[JA91] J.Adamek, *Foundations of coding. Theory and applications of error-correcting codes with an introduction to cryptography and information theory,* Edit. John Wiley & Sons, New York, 1991

[MEB99]Monica Elena Borda,*Teoria transmiterii informatiei.Teoria informatiei si codarii.Fundamente si aplicatii,* Edit.Dacia, Cluj-Napoca, 1999

[CUL72] G.Cullman, *Coduri detectoare si corectoare de erori,* Edit.Tehnica, Bucuresti,1972

[GAL68] R.G.Gallager, *Information theory and reliable communications,* Edit. John Wiley & Sons, New York, 1968

[KAY02] D.J.C. MacKay, *Information theory,Inference, and Learning Algorithms,* Draft 3.1.1, October, 2002

[JZ98] R.Johannesson, K.Sh.Zigangirov, *Fundamentals of convolutional coding,* IEEE Press, New York,1998

[HW99] C.Heegard, S.B.Wicker, *Turbo coding,* Kluwer Academic Publisher, Boston,1999

[HLY02] L.Hanzo, T.H.Liew, B.L.Yeap, *Turbo coding, turbo equalization and space-time coding for transmission over fading channels,* IEEE Press, Edit. John Wiley & Sons, England

[JIH03] J.H.Hall, *Notes on Coding Theory*, www.mth.msu.edu/jhall/classes/codesnotes/coding-notes.html

[VM01]V.Munteanu, *Teoria transmiterii informatiei,* edit.Gh.Asachi, Iasi, 2001

[MR00] A.T.Murgan, R.Radescu, *Principiile teoriei codurilor. Algoritmi si aplicatii,* Edit. Tehnica, Bucuresti, 2000

[MSG83]A.T.Murgan,I.Spanu, I.Gavat, I.Sztojanov, V.E.Neagoe, A.Vlad, *Teoria transmisiunii informatiei. Probleme,* Edit. Didactica si Pedagogica Bucuresti,1983

[ATM98] A.T.Murgan, *Principiile teoriei informatiei in ingineria informatiei si a comunicatiilor,* Edit.Academiei Romane, Bucuresti, 1998

[MOR95] N.Moreau, *Techniques de compression des signaux,* Edit.Masson, Paris, 1995

[AS87] A.Spataru, *Fondement de la theorie de la transmission de l'information*, Presse Polytechniques Romandes,Lausanne,1987

[PM95] M.Purser, *Introduction to error-correcting codes,* Artech House, Boston, London, 1995

[PRO00] J.G. Proakis, *Digital Communications,* Edit. 4-a, Edit. McGraw Hill, 2000

[AS83] A.Spataru, *Teoria transmisiunii informatiei*, Edit. Didactica si Pedagogica, Bucuresti,1983

[AS83] A.Spataru, *Teoria transmisiunii informatiei. Semnale si perturbatii*, Edit.Tehnica, Bucuresti,1965

[AS83] A.Spataru, *Teoria transmisiunii informatiei*. *Coduri si decizii statistic*e, Edit. Tehnica, Bucuresti, 1971

[SAL97] D.Salomon, *Data compression. The complete reference,* Edit. Springer Verlag, New York, 1997

[SHL94] M.K.Simon, S.M.Hinedi, W.C.Lindsey, *Digital communication techniques. Signal design and detection,* Edit. Prentice Hall, New Jersey, 1994

[TT04] Terrien Ch.W., Tumala M., *Probability for Electrical and Computer Engineers*, CRC Press, Washington, 2004

[WAD00] G.Wade, *Coding techniques.An introduction to compression and error control,* Edit. Creative Print and Design, Wales, 2000

[VY00] Branka Vucetici, J.Yuan, *Turbo codes. Principles and applications,* Kluwer Academic Publisher, Boston,2000

[MU03] M.Uro, *Basic concepts on information theory,* www-citi.int-evry.fr

[HAY01] S.Haykin, *Communication Systems,* Edit. 4-a, Edit. John Willey& Sons, 2001

Teoria informației şi a codării

Momente importante din istoria comunicatiilor.

In anii ’20, **Harry Nyquist** si **Ralph Hartley** au dezvoltat o serie de idei fundamentale pentru transmiterea informatiei pe canalele telegrafice, fara ca aceste idei sa fie cuprinse intr-o teorie unitara. In anii ’40, **Claude Shannon** a dezvoltat conceptul de capacitate a canalului, folosind ideile lui Nyquist si Hartley, dupa care a formulat o teorie completa despre informatie si transmiterea sa.

- In 1924 Nyquist enunta *teorema esantionarii pentru semnale de banda limitata,* care afirma ca este posibila reconstructia exacta a unui semnal in banda de baza, continuu in timp, din esantioanele sale, daca semnalul este limitat ca banda, si frecventa de esantionare este mai mare decat dublul benzii semnalului.

$$s(t) = \sum_n s(nT) \frac{\sin 2\pi B(t - nT)}{2\pi B(t - nT)}$$

$f_s > 2B$ frecventa de esantionare (esantioane pe secunda)

$2B$ viteza Nyquist (esantioane pe secunda)

B banda de frecvente a semnalului sau frecventa Nyquist (Hertzi)

$T \equiv \frac{1}{f_s}$ interval de esantionare sau timpul dintre doua esantioane succesive (secunde)

Teorema esantionarii mai este numita teorema Nyquist-Shannon, Nyquist-Shannon-Kotelnikov, Whittaker-Shannon-Kotelnikov, WKS, etc,.

- In **1927** Nyquist a stabilit ca numarul de simboluri independente care pot fi transmise printr-un canal telegrafic in unitatea de timp, e limitat superior de dublul benzii canalului:

$$f_p \leq 2B,$$

unde f_p este frecventa impulsurilor (numarul de impulsuri pe secunda), iar B este banda de frecventa (hertzi). Transmiterea la viteza de 2B impulsuri pe secunda se numeste semnalizare la viteza Nyquist .

- In **1927 (1930)** Hartley a introdus *masura logaritmica a informatiei pentru comunicatii*, ca logaritmul dimensiunii alfabetului. Hartley a incercat sa cuantifice informatia si viteza de transmitere a informatiei prin canalul de comunicatie. Metoda propusa de el, cunoscuta ulterior ca legea lui Hartley, a precedat notiunea mult mai sofisticata de *capacitate a canalului*.

Hartley a aratat ca numarul maxim de impulsuri distincte care pot fi transmise printr-un canal de comunicatie si receptionate in siguranta e limitat de gama dinamica a amplitudinii semnalului si de precizia cu care receptorul poate distinge nivelurile amplitudinii. Daca domeniul amplitudinilor este [+A, -A] volt si precizia receptorului este de $\pm\Delta V$ volt atunci numarul maxim M de impulsuri distincte este de:

$$M = 1 + \frac{A}{\Delta V}$$

Hartley a considerat *ca informatia transportata de un impuls este logaritm in baza 2 din numarul mesajelor distincte M,* care pot fi transmise. Apoi a stabilit ca viteza de transmitere a informatiei R (sau rata de transmisie) este:

$$R = f_p \log_2 M$$

unde f_p viteza de transmitere a impulsurilor este numita si *viteza de semnalizare*, masurata in simboluri pe secunda sau baud (Bd), iar R, rata de transmisie este masurata in biti pe secunda (bps).

Hartley a combinat relatia precedenta cu observatia lui Nyquist, referitoare la faptul ca printr-un canal de banda B, pot fi transmise maxim 2B impulsuri pe secunda, ajungand astfel la viteza maxima de transmisiune care poate fi atinsa:

$$R \leq 2B \log_2 M$$

Aceasta relatie leaga B, banda analogica (Hz), de R banda numerica (bps). Banda numerica sau digitala R poate fi vazuta ca si capacitatea unui canal M-ar fara erori.

Hartley nu a stabilit dependenta lui M de zgomotul din canal si cum poate fi asigurata siguranta transmisiei pentru distingerea certa la receptor a celor M impulsuri afectate de zgomot. Pentru canalul cu zgomot gaussian, valoarea lui M trebuie aleasa mult mai mica decat cea teoretica, pentru a avea o probabilitate mica a erorii.

In **1948** Shannon a publicat lucrarea sa „A Mathematical Theory of Communications". Inainte de publicarea acestei lucrari, se credea ca prin cresterea vitezei de transmisie prin canal, creste si probabilitatea erorii. Shannon a aratat ca acest lucru nu e adevarat, atata timp cat viteza de transmitere *R* se pastreaza mai mica decat *capacitatea canalului,* chiar daca transmisia se face prin canale afectate de zgomot..

Capacitatea informationala a canalului, sau capacitatea canalului pentru semnale de banda limitata afectate de zgomot alb Gaussian (zgomot termic):

$$C = B \log_2 (1 + SNR) \ \ b/s$$

unde *C capacitatea canalului este viteza maxima cu care se poate transmite fara erori informatia prin canal*, masurata in biti pe secunda (bps); *B* este banda de frecvente a semnalului (Hz)**,** iar *SNR* este raportul dintre puterea *P* (watt) a semnalului receptionat si puterea *N* a zgomotului (watt/Hz). Astfel $SNR = \frac{P}{BN_0}$, N_0 fiind densitatea spectrala de putere a zgomotului(watt/s/Hz), $N_0 = k\ T$, *T= temperatura (K),* iar *k* este constanta lui Boltzman $1{,}38 \times 10^{-23}$ $\left(\text{J/K}\right)$.

Majoritatea comunității științifice de profil consideră că începutul teoriei informației a fost marcat de apariția, în 1948, a articolului lui Claude Shannon "The Mathematical Theory of Communications", devenit celebru. Au apărut astfel două

discipline înrudite, **teoria informației** şi **teoria codării**. *Scopul principal este o* ***transmisie sigură şi eficientă a informației, printr-un mediu de obicei ostil***. Pentru ca transmisia să fie sigură, informația recepționată trebuie să fie identică cu cea transmisă, sau să ”semene” cu aceasta, gradul de toleranță impus fiind relativ mic. Pentru ca transmisia să fie eficientă, efortul şi timpul consumate trebuie să fie cât mai reduse. Aceste două condiții impuse transmisiei, *siguranța* şi *eficiența*, sunt contradictorii, astfel că ne revine sarcina de a ajunge la cel mai bun compromis între ele. Evident că, de la o aplicație la alta, cel mai bun compromis va diferi.

Teoria informației, apelând prin excelență la un aparat analitic şi probabilistic, răspunde la întrebările:

- ce este informația (răspunsul este: *o nedeterminare înlăturată*)
- care este gradul maxim de compresie a informației (răspunsul este: *entropia H*),
- care este viteza maximă de transmitere a informației (răspunsul este: *capacitatea C a canalului*).

Există tendința să se considere teoria informației ca fiind o parte a teoriei comunicațiilor. Dar teoria informației este mult mai cuprinzătoare şi a avut contribuții importante în dezvoltarea mai multor domenii, după cum urmează.

1. *Ingineria electrică - teoria comunicațiilor*

La începutul anilor ’40 s-a crezut că dacă viteza de transmitere prin canal creşte, atunci creşte şi probabilitatea de eroare. Shannon a arătat că acest lucru nu e adevărat, atâta timp cât viteza de transmitere prin canal este mai mică decât capacitatea C a canalului. Capacitatea canalului poate fi uşor calculată din zgomotul caracteristic canalului. Ulterior, Shannon a arătat că procesele aleatoare, cum sunt vorbirea şi muzica, au o complexitate ireductibilă, sub care semnalul nu mai poate fi comprimat, pe care a numit-o entropie, prin similitudine cu entropia din termodinamică. Shannon a arătat că dacă entropia sursei e mai mică decât capacitatea canalului, se poate ajunge asimptotic, la o comunicație fără erori.

Teoria informației indică *extremele între care se încadrează toate sistemele de comunicație posibile*. Pe de o parte se află entropia sursei, care dă limita inferioară de compresibilitate a datelor şi pe cealaltă parte se află capacitatea canalului, care dă limita superioară a vitezei de transmitere a datelor prin canal. Orice schemă de compresie sau de modulare se încadrează între aceste două limite. Teoria informației sugerează şi mijloacele de a ajunge la aceste limite, dar implementarea lor nu este fezabilă din punct de vedere practic, din cauza volumului imens de calcul.

2. *Ştiința calculatoarelor - complexitatea Kolmogorov*

Definirea complexității unui şir de date, prin lungimea celui mai scurt program binar necesar pentru calculul acelui şir, aparține lui Kolmogorov, Chaitin şi Solomonov. Definiția este universală, nu depinde de calculatorul folosit. Are o importanță fundamentală, stând la baza teoriei complexității descrierii. Complexitatea Kolmogorov, *K*, este aproximativ egală cu entropia *H*, dar este mai generală decât entropia şi reprezintă limita până la care pot fi comprimate datele, oferind bazele logice pentru inferențe.

Complexitatea Kolmogorov este lungimea programului, iar complexitatea de calcul este timpul necesar rulării programului. Cele două sunt complementare. Deşi s-au depus eforturi pentru minimizarea separată a fiecăreia dintre ele, sunt puține lucrări care încearcă minimizarea lor simultană.

3. *Fizica – termodinamica*

Mecanica statistică a propus noțiunea de *entropie*, ca o măsură a gradului de incertitudine sau dezorganizare într-un sistem fizic. Tot mecanica statistică a enunțat şi legea a doua a termodinamicii, care spune că entropia unui sistem închis nu poate descreşte. Legea a doua a termodinamicii ne avertizează că nu are rost să visăm la un „perpetuum mobile".

4. *Matematica - teoria probabilităților şi statistica*

Mărimile fundamentale din teoria informației – *entropia, entropia relativă şi informația mutuală* – sunt definite ca funcționale de distribuții de probabilitate. Ele caracterizează comportarea secvențelor lungi de variabile aleatoare şi permit estimarea probabilităților evenimentelor rare (teoria deviațiilor mari) şi găsirea celui mai bun exponent al erorii pentru testarea ipotezelor.

5. *Filozofia ştiinței – regula sau briciul lui Occam (Occam's razor)*

William din Occam, filozof reducționist din secolul 14, a enunțat o regulă: „problemele nu trebuie complicate mai mult decât e necesar", care parafrazată devine „*explicația cea mai simplă este cea mai bună*". Ea mai este numită şi *legea conciziunii*. Solomonov şi apoi Chaitin au arătat că poate fi găsită o procedură de predicție universal valabilă, dacă se foloseşte o combinație ponderată a tuturor programelor care explicitează datele şi observând următorul caracter generat. Aceasta inferență e valabilă şi pentru alte domenii decât statistica, dar pentru multă vreme de acum înainte, va fi dificil de implementat în practică.

6. *Economie – investiții*

Investițiile repetate într-o piață de stocuri staționară duc la creşterea exponențială a bogăției, a cărei *rată de creştere* sau rată *de dublare* este duala ratei entropiei stocurilor. Exista un paralelism între teoria informației şi teoria investițiilor optime în stocuri.

7. *Calculatoarele şi comunicațiile*

Pe măsură ce construim calculatoare din ce în ce mai puternice din componente din ce în ce mai mici, percepem limitele calculului şi cele ale comunicațiilor. Comunicațiile sunt limitate de capacitatea de calcul, iar capacitatea de calcul e limitată de comunicații. Progresele din teoria comunicațiilor au, prin intermediul teoriei informației, un impact direct asupra teoriei calculatoarelor.

Teoria codării oferă modalitățile de atingere a limitelor referitoare la gradul de compresibilitate a datelor şi viteza maxima de transmitere a informației prin canal, folosind metode algebrice.

Tehnicile de codare stau la baza sistemelor numerice de comunicații şi s-au concretizat într-o serie de *algoritmi complecşi de compresie şi de control a erorilor*. De exemplu, algoritmul LZW stă la baza tehnicilor de compresie fără pierderi a fişierelor, codarea CELP a semnalului vocal e folosită în comunicațiile personale, iar codarea video MPEG-2 oferă o compresie tipică de 30:1 pentru difuzarea video. În domeniul controlului erorilor, decodarea Viterbi cu decizie soft e un standard pentru sistemele cu sateliți, codurile ciclice sunt folosite la protecția datelor atât în rețelele terestre punct la punct cât şi în rețelele radio, iar turbo-decodoarele au permis apropierea la 1 dB față de

limita teoretică indicată de Shannon. Secvențele pseudo-aleatoare sunt des folosite în modemuri, în sistemele de telefonie de tip CDMA (Code Division Multiple Acces) şi mai recent în sistemele de marcare transparentă a imaginilor şi produselor video.

Considerații generale asupra comunicațiilor

Atunci când ne pregătim să transmitem informația de la sursă la destinație ne gândim la *eficiența* şi la *siguranța transmisiei*. Pentru asigurarea eficienței trebuie să reducem pe cât posibil volumul datelor de transmis, deci să facem o *compresie*. Vom vedea la momentul potrivit, că această compresie poate să fie fără pierderi sau cu pierderi de informație, după cum permite aplicația în cauză. Un fişier cu date ştiințifice sau bancare, evident că nu va permite o compresie cu pierderi, în timp ce o imagine statică sau în mişcare va permite acest lucru. O altă problemă pe care ne-o punem este asigurarea *confidențialității* conținutului mesajului, deci a securizării acestuia față de acțiunile unor intruşi umani, prin codări cu metode criptografice. *Compresia şi secretizarea* informației sunt operații care fac parte din ***codarea sursei***.

Informația este transmisă de la sursă la destinatar prin intermediul unui *canal de comunicație.* Putem alege exact modul în care este structurată informația la sursă şi modul în care este tratată la receptor, dar *comportarea canalului nu depinde de noi*. Există foarte multe tipuri de canale. Oricare ar fi însă canalul, efectul este distorsionarea informației care trece prin el. Reacția normală este deci să încercăm să protejăm informația, sau mai general comunicația, de efectul canalului, folosind *codurile detectoare şi corectoare de erori.* Codarea informației, cu scopul de a o proteja împotriva erorilor cauzate de canal face parte din ***codarea canalului***.

In multe situații, dacă nu am înțeles informația recepționată, putem să cerem repetarea ei, cu întrebări de genul : ce? ce ai spus? (lucru posibil în cazul unei conversații, dar nu şi în cazul citirii unei cărți), ceea ce implică însă un consum suplimentar de timp. Soluția mai generală este adăugarea de *redundanță* mesajului original, astfel încât deşi perturbat, în anumite limite evident, acesta să mai poată fi reconstituit la recepție, cu ajutorul acestei redundanțe. Orice limbă, engleza, franceza, româna, etc. are inclusă în ea o redundanță naturală, care ne permite să reconstituim un cuvânt sau o frază când apar litere şterse, sau dacă au fost făcute prescurtări.

Putem comunica *în spațiu*, ca de exemplu atunci când vorbim într-o cameră cu mult zgomot, sau *în timp,* ca atunci când citim o carte scrisă cu mulți ani înainte.

Comunicația în spațiu, a utilizat cu succes codarea, sub forme simple la început şi din ce în ce mai sofisticate în prezent. Astfel, C. Shannon, R.Hamming şi alți câțiva care au pus bazele teoriei comunicațiilor, au lucrat la Bell Telephone Laboratories, având ca scop să trateze erorile ce apăreau în mesajele transmise pe liniile telefonice, erori cauzate în principal de diafonii şi descărcări electrice. Incorporarea în hardware-ul modemurilor a unor funcții de tratare a erorilor a îmbunătățit capacitatea de transmisie şi recepție a echipamentului. In cosmos, comunicațiile sunt perturbate din cauza condițiilor atmosferice şi activității solare. Misiunile spațiale au folosit de mulți ani diverse tipuri de codări, soluția retransmisiei datelor eronate, folosită la rețelele terestre, nefiind posibilă din cauza întârzierilor mari.

Este important să protejam şi în timp informația memorată sub o formă sau alta. De exemplu, datele memorate într-un calculator sunt expuse la diferite perturbații electromagnetice astfel că multe hard-disk-uri au prevăzute sume ciclice de control, CRC (Cyclic Redundancy Check) pentru detectarea erorilor. Când firma Phillips a introdus

compact-discurile le-a prevăzut cu coduri pentru controlul erorilor specifice acestora: zgârieturi, bule de aer în plastic, amprente, etc. Împreună cu compania Sony au propus un standard pentru memorarea şi reproducerea digitală a semnalelor audio, bazat pe întreţeserea a două coduri Reed-Solomon.

Exemple

*1- Transmiterea unui facsimil***.** Pagina a cărei imagine trebuie transmisă constă dintr-o serie de puncte, albe si negre reprezentate prin cifre binare (”1” pentru un punct negru, respectiv ”0” pentru un punct alb). Dimensiunea paginii este de 30cm x 21cm. Rezolutia este de 78 de puncte per cm, adică 6084 puncte per cm^2. Prin urmare, numărul de cifre binare corespunzătoare paginii este de:

$$30 \text{ x } 21 \text{ x } 6084 = 3{,}83 \text{ Mbiți.}$$

Cu un modem cu viteza de 14,4 kbps transmisia unei pagini va dura 266 sec, adică *4 minute şi 26 de secunde*. Dacă se codează sursa (codare cu pas variabil, codare Huffman) se poate reduce timpul de transmisie a sursei la *17 secunde*.

2- Memorarea unui fişier audio MP3. Codarea MP3 se referă la nivelul 3 de la Moving Picture Expert Group, fiind un standard pentru compresia fişierelor audio, conform cu modelul psihoacustic al auzului uman. Pentru reducerea volumului de informaţie necesar reprezentării unui semnal audio, se folosesc mascarea în timp şi în frecvenţă, limitarea benzii şi codarea Huffman, astfel încât urechea umană nu mai face distincţia între sunetul original şi cel codat.

Considerăm un semnal muzical stereo analogic. La un CD (Compact Disc) de calitate, eşantionarea se face la 44,1 Khz, atât pentru canalul stâng cât şsi pentru canalul drept. Eşantioanele sunt cuantizate cu 16 biţi per eşantion. O secundă de muzica stereo în format CD generează:

$$44{,}1 \text{ x } 10^3 \text{ x } 16 \text{ x } 2 = 1{,}411 \text{ Mbiți}$$

Folosind algoritmul MP3 de codare, această valoare scade la 128 Kbit, fără pierderi perceptibile ale calităţii sunetului. Practic, un minut de muzică stereo va necesita:

$$\frac{128 \cdot 10^3 \cdot 60}{8} \approx 1 \text{ MB/ min}$$

(1 Byte = 8 biţi). Astfel că un *CD ROM*, care are o capacitate de 650 MB, *poate memora mai mult de 10 ore de muzică MP3.*

3 - Descărcarea fişierelor MP3

a) - folosind o linie telefonică

O linie telefonică analogică e formată dintr-o pereche de fire de cupru a cărei bandă de frecvenţe este limitată la B = 4 KHz. O asemenea linie transmite semnale analogice având un raport semnal pe zgomot *SNR* (Signal to Noise Ratio) ≈ 30 dB, şi poate fi

considerată ca un canal gaussian, cu zgomot aditiv, fără memorie. Cu *snr* se notează raportul $snr = \frac{S}{N}$ dintre puterea *S* a semnalului şi puterea *N* a zgomotului, iar cu *SNR* acelaşi raport exprimat în decibeli (dB). Teoria informației ne permite să-i calculăm capacitatea (exprimată în biți/secundă sau bps):

$C = B \log_2 (1+snr)$

sau

$C \approx \frac{B}{3} SNR$ unde $SNR = 10 \log_{10} (snr)$

Pe scurt, *capacitatea* este viteza maximă cu care putem transmite informația, cu o probabilitate a erorii oricât de mică, folosind metode adecvate. Astfel, obținem:

$C \approx 33\ 800$ biți/sec $\approx$ 4 KB/sec.

Astfel, descărcarea a trei minute de muzică MP3, printr-o linie telefonică analogică, folosind un modem V.90 (56 Kbps) va dura:

$$\frac{3 \cdot 10^6}{4 \cdot 10^3} = 750 \text{ sec} = \textit{12minute şi 30 secunde}$$

La orele de trafic maxim (busy hours) viteza de descărcare poate scădea sub 1 KB/sec, astfel că timpul total de descărcare poate ajunge la *50 minute*.

b) - folosind o linie numerică sau digitală
Banda semnalelor telefonice este de 4 Khz, deci frecvența de eşantionare este de 8 KHz. In plus, la cuantizarea fiecărui esantion, se folosesc câte 8 biți,astfel ca rezultă un debit de:

8 x 8 = 64 Kbps = 8 KB/sec.

Viteza de descărcare sau de transfer este dublă față de a unei linii telefonice analogice, deci vor fi necesare doar *6 minute şi 15 secunde* pentru descărcarea a 3 minute de muzică MP3.

c) - folosind un modem şi tehnologia ADSL (Assymetric Digital Subscriber Line)
Această tehnologie pretinde să avem un USB (Universal Serial Bus) sau un modem Ethernet. Ea constă din divizarea benzii disponibile în trei canale :

- un canal de mare viteză dinspre Internet spre utilizator (downstream channel)
- un canal de viteză medie dinspre utilizator înspre Internet (upstream channel)
- un canal clasic POTS (Plain Old Telephone Service)

Avantajul principal constă în faptul ca îți poți folosi telefonul, în timp ce eşti conectat şi la Internet. Cu un modem de 512 Kbps, descărcarea datelor se poate face la 60 KB/sec (480Kbps downstream şi 32 Kbps upstream). Descărcarea a 3 minute de muzică MP3 va dura doar :

$$\frac{1 \cdot 3 \cdot 10^3}{60} = 50 \text{ secunde}$$

Câteva noțiuni introductive

Primele probleme tratate de teoria informației au fost cele din domeniul transmisiei şi compresiei de date. Răspunsurile au constat în noțiuni ca entropia şi informația mutuală, care sunt funcții de distribuțiile de probabilități ale comunicației.

Entropia unei variabile aleatoare X, având funcția de masă a probabilității $p(x)$, este definită prin:

$H(X) = -\sum p(x) \log_2 p(x)$.

Se foloseşte logaritmul în baza 2, astfel că entropia va fi măsurată în biți. Entropia este o măsură a incertitudinii medii pentru o variabilă aleatoare şi reprezintă numărul mediu de biți necesari pentru a descrie o variabilă aleatoare.

Exemplul 1.1. Considerăm o variabilă aleatoare care are o distribuție uniformă a celor 32 de rezultate posibile. Pentru a identifica rezultatul avem nevoie de o etichetă care să poată lua 32 de valori, deci pentru etichetă va fi suficient un şir de 5 biți.

Entropia acestei variabile aleatoare este:

$$H(X) = -\sum_{i=1}^{32} p(x) \log_2 p(x) = -\sum_{i=1}^{32} \frac{1}{32} \log_2 \frac{1}{32} = 5 \text{ biti},$$

care corespunde numărului de biți necesari pentru descrierea lui *X*. În acest exemplu, toate rezultatele au reprezentări de aceeaşi lungime.

Exemplul 1.2. Considerăm acum un exemplu cu o distribuție neuniformă: cazul unei curse la care participă 8 cai, avand distribuția de probabilități, astfel: $\left(\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{64}, \frac{1}{64}, \frac{1}{64}, \frac{1}{64}\right)$. Putem să calculăm entropia cursei ca fiind:

$$H(X) = -\frac{1}{2}\log_2 \frac{1}{2} - \frac{1}{4}\log_2 \frac{1}{4} - \frac{1}{8}\log_2 \frac{1}{8} - \frac{1}{16}\log_2 \frac{1}{16} - 4\frac{1}{64}\log_2 \frac{1}{64}$$
$$= 2 \text{ biti}$$

Presupunem acum că vrem să transmitem altei persoane care este calul câştigător. O cale este să transmitem indexul calului câştigător, pentru care avem nevoie de 3 biți, fiind 8 cai în total. Dar cum probabilitățile de a câştiga nu sunt uniforme, e logic să folosim descrieri mai scurte pentru caii cu probabilitate mare de câştig, şi descrieri mai lungi pentru caii cu probabilitate mică de câştig, astfel încât valoarea medie a descrierii să fie mai mica de cei 3 biți din cazul descrierii uniforme. Putem folosi, de exemplu, următoarele şiruri de biți, pentru descrierea celor 8 cai :

0, 10, 110, 1110, 111100, 111101, 111110, 111111.

În acest caz *lungimea medie a descrierii* $\bar{l} = \sum_{i=1}^{8} p(x_i)\, l(x_i)$ biti= 2 biti şi nu 3 biți ca în cazul descrierii uniforme; cu $l(x_i)$ a fost notată lungimea fiecărei descrieri. În acest caz, lungimea medie a descrierii este egală cu entropia.

Entropia din teoria informatiei este strâns legată de entropia din mecanica statistică. Dacă e generat un şir de n variabile aleatoare independente şi idendic distribuite, i.i.d., probabilitatea unei secvenţe „tipice" este în jur de $2^{-nH(X)}$ şi există în jur de $2^{nH(X)}$ asemenea secvenţe tipice. Această proprietate, numită proprietatea echipartiţiei asimptotice, AEP (Asymptotic Equipartition Property) stă la baza multor demonstraţii din teoria informaţiei.

Noţiunea complexităţii descrierii unei variabile aleatoare poate fi extinsă pentru a defini *complexitatea descrierii unui şir*. Complexitatea Kolmogorov a unui şir binar este definită ca lungimea celui mai scurt program de calculator care poate tipări şirul. Dacă şirul este aleator cu adevărat, atunci complexitatea Kolmogorov tinde spre entropie. Complexitatea Kolmogorov este un mediu natural în care se consideră problemele inferenţelor şi modelării statistice şi permite o înţelegere mai bună a principiului lui Occam, „cea mai simplă explicaţie este cea mai bună".

Entropia este nedeterminarea unei variabile aleatoare. Putem defini *entropia condiţionată*, care este entropia unei variabile aleatoare, având dată o altă variabilă aleatoare. Reducerea nedeterminării, datorată altei variabile aleatoare, se numeşte *informaţie mutuală*. Pentru două variabile aleatoare, X şi Y, această reducere este:

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

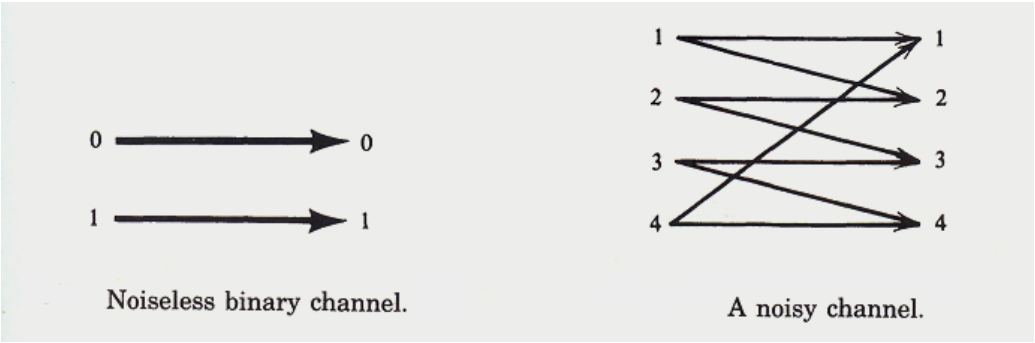
Informaţia mutuală $I(X;Y)$ este o măsură a dependenţei dintre cele două variabile aleatoare. Ea este simetrică faţă de X şi Y şi este întotdeauna ne-negativă.

Un *canal de comunicaţie* este un sistem la care ieşirea depinde probabilistic de intrare. El este caracterizat de matricea probabilităţilor de tranziţie, care determină distribuţia condiţionată a ieşirii pentru o intrare dată. Pentru un canal de comunicaţie cu intrarea X şi ieşirea Y, se defineşte *capacitatea C*, prin:

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

Capacitatea este viteza maximă cu care se poate transmite informaţia prin canal şi se poate recupera informaţia la ieşire cu o probabilitate a erorii extrem de mică.

Exemplul 1.3. Canalul binar simetric fără zgomot. La acest canal, intrarea binară, 1 sau 0, este reprodusă exact de ieşire, fără erori. La fiecare transmisie se poate emite 1 bit, în siguranţă şi capacitatea este $C = \max I(X;Y) = 1$ bit .

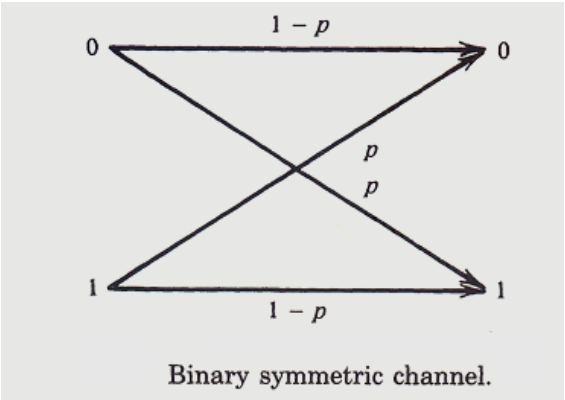


Noiseless binary channel. A noisy channel.

Exemplul 1.4. Canalul cu zgomot cu patru simboluri. Acesta admite 4 simboluri la intrare şi fiecare simbol va fi recepționat corect cu probabilitatea $1/2$ sau se transformă în simbolul imediat următor $(1 \to 2,\ 2 \to 3,\ 3 \to 4,\ 4 \to 1)$ cu probabilitatea $1/2$. Dacă se folosesc toate cele 4 simboluri, atunci la ieşire nu putem spune cu certitudine care simbol a fost emis. Daca însă se folosesc doar două simboluri, neadiacente, sau disjuncte, 1 şi 3 de exemplu, atunci la ieşire se poate spune cu certitudine care simbol a fost emis. Acest canal apare ca şi canalul fără zgomot din exemplul precedent, deci putem transmite 1 bit fără erori. Capacitatea acestui canal va fi $C = \max I(X;Y)$ de 1 bit per transmisiune, conform cu analiza anterioară.

In general, canalele de comunicație nu au structura simplă din exemplul precedent, şi nu putem selecta întotdeauna o submulțime a intrărilor astfel încât să putem transmite informația fără erori. Totuşi, considerând o secvență de transmisiuni, atunci orice canal apare ca cel din exemplul precedent, şi putem selecta o submulțime a secvențelor de intrare (cuvinte de cod), în aşa fel încât fiecare din cuvintele de cod să fie aproximativ disjuncte. Analizând secvențele de ieşire, putem identifica secvențele de intrare, cu o probabilitate a erorii oricât de mică.

Exemplul 1.5. Canalul binar simetric : reprezintă un exemplu de bază pentru sistemele de comunicații afectate de zgomot.



Binary symmetric channel.

Canalul are intrarea binară ; cu probabilitatea $1-p$ ieşirea este aceeaşi cu intrarea, iar cu probabilitatea *p,* 0 va fi recepționat ca 1, respectiv 1 va fi recepționat ca 0. Capacitatea în acest caz va fi $C = 1 + p\log p + (1-p)\log(1-p)$ biți per transmisiune. Nu e evident cum se obține aceasta capacitate, dar dacă folosim canalul de multe ori, va semăna cu canalul cu 4 simboluri din exemplul anterior, şi se poate transmite informația cu o rată de C biți per transmisiune, cu o probabilitate a erorii oricât de mică.

Limita superioară a vitezei de transmitere a informației prin canal este dată de capacitatea canalului. *Teorema codării canalului* spune că această limită poate fi atinsă folosind coduri cu blocuri de lungime mare. Pentru sistemele de comunicație practice, apar limitări ale complexității codurilor ce pot fi folosite, astfel că nu putem atinge capacitatea.

Informaţia mutuală este un caz particular al unei mărimi mult mai generală, numită *entropie relativă* $D\left(p\|q\right)$, care este o măsură a „distanţei”dintre două funcţii de masă a probabilităţii, *p* şi *q*. Entropia relativă este definită ca:

$$D\left(p\|q\right)=\sum_{x}p\left(x\right)\log\frac{p\left(x\right)}{q\left(x\right)}$$

Deşi entropia relativă nu e o metrică adevarată are anumite proprietăţi ale unei metrici. Ea este întotdeauna ne-negativă şi este zero dacă şi numai dacă $p=q$. Entropia relativă apare ca exponent al probabilităţii de eroare în testul ipotezelor dintre distribuţiile *p* şi *q*. Entropia relativă poate fi folosită pentru definirea geometriei distribuţiilor de probabilitate, care permite interpretarea multor rezultate din teoria abaterilor mari.

Există multe paralelisme între teoria informaţiei şi teoria investiţiilor în pieţele de stocuri. O piaţă de stocuri e definită de un vector aleator $\mathbf{X}$ ale cărui elemente sunt numere ne-negative care sunt date de raportul dintre preţul stocului la sfârşitul zilei şi preţul stocului la începutul zilei. Pentru o piaţă de stocuri cu distribuţia $\boldsymbol{F}\left(\boldsymbol{x}\right)$, se poate defini rata de dublare *W*, ca fiind:

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

Rata de dublare este exponentul asimptotic maxim pentru creşterea bogăţiei, având o serie de proprietăţi similare cu ale entropiei.

Mărimile H,I,C,D,K,W apar în mod natural în următoarele domenii:

• *Compresia de date*. Entropia *H* a unei variabile aleatoare este o limită inferioară a lungimii celei mai scurte descrieri a acelei variabile aleatoare. Putem construi descrieri cu o lungime medie de un bit a entropiei.

Dacă relaxăm condiţiile de regăsire perfectă a sursei, putem pune întrebarea ce rate (câtă informaţie sau entropie) sunt necesare pentru a descrie sursa cu distorsiunea *D* ? Şi ce capacitate a canalului e suficientă ca să ne permită transmiterea acestei surse prin canal şi reconstruirea ei cu o distorsiune mai mică sau egală cu *D* ? Acesta este subiectului teoriei distorsiune-rată creată de C. Shannon.

Observaţie. Rată aici înseamnă numărul de biţi ai sursei (numărul de biţi per eşantion) care trebuie memoraţi sau transmişi. Distorsiune înseamnă varianţa dintre semnalul de intrare şi semnalul de ieşire (eroarea medie patratică a diferenţei dintre aceste două semnale).

Încercarea de a formaliza noţiunea de cea mai scurtă descriere pentru obiecte nealeatoare conduce la complexitatea Kolmogorov *K*. Complexitatea Kolmogorov este universală şi corespunde multor condiţii intuitive din teoria celei mai scurte descrieri.

• *Transmisiunile de date*. Considerăm problema transmisiunii informaţiei astfel încât receptorul să poată decoda mesajul cu o probabilitate mică a erorii. In esenţă, am dori să găsim cuvinte de cod (secvenţele simbolurilor de intrare în canal) care sunt mutual sau reciproc suficient de îndepărtate unul de celălalt, astfel încât versiunile lor afectate de zgomot (recepţionate la ieşirea din canal) să fie distincte una de cealaltă. Această problemă este echivalentă cu problema împachetării sferelor într-un spaţiu

multidimensional. Pentru orice set sau mulțime de cuvinte de cod este posibil să se calculeze probabilitatea ca receptorul să facă o eroare, adică să ia o decizie incorectă referitoare asupra cuvântului de cod care a fost transmis. În majoritatea cazurilor, calculul este lung şi dificil.

Folosind un cod generat aleator, Shannon a arătat că se poate transmite informația prin canal cu o viteză mai mică decât capacitatea canalului, cu o probabilitate a erorii oricât de mică. Ideea unui cod generat aleator era neobişnuită, dar oferea bazele unei analize simple pentru o problemă extrem de dificilă. Unul din elementele principale din demonstrația acestui concept este reprezentat de şirurile tipice.

• *Teoria informației pentru rețele*. In tot ce s-a expus anterior, a fost presupusă existența unei singure surse şi a unui singur receptor. Dar dacă cineva vrea să comprime simultan mai multe surse şi apoi să pună descrierile lor comprimate împreună, într-o reconstrucție comună a surselor ? Această problemă e rezolvată cu ajutorul teoremei Slepian-Wolf. Sau ce se întâmplă dacă mai multe emițătoare transmit simultan aceluiaşi receptor? Cât este capacitatea canalului pentru acest canal ? Acesta este canalul cu acces multiplu soluționat de Liao şi Ahlswede. Sau ce se întâmplă dacă există un singur emițător şi mai multe receptoare care doresc să comunice simultan, informații poate diferite, spre fiecare dintre receptoare ? Acesta este canalul cu difuzare. Şi, în sfârşit, ce se întâmplă dacă există simultan, mai multe emițătoare şi mai multe receptoare, într-un mediu cu zgomote şi interferențe ? Care este regiunea capacității ratelor obtenabile pentru diferitele emițătoare spre receptoare ? Aceasta este problema teoriei informației generalizată pentru rețele. Toate aceste probleme cad în domeniul general al teoriei informației pentru rețele. Deşi aceasta teorie înca nu e complet creată, răspunsurile vor necesita forme elaborate ale informației mutuale şi entropiei relative.

• *Teoria ergodicității*. Teorema echipartiției asimptotice spune că majoritatea celor n secvențe de eşantioane ale unui proces ergodic au probabilitatea de aproximativ $2^{-nH(X)}$ şi că există aproximativ $2^{nH(X)}$ asemenea secvențe tipice.

• *Testarea ipotezelor*. Entropia relativă *D* apare ca un exponent al probabilității erorii în testul ipotezelor dintre două distribuții, fiind o măsură naturală a distanței dintre distribuții.

• *Mecanica statistică*. Entropia *H* apare în mecanica statistică ca o măsură a nedeterminării sau dezorganizării dintr-un sistem fizic. Legea a doua a termodinamicii spune că entropia unui sistem închis nu poate descreşte.

• *Inferențele*. Putem folosi noțiunea de complexitate Kolmogorov *K* pentru a găsi cea mai scurtă descriere a datelor şi să folosim acest model pentru predicția caracterului care urmează. Modelul care maximizează nedeterminarea sau entropia conduce la inferențe referitoare la entropia maximă.

• *Jocuri şi investiții*. Exponentul optim al creşterii bogății este dat de rata de dublare *W*. Pentru o cursă de cai cu o distribuție uniformă, suma dintre rata de dublare *W* şi entropia *H* este constantă. Informația mutuală *I* dintre cursa de cai şi unele informații

colaterale este limita superioară a creşterii ratei de dublare datorată informaţiilor colaterale. Rezultatele sunt asemănătoare pentru investiţiile în piaţa de stocuri.

• *Teoria probabilităţilor*. Proprietatea echipartiţiei asimptotice, AEP, arată că majoritatea secvenţelor sunt tipice, în sensul că au entropia eşantioanelor apropiată de *H*. Deci atenţie trebuie acordată doar acestor aproximativ $2^{nH(X)}$ secvenţe tipice. În teoria deviaţiilor mari, probabilitatea setului este de aproximativ 2^{-nD}, unde *D* este distanţa entropiei relative dintre cel mai apropiat element al setului şi adevărata distribuţie.

• *Teoria complexităţii.* Complexitatea Kolmogorov *K* este o măsură a complexităţii descrierii unui obiect. Ea este legată de, dar diferită de complexitatea de calcul, care este o măsură a timpului sau spaţiului necesar calculului.

Mărimile ce apar în teoria informaţiei, entropia şi entropia relativă, apar, mereu şi mereu, ca răspunsuri la întrebări fundamentale din comunicaţii şi statistică. Înainte de a analiza aceste întrebări, vom studia unele din proprietăţile răspunsurilor, adică ale entropiei şi entropiei relative.

Şir tipic: prin *şir tipic* al unei surse fără memorie se înţelege şirul care conţine $n_1 = np_1$ simboluri x_1, $n_2 = np_2$ simboluri x_2, etc., unde p_i este probabilitatea simbolului x_i, iar $n = \sum n_i$ este un număr ce tinde spre infinit. Mulţimea şirurilor tipice are o probabilitate $p \neq 0$ si $p \neq 1$, dar tinde către 1 pe măsură ce creşte n. Mulţimea şirurilor netipice, adică cele care au o compoziţie diferită de $n_1 = np_1$ simboluri x_1, $n_2 = np_2$ simboluri x_2, etc., are o probabilitate ce tinde spre zero pe măsură ce creşte n. Deci frecvenţele simbolurilor obţinute din şiruri particulare vor tinde în probabilitate către o limită definită $p_1, p_2, ..., p_k$, independentă de şirul particular evaluat, dacă lungimea şirului tinde spre infinit. Sensul limitei în probabilitate este că, deşi există şiruri pentru care afirmaţia precedentă este falsă, probabilitatea lor tinde către zero.

La aceleaşi valori ale probabilităţilor simbolurilor se ajunge şi dacă se consideră n surse identice şi la un moment dat de timp t, se numără câte surse dau simbolul x_1, adică n_1 surse, cele care dau simbolul n_2, adică n_2 surse, etc. Frecvenţele $\frac{n_1}{n}, \frac{n_2}{n}, ...$ când $n \to \infty$ tind spre probabilităţile $p_1, p_2, ...$ Sursa staţionară cu memorie finită, la care toate şirurile de simboluri sunt şiruri tipice, este o *sursă ergodică*. Se vede că ergodicitatea presupune identificarea valorilor medii de-a lungul secvenţei realizate de o singură sursă, de-a lungul axei timpului, cu valorile obţinute asupra ansamblului secvenţelor de la cele n surse, la un moment dat. Asemănător pot fi formate şiruri tipice pentru sursele cu memorie finită, luând în considerare grupurile de simboluri peste care se extinde memoria sursei.

Inferenţa: concluzie, deducere, consecinţă. Este un raţionament prin care se ajunge la unele concluzii. De fapt înseamnă efectuarea de raţionamente logice pe baza unor rezultate sau cunoştinţe anterioare, mai degrabă decât pe baza unor observaţii directe. Procedura de inferenţă are loc printr-o deducţie sau printr-o inducţie. O inferenţă este o afirmaţie, presupusă adevărată deoarece se bazează pe unele fapte cunoscute. Dacă despre ceva se spune doar că e adevărat, atunci este o *afirmaţie*. Dacă această afirmaţie se constată că este adevărată, în urma unor argumente şi raţionamente, atunci ea este o *concluzie*.