητικότητα.

Όπως αποδεικνύεται, η αμοιβαία πληροφορία αποτελεί ειδική περίπτωση μιας γενικότερης ποσότητας που ονομάζεται *σχετική εντροπία* $D(p||q)$, η οποία είναι ένα μέτρο της «απόστασης» μεταξύ δύο συναρτήσεων μάζας πιθανότητας p και q, και ορίζεται ως εξής:

$$D(p||q) = \sum_x p(x)\log\frac{p(x)}{q(x)}. \tag{1.6}$$

Παρότι η σχετική εντροπία δεν είναι πραγματική μετρική, έχει μερικές από τις ιδιότητες μιας μετρικής. Ειδικότερα, είναι πάντα μη αρνητική και είναι μηδέν αν και μόνο αν $p = q$. Η σχετική εντροπία εμφανίζεται ως ο εκθέτης της πιθανότητας σφάλματος κατά τον έλεγχο μιας υπόθεσης μεταξύ των κατανομών p και q. Η σχετική εντροπία μπορεί να χρησιμοποιηθεί για να οριστεί μια γεωμετρία για τις κατανομές πιθανότητας που μας επιτρέπει να ερμηνεύσουμε πολλά από τα αποτελέσματα της θεωρίας μεγάλων αποκλίσεων.

Υπάρχουν αρκετές αντιστοιχίες μεταξύ της θεωρίας πληροφορίας και της θεωρίας επενδύσεων σε μια χρηματιστηριακή αγορά. Μια χρηματιστηριακή αγορά ορίζεται μέσω ενός τυχαίου διανύσματος $\mathbf{X}$ του οποίου τα στοιχεία είναι μη αρνητικοί αριθμοί που ισούνται με τον λόγο της τιμής μιας μετοχής στο τέλος της ημέρας προς την τιμή της μετοχής στην αρχή της ημέρας. Για μια χρηματιστηριακή αγορά με κατανομή $F(\mathbf{x})$, μπορούμε να ορίσουμε τον ρυθμό διπλασιασμού W ως εξής:

$$W = \max_{\mathbf{b}:b_i\geq 0,\sum b_i=1} \int \log \mathbf{b}^t\mathbf{x}\; dF(\mathbf{x}). \tag{1.7}$$

Ο ρυθμός διπλασιασμού είναι ο μέγιστος ασυμπτωτικός εκθέτης της μεγέθυνσης του πλούτου. Ο ρυθμός διπλασιασμού έχει ορισμένες ιδιότητες που είναι αντί-

στοιχες με αυτές της εντροπίας. Θα εξετάσουμε μερικές από αυτές τις ιδιότητες στο Κεφάλαιο 16.

Οι ποσότητες H, I, C, D, K, W ανακύπτουν με φυσικό τρόπο στις ακόλουθες γνωστικές περιοχές:

- *Συμπίεση δεδομένων*. Η εντροπία H μιας τυχαίας μεταβλητής είναι ένα κάτω φράγμα του μέσου μήκους της μικρότερης δυνατής περιγραφής της τυχαίας μεταβλητής. Μπορούμε να κατασκευάσουμε περιγραφές με μέσο μήκος που να διαφέρει το πολύ κατά 1 δυφίο από την εντροπία. Αν χαλαρώσουμε τον περιορισμό τέλειας ανάκτησης της πηγής, το ερώτημα που τίθεται είναι ποιοι ρυθμοί επικοινωνίας απαιτούνται ώστε να μπορέσουμε να περιγράψουμε την πηγή με προσέγγιση κάποιας παραμόρφωσης D. Και ποιες χωρητικότητες διαύλου αρκούν για να μπορέσουμε να μεταδώσουμε την πηγή διαμέσου του διαύλου και να την ανακατασκευάσουμε με παραμόρφωση μικρότερη ή ίση της D; Αυτό είναι το αντικείμενο της θεωρίας ρυθμού-παραμόρφωσης.

  Προσπαθώντας να διατυπώσουμε αυστηρά την έννοια της μικρότερης δυνατής περιγραφής για μη τυχαία αντικείμενα, οδηγούμαστε στον ορισμό της πολυπλοκότητας Kolmogorov K. Στην πορεία θα δείξουμε ότι η πολυπλοκότητα Kolmogorov είναι καθολική και ικανοποιεί πολλές από τις απαιτήσεις που θα ήταν διαισθητικά αναμενόμενες για τη θεωρία των μικρότερων δυνατών περιγραφών.
- *Μετάδοση δεδομένων*. Το κεντρικό πρόβλημα στη συγκεκριμένη γνωστική περιοχή είναι η μετάδοση της πληροφορίας με τρόπο ώστε ο δέκτης να μπορεί να αποκωδικοποιεί το μήνυμα με μικρή πιθανότητα σφάλματος. Ουσιαστικά, θέλουμε να βρούμε *κωδικολέξεις* (ακολουθίες συμβόλων εισόδου ενός διαύλου) που να απέχουν πολύ μεταξύ τους, ώστε οι θορυβώδεις εκδοχές τους (που εμφανίζονται στην έξοδο του διαύλου) να μπορούν να διακριθούν η μία από την άλλη. Αυτό είναι ισοδύναμο με το πρόβλημα της στοίβαξης σφαιρών σε έναν πολυδιάστατο χώρο. Για οποιοδήποτε σύνολο κωδικολέξεων μπορούμε να υπολογίσουμε την πιθανότητα ο δέκτης να κάνει κάποιο σφάλμα (δηλαδή να λάβει εσφαλμένη απόφαση αναφορικά με το ποια κωδικολέξη στάλθηκε). Ωστόσο, στις περισσότερες περιπτώσεις ο υπολογισμός αυτός είναι κοπιώδης.

  Χρησιμοποιώντας έναν τυχαία παραχθέντα κώδικα, ο Shannon έδειξε ότι μπορούμε να στείλουμε πληροφορία με οποιονδήποτε ρυθμό μικρότερο της χωρητικότητας C του διαύλου με αυθαίρετα μικρή πιθανότητα σφάλματος. Η έννοια του τυχαία παραγόμενου κώδικα είναι εξαιρετικά ασυνήθιστη. Μας παρέχει τη βάση για την απλή ανάλυση ενός πολύ δύσκολου προβλήματος. Μια από τις βασικές ιδέες της απόδειξης είναι η έννοια των τυπικών ακολουθιών. Η χωρητικότητα C είναι ο λογάριθμος του πλήθους των δια-

κρίσιμων σημάτων εισόδου.

- *Δικτυακή θεωρία πληροφορίας*. Όλα τα παραπάνω ζητήματα αφορούν μια απλή πηγή ή έναν απλό δίαυλο. Τι συμβαίνει αν θέλουμε να συμπιέσουμε ξεχωριστά πολλές πηγές και στη συνέχεια να τοποθετήσουμε μαζί τις συμπιεσμένες περιγραφές σε μια από κοινού αναπαράσταση των πηγών; Η λύση αυτού του προβλήματος δίνεται από το θεώρημα Slepian–Wolf. Ή τι συμβαίνει αν έχουμε πολλούς πομπούς που στέλνουν ανεξάρτητα ο καθένας πληροφορίες σε έναν κοινό δέκτη; Ποια είναι η χωρητικότητα αυτού του διαύλου; Πρόκειται για το πρόβλημα του διαύλου πολλαπλής πρόσβασης που λύθηκε από τους Liao και Ahlswede. Ή τι συμβαίνει αν έχουμε έναν πομπό και πολλούς δέκτες και θέλουμε να μεταδώσουμε ταυτόχρονα (πιθανόν διαφορετικές) πληροφορίες σε καθέναν από τους δέκτες; Στην περίπτωση αυτή έχουμε έναν δίαυλο εκπομπής. Τέλος, τι συμβαίνει αν έχουμε ένα αυθαίρετο πλήθος πομπών και δεκτών σε ένα περιβάλλον με παρεμβολές και θόρυβο; Ποια είναι η περιοχή χωρητικότητας των επιτεύξιμων ρυθμών από τους διάφορους πομπούς προς τους δέκτες; Αυτό είναι το γενικό πρόβλημα της δικτυακής θεωρίας πληροφορίας. Όλα τα παραπάνω προβλήματα εντάσσονται στη γενική περιοχή της δικτυακής θεωρίας πληροφορίας ή θεωρίας πληροφοριών πολλών χρηστών. Παρότι οι ελπίδες για μια συνολική θεωρία δικτύων μάλλον υπερβαίνουν τις δυνατότητες των σημερινών ερευνητικών μεθοδολογιών, εξακολουθεί να υπάρχει η ελπίδα πως σε όλες τις απαντήσεις υπεισέρχονται απλώς και μόνο πολύπλοκες μορφές της αμοιβαίας πληροφορίας και της σχετικής εντροπίας.
- *Εργοδική θεωρία*. Σύμφωνα με το θεώρημα της ασυμπτωτικής ισοκατανομής, οι περισσότερες δειγματικές n-ακολουθίες μιας εργοδικής διεργασίας έχουν πιθανότητα περίπου 2^{-nH} και υπάρχουν περίπου 2^{nH} τέτοιες τυπικές ακολουθίες.
- *Έλεγχος υποθέσεων*. Η σχετική εντροπία D εμφανίζεται ως ο εκθέτης της πιθανότητας σφάλματος κατά τον έλεγχο μιας υπόθεσης μεταξύ δύο κατανομών. Είναι ένα φυσικό μέτρο της απόστασης μεταξύ των κατανομών.
- *Στατιστική μηχανική*. Η εντροπία H εμφανίζεται στη στατιστική μηχανική ως μέτρο της αβεβαιότητας ή της έλλειψης οργάνωσης ενός φυσικού συστήματος. Χοντρικά, η εντροπία είναι ο λογάριθμος του πλήθους των τρόπων με τους οποίους μπορεί να διαμορφωθεί το φυσικό σύστημα. Ο δεύτερος νόμος της θερμοδυναμικής ορίζει ότι η εντροπία ενός κλειστού συστήματος δεν μπορεί να μειωθεί. Στην πορεία της μελέτης μας θα αναφέρουμε μερικές ερμηνείες του δεύτερου νόμου.
- *Κβαντομηχανική*. Στην κβαντομηχανική, η εντροπία von Neumann $S = \mathrm{tr}(\rho \ln \rho) = \sum_i \lambda_i \log \lambda_i$ παίζει τον ρόλο της κλασικής εντροπίας Shannon–Boltzmann $H = -\sum_i p_i \log p_i$. Με βάση αυτήν μπορούν να βρεθούν οι

κβαντομηχανικές εκδοχές της συμπίεσης δεδομένων και της χωρητικότητας διαύλου.

- *Εξαγωγή συμπερασμάτων.* Η έννοια της πολυπλοκότητας Kolmogorov K μπορεί να χρησιμοποιηθεί για την εύρεση της μικρότερης δυνατής περιγραφής των δεδομένων, η οποία με τη σειρά της μπορεί να χρησιμοποιηθεί ως μοντέλο για την πρόβλεψη όσων έπονται. Από ένα μοντέλο που μεγιστοποιεί την αβεβαιότητα ή την εντροπία προκύπτει η προσέγγιση μέγιστης εντροπίας για το πρόβλημα της εξαγωγής συμπερασμάτων.
- *Τυχοπαιξία και επενδύσεις.* Ο βέλτιστος εκθέτης του ρυθμού μεγέθυνσης του πλούτου δίνεται από τον ρυθμό διπλασιασμού W. Για μια ιπποδρομία με ομοιόμορφες αποδόσεις, το άθροισμα του ρυθμού διπλασιασμού W και της εντροπίας H είναι σταθερό. Η αύξηση του ρυθμού διπλασιασμού λόγω παράπλευρης πληροφορίας ισούται με την αμοιβαία πληροφορία I μεταξύ της ιπποδρομίας και της παράπλευρης πληροφορίας. Παρόμοια αποτελέσματα ισχύουν για τις επενδύσεις στη χρηματιστηριακή αγορά.
- *Θεωρία πιθανοτήτων.* Η ιδιότητα της ασυμπτωτικής ισοκατανομής (ΙΑΙ) δείχνει ότι οι περισσότερες ακολουθίες είναι τυπικές υπό την έννοια ότι έχουν δειγματική εντροπία κοντά στην H. Αυτό σημαίνει ότι μπορούμε να εστιάσουμε την προσοχή μας σε αυτές τις κατά προσέγγιση 2^{nH} τυπικές ακολουθίες. Στη θεωρία μεγάλων αποκλίσεων, η πιθανότητα ενός συνόλου είναι κατά προσέγγιση 2^{-nD}, όπου D είναι η απόσταση σχετικής εντροπίας του πλησιέστερου στοιχείου του συνόλου από την πραγματική κατανομή.
- *Θεωρία πολυπλοκότητας.* Η πολυπλοκότητα Kolmogorov K είναι ένα μέτρο της περιγραφικής πολυπλοκότητας ενός αντικειμένου. Σχετίζεται με, αλλά διαφέρει από την υπολογιστική πολυπλοκότητα, η οποία μετρά τον χρόνο ή τον χώρο που απαιτείται για κάποιον υπολογισμό.

Οι πληροφοριοθεωρητικές ποσότητες, όπως η εντροπία και η σχετική εντροπία, εμφανίζονται ξανά και ξανά ως απαντήσεις σε θεμελιώδη ερωτήματα της θεωρίας επικοινωνιών και της στατιστικής. Προτού μελετήσουμε αυτά τα ερωτήματα, θα μελετήσουμε μερικές από τις ιδιότητες των απαντήσεων. Θα ξεκινήσουμε το Κεφάλαιο 2 με τους ορισμούς και τις βασικές ιδιότητες της εντροπίας, της σχετικής εντροπίας και της αμοιβαίας πληροφορίας.

ΚΕΦΑΛΑΙΟ 2

ΕΝΤΡΟΠΙΑ, ΣΧΕΤΙΚΗ ΕΝΤΡΟΠΙΑ ΚΑΙ ΑΜΟΙΒΑΙΑ ΠΛΗΡΟΦΟΡΙΑ

Σε αυτό το κεφάλαιο εισάγουμε τους περισσότερους από τους βασικούς ορισμούς που απαιτούνται για την ανάπτυξη της θεωρίας στη συνέχεια του βιβλίου. Είναι αδύνατο να αντισταθούμε στον πειρασμό και να μην παίξουμε με τις μεταξύ τους σχέσεις και ερμηνείες εν όψει της μετέπειτα χρησιμότητάς τους. Αφού ορίσουμε την εντροπία και την αμοιβαία πληροφορία, θα αποδείξουμε κάποιους κανόνες αλυσίδας, τη μη αρνητικότητα της αμοιβαίας πληροφορίας, την ανισότητα επεξεργασίας δεδομένων, και ως παραδείγματα των ορισμών θα μελετήσουμε τις επαρκείς στατιστικές και την ανισότητα του Fano.

Η έννοια της πληροφορίας είναι πολύ ευρεία για να καλυφθεί πλήρως από έναν και μόνο ορισμό. Ωστόσο, για κάθε κατανομή πιθανότητας θα ορίσουμε μια ποσότητα που ονομάζεται *εντροπία*, η οποία έχει πολλές ιδιότητες που συμφωνούν με όσα θα αναμέναμε διαισθητικά από ένα μέτρο πληροφορίας. Επεκτείνοντας αυτή την έννοια, θα ορίσουμε την *αμοιβαία πληροφορία*, η οποία είναι ένα μέτρο της ποσότητας πληροφορίας που περιέχει μια τυχαία μεταβλητή σχετικά με κάποια άλλη. Υπό αυτό το πρίσμα, η εντροπία είναι η αυτοπληροφορία μιας τυχαίας μεταβλητής. Η αμοιβαία πληροφορία είναι ειδική περίπτωση μιας γενικότερης ποσότητας που ονομάζεται *σχετική εντροπία*, η οποία είναι ένα μέτρο της απόστασης μεταξύ δύο κατανομών πιθανότητας. Όλες αυτές οι ποσότητες σχετίζονται στενά μεταξύ τους και έχουν ορισμένες απλές κοινές ιδιότητες, μερικές από τις οποίες θα αποδείξουμε σε αυτό το κεφάλαιο.

Σε επόμενα κεφάλαια θα δείξουμε πώς αυτές οι ποσότητες αποτελούν φυσικές απαντήσεις σε διάφορα ερωτήματα που αφορούν τις επικοινωνίες, τη στατιστική, την πολυπλοκότητα και την τυχοπαιξία. Αυτό θα αποτελέσει και την τελική επιβεβαίωση της αξίας αυτών των ορισμών.

2.1 ΕΝΤΡΟΠΙΑ

Θα ξεκινήσουμε εισάγοντας την έννοια της *εντροπίας*, η οποία είναι ένα μέτρο της αβεβαιότητας μιας τυχαίας μεταβλητής. Έστω X μια διακριτή τυχαία μεταβλητή με αλφάβητο $\mathcal{X}$ και συνάρτηση μάζας πιθανότητας $p(x) = \Pr\{X = x\}$,

$x \in \mathcal{X}$. Για λόγους ευκολίας, θα συμβολίζουμε τη συνάρτηση μάζας πιθανότητας με $p(x)$ αντί με $p_X(x)$. Επομένως, οι $p(x)$ και $p(y)$ αναφέρονται σε δύο διαφορετικές τυχαίες μεταβλητές και στην πραγματικότητα είναι οι δύο διαφορετικές συναρτήσεις μάζας πιθανότητας $p_X(x)$ και $p_Y(y)$, αντίστοιχα.

Ορισμός Η *εντροπία* $H(X)$ μιας διακριτής τυχαίας μεταβλητής X ορίζεται ως εξής:

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x). \tag{2.1}$$

Θα συμβολίζουμε την παραπάνω ποσότητα και με $H(p)$. Η βάση του λογαρίθμου είναι το 2, και η εντροπία μετριέται σε δυφία. Για παράδειγμα, η εντροπία της ρίψης ενός τίμιου κέρματος είναι 1 δυφίο. Θα χρησιμοποιήσουμε τη σύμβαση $0 \log 0 = 0$, η οποία δικαιολογείται εύκολα βάσει της συνέχειας, αφού $x \log x \to 0$ καθώς $x \to 0$. Η προσθήκη όρων μηδενικής πιθανότητας δεν μεταβάλλει την εντροπία.

Αν η βάση του λογαρίθμου είναι το b, θα συμβολίζουμε την εντροπία με $H_b(X)$. Αν η βάση του λογαρίθμου είναι το e, η εντροπία μετριέται σε *nat*. Εκτός και αν δηλώνουμε ρητά κάτι διαφορετικό, θα θεωρούμε ότι η βάση όλων των λογαρίθμων είναι το 2 και συνεπώς όλες οι εντροπίες θα μετριούνται σε δυφία. Σημειωτέον ότι η εντροπία είναι ένα συναρτησιοειδές της κατανομής της X. Δεν εξαρτάται από τις πραγματικές τιμές που παίρνει η τυχαία μεταβλητή X, αλλά μόνο από τις πιθανότητες.

Θα συμβολίζουμε την αναμενόμενη τιμή με E. Επομένως, αν $X \sim p(x)$, η αναμενόμενη τιμή της τυχαίας μεταβλητής $g(X)$ γράφεται ως

$$E_p g(X) = \sum_{x \in \mathcal{X}} g(x) p(x) \tag{2.2}$$

ή απλούστερα ως $Eg(X)$, όταν η συνάρτηση μάζας πιθανότητας εννοείται από τα συμφραζόμενα. Θα μας απασχολήσει ιδιαίτερα η μυστηριώδης αυτοαναφορική αναμενόμενη τιμή της $g(X)$ ως προς την $p(x)$ όταν $g(X) = \log \frac{1}{p(X)}$.

Παρατήρηση Η εντροπία της X μπορεί επίσης να ερμηνευτεί ως η αναμενόμενη τιμή της τυχαίας μεταβλητής $\log \frac{1}{p(X)}$, όπου η X λαμβάνεται σύμφωνα με τη συνάρτηση μάζας πιθανότητας $p(x)$. Συνεπώς,

$$H(X) = E_p \log \frac{1}{p(X)}. \tag{2.3}$$

Αυτός ο ορισμός της εντροπίας συνδέεται με τον ορισμό της εντροπίας στη θερμοδυναμική· θα μελετήσουμε μερικές από τις σχέσεις των δύο ορισμών στην

πορεία. Ο ορισμός της εντροπίας μπορεί να συναχθεί αξιωματικά μέσω του ορισμού κάποιων ιδιοτήτων που πρέπει να ικανοποιεί η εντροπία μιας τυχαίας μεταβλητής. Η προσέγγιση αυτή παρουσιάζεται στο Πρόβλημα 2.46. Σε αυτό το βιβλίο δεν ακολουθούμε την αξιωματική προσέγγιση για να αιτιολογήσουμε τον ορισμό της εντροπίας, αντιθέτως δείχνουμε ότι η εντροπία αποτελεί την απάντηση σε διάφορα φυσικά ερωτήματα, όπως «Ποιο είναι το μέσο μήκος της μικρότερης δυνατής περιγραφής μιας τυχαίας μεταβλητής;». Κατ' αρχάς θα συναγάγουμε μερικές άμεσες συνέπειες του ορισμού.

Λήμμα 2.1.1 $H(X) \geq 0.$

Απόδειξη: Από τη σχέση $0 \leq p(x) \leq 1$ έπεται ότι $\log \frac{1}{p(x)} \geq 0.$ □

Λήμμα 2.1.2 $H_b(X) = (\log_b a) H_a(X).$

Απόδειξη: $\log_b p = \log_b a \log_a p.$ □

Η δεύτερη ιδιότητα της εντροπίας μάς επιτρέπει να αλλάζουμε τη βάση του λογαρίθμου στον ορισμό. Μπορούμε να αλλάζουμε τη βάση της εντροπίας από τη μία στην άλλη πολλαπλασιάζοντας με τον κατάλληλο συντελεστή.

Παράδειγμα 2.1.1 Αν

$$X = \begin{cases} 1 & \text{με πιθανότητα } p, \\ 0 & \text{με πιθανότητα } 1-p, \end{cases} \tag{2.4}$$

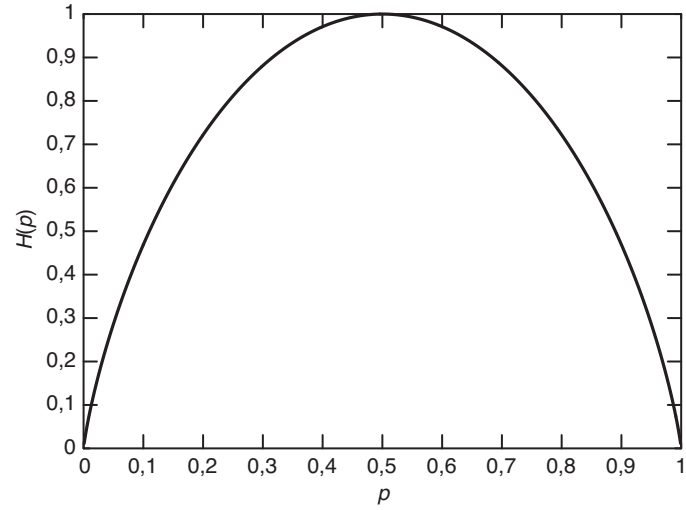
τότε

$$H(X) = -p \log p - (1-p) \log(1-p) \overset{\text{ορ.}}{=\!=} H(p). \tag{2.5}$$

Ειδικότερα, $H(X) = 1$ δυφίο όταν $p = \frac{1}{2}$. Η γραφική παράσταση της συνάρτησης $H(p)$ παρουσιάζεται στο Σχήμα 2.1, όπου απεικονίζονται μερικές από τις βασικές ιδιότητες της εντροπίας: Είναι κοίλη συνάρτηση της κατανομής και ισούται με 0 όταν $p = 0$ ή 1. Αυτό είναι εύλογο, διότι όταν $p = 0$ ή 1, η μεταβλητή δεν είναι τυχαία και δεν υπάρχει αβεβαιότητα. Αντίστοιχα, η αβεβαιότητα είναι μέγιστη όταν $p = \frac{1}{2}$, οπότε έχουμε τη μέγιστη τιμή της εντροπίας.

Παράδειγμα 2.1.2 Έστω

$$X = \begin{cases} a & \text{με πιθανότητα } \frac{1}{2}, \\ b & \text{με πιθανότητα } \frac{1}{4}, \\ c & \text{με πιθανότητα } \frac{1}{8}, \\ d & \text{με πιθανότητα } \frac{1}{8}. \end{cases} \tag{2.6}$$



ΣΧΗΜΑ 2.1. $H(p)$ συναρτήσει της p.

Η εντροπία της X είναι

$$H(X) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} = \frac{7}{4} \text{ δυφία.} \qquad (2.7)$$

Υποθέστε ότι θέλουμε να προσδιορίσουμε την τιμή της X με το ελάχιστο πλήθος δυαδικών ερωτήσεων. Μια καλή πρώτη ερώτηση είναι η εξής: «Είναι η X ίση με a;» Αυτό χωρίζει την πιθανότητα «στη μέση». Αν η απάντηση στην πρώτη ερώτηση είναι αρνητική, η δεύτερη ερώτηση μπορεί να είναι η εξής: «Είναι η X ίση με b;» Η τρίτη ερώτηση μπορεί να είναι η εξής: «Είναι η X ίση με c;» Το αναμενόμενο πλήθος δυαδικών ερωτήσεων που τελικά απαιτούνται είναι $1{,}75$. Αυτό είναι και το ελάχιστο αναμενόμενο πλήθος δυαδικών ερωτήσεων που απαιτούνται για να προσδιοριστεί η τιμή της X. Στο Κεφάλαιο 5 θα δείξουμε ότι το ελάχιστο αναμενόμενο πλήθος δυαδικών ερωτήσεων που απαιτούνται για τον προσδιορισμό της X βρίσκεται μεταξύ $H(X)$ και $H(X) + 1$.

2.2 ΑΠΟ ΚΟΙΝΟΥ ΕΝΤΡΟΠΙΑ ΚΑΙ ΔΕΣΜΕΥΜΕΝΗ ΕΝΤΡΟΠΙΑ

Στην Ενότητα 2.1 ορίσαμε την εντροπία μιας απλής τυχαίας μεταβλητής. Σε αυτή την ενότητα θα επεκτείνουμε τον ορισμό σε ζεύγη τυχαίων μεταβλητών. Ο ορισμός αυτός δεν περιέχει τίποτε ουσιαστικά καινούργιο, διότι το (X, Y) μπορεί να θεωρηθεί ως μια απλή διανυσματική τυχαία μεταβλητή.

Ορισμός Η *από κοινού εντροπία* $H(X,Y)$ ενός ζεύγους διακριτών τυχαίων μεταβλητών (X,Y) με από κοινού κατανομή $p(x,y)$ ορίζεται ως εξής:

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x,y), \tag{2.8}$$

το οποίο μπορεί να γραφτεί και ως

$$H(X,Y) = -E\log p(X,Y). \tag{2.9}$$

Ορίζουμε επίσης ως δεσμευμένη εντροπία μιας τυχαίας μεταβλητής με δεδομένη μια άλλη τυχαία μεταβλητή την αναμενόμενη τιμή των εντροπιών των δεσμευμένων κατανομών, όπου ο μέσος όρος υπολογίζεται ως προς τη δεσμεύουσα τυχαία μεταβλητή.

Ορισμός Αν $(X,Y)\sim p(x,y)$, η *δεσμευμένη εντροπία* $H(Y|X)$ ορίζεται ως εξής:

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathcal{X}} p(x)H(Y|X=x) && (2.10)\\ &= -\sum_{x\in\mathcal{X}} p(x)\sum_{y\in\mathcal{Y}} p(y|x)\log p(y|x) && (2.11)\\ &= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(y|x) && (2.12)\\ &= -E\log p(Y|X). && (2.13) \end{aligned}$$

Η φυσικότητα του ορισμού της από κοινού εντροπίας και της δεσμευμένης εντροπίας αποκαλύπτεται από το γεγονός ότι η εντροπία ενός ζεύγους τυχαίων μεταβλητών είναι η εντροπία της μιας συν τη δεσμευμένη εντροπία της άλλης. Αυτό αποδεικνύεται στο ακόλουθο θεώρημα.

Θεώρημα 2.2.1 (*Κανόνας αλυσίδας*)

$$H(X,Y) = H(X) + H(Y|X). \tag{2.14}$$

Απόδειξη

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x,y) \tag{2.15}$$

$$= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x)p(y|x) \tag{2.16}$$

$$= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x) - \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(y|x) \tag{2.17}$$

$$= -\sum_{x\in\mathcal{X}} p(x)\log p(x) - \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(y|x) \tag{2.18}$$

$$= H(X) + H(Y|X). \tag{2.19}$$

Ισοδύναμα, μπορούμε να γράψουμε

$$\log p(X,Y) = \log p(X) + \log p(Y|X) \tag{2.20}$$

και να πάρουμε την αναμενόμενη τιμή και των δύο μελών της εξίσωσης ώστε να προκύψει το θεώρημα. □

Πόρισμα

$$H(X,Y|Z) = H(X|Z) + H(Y|X,Z). \tag{2.21}$$

Απόδειξη: Αποδεικνύεται με τον ίδιο τρόπο όπως το θεώρημα. □

Παράδειγμα 2.2.1 Έστω ότι το (X,Y) έχει την εξής από κοινού κατανομή:

Y \ X	1	2	3	4
1	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{32}$
2	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{32}$
3	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
4	$\frac{1}{4}$	0	0	0

Η περιθώρια κατανομή της X είναι $(\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{8})$ και η περιθώρια κατανομή της Y είναι $(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4})$, επομένως $H(X) = \frac{7}{4}$ δυφία και $H(Y) = 2$ δυφία. Επιπλέον,

$$H(X|Y) = \sum_{i=1}^{4} p(Y=i)H(X|Y=i) \tag{2.22}$$

$$= \frac{1}{4}H\left(\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{8}\right) + \frac{1}{4}H\left(\frac{1}{4},\frac{1}{2},\frac{1}{8},\frac{1}{8}\right) + \frac{1}{4}H\left(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4}\right) + \frac{1}{4}H(1,0,0,0) \tag{2.23}$$

$$= \frac{1}{4} \times \frac{7}{4} + \frac{1}{4} \times \frac{7}{4} + \frac{1}{4} \times 2 + \frac{1}{4} \times 0 \tag{2.24}$$

$$= \frac{11}{8} \text{ δυφία.} \tag{2.25}$$

Με αντίστοιχο τρόπο, $H(Y|X) = \frac{13}{8}$ δυφία και $H(X,Y) = \frac{27}{8}$ δυφία.

Παρατήρηση Σημειωτέον ότι $H(Y|X) \neq H(X|Y)$. Ωστόσο, $H(X) - H(X|Y) = H(Y) - H(Y|X)$, μια ιδιότητα που θα εκμεταλλευτούμε στην πορεία.

2.3 ΣΧΕΤΙΚΗ ΕΝΤΡΟΠΙΑ ΚΑΙ ΑΜΟΙΒΑΙΑ ΠΛΗΡΟΦΟΡΙΑ

Η εντροπία μιας τυχαίας μεταβλητής είναι ένα μέτρο της αβεβαιότητας της τυχαίας μεταβλητής· είναι ένα μέτρο της ποσότητας πληροφορίας που απαιτείται κατά μέσο όρο για να περιγραφεί η τυχαία μεταβλητή. Σε αυτή την ενότητα θα εισαγάγουμε δύο σχετιζόμενες έννοιες: τη σχετική εντροπία και την αμοιβαία πληροφορία.

Η *σχετική εντροπία* είναι ένα μέτρο της απόστασης μεταξύ δύο κατανομών. Στη στατιστική, εμφανίζεται ως αναμενόμενος λογάριθμος του λόγου πιθανοφανειών. Η σχετική εντροπία $D(p||q)$ είναι ένα μέτρο του πόσο άστοχο είναι να θεωρήσουμε ότι η κατανομή είναι η q όταν η πραγματική κατανομή είναι η p. Για παράδειγμα, αν γνωρίζαμε την πραγματική κατανομή p της τυχαίας μεταβλητής, θα μπορούσαμε να κατασκευάσουμε έναν κώδικα με μέσο μήκος περιγραφής $H(p)$. Αν αντ' αυτού χρησιμοποιούσαμε τον κώδικα για μια κατανομή q, θα χρειαζόμασταν κατά μέσο όρο $H(p) + D(p||q)$ δυφία για να περιγράψουμε την τυχαία μεταβλητή.

Ορισμός Η *σχετική εντροπία* ή *απόσταση Kullback–Leibler* μεταξύ δύο συναρτήσεων μάζας πιθανότητας $p(x)$ και $q(x)$ ορίζεται ως εξής:

$$D(p||q) = \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)} \tag{2.26}$$

$$= E_p \log \frac{p(X)}{q(X)}. \tag{2.27}$$

Στον παραπάνω ορισμό χρησιμοποιούμε τη σύμβαση $0 \log \frac{0}{0} = 0$, καθώς και τη σύμβαση (που στηρίζεται σε ένα σκεπτικό συνέχειας) $0 \log \frac{0}{q} = 0$ και $p \log \frac{p}{0} = \infty$. Επομένως, αν υπάρχει κάποιο σύμβολο $x \in \mathcal{X}$ τέτοιο ώστε $p(x) > 0$ και $q(x) = 0$, τότε $D(p||q) = \infty$.

Στη συνέχεια της ανάλυσής μας θα δείξουμε ότι η σχετική εντροπία είναι πάντα μη αρνητική και ισούται με μηδέν αν και μόνο αν $p = q$. Ωστόσο, δεν είναι μια πραγματική απόσταση μεταξύ κατανομών, διότι δεν είναι συμμετρική και δεν ικανοποιεί την τριγωνική ανισότητα. Παρόλα αυτά, συχνά είναι χρήσιμο να φανταζόμαστε τη σχετική εντροπία ως «απόσταση» μεταξύ κατανομών.

Θα προχωρήσουμε εισάγοντας την αμοιβαία πληροφορία, η οποία είναι ένα μέτρο της ποσότητας πληροφορίας που περιέχει μια τυχαία μεταβλητή για κάποια άλλη τυχαία μεταβλητή. Πρόκειται για τη μείωση που υφίσταται η αβεβαιότητα μιας τυχαίας μεταβλητής λόγω της γνώσης της άλλης.

Ορισμός Έστω δύο τυχαίες μεταβλητές X και Y με από κοινού συνάρτηση μάζας πιθανότητας $p(x, y)$ και περιθώριες συναρτήσεις μάζας πιθανότητας $p(x)$ και $p(y)$. Η *αμοιβαία πληροφορία* $I(X;Y)$ είναι η σχετική εντροπία μεταξύ της από κοινού κατανομής και της γινόμενης κατανομής $p(x)p(y)$:

$$I(X;Y) = \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \tag{2.28}$$

$$= D(p(x,y)||p(x)p(y)) \tag{2.29}$$

$$= E_{p(x,y)} \log \frac{p(X,Y)}{p(X)p(Y)}. \tag{2.30}$$

Στο Κεφάλαιο 8 θα γενικεύσουμε αυτόν τον ορισμό για συνεχείς τυχαίες μεταβλητές και στην (8.54) για γενικές τυχαίες μεταβλητές που μπορεί να είναι μείγμα διακριτών και συνεχών τυχαίων μεταβλητών.

Παράδειγμα 2.3.1 Έστω $\mathcal{X} = \{0, 1\}$, και θεωρήστε δύο κατανομές p και q επί του $\mathcal{X}$. Αν $p(0) = 1 - r$, $p(1) = r$ και $q(0) = 1 - s$, $q(1) = s$, τότε

$$D(p||q) = (1-r) \log \frac{1-r}{1-s} + r \log \frac{r}{s} \tag{2.31}$$

και

$$D(q||p) = (1-s) \log \frac{1-s}{1-r} + s \log \frac{s}{r}. \tag{2.32}$$

Αν $r = s$, τότε $D(p||q) = D(q||p) = 0$. Αν $r = \frac{1}{2}$ και $s = \frac{1}{4}$, τότε

$$D(p||q) = \frac{1}{2} \log \frac{\frac{1}{2}}{\frac{3}{4}} + \frac{1}{2} \log \frac{\frac{1}{2}}{\frac{1}{4}} = 1 - \frac{1}{2} \log 3 = 0{,}2075 \text{ δυφία}, \tag{2.33}$$

ενώ

$$D(q||p) = \frac{3}{4} \log \frac{\frac{3}{4}}{\frac{1}{2}} + \frac{1}{4} \log \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{3}{4} \log 3 - 1 = 0{,}1887 \text{ δυφία}. \tag{2.34}$$

Σημειωτέον ότι εν γένει $D(p||q) \neq D(q||p)$.

2.4 ΣΧΕΣΗ ΜΕΤΑΞΥ ΕΝΤΡΟΠΙΑΣ ΚΑΙ ΑΜΟΙΒΑΙΑΣ ΠΛΗΡΟΦΟΡΙΑΣ

Ο ορισμός της αμοιβαίας πληροφορίας $I(X;Y)$ μπορεί να γραφτεί και ως εξής:

$$I(X;Y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \tag{2.35}$$

$$= \sum_{x,y} p(x,y) \log \frac{p(x|y)}{p(x)} \tag{2.36}$$

$$= -\sum_{x,y} p(x,y) \log p(x) + \sum_{x,y} p(x,y) \log p(x|y) \tag{2.37}$$

$$= -\sum_{x} p(x) \log p(x) - \left(-\sum_{x,y} p(x,y) \log p(x|y) \right) \tag{2.38}$$

$$= H(X) - H(X|Y). \tag{2.39}$$

Άρα η αμοιβαία πληροφορία $I(X;Y)$ είναι η μείωση που υφίσταται η αβεβαιότητα της X λόγω της γνώσης της Y.

Λόγω συμμετρίας έπεται επίσης ότι

$$I(X;Y) = H(Y) - H(Y|X). \tag{2.40}$$

Άρα η X λέει για την Y όσα λέει η Y για την X.

Όπως δείξαμε στην Ενότητα 2.2, $H(X,Y) = H(X) + H(Y|X)$, επομένως

$$I(X;Y) = H(X) + H(Y) - H(X,Y). \tag{2.41}$$

Τέλος, παρατηρούμε ότι

$$I(X;X) = H(X) - H(X|X) = H(X). \tag{2.42}$$

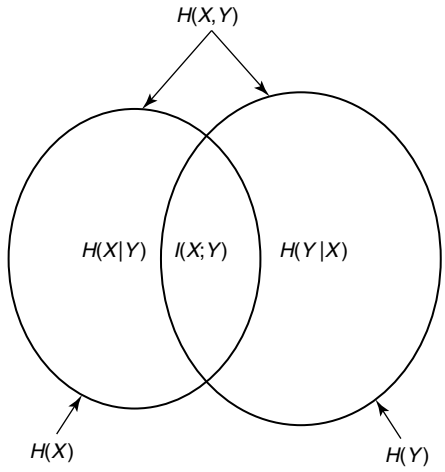
Άρα η αμοιβαία πληροφορία μιας τυχαίας μεταβλητής με τον εαυτό της είναι η εντροπία της τυχαίας μεταβλητής. Αυτός είναι ο λόγος για τον οποίο μερικές φορές η εντροπία καλείται *αυτοπληροφορία*.

Συγκεντρώνοντας αυτά τα αποτελέσματα καταλήγουμε στο ακόλουθο θεώρημα.

Θεώρημα 2.4.1 (*Αμοιβαία πληροφορία και εντροπία*)

$$I(X;Y) = H(X) - H(X|Y) \tag{2.43}$$

$$I(X;Y) = H(Y) - H(Y|X) \tag{2.44}$$



ΣΧΗΜΑ 2.2. Σχέση μεταξύ εντροπίας και αμοιβαίας πληροφορίας.

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \tag{2.45}$$

$$I(X;Y) = I(Y;X) \tag{2.46}$$

$$I(X;X) = H(X). \tag{2.47}$$

Η σχέση μεταξύ $H(X)$, $H(Y)$, $H(X,Y)$, $H(X|Y)$, $H(Y|X)$ και $I(X;Y)$ μπορεί να εκφραστεί μέσω ενός διαγράμματος Venn (Σχήμα 2.2). Παρατηρήστε ότι η αμοιβαία πληροφορία $I(X;Y)$ αντιστοιχεί στην τομή της πληροφορίας που περιέχει η X με την πληροφορία που περιέχει η Y.

Παράδειγμα 2.4.1 Για την από κοινού κατανομή του Παραδείγματος 2.2.1 μπορούμε εύκολα να υπολογίσουμε την αμοιβαία πληροφορία: $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = 0{,}375$ δυφία.

2.5 ΚΑΝΟΝΕΣ ΑΛΥΣΙΔΑΣ ΓΙΑ ΤΗΝ ΕΝΤΡΟΠΙΑ, ΤΗ ΣΧΕΤΙΚΗ ΕΝΤΡΟΠΙΑ ΚΑΙ ΤΗΝ ΑΜΟΙΒΑΙΑ ΠΛΗΡΟΦΟΡΙΑ

Σε αυτό το σημείο θα δείξουμε ότι η εντροπία μιας συλλογής τυχαίων μεταβλητών είναι το άθροισμα των δεσμευμένων εντροπιών.

Θεώρημα 2.5.1 (*Κανόνας αλυσίδας για την εντροπία*) *Αν οι* $X_1, X_2, \ldots, X_n$ *λαμβάνονται σύμφωνα με την* $p(x_1, x_2, \ldots, x_n)$*, τότε*

$$H(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} H(X_i|X_{i-1}, \ldots, X_1). \tag{2.48}$$

Απόδειξη: Εφαρμόζοντας κατ' επανάληψη τον κανόνα για το ανάπτυγμα της εντροπίας για δύο μεταβλητές, έχουμε

$$H(X_1, X_2) = H(X_1) + H(X_2|X_1), \tag{2.49}$$

$$H(X_1, X_2, X_3) = H(X_1) + H(X_2, X_3|X_1) \tag{2.50}$$

$$= H(X_1) + H(X_2|X_1) + H(X_3|X_2, X_1), \tag{2.51}$$

$$\vdots$$

$$H(X_1, X_2, \ldots, X_n) = H(X_1) + H(X_2|X_1) + \cdots + H(X_n|X_{n-1}, \ldots, X_1) \tag{2.52}$$

$$= \sum_{i=1}^{n} H(X_i|X_{i-1}, \ldots, X_1). \quad \square \tag{2.53}$$

Εναλλακτική απόδειξη: Γράφουμε $p(x_1, \ldots, x_n) = \prod_{i=1}^{n} p(x_i|x_{i-1}, \ldots, x_1)$, οπότε έχουμε

$$H(X_1, X_2, \ldots, X_n)$$

$$= -\sum_{x_1, x_2, \ldots, x_n} p(x_1, x_2, \ldots, x_n) \log p(x_1, x_2, \ldots, x_n) \tag{2.54}$$

$$= -\sum_{x_1, x_2, \ldots, x_n} p(x_1, x_2, \ldots, x_n) \log \prod_{i=1}^{n} p(x_i|x_{i-1}, \ldots, x_1) \tag{2.55}$$

$$= -\sum_{x_1, x_2, \ldots, x_n} \sum_{i=1}^{n} p(x_1, x_2, \ldots, x_n) \log p(x_i|x_{i-1}, \ldots, x_1) \tag{2.56}$$

$$= -\sum_{i=1}^{n} \sum_{x_1, x_2, \ldots, x_n} p(x_1, x_2, \ldots, x_n) \log p(x_i|x_{i-1}, \ldots, x_1) \tag{2.57}$$

$$= -\sum_{i=1}^{n} \sum_{x_1, x_2, \ldots, x_i} p(x_1, x_2, \ldots, x_i) \log p(x_i|x_{i-1}, \ldots, x_1) \tag{2.58}$$

$$= \sum_{i=1}^{n} H(X_i|X_{i-1}, \ldots, X_1). \quad \square \tag{2.59}$$

Ακολούθως ορίζουμε τη δεσμευμένη αμοιβαία πληροφορία ως τη μείωση που υφίσταται η αβεβαιότητα της X λόγω της γνώσης της Y όταν δίνεται η Z.

Ορισμός Η *δεσμευμένη αμοιβαία πληροφορία* των τυχαίων μεταβλητών X και Y με δεδομένη τη Z ορίζεται ως εξής:

$$I(X;Y|Z) = H(X|Z) - H(X|Y,Z) \tag{2.60}$$

$$= E_{p(x,y,z)} \log \frac{p(X,Y|Z)}{p(X|Z)p(Y|Z)}. \tag{2.61}$$

Η αμοιβαία πληροφορία ικανοποιεί και αυτή έναν κανόνα αλυσίδας.

Θεώρημα 2.5.2 (*Κανόνας αλυσίδας για την αμοιβαία πληροφορία*)

$$I(X_1, X_2, \ldots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y|X_{i-1}, X_{i-2}, \ldots, X_1). \tag{2.62}$$

Απόδειξη

$$I(X_1, X_2, \ldots, X_n; Y)$$

$$= H(X_1, X_2, \ldots, X_n) - H(X_1, X_2, \ldots, X_n|Y) \tag{2.63}$$

$$= \sum_{i=1}^{n} H(X_i|X_{i-1}, \ldots, X_1) - \sum_{i=1}^{n} H(X_i|X_{i-1}, \ldots, X_1, Y)$$

$$= \sum_{i=1}^{n} I(X_i; Y|X_1, X_2, \ldots, X_{i-1}). \quad \square \tag{2.64}$$

Ακολούθως ορίζουμε μια δεσμευμένη εκδοχή της σχετικής εντροπίας.

Ορισμός Αν οι $p(x, y)$ και $q(x, y)$ είναι από κοινού συναρτήσεις μάζας πιθανότητας, η *δεσμευμένη σχετική εντροπία* $D(p(y|x)||q(y|x))$ είναι ο μέσος όρος των σχετικών εντροπιών μεταξύ των δεσμευμένων συναρτήσεων μάζας πιθανότητας $p(y|x)$ και $q(y|x)$ υπολογισμένος ως προς τη συνάρτηση μάζας πιθανότητας $p(x)$. Συγκεκριμένα,

$$D(p(y|x)||q(y|x)) = \sum_x p(x) \sum_y p(y|x) \log \frac{p(y|x)}{q(y|x)} \tag{2.65}$$

$$= E_{p(x,y)} \log \frac{p(Y|X)}{q(Y|X)}. \tag{2.66}$$

Ο παραπάνω συμβολισμός για τη δεσμευμένη σχετική εντροπία δεν είναι πλήρης, διότι δεν αναφέρει την κατανομή $p(x)$ της δεσμεύουσας τυχαίας μεταβλητής. Συνήθως όμως εννοείται από τα συμφραζόμενα.

Η σχετική εντροπία μεταξύ δύο από κοινού κατανομών ενός ζεύγους τυχαίων μεταβλητών μπορεί να εκφραστεί ως άθροισμα μιας σχετικής εντροπίας και μιας δεσμευμένης σχετικής εντροπίας. Ο κανόνας αλυσίδας για τη σχετική εντροπία χρησιμοποιείται στην Ενότητα 4.4 για την απόδειξη μιας εκδοχής του δεύτερου νόμου της θερμοδυναμικής.

Θεώρημα 2.5.3 (*Κανόνας αλυσίδας για τη σχετική εντροπία*)

$$D(p(x, y)||q(x, y)) = D(p(x)||q(x)) + D(p(y|x)||q(y|x)). \tag{2.67}$$

Απόδειξη

$$D(p(x, y)||q(x, y))$$

$$= \sum_x \sum_y p(x, y) \log \frac{p(x, y)}{q(x, y)} \tag{2.68}$$

$$= \sum_x \sum_y p(x, y) \log \frac{p(x)p(y|x)}{q(x)q(y|x)} \tag{2.69}$$

$$= \sum_x \sum_y p(x, y) \log \frac{p(x)}{q(x)} + \sum_x \sum_y p(x, y) \log \frac{p(y|x)}{q(y|x)} \tag{2.70}$$

$$= D(p(x)||q(x)) + D(p(y|x)||q(y|x)). \quad \square \tag{2.71}$$

2.6 Η ΑΝΙΣΟΤΗΤΑ ΤΟΥ JENSEN ΚΑΙ ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΗΣ

Σε αυτή την ενότητα θα αποδείξουμε μερικές απλές ιδιότητες των ποσοτήτων που ορίσαμε παραπάνω. Θα ξεκινήσουμε με τις ιδιότητες των κυρτών συναρτήσεων.

Ορισμός Λέμε ότι μια συνάρτηση $f(x)$ είναι *κυρτή* σε ένα διάστημα (a, b) αν για κάθε $x_1, x_2 \in (a, b)$ και $0 \leq \lambda \leq 1$,

$$f(\lambda x_1 + (1-\lambda)x_2) \leq \lambda f(x_1) + (1-\lambda)f(x_2). \tag{2.72}$$

Λέμε ότι μια συνάρτηση f είναι *γνησίως κυρτή* αν η ισότητα ισχύει μόνο αν $\lambda = 0$ ή $\lambda = 1$.

Ορισμός Μια συνάρτηση f είναι *κοίλη* αν η $-f$ είναι κυρτή. Μια συνάρτηση είναι κυρτή αν κείται πάντα κάτω από οποιαδήποτε χορδή της. Μια συνάρτηση είναι κοίλη αν κείται πάντα πάνω από οποιαδήποτε χορδή της.

Παραδείγματα κυρτών συναρτήσεων είναι οι x^2, $|x|$, e^x, $x \log x$ (για $x \geq 0$), κ.ο.κ. Παραδείγματα κοίλων συναρτήσεων είναι οι $\log x$ και $\sqrt{x}$ για $x \geq 0$. Στο Σχήμα 2.3 παρουσιάζονται μερικά παραδείγματα κυρτών και κοίλων συναρτήσεων. Σημειωτέον ότι οι γραμμικές συναρτήσεις $ax+b$ είναι και κυρτές και κοίλες. Η κυρτότητα βρίσκεται πίσω από πολλές βασικές ιδιότητες πληροφοριοθεωρητικών ποσοτήτων όπως είναι η εντροπία και η αμοιβαία πληροφορία. Προτού αποδείξουμε κάποιες από αυτές τις ιδιότητες, θα αποδείξουμε μερικές απλές προτάσεις που αφορούν τις κυρτές συναρτήσεις.

Θεώρημα 2.6.1 *Αν η συνάρτηση f έχει μη αρνητική (θετική) δεύτερη παράγωγο σε κάποιο διάστημα, η συνάρτηση είναι κυρτή (γνησίως κυρτή) σε αυτό το διάστημα.*

Απόδειξη: Χρησιμοποιούμε το ανάπτυγμα της συνάρτησης σε σειρά Taylor γύρω από το x_0:

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + \frac{f''(x^*)}{2}(x - x_0)^2, \tag{2.73}$$

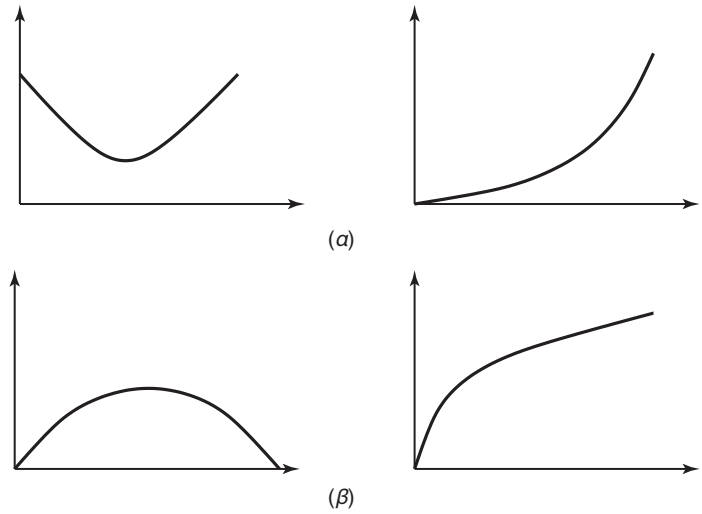
όπου το x^* βρίσκεται ανάμεσα στο x_0 και το x. Εξ υποθέσεως, $f''(x^*) \geq 0$, άρα ο τελευταίος όρος είναι μη αρνητικός για κάθε x.

Αν θέσουμε $x_0 = \lambda x_1 + (1-\lambda)x_2$ και πάρουμε $x = x_1$, προκύπτει ότι

$$f(x_1) \geq f(x_0) + f'(x_0)((1-\lambda)(x_1 - x_2)). \tag{2.74}$$

Με αντίστοιχο τρόπο, παίρνοντας $x = x_2$, έχουμε

$$f(x_2) \geq f(x_0) + f'(x_0)(\lambda(x_2 - x_1)). \tag{2.75}$$



ΣΧΗΜΑ 2.3. Παραδείγματα (α) κυρτών και (β) κοίλων συναρτήσεων.

Πολλαπλασιάζοντας την (2.74) με λ και την (2.75) με $1-\lambda$ και προσθέτοντας κατά μέλη καταλήγουμε στην (2.72). Η απόδειξη της γνήσιας κυρτότητας γίνεται με αντίστοιχο τρόπο. □

Το Θεώρημα 2.6.1 μας επιτρέπει να επιβεβαιώσουμε αμέσως ότι οι x^2, e^x και $x \log x$ για $x \geq 0$ είναι γνησίως κυρτές, και ότι οι $\log x$ και $\sqrt{x}$ για $x \geq 0$ είναι γνησίως κοίλες.

Έστω ότι με E συμβολίζουμε την αναμενόμενη τιμή. Άρα, $EX = \sum_{x \in \mathcal{X}} p(x)x$ στη διακριτή περίπτωση και $EX = \int x f(x)\, dx$ στη συνεχή περίπτωση.

Η ανισότητα που ακολουθεί χρησιμοποιείται ευρύτατα στα μαθηματικά και σε αυτήν βασίζονται πολλά θεμελιώδη θεωρήματα της θεωρίας πληροφορίας.

Θεώρημα 2.6.2 (*Ανισότητα του Jensen*) *Αν f είναι μια κυρτή συνάρτηση και X μια τυχαία μεταβλητή,*

$$Ef(X) \geq f(EX). \tag{2.76}$$

Επιπλέον, αν η f είναι γνησίως κυρτή, από την ισότητα στην (2.76) έπεται ότι $X = EX$ με πιθανότητα 1 (δηλαδή η X είναι μια σταθερά).

Απόδειξη: Θα αποδείξουμε το θεώρημα για διακριτές κατανομές με επαγωγή ως προς το πλήθος των σημείων μάζας. Η απόδειξη όσων ισχύουν όταν η f είναι γνησίως κυρτή αφήνεται στον αναγνώστη.

Για μια κατανομή με δύο σημεία μάζας, η ανισότητα γράφεται

$$p_1 f(x_1) + p_2 f(x_2) \geq f(p_1 x_1 + p_2 x_2), \tag{2.77}$$

η οποία έπεται άμεσα από τον ορισμό των κυρτών συναρτήσεων. Υποθέτουμε ότι το θεώρημα ισχύει για κατανομές με $k-1$ σημεία μάζας, οπότε γράφοντας $p'_i = p_i/(1-p_k)$ για $i = 1, 2, \ldots, k-1$, έχουμε

$$\sum_{i=1}^{k} p_i f(x_i) = p_k f(x_k) + (1-p_k) \sum_{i=1}^{k-1} p'_i f(x_i) \tag{2.78}$$

$$\geq p_k f(x_k) + (1-p_k) f\left(\sum_{i=1}^{k-1} p'_i x_i \right) \tag{2.79}$$

$$\geq f\left(p_k x_k + (1-p_k) \sum_{i=1}^{k-1} p'_i x_i \right) \tag{2.80}$$

$$= f\left(\sum_{i=1}^{k} p_i x_i \right), \tag{2.81}$$

όπου η πρώτη ανισότητα προκύπτει από την υπόθεση της επαγωγής και η δεύτερη από τον ορισμό της κυρτότητας.

Στηριζόμενοι στη συνέχεια των συναρτήσεων μπορούμε να επεκτείνουμε την απόδειξη σε συνεχείς κατανομές. □

Ακολούθως θα χρησιμοποιήσουμε αυτά τα αποτελέσματα για να αποδείξουμε μερικές από τις ιδιότητες της εντροπίας και της σχετικής εντροπίας. Το ακόλουθο θεώρημα είναι θεμελιώδους σημασίας.

Θεώρημα 2.6.3 (*Πληροφοριακή ανισότητα*) *Αν $p(x)$ και $q(x)$, $x \in \mathcal{X}$, είναι δύο συναρτήσεις μάζας πιθανότητας, τότε*

$$D(p||q) \geq 0 \tag{2.82}$$

με ισότητα αν και μόνο αν $p(x) = q(x)$ για κάθε x.

Απόδειξη: Αν $A = \{x : p(x) > 0\}$ είναι το σύνολο υποστήριξης της $p(x)$, τότε

$$-D(p||q) = -\sum_{x \in A} p(x) \log \frac{p(x)}{q(x)} \tag{2.83}$$

$$= \sum_{x \in A} p(x) \log \frac{q(x)}{p(x)} \tag{2.84}$$

$$\leq \log \sum_{x \in A} p(x) \frac{q(x)}{p(x)} \tag{2.85}$$

$$= \log \sum_{x \in A} q(x) \tag{2.86}$$

$$\leq \log \sum_{x \in \mathcal{X}} q(x) \tag{2.87}$$

$$= \log 1 \tag{2.88}$$

$$= 0, \tag{2.89}$$

όπου η (2.85) έπεται από την ανισότητα του Jensen. Αφού η $\log t$ είναι γνησίως κοίλη συνάρτηση του t, η (2.85) ισχύει με ισότητα αν και μόνο αν η $q(x)/p(x)$ είναι σταθερή παντού (δηλαδή αν $q(x) = cp(x)$ για κάθε x). Επομένως, $\sum_{x \in A} q(x) = c \sum_{x \in A} p(x) = c$. Η (2.87) ισχύει με ισότητα μόνο αν $\sum_{x \in A} q(x) = \sum_{x \in \mathcal{X}} q(x) = 1$, απ' όπου έπεται ότι $c = 1$. Άρα $D(p||q) = 0$ αν και μόνο αν $p(x) = q(x)$ για κάθε x. □

Πόρισμα (*Μη αρνητικότητα της αμοιβαίας πληροφορίας*) *Για δύο οποιεσδήποτε τυχαίες μεταβλητές X και Y,*

$$I(X;Y) \geq 0, \tag{2.90}$$

με ισότητα αν και μόνο αν οι X και Y είναι ανεξάρτητες.

Απόδειξη: $I(X;Y) = D(p(x,y)||p(x)p(y)) \geq 0$, με ισότητα αν και μόνο αν $p(x,y) = p(x)p(y)$ (δηλαδή αν οι X και Y είναι ανεξάρτητες). □

Πόρισμα

$$D(p(y|x)||q(y|x)) \geq 0, \tag{2.91}$$

με ισότητα αν και μόνο αν $p(y|x) = q(y|x)$ για κάθε y και x τέτοιο ώστε $p(x) > 0$.

Πόρισμα

$$I(X;Y|Z) \geq 0, \tag{2.92}$$

με ισότητα αν και μόνο αν οι X και Y είναι δεσμευμένα ανεξάρτητες με δεδομένη τη Z.

Ακολούθως θα δείξουμε ότι η ομοιόμορφη κατανομή επί ενός πεδίου τιμών $\mathcal{X}$ είναι η κατανομή μέγιστης εντροπίας επί αυτού του πεδίου τιμών. Έπεται ότι η εντροπία οποιασδήποτε τυχαίας μεταβλητής με αυτό το πεδίο τιμών δεν μπορεί να είναι μεγαλύτερη από $\log |\mathcal{X}|$.

Θεώρημα 2.6.4 *$H(X) \leq \log|\mathcal{X}|$, όπου $|\mathcal{X}|$ είναι το πλήθος των στοιχείων του πεδίου τιμών της X, με ισότητα αν και μόνο αν η X είναι ομοιόμορφα κατανεμημένη επί του $\mathcal{X}$.*

Απόδειξη: Αν $u(x) = \frac{1}{|\mathcal{X}|}$ είναι η ομοιόμορφη συνάρτηση μάζας πιθανότητας επί του $\mathcal{X}$ και $p(x)$ η συνάρτηση μάζας πιθανότητας της X, τότε

$$D(p||u) = \sum p(x) \log \frac{p(x)}{u(x)} = \log|\mathcal{X}| - H(X). \tag{2.93}$$

Επομένως, λόγω της μη αρνητικότητας της σχετικής εντροπίας,

$$0 \leq D(p||u) = \log|\mathcal{X}| - H(X). \quad \square \tag{2.94}$$

Θεώρημα 2.6.5 (*Η δέσμευση μειώνει την εντροπία*) (*Η πληροφορία δεν βλάπτει*)

$$H(X|Y) \leq H(X) \tag{2.95}$$

με ισότητα αν και μόνο αν οι X και Y είναι ανεξάρτητες.

Απόδειξη: $0 \leq I(X;Y) = H(X) - H(X|Y)$. $\square$

Σε διαισθητικό επίπεδο, το θεώρημα ορίζει ότι η γνώση μιας άλλης τυχαίας μεταβλητής Y μπορεί μόνο να μειώσει την αβεβαιότητα της X. Σημειωτέον ότι αυτό ισχύει μόνο κατά μέσο όρο. Ειδικότερα, η $H(X|Y = y)$ μπορεί να είναι μεγαλύτερη, μικρότερη ή ίση με την $H(X)$, αλλά κατά μέσο όρο $H(X|Y) = \sum_y p(y)H(X|Y = y) \leq H(X)$. Για παράδειγμα, σε ένα δικαστήριο ένα νέο στοιχείο μπορεί να αυξήσει την αβεβαιότητα, αλλά κατά μέσο όρο τα επιπλέον στοιχεία μειώνουν την αβεβαιότητα.

Παράδειγμα 2.6.1 Έστω ότι οι (X, Y) έχουν την ακόλουθη από κοινού κατανομή:

Y \ X	1	2
1	0	$\frac{3}{4}$
2	$\frac{1}{8}$	$\frac{1}{8}$

Στην περίπτωση αυτή, $H(X) = H(\frac{1}{8}, \frac{7}{8}) = 0{,}544$ δυφία, $H(X|Y = 1) = 0$ δυφία και $H(X|Y = 2) = 1$ δυφίο. Επομένως, $H(X|Y) = \frac{3}{4}H(X|Y = 1) + \frac{1}{4}$