

Az információ- és kódelmélet alapjai

Baran Sándor

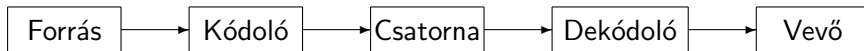
2022/23 tanév, 2. félév

- ❶ Györfi László, Györi Sándor, Vajda István: *Információ- és kódelmélet*. Typotex, 2010.
- ❷ Csiszár Imre, Fritz József: *Információelmélet*. Tankönyvkiadó, 1980.
- ❸ Cover, Thomas M. and Thomas, Joy A.: *Elements of Information Theory*. Wiley, 2006.
- ❹ Togneri, Roberto and de Silva, Christopher J. S.: *Fundamentals of Information Theory and Coding Design*. Chapman & Hall/CRC, 2006.
- ❺ Ash, Robert B.: *Information Theory*. Dover Publications, 1990.

Tartalom

- 1 A forráskódolás alapjai
- 2 Univerzális forráskódolás
- 3 Entrópia és tulajdonságai
- 4 Csatornakapacitás
- 5 Véletlen keresés
- 6 Általános információforrások
- 7 Differenciális entrópia
- 8 A hibajavító kódolás alapjai

Távközlési rendszer általános alakja



Példák.

Füstjelek



Jelzőzászlók



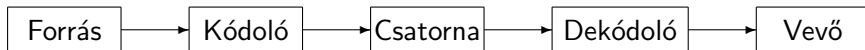
Távírókészülék



Internet



A távközlési rendszer elemei



Forrás: Egyenlő időközönként folyamatosan jeleket (**betűket**) sugároz, melyek egy véges halmaz, ún. **forrásábécé** elemei.

Közlemény (üzenet): A forrásábécé betűinek tetszőleges véges hosszúságú sorozata.

Csatorna: egyenlő időközönként egymás után következő jeleket (**kódjelek**) továbbít, amik egy véges halmaz (**kódábécé, csatornaábécé**) elemei. Lehetnek **zajmentesek** és **zajosak**.

Bináris csatorna: a kódábécé kételemű, például $\{0, 1\}$.

Kódközlemény: A kódábécé jeleinek tetszőleges véges hosszúságú sorozata.

Kódoló, kódolási eljárás: a közlemények (végtelen) halmazát a kódközlemények (végtelen) halmazába képező függvény.

Egyértelműen dekódolható kódolási eljárás: különböző közleményekhez különböző kódközleményeket rendelő kódoló.

Morse-abc

Lehetséges módszer az egyértelmű dekódolhatóság biztosítására: a kódszavak elválasztása.

A ● —	U ● ● —
B — ● ● ●	V ● ● ● —
C — ● — ●	W ● — —
D — ● ●	X — ● ● —
E ●	Y — ● — —
F ● ● — ●	Z — — ● ●
G — — ●	
H ● ● ● ●	
I ● ●	
J ● — — —	
K — ● — —	1 ● — — — —
L ● — ● ●	2 ● ● — — —
M — —	3 ● ● ● — —
N — ●	4 ● ● ● ● —
O — — — —	5 ● ● ● ● ●
P ● — — ● ●	6 — ● ● ● ●
Q — — — ● —	7 — — ● ● ●
R ● — ● ●	8 — — — ● ●
S ● ● ●	9 — — — — ●
T —	0 — — — — —

- 1 A „pont” hossza egy egység.
- 2 A „vonal” hossza három egység.
- 3 Ugyanazon betű elemei között egy egység szünet.
- 4 Két betű között három egység szünet.
- 5 Két szó között hét egység szünet.

Bináris reprezentáció

- 1: egységnyi impulzus
- 0: egységnyi szünet

Példa.

SOS : $\underbrace{10101}_{S} 000 \underbrace{11101110111}_{O} 000 \underbrace{10101}_{S}$

Csak számok (Samuel Morse): 1837

American Morse Code (Alfred Vail): 1844

International Morse Code: 1865

Állandó hosszúságú kódok

1. Baudot-Murray kód

ITA2 (International Telegraph Alphabet No 2) szabvány (1924)

26 betű, 10 számjegy, 10 írásjel, vezérlőkarakterek.

5 bites kód, legfeljebb 32 kódszó. Több kódszót is kétszer használ. Váltás vezérlőkarakterekkel (FIGS, LTRS).

Alkalmazás: telex rendszerek, diplomáciai, katonai kommunikáció (1940-80), manapság rádióamatőrök.

2. ASCII kód

American Standard Code for Information Interchange

8 bites kód. Az ITA2-t váltotta 1963-ban.

#	Ltr	Fig	Hex	Bin	
0	NUL	00	000-00		NULL, Nothing (blank tape)
1	E	3	01	000-01	
2	LF	02	000-10		Line Feed (new line)
3	A	-	03	000-11	
4	SP	04	001-00		Space
5	S	*	05	001-01	
6	I	8	06	001-10	
7	U	7	07	001-11	
8	CR	08	010-00		Carriage Return
9	D	ENC	09	010-01	Enquiry (Who are you?, WRU)
10	R	4	0A	010-10	
11	J	BEL	0B	010-11	BELL (ring bell at the other end)
12	N	.	0C	011-00	
13	F	!	0D	011-01	Can also be %
14	C	:	0E	011-10	
15	K	(0F	011-11	
16	T	5	10	100-00	
17	Z	+	11	100-01	
18	L)	12	100-10	
19	W	2	13	100-11	
20	H	\$	14	101-00	Currency symbol — Can also be £
21	Y	6	15	101-01	
22	P	0	16	101-10	
23	Q	1	17	101-11	
24	O	9	18	110-00	
25	B	?	19	110-01	
26	G	&	1A	110-10	Can also be @
27	FIGS	1B	110-11		Figures (Shift on)
28	M	-	1C	111-00	
29	X	/	1D	111-01	
30	V	:	1E	111-10	
31	LTRS	1F	11-111		Letters (Shift off)



Forrás: cryptomuseum.com

Betűnkénti vs. blokk kódolás

Betűnkénti kódolás: egy közlemény kódját az egyes forrásbetűk kódjainak egymás után írásával kapjuk.

Blokk kódolás: a forrásüzenetet k hosszúságú blokkokra bontjuk és a blokkokat kódoljuk.

Példa. Kódoljuk az $\{a, b, c, d, e\}$ forrásábécét állandó hosszúságú bináris kóddal betűnként és $k = 3$ blokk-hosszúságú blokk kóddal.

Betűnkénti kódolás: 5 kódolandó betű; 3 bites kód; $2^3 = 8$ lehetséges kódszó, amiből 3 szabadon marad.

Egy forrásbetűre jutó átlagos kódszóhossz: **3**.

Blokkonkénti kódolás: $5^3 = 125$ kódolandó blokk; 7 bites kód; $2^7 = 128$ lehetséges kódszó, amiből 3 szabadon marad.

Egy forrásbetűre jutó átlagos kódszóhossz: **7/3**.

Cél: az egy forrásbetűre jutó átlagos kódszóhossz minimalizálása. Elérhető például a blokk-hossz növelésével, vagy változó hosszúságú kód használatával.

Természetes elvárás: minél gyakoribb egy betű, annál rövidebb legyen a kódja.

Gyakoriságok

Morse-abc: megszámolták a Morristownban (New Jersey) kiadott helyi újság szedésekor használt betűk gyakoriságát (Alfred Veil).

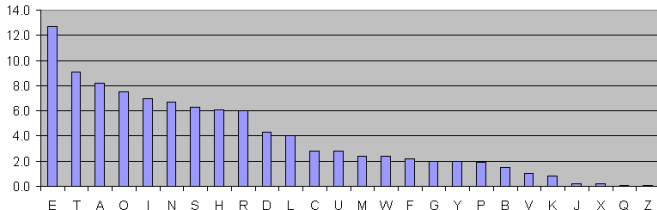
A ● ■
 B ■ ■ ● ●
 C ■ ● ■ ■
 D ■ ● ●
 E ●
 F ● ● ■ ●
 G ■ ■ ■ ●
 H ● ● ● ●
 I ● ●
 J ● ■ ■ ■ ■
 K ■ ● ■ ■
 L ● ■ ■ ●
 M ■ ■ ■
 N ■ ●
 O ■ ■ ■ ■
 P ● ■ ■ ■ ●
 Q ■ ■ ■ ● ■
 R ● ■ ■ ●
 S ● ● ●
 T ■

U ● ● ■ ■
 V ● ● ■ ■ ■
 W ● ■ ■ ■
 X ■ ● ● ■ ■
 Y ■ ● ■ ■ ■
 Z ■ ■ ■ ● ●

1 ● ■ ■ ■ ■ ■
 2 ● ● ■ ■ ■ ■
 3 ● ● ■ ■ ■ ■
 4 ● ■ ■ ■ ■ ■
 5 ● ● ■ ■ ■
 6 ■ ■ ■ ■ ●
 7 ■ ■ ■ ● ● ●
 8 ■ ■ ■ ■ ● ●
 9 ■ ■ ■ ■ ■ ●
 0 ■ ■ ■ ■ ■ ■

Gyak.	Betű	Gyak.	Betű	Gyak.	Betű
12 000	E	4 000	L	1 600	B
9 000	T	3 400	U	1 200	V
8 000	A, I, N, O, S	3 000	C, M	800	K
6 400	H	2 500	F	500	Q
6 200	R	2 000	W, Y	400	J, X
4 400	D	1 700	G, P	200	Z

Relatív gyakoriságok (%) a standard angolban



Jelölések, alapfogalmak

Forrásábécé: $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$, $n \geq 2$, véges halmaz. Elemeit (forrás)betűknek nevezzük. Felfoghatóak úgy, mint egy X diszkrét valószínűségi változó (forrás) lehetséges értékei.

\mathcal{X}^* : az \mathcal{X} elemeiből álló véges sorozatok halmaza. \mathcal{X}^* elemeit üzeneteknek, vagy közleményeknek nevezzük.

Kódábécé: $\mathcal{Y} = \{y_1, y_2, \dots, y_s\}$, $s \geq 2$, véges halmaz. Elemeit kódjeleknek nevezzük.

\mathcal{Y}^* : az \mathcal{Y} elemeiből álló véges sorozatok halmaza. \mathcal{Y}^* elemei a kódszavak.

Kód: egy $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ függvény, illetve annak $\mathcal{K} = f(\mathcal{X}) = \{K_1, K_2, \dots, K_n\}$ értékkészlete, ahol $K_i = f(x_i)$ az x_i kódszava. $s = 2$: bináris kód.

$|f(x)|$: az $x \in \mathcal{X}$ betű $f(x)$ kódjának a kódszóhossza. $\mathcal{L} = \{L_1, L_2, \dots, L_n\}$ jelöli egy f kódhoz tartozó kódszóhosszak halmazát, ahol $L_i = |f(x_i)| = |K_i|$.

Ha az f kód értékkészlete különböző hosszúságú kódszavakból áll, akkor változó hosszúságú kódolásról beszélünk.

Blokk kódolás: a forrásüzenetet k hosszúságú blokkokra bontjuk és a blokkokat kódoljuk. Formálisan egy $f : \mathcal{X}^k \rightarrow \mathcal{Y}^*$ kód, ahol \mathcal{X}^k az új forrásábécé.

Egyértelműen dekódolható kódok

Definíció. Az $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ kód *egyértelműen dekódolható*, ha tetszőleges $\mathbf{u} \in \mathcal{X}^*$, $\mathbf{v} \in \mathcal{X}^*$ üzenetek esetén, ahol $\mathbf{u} = u_1 u_2 \dots u_k$, $\mathbf{v} = v_1 v_2 \dots v_\ell$ és $\mathbf{u} \neq \mathbf{v}$, teljesül, hogy

$$f(u_1)f(u_2)\dots f(u_k) \neq f(v_1)f(v_2)\dots f(v_\ell).$$

Minden véges kódjelsorozat legfeljebb egy közlemény kódolásával állhat elő.

Példák.

1. $\mathcal{X} = \{a, b, c\}$, $\mathcal{Y} = \{0, 1\}$, és $f(a) = 1$, $f(b) = 01$, $f(c) = 10110$.

Az f kódoló függvény invertálható, de a kód **nem** egyértelműen dekódolható.

Például: $f(c)f(a) = 101101 = f(a)f(b)f(a)f(b)$.

2. $\mathcal{X} = \{a, b, c\}$, $\mathcal{Y} = \{0, 1\}$, és $f(a) = 1$, $f(b) = 10$, $f(c) = 100$.

A kód *egyértelműen dekódolható*, mivel az 1 mindig egy új kódszó kezdetét jelzi.

3. $\mathcal{X} = \{a, b, c\}$, $\mathcal{Y} = \{0, 1\}$, és $f(a) = 1$, $f(b) = 00$, $f(c) = 01$.

A kód *egyértelműen dekódolható*.

Prefix kódok

Definíció. Egy kód *prefix*, ha a lehetséges kódszavak mind különbözőek és egyik kódszó sem folytatása a másiknak.

Megjegyzések.

- 1 Minden prefix kód egyértelműen dekódolható.
- 2 Állandó hosszúságú kód mindig prefix, ha a kódszavai különbözőek.

Példák.

1. $\mathcal{X} = \{a, b, c\}$, $\mathcal{Y} = \{0, 1\}$, és $f(a) = 1$, $f(b) = 00$, $f(c) = 01$.

A kód *prefix*.

2. $\mathcal{X} = \{a, b, c\}$, $\mathcal{Y} = \{0, 1\}$, és $f(a) = 1$, $f(b) = 10$, $f(c) = 100$.

A kód **nem** prefix, de egyértelműen dekódolható.

3. $\mathcal{X} = \{a, b, c, d, e, f, g\}$, $\mathcal{Y} = \{0, 1, 2\}$, és
 $f(a) = 0$, $f(b) = 10$, $f(c) = 11$, $f(d) = 20$, $f(e) = 21$, $f(f) = 220$, $f(g) = 221$.

A kód *prefix*.

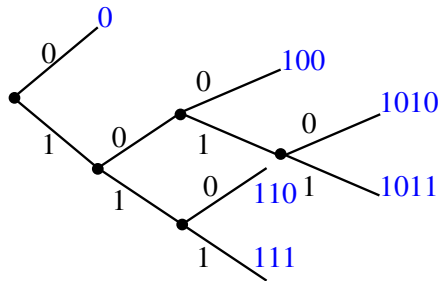
Kódfák

Minden prefix kód ábrázolható egy fagráffal, ahol az egyes kódszavaknak a gyökértől az egyes levelekig tartó töröttvonalak felelnek meg.

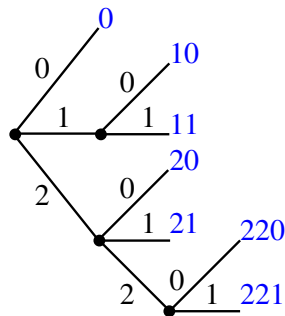
Bináris kód esetén pl. a 0-nak a bináris fa „felfelé” tartó ágai, az 1-nek pedig a „lefelé” mutatók felelnek meg.

Példák. Rajzoljuk fel a megfelelő fagráfokat.

1. $\mathcal{Y} = \{0, 1\}$, $\mathcal{K} = \{0, 100, 1010, 1011, 110, 111\}$.



2. $\mathcal{Y} = \{0, 1, 2\}$, $\mathcal{K} = \{0, 10, 11, 20, 21, 220, 221\}$.



McMillan egyenlőtlenség

Tétel (McMillan). Minden egyértelműen dekódolható $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ kódra

$$\sum_{i=1}^n s^{-|f(x_i)|} \leq 1,$$

ahol s a kódábécé elemszáma.

Indoklás. Csak prefix kódra. Legyen $M := \max_{1 \leq i \leq n} |f(x_i)|$. Egészítsük ki a $\mathcal{K} = f(\mathcal{X})$ kódszavait M hosszúságúra minden lehetséges módon. Mivel a \mathcal{K} kódfájában minden csúcsból s él indulhat ki, egy $|f(x_i)|$ hosszúságú kódszót $s^{M-|f(x_i)|}$ féleképpen egészíthetünk ki. A kiegészítésekkel kapott kódsorozatok száma

$$s^{M-|f(x_1)|} + s^{M-|f(x_2)|} + \dots + s^{M-|f(x_n)|},$$

ami nem lehet több, mint az összes M hosszú kódsorozat s^M száma, azaz

$$s^{M-|f(x_1)|} + s^{M-|f(x_2)|} + \dots + s^{M-|f(x_n)|} \leq s^M.$$

Az egyenlőtlenséget s^M -el osztva kapjuk az állítást. □

Példa. Nem létezik olyan 4 kódszóból álló egyértelműen dekódolható bináris kód, melynek a kódszóhosszai $\{1, 2, 2, 2\}$. Egy ilyen kódra ugyanis $2^{-1} + 3 \cdot 2^{-2} > 1$ teljesül, ami ellentmond a McMillan egyenlőtlenségnek.

Kraft egyenlőtlenség

Tétel (Kraft). Ha az L_1, L_2, \dots, L_n pozitív egész számokra

$$\sum_{i=1}^n s^{-L_i} \leq 1,$$

akkor létezik olyan f prefix kód, melyre

$$|f(x_i)| = L_i, \quad i = 1, 2, \dots, n.$$

Példa. Legyen $s = 2$ és $\mathcal{L} = \{1, 3, 3, 3, 4, 4\}$. Ekkor

$$2^{-1} + 3 \cdot 2^{-3} + 2 \cdot 2^{-4} = 1.$$

Egy lehetséges prefix kód:

$$\mathcal{K} = \{0, 100, 101, 110, 1110, 1111\}.$$

Megjegyzés. A McMillan és Kraft egyenlőtlenségekből következik, hogy minden egyértelműen dekódolható kódhoz létezik vele azonos kódhosszú prefix kód. Így elég, ha egy kódtól a speciálisabb prefix tulajdonságot követeljük meg.

Átlagos kódszóhossz

$\mathcal{X} = \{x_1, x_2, \dots, x_n\}$: forrásábécé; egy X diszkrét forrás lehetséges értékei.

$\mathcal{P} = \{p_1, p_2, \dots, p_n\}$: a forrásábécé betűinek előfordulási valószínűségei; az X diszkrét forrás eloszlása, vagyis $p_i = p(x_i)$, ahol $p(x) := P(X = x)$, $x \in \mathcal{X}$.

$f : \mathcal{X} \rightarrow \mathcal{Y}^*$: a \mathcal{X} forrásábécé egy kódja $\mathcal{K} = \{K_1, K_2, \dots, K_n\}$ kódszavakkal, melyek hosszai rendre $\mathcal{L} = \{L_1, L_2, \dots, L_n\}$, azaz $K_i = f(x_i)$ és $L_i = |f(x_i)| = |K_i|$.

Definíció. Egy $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ kód *átlagos kódszóhossza*

$$E(f) := E(\mathcal{K}) = E|f(\mathcal{X})| = \sum_{i=1}^n p(x_i) |f(x_i)| = \sum_{i=1}^n p_i L_i.$$

Cél: az átlagos kódszóhossz alsó határának meghatározása. Egy s elemű kódábécé esetén keressük azt az f kódot, mely minimalizálja az

$$E(f) = \sum_{i=1}^n p(x_i) |f(x_i)| \quad \text{függvényt a} \quad \sum_{i=1}^n s^{-|f(x_i)|} \leq 1 \quad \text{feltétel mellett.}$$

Az alsó határ függ attól, hogy a forrásábécé **mennyi információt** tartalmaz.

Az információmennyiség mérőszáma I.

Hartley (1928): Az n elemű \mathcal{X} halmaz egyes elemeinek azonosításához

$$I = \log_2 n$$

mennyiségű információra van szükség.

Heurisztika. Ha $n = 2^k$, akkor az \mathcal{X} elemeinek reprezentálásához $k = \log_2 n$ hosszú bináris sorozatokat érdemes használni. Ha $\log_2 n \notin \mathbb{Z}$, akkor a szükséges bináris jegyek száma a $\log_2 n$ utáni első egész. Ha \mathcal{X} elemeiből alkotható m hosszú sorozatokat kell binárisan reprezentálni (ezek száma n^m), akkor olyan k hosszra van szükség, melyre $2^{k-1} < n^m \leq 2^k$. Az \mathcal{X} egy elemére eső bináris jegyek $K = k/m$ számára teljesül, hogy

$$\log_2 n < K \leq \log_2 n + 1/m.$$

A $\log_2 n$ alsó határ így tetszőlegesen megközelíthető.

A formula az információ mennyiségét a megadáshoz szükséges állandó hosszúságú bináris sorozatok hosszának alsó hataraként definiálja. Az információmennyiség egysége: **bit**. Egy kételemű halmaz azonosításához 1 bit információ szükséges.

Probléma: Hartley nem veszi figyelembe, hogy az \mathcal{X} elemei esetleg nem egyforma valószínűek.

Az információmennyiség mérőszáma II.

Shannon (1948): Egy $P(A)$ valószínűségű A esemény bekövetkezése

$$I(A) = \log_2 \frac{1}{P(A)} = -\log_2 P(A)$$

mennyiségű információt szolgáltat.

Heurisztika. Követelmények az $I(A)$ információmennyiséggel kapcsolatban.

- Ha $P(A) \leq P(B)$, akkor $I(A) \geq I(B)$.
Következmény: $I(A)$ csak a $P(A)$ értékétől függ, azaz $I(A) = g(P(A))$.
- Független események együttes bekövetkezése esetén az információ összeadódik, azaz ha $P(A \cdot B) = P(A)P(B)$, akkor $I(A \cdot B) = I(A) + I(B)$. Ez azt jelenti, hogy $g(p \cdot q) = g(p) + g(q)$, $p, q \in]0, 1]$.
- Ha $P(A) = 1/2$, akkor $I(A) := 1$, azaz $g(1/2) = 1$.

Tétel. Ha $g : [0, 1] \rightarrow \mathbb{R}$ egy olyan függvény, melyre

- $g(p) \geq g(q)$, ha $0 < p \leq q \leq 1$;
- $g(p \cdot q) = g(p) + g(q)$, $p, q \in]0, 1]$;
- $g(1/2) = 1$,

akkor

$$g(p) = \log_2 \frac{1}{p}, \quad p \in]0, 1].$$

Példa

Átlagosan mennyi információt tartalmaz egy szabványos (3 betű, 3 számjegy) gépjármű rendszám, ha mind a 26 betű és mind a 10 számjegy egyformán valószínű? Mennyivel csökken ez az információmennyiség, ha az első betű csak az A – S halmazból választható, valamint a Q és a 000 számsorozat nem megengedett?

Megoldás. Egy véletlenszerűen kiválasztott betű információtartalma $\log_2 26$ bit, egy számjegy esetén ugyanez $\log_2 10$ bit. Teljesen véletlen 3 betű 3 számjegy esetén az információtartalom:

$$I_1 = 3(\log_2 26 + \log_2 10) = 24.0671 \text{ bit.}$$

Ha az első betű csak az A – S halmazból választható, valamint a Q nem megengedett, az első betű $\log_2 18$, a másik kettő $\log_2 25$ bit információt tartalmaz, míg az utánuk következő háromjegyű számban $\log_2 999$ bitnyi információ van. Az információtartalom:

$$I_2 = \log_2 18 + 2 \log_2 25 + \log_2 999 = 23.4220 \text{ bit.}$$

Az információmennyiség csökkenése:

$$I_1 - I_2 = 0.6451 \text{ bit.}$$



Entrópia

Definíció. Az $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ értékészletű és $\{p_1, p_2, \dots, p_n\}$ eloszlású X diszkrét valószínűségi változó **entrópiája**

$$H(X) := \sum_{i=1}^n P(X = x_i) \log_2 \left(\frac{1}{p_i} \right) = - \sum_{i=1}^n p_i \log_2 p_i,$$

ahol $0 \log_2 0 := 0$.

Megjegyzések.

- 1 Az entrópia az X értékéhez tartozó **átlagos információmennyiség**.
- 2 Ugyanezzel a formulával definiáljuk a

$$\mathcal{P} := \{p_1, p_2, \dots, p_n\}$$

eloszlású \mathcal{X} forrásábécé $H(\mathcal{X})$ entrópiáját (az egy betűre jutó **átlagos információmennyiséget**), azaz

$$H(\mathcal{X}) := \sum_{i=1}^n p_i \log_2 \left(\frac{1}{p_i} \right) = - \sum_{i=1}^n p_i \log_2 p_i.$$

Entrópia és átlagos kódszóhossz

\mathcal{X} : $\mathcal{P} := \{p(x_1), p(x_2), \dots, p(x_n)\}$ eloszlású forrásábéce.

$f: \mathcal{X} \rightarrow \mathcal{Y}^*$: az \mathcal{X} kódja; kódszavai $\mathcal{K} = \{f(x_1), f(x_2), \dots, f(x_n)\}$.

Entrópia: $H(\mathcal{X}) := -\sum_{i=1}^n p(x_i) \log_2 p(x_i)$. **Átlagos kódszóhossz:** $E(f) := \sum_{i=1}^n p(x_i) |f(x_i)|$.

Példák.

1. $\mathcal{X} = \{a, b, c\}$, $\mathcal{Y} = \{0, 1\}$, és $f(a) = 1$, $f(b) = 00$, $f(c) = 01$.

Valószínűségek: $p(a) = 0.6$, $p(b) = 0.3$, $p(c) = 0.1$.

Rövidebb felírás: $s = 2$, $\mathcal{K} = \{1, 00, 01\}$, $\mathcal{L} = \{1, 2, 2\}$, $\mathcal{P} = \{0.6, 0.3, 0.1\}$.

$$H(\mathcal{X}) = -0.6 \cdot \log_2 0.6 - 0.3 \cdot \log_2 0.3 - 0.1 \cdot \log_2 0.1 \approx 1.2955; \quad E(f) = 0.6 \cdot 1 + 0.3 \cdot 2 + 0.1 \cdot 2 = 1.4.$$

2. $s = 2$, $\mathcal{L} = \{1, 3, 3, 3, 4, 4\}$, $\mathcal{P} = \{\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{16}, \frac{1}{16}\}$.

$$H(\mathcal{X}) = -\frac{1}{2} \cdot \log_2 \frac{1}{2} - 3 \cdot \frac{1}{8} \cdot \log_2 \frac{1}{8} - 2 \cdot \frac{1}{16} \cdot \log_2 \frac{1}{16} = 2.125;$$

$$E(f) = \frac{1}{2} \cdot 1 + 3 \cdot \frac{1}{8} \cdot 3 + 2 \cdot \frac{1}{16} \cdot 4 = 2.125.$$

Az átlagos kódszóhossz határai

Tétel (Shannon). Tetszőleges s elemű kódábécét használó egyértelműen dekódolható $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ kódra

$$E(f) = \sum_{i=1}^n p(x_i) |f(x_i)| \geq - \sum_{i=1}^n p(x_i) \log_s p(x_i) = \frac{H(\mathcal{X})}{\log_2 s},$$

egyenlőség pedig pontosan akkor áll fenn, ha $p(x_i) = s^{-|f(x_i)|}$, $i = 1, 2, \dots, n$.

Ha $p(x_i) = s^{-L_i}$, ahol $L_i \in \mathbb{N}$, akkor létezik olyan f prefix kód, melyre $|f(x_i)| = L_i$, $i = 1, 2, \dots, n$, és

$$E(f) = \frac{H(\mathcal{X})}{\log_2 s}.$$

Tetszőleges eloszlású \mathcal{X} forrásábécé esetén létezik olyan $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ prefix kód, melyre

$$E(f) < \frac{H(\mathcal{X})}{\log_2 s} + 1.$$

Kódok hatásfoka

Shannon tétel: tetszőleges egyértelműen dekódolható $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ kódra $E(f) \geq \frac{H(\mathcal{X})}{\log_2 s}$.

Definíció. Az \mathcal{X} forrásábécé $f : \mathcal{X} \rightarrow \mathcal{Y}^*$ kódjának *hatásfoka*

$$\text{Eff}(f) := \frac{H(\mathcal{X})}{E(f) \log_2 s} (\times 100 \%).$$

Megjegyzések.

- 1 Ha az f kód egyértelműen dekódolható, akkor $\text{Eff}(f) \in]0, 1]$.
- 2 Egy kód hatásfoka pontosan akkor 1 (100 %), ha a forrásábécé elemeinek valószínűségei $p(x_i) = s^{-|f(x_i)|}$, $i = 1, 2, \dots, n$.

Tétel. Tetszőleges forrásábécé esetén létezik *maximális hatásfokú* egyértelműen dekódolható kód, amit *optimális kódnak* nevezünk.

Példák

1. $s = 2$, $\mathcal{X} = \{a, b, c\}$, $\mathcal{K} = f(\mathcal{X}) = \{1, 00, 01\}$, $\mathcal{L} = \{1, 2, 2\}$, $\mathcal{P} = \{0.6, 0.3, 0.1\}$.

$$H(\mathcal{X}) = 1.2955, \quad E(f) = 1.4 \implies \text{Eff}(f) = \frac{1.2955}{1.4 \cdot 1} = 0.9253 \text{ (92.53 \%)}.$$

Optimális kód.

2. $s = 2$, $\mathcal{X} = \{a, b, c\}$, $\mathcal{K} = f(\mathcal{X}) = \{00, 1, 01\}$, $\mathcal{L} = \{2, 1, 2\}$, $\mathcal{P} = \{0.6, 0.3, 0.1\}$.

$$H(\mathcal{X}) = 1.2955, \quad E(f) = 0.6 \cdot 2 + 0.3 \cdot 1 + 0.1 \cdot 2 = 1.7 \implies \text{Eff}(f) = \frac{1.2955}{1.7 \cdot 1} = 0.7620 \text{ (76.20 \%)}.$$

3. $s = 2$, $\mathcal{X} = \{a, b, c\}$, $\mathcal{K} = f(\mathcal{X}) = \{00, 01, 1\}$, $\mathcal{L} = \{2, 2, 1\}$, $\mathcal{P} = \{0.6, 0.3, 0.1\}$.

$$H(\mathcal{X}) = 1.2955, \quad E(f) = 0.6 \cdot 2 + 0.3 \cdot 2 + 0.1 \cdot 1 = 1.9 \implies \text{Eff}(f) = \frac{1.2955}{1.9 \cdot 1} = 0.6818 \text{ (68.18 \%)}.$$

4. $s = 2$, $\mathcal{L} = \{1, 3, 3, 3, 4, 4\}$, $\mathcal{P} = \{\frac{1}{2}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{16}, \frac{1}{16}\}$.

$$H(\mathcal{X}) = 2.125, \quad E(f) = 2.125 \implies \text{Eff}(f) = 1 \text{ (100 \%)}.$$

Optimális kód.

Optimális kódok jellemzői

Bináris eset: $s = 2$.

Tétel. Ha az $f : \mathcal{X} \rightarrow \{0, 1\}^*$ prefix kód optimális, és \mathcal{X} elemei úgy vannak indexelve, hogy $p(x_1) \geq p(x_2) \geq \dots \geq p(x_n) > 0$, akkor feltehető, hogy az f kódra teljesül az alábbi három tulajdonság.

- a) $|f(x_1)| \leq |f(x_2)| \leq \dots \leq |f(x_n)|$, azaz nagyobb valószínűségekhez rövidebb kódszavak tartoznak.
- b) $|f(x_{n-1})| = |f(x_n)|$, vagyis a két legkisebb valószínűségű forrásbetűhöz tartozó kódszó azonos hosszúságú.
- c) Az $f(x_{n-1})$ és az $f(x_n)$ kódszavak csak az utolsó bitjükben különböznek.

Heurisztika. a) Ha $p(x_k) > p(x_j)$ és $|f(x_k)| > |f(x_j)|$, akkor x_j és x_k kódszavát felcserélve egy az eredeténél rövidebb átlagos kódszóhosszú kódot kapunk. Az eredeti így nem lehet optimális.

b) Ha $|f(x_{n-1})| < |f(x_n)|$, akkor $f(x_n)$ utolsó bitjét levágva egy az eredeténél rövidebb átlagos kódszóhosszú, ugyancsak prefix kódot kapunk. Az eredeti így nem lehet optimális.

c) Ha létezik olyan $f(x_i)$ kódszó, hogy $f(x_i)$ és $f(x_n)$ csak az utolsó bitben különböznek, akkor a korábbiak alapján $|f(x_i)| = |f(x_{n-1})| = |f(x_n)|$. Ha $i \neq n-1$, akkor cseréljük fel x_i és x_{n-1} kódját. □

Bináris Huffman-kód

Tétel. Tegyük fel, hogy az $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ forrásábécé elemei úgy vannak indexelve, hogy $p(x_1) \geq p(x_2) \geq \dots \geq p(x_n) > 0$, és tekintsük azt az $\tilde{\mathcal{X}} = \{x_1, x_2, \dots, x_{n-2}, \tilde{x}_{n-1}\}$ forrásábécét, ahol az \tilde{x}_{n-1} szimbólumot az x_{n-1} és x_n forrásbetűk összevonásával kapjuk és $p(\tilde{x}_{n-1}) = p(x_{n-1}) + p(x_n)$.

Ha az új $\{p(x_1), p(x_2), \dots, p(x_{n-2}), p(x_{n-1}) + p(x_n)\}$ eloszláshoz ismerünk egy g optimális bináris prefix kódot, akkor az eredeti $\{p(x_1), p(x_2), \dots, p(x_n)\}$ eloszlás egy optimális f prefix kódját kapjuk, ha a $g(\tilde{x}_{n-1})$ kódszót kiegészítjük egy nullával és egy egyessel, a többi kódszót pedig változatlanul hagyjuk.

A fenti algoritmus alapján kapott kódot **bináris Huffman-kód**nak nevezzük.

Példa. Határozza meg

$$\mathcal{P} = \{0.07, 0.02, 0.49, 0.14, 0.01, 0.14, 0.07, 0.04, 0.02\}$$

eloszlású $\mathcal{X} = \{a, b, c, d, e, f, g, h, i\}$ forrásábécé bináris Huffman-kódját és adja meg a kód hatásfokát.

Megoldás

Rendezzük át a forrásábécét, hogy a valószínűségek csökkenő sorrendben legyenek.

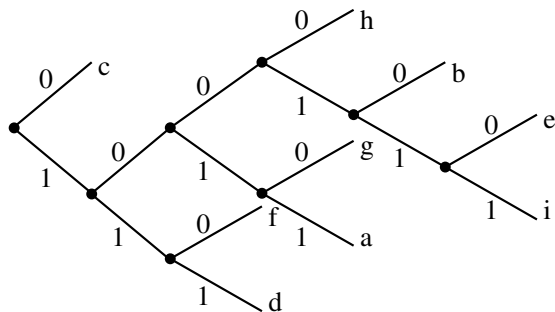
\mathcal{X}	\mathcal{P}	$\mathcal{X}^{(1)}$	$\mathcal{P}^{(1)}$	$\mathcal{X}^{(2)}$	$\mathcal{P}^{(2)}$	$\mathcal{X}^{(3)}$	$\mathcal{P}^{(3)}$	$\mathcal{X}^{(4)}$	$\mathcal{P}^{(4)}$	$\mathcal{X}^{(5)}$	$\mathcal{P}^{(5)}$	$\mathcal{X}^{(6)}$	$\mathcal{P}^{(6)}$	$\mathcal{X}^{(7)}$	$\mathcal{P}^{(7)}$
c	0.49	c	0.49	c	0.49	c	0.49	c	0.49	c	0.49	c	0.49	c	0.49
d	0.14	d	0.14	d	0.14	d	0.14	d	0.14	d	0.14	df	0.28	dfag	0.51
f	0.14	f	0.14	f	0.14	f	0.14	f	0.14	f	0.14	agh	0.23	hbie	
a	0.07	a	0.07	a	0.07	a	0.07	ag	0.14	agh	0.23	bie			
g	0.07	g	0.07	g	0.07	g	0.07	hbie	0.09	bie					
h	0.04	h	0.04	h	0.04	hbie	0.09								
b	0.02	b	0.02	bie	0.05										
i	0.02	ie	0.03												
e	0.01														

\mathcal{X}	\mathcal{K}	$\mathcal{X}^{(1)}$	$\mathcal{K}^{(1)}$	$\mathcal{X}^{(2)}$	$\mathcal{K}^{(2)}$	$\mathcal{X}^{(3)}$	$\mathcal{K}^{(3)}$	$\mathcal{X}^{(4)}$	$\mathcal{K}^{(4)}$	$\mathcal{X}^{(5)}$	$\mathcal{K}^{(5)}$	$\mathcal{X}^{(6)}$	$\mathcal{K}^{(6)}$	$\mathcal{X}^{(7)}$	$\mathcal{K}^{(7)}$
c	0	c	0	c	0	c	0	c	0	c	0	c	0	c	0
d	111	d	111	d	111	d	111	d	111	d	111	df	11	dfag	1
f	110	f	110	f	110	f	110	f	110	f	110	agh	10	hbie	
a	1011	a	1011	a	1011	a	1011	ag	101	agh	10	bie			
g	1010	g	1010	g	1010	g	1010	hbie	100	bie					
h	1000	h	1000	h	1000	hbie	100								
b	10010	b	10010	bie	1001										
i	100111	ie	10011												
e	100110														

Megoldás

\mathcal{X}	\mathcal{K}	$\mathcal{K}^{(1)}$	$\mathcal{K}^{(2)}$	$\mathcal{K}^{(3)}$	$\mathcal{K}^{(4)}$	$\mathcal{K}^{(5)}$	$\mathcal{K}^{(6)}$	$\mathcal{K}^{(7)}$
c	0	0	0	0	0	0	0	0
d	111	111	111	111	111	111	11	1
f	110	110	110	110	110	110	10	
a	1011	1011	1011	1011	101	10		
g	1010	1010	1010	1010	100			
h	1000	1000	1000	100				
b	10010	10010	1001					
i	100111	10011						
e	100110							

- Minden egyes összevonás eggyel csökkenti a forrásábécé elemszámát.
- Az egyes lépések egy növekvő kódfat eredményeznek.
- Minden lépésben két új ág nő ki egy adott csúcsból, így egy **teljes** fát kapunk.



Megoldás

Forrásábécé: $\mathcal{X} = \{a, b, c, d, e, f, g, h, i\}$

A forrásábécé eloszlása: $\mathcal{P} = \{0.07, 0.02, 0.49, 0.14, 0.01, 0.14, 0.07, 0.04, 0.02\}$

A forrásábécé Huffman-kódja: $\mathcal{K} = \{1011, 10010, 0, 111, 100110, 110, 1010, 1000, 100111\}$

Kódszóhosszak: $\mathcal{L} = \{4, 5, 1, 3, 6, 3, 4, 4, 6\}$

Entrópia: $H(\mathcal{X}) = -0.07 \cdot \log_2 0.07 - 0.02 \cdot \log_2 0.02 - \dots - 0.02 \cdot \log_2 0.02 = 2.3136$

Átlagos kódszóhossz: $E(\mathcal{K}) = 0.07 \cdot 4 + 0.02 \cdot 5 + 0.49 \cdot 1 + \dots + 0.02 \cdot 6 = 2.33$

A Huffman-kód hatásfoka:

$$\text{Eff}(\mathcal{K}) = \frac{2.3136}{2.33 \cdot 1} = 0.9929 \quad (99.29 \%)$$

□

Huffman-kód általános kódábécére

Bináris eset: minden egyes összevonás eggyel csökkenti a forrásábécé elemszámát. Teljes kódfát eredményez, ahol minden elágazási pontból pontosan két ág indul ki.

Általános kódábécé ($s > 2$): s darab forrásbetű összevonása $s - 1$ elemmel kisebb új forrásábécét eredményez. A kapott kód pontosan akkor lesz optimális, ha s -nél kevesebb forrásbetűt kizárólag a legelső lépésben vonunk össze.

Az optimális kód nem feltétlenül eredményez teljes kódfát, ahol minden elágazási pontból pontosan s ág indul ki.

Speciális eset: $s = 3$ (trináris kód)

- Ha $n = 2k + 1$ (páratlan), akkor minden lépésben 3 forrásbetűt kell összevonni. Teljes kódfát eredményez.
- Ha $n = 2k$ (páros), akkor az első lépésben 2, minden további lépésben 3 forrásbetűt kell összevonni. Nem eredményez teljes kódfát.

Példa

Határozza meg

$$\mathcal{P} = \{0.07, 0.02, 0.49, 0.14, 0.01, 0.14, 0.07, 0.04, 0.02\}$$

eloszlású $\mathcal{X} = \{a, b, c, d, e, f, g, h, i\}$ forrásábécé trináris Huffman-kódját és adja meg a kód hatásfokát.

Megoldás. Rendezzük át a forrásábécét, hogy a valószínűségek csökkenő sorrendben legyenek.

\mathcal{X}	\mathcal{P}	$\mathcal{X}^{(1)}$	$\mathcal{P}^{(1)}$	$\mathcal{X}^{(2)}$	$\mathcal{P}^{(2)}$	$\mathcal{X}^{(3)}$	$\mathcal{P}^{(3)}$	\mathcal{X}	\mathcal{K}	$\mathcal{X}^{(1)}$	$\mathcal{K}^{(1)}$	$\mathcal{X}^{(2)}$	$\mathcal{K}^{(2)}$	$\mathcal{X}^{(3)}$	$\mathcal{K}^{(3)}$
c	0.49	c	0.49	c	0.49	c	0.49	c	2	c	2	c	2	c	2
d	0.14	d	0.14	d	0.14	dfa	0.35	d	12	d	12	d	12	dfa	1
f	0.14	f	0.14	f	0.14	ghb	0.16	f	11	f	11	f	11	ghb	0
a	0.07	a	0.07	a	0.07	ie		a	10	a	10	a	10	ie	
g	0.07	g	0.07	ghb	0.16			g	02	g	02	ghb	0		
h	0.04	h	0.04	ie				h	00	h	00	ie			
b	0.02	bie	0.05					b	012	bie	01				
i	0.02							i	011						
e	0.01							e	010						

Trináris Huffman-kód: $\mathcal{K} = \{10, 012, 2, 12, 010, 11, 02, 00, 011\}$

Átlagos kódszóhossz: $E(\mathcal{K}) = 0.07 \cdot 2 + 0.02 \cdot 3 + 0.49 \cdot 1 + \dots + 0.02 \cdot 3 = 1.56$

A trináris Huffman-kód hatásfoka:

$$\text{Eff}(\mathcal{K}) = \frac{H(\mathcal{X})}{E(\mathcal{K}) \cdot \log_2 s} = \frac{2.3136}{1.56 \cdot \log_2 3} = 0.9357 \quad (93.57\%)$$



Példa

Egy nyolcelemű forrásábécé betűinek eloszlása

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}.$$

- 1 Határozza meg a forrásábécé bináris Huffman-kódját, rajzolja fel a megfelelő kódfát és adja meg a kód hatásfokát.
- 2 Határozza meg a forrásábécé trináris Huffman-kódját, rajzolja fel a megfelelő kódfát és adja meg a kód hatásfokát.

Megoldás. Rendezzük át a forrásábécét, hogy a valószínűségek csökkenő sorrendben legyenek.

1. Bináris kód: $s = 2$.

\mathcal{P}	$\mathcal{P}^{(1)}$	$\mathcal{P}^{(2)}$	$\mathcal{P}^{(3)}$	$\mathcal{P}^{(4)}$	$\mathcal{P}^{(5)}$	$\mathcal{P}^{(6)}$		\mathcal{K}_2	$\mathcal{K}_2^{(1)}$	$\mathcal{K}_2^{(2)}$	$\mathcal{K}_2^{(3)}$	$\mathcal{K}_2^{(4)}$	$\mathcal{K}_2^{(5)}$	$\mathcal{K}_2^{(6)}$
0.15	0.15	0.15	0.15	0.15	0.43	0.43		00	00	00	00	00	0	0
0.15	0.15	0.15	0.15	0.29	0.29	0.57		111	111	111	111	11	11	1
0.14	0.14	0.14	0.14	0.28	0.28			110	110	110	110	10	10	
0.14	0.14	0.14	0.28	0.28				101	101	101	10	01		
0.14	0.14	0.14	0.28					100	100	100	01			
0.14	0.14	0.28						011	011	01				
0.09	0.14							010	010					
0.05								0100						

Megoldás

Eloszlás:

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$$

Bináris Huffman-kód:

$$\mathcal{K}_2 = \{110, 101, 00, 0101, 100, 0100, 011, 111\}$$

Kódszóhosszak:

$$\mathcal{L}_2 = \{3, 3, 2, 4, 3, 4, 3, 3\}$$

Entrópia:

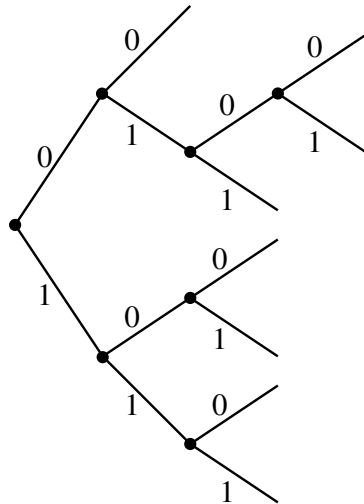
$$H(\mathcal{X}) = -2 \cdot 0.15 \cdot \log_2 0.15 - \dots - 0.04 \cdot \log_2 0.04 = 2.9383$$

Átlagos kódszóhossz:

$$E(\mathcal{K}_2) = 0.15 \cdot (2 + 3) + 4 \cdot 0.14 \cdot 3 + (0.09 + 0.05) \cdot 4 = 2.99$$

A bináris Huffman-kód hatásfoka:

$$\text{Eff}(\mathcal{K}_2) = \frac{2.9383}{2.99 \cdot 1} = 0.9827 \quad (98.27\%)$$



Megoldás

2. Trináris kód: $s = 3$.

\mathcal{P}	$\mathcal{P}^{(1)}$	$\mathcal{P}^{(2)}$	$\mathcal{P}^{(3)}$	\mathcal{K}_3	$\mathcal{K}_3^{(2)}$	$\mathcal{K}_3^{(2)}$	$\mathcal{K}_3^{(3)}$
0.15	0.15	0.15	0.15	0	0	0	0
0.15	0.15	0.15	0.43	22	22	22	2
0.14	0.14	0.14	0.42	21	21	21	1
0.14	0.14	0.14		20	20	20	
0.14	0.14	0.42		12	12	1	
0.14	0.14			11	11		
0.09	0.14			102	10		
0.05				101			

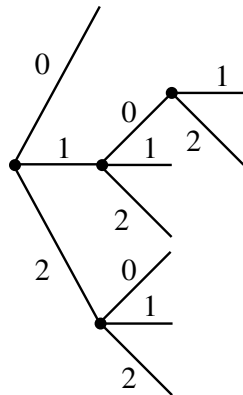
Eloszlás: $\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$

Trináris Huffman-kód: $\mathcal{K}_3 = \{21, 20, 0, 102, 12, 101, 11, 22\}$

Kódszóhosszak: $\mathcal{L}_3 = \{2, 2, 1, 3, 2, 3, 2, 2\}$

Entrópia: $H(\mathcal{X}) = 2.9383$

Átlagos kódszóhossz: $E(\mathcal{K}_3) = 1.99$



A trináris Huffman-kód hatásfoka:

$$\text{Eff}(\mathcal{K}_3) = \frac{2.9383}{1.99 \cdot \log_2 3} = 0.9316 \text{ (93.16 \%)}$$

□

Shannon-Fano-kód

Huffman-kód: optimális prefix kód. **Probléma:** minden lépésnél szükség van egy rendezésre.

Lehetséges megoldás: **Shannon-Fano-kód.** Tegyük fel, hogy az $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ forrás-ábécé elemei úgy vannak indexelve, hogy $p(x_1) \geq p(x_2) \geq \dots \geq p(x_n) > 0$. Legyen

$$L_i := \lceil -\log_s p(x_i) \rceil, \quad \text{ahol} \quad \lceil a \rceil := \min\{n \in \mathbb{Z}, n \geq a\},$$

s pedig a kódábécé elemszáma, és

$$w_1 := 0, \quad w_i := \sum_{\ell=1}^{i-1} p(x_\ell), \quad i = 2, 3, \dots, n.$$

Az x_i forrásbetű $f(x_i)$ kódja legyen $\lfloor s^{L_i} w_i \rfloor$ s -adikus (s alapú számrendszerbeli) alakja L_i hosszon ábrázolva, ahol $\lfloor a \rfloor := \max\{n \in \mathbb{Z}, n \leq a\}$.

Tétel. A Shannon-Fano-kód prefix és az átlagos kódszóhosszára teljesül

$$\frac{H(\mathcal{X})}{\log_2 s} \leq E(f) < \frac{H(\mathcal{X})}{\log_2 s} + 1.$$

Példa

Határozza meg

$$\mathcal{P} = \{0.07, 0.02, 0.49, 0.14, 0.01, 0.14, 0.07, 0.04, 0.02\}$$

eloszlású $\mathcal{X} = \{a, b, c, d, e, f, g, h, i\}$ forrásábécé bináris Shannon-Fano-kódját és adja meg a kód hatásfokát.

Megoldás. Rendezzük át a forrásábécét, hogy a valószínűségek csökkenő sorrendben legyenek. $s = 2$ eset.

x_i	$p(x_i)$	$L_i := \lceil -\log_2 p(x_i) \rceil$	w_i	$\lfloor 2^{L_i} w_i \rfloor$	$K_i = f(x_i)$
c	0.49	$\lceil 1.0291 \rceil = 2$	0	$\lfloor 0 \rfloor = 0$	00
d	0.14	$\lceil 2.8365 \rceil = 3$	0.49	$\lfloor 3.92 \rfloor = 3$	011
f	0.14	$\lceil 2.8365 \rceil = 3$	0.63	$\lfloor 5.04 \rfloor = 5$	101
a	0.07	$\lceil 3.8365 \rceil = 4$	0.77	$\lfloor 12.32 \rfloor = 12$	1100
g	0.07	$\lceil 3.8365 \rceil = 4$	0.84	$\lfloor 13.44 \rfloor = 13$	1101
h	0.04	$\lceil 4.6439 \rceil = 5$	0.91	$\lfloor 29.12 \rfloor = 29$	11101
b	0.02	$\lceil 5.6439 \rceil = 6$	0.95	$\lfloor 60.80 \rfloor = 60$	111100
i	0.02	$\lceil 5.6439 \rceil = 6$	0.97	$\lfloor 62.08 \rfloor = 62$	111110
e	0.01	$\lceil 6.6439 \rceil = 7$	0.99	$\lfloor 126.72 \rfloor = 126$	1111110

Entrópia:

$$H(\mathcal{X}) = 2.3136$$

Átlagos kódszóhossz:

$$E(\mathcal{K}) = 0.49 \cdot 2 + \dots + 0.01 \cdot 7 = 2.89$$

Bináris Shannon-Fano-kód: $\mathcal{K} = \{1100, 111100, 00, 011, 1111110, 101, 1101, 11101, 111110\}$

A bináris Shannon-Fano-kód hatásfoka:

$$\text{Eff}(\mathcal{K}) = \frac{H(\mathcal{X})}{E(\mathcal{K}) \cdot \log_2 s} = \frac{2.3136}{2.89 \cdot 1} = 0.8005 \quad (80.05 \%)$$

□

Példa

Határozza meg

$$\mathcal{P} = \{0.07, 0.02, 0.49, 0.14, 0.01, 0.14, 0.07, 0.04, 0.02\}$$

eloszlású $\mathcal{X} = \{a, b, c, d, e, f, g, h, i\}$ forrásábécé trináris Shannon-Fano-kódját és adja meg a kód hatásfokát.

Megoldás. Rendezzük át a forrásábécét, hogy a valószínűségek csökkenő sorrendben legyenek. $s = 3$ eset.

x_i	$p(x_i)$	$L_i := \lceil -\log_3 p(x_i) \rceil$	w_i	$\lfloor 3^{L_i} w_i \rfloor$	$K_i = f(x_i)$
c	0.49	$\lceil 0.6493 \rceil = 1$	0	$\lfloor 0 \rfloor = 0$	0
d	0.14	$\lceil 1.7896 \rceil = 2$	0.49	$\lfloor 4.41 \rfloor = 4$	11
f	0.14	$\lceil 1.7896 \rceil = 2$	0.63	$\lfloor 5.67 \rfloor = 5$	12
a	0.07	$\lceil 2.4206 \rceil = 3$	0.77	$\lfloor 20.79 \rfloor = 20$	202
g	0.07	$\lceil 2.4206 \rceil = 3$	0.84	$\lfloor 22.68 \rfloor = 22$	211
h	0.04	$\lceil 2.9299 \rceil = 3$	0.91	$\lfloor 24.57 \rfloor = 24$	220
b	0.02	$\lceil 3.5609 \rceil = 4$	0.95	$\lfloor 76.95 \rfloor = 76$	2211
i	0.02	$\lceil 3.5609 \rceil = 4$	0.97	$\lfloor 78.57 \rfloor = 78$	2220
e	0.01	$\lceil 4.1918 \rceil = 5$	0.99	$\lfloor 240.57 \rfloor = 240$	22220

Entrópia:

$$H(\mathcal{X}) = 2.3136$$

Átlagos kódszóhossz:

$$E(\mathcal{K}) = 0.49 \cdot 1 + \dots + 0.01 \cdot 5 = 1.8$$

Trináris Shannon-Fano-kód: $\mathcal{K} = \{202, 2211, 0, 11, 22220, 12, 211, 220, 2220\}$

A trináris Shannon-Fano-kód hatásfoka:

$$\text{Eff}(\mathcal{K}) = \frac{H(\mathcal{X})}{E(\mathcal{K}) \cdot \log_2 s} = \frac{2.3136}{1.8 \cdot \log_2 3} = 0.8109 \quad (81.09\%)$$



Példa

Egy nyolcelemű forrásábécé betűinek eloszlása

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}.$$

- ❶ Határozza meg a forrásábécé bináris Shannon-Fano-kódját, rajzolja fel a megfelelő kódfát és adja meg a kód hatásfokát.
- ❷ Határozza meg a forrásábécé trináris Shannon-Fano-kódját, rajzolja fel a megfelelő kódfát és adja meg a kód hatásfokát.

Megoldás. Rendezzük át a forrásábécét, hogy a valószínűségek csökkenő sorrendben legyenek.

1. Bináris kód: $s = 2$, $L_i := \lceil -\log_2 p(x_i) \rceil$.

2. Trináris kód: $s = 3$, $L_i := \lceil -\log_3 p(x_i) \rceil$.

$p(x_i)$	L_i	w_i	$\lfloor 2^{L_i} w_i \rfloor$	K_i
0.15	3	0	0	000
0.15	3	0.15	1	001
0.14	3	0.30	2	010
0.14	3	0.44	3	011
0.14	3	0.58	4	100
0.14	3	0.72	5	101
0.09	4	0.86	13	1101
0.05	5	0.95	30	11110

$p(x_i)$	L_i	w_i	$\lfloor 3^{L_i} w_i \rfloor$	K_i
0.15	2	0	0	00
0.15	2	0.15	1	01
0.14	2	0.30	2	02
0.14	2	0.44	3	10
0.14	2	0.58	5	12
0.14	2	0.72	6	20
0.09	3	0.86	23	212
0.05	3	0.95	25	221

Megoldás

1. Bináris kód: $s = 2$.

Eloszlás:

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$$

Bináris Shannon-Fano-kód:

$$\mathcal{K}_2 = \{010, 011, 000, 1101, 100, 11110, 101, 001\}$$

Kódszóhosszak:

$$\mathcal{L}_2 = \{3, 3, 3, 4, 3, 5, 3, 3\}$$

Entropia:

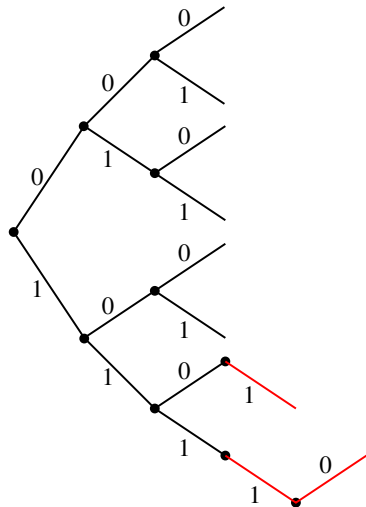
$$H(\mathcal{X}) = 2.9383$$

Átlagos kódszóhossz:

$$E(K_2) = (2 \cdot 0.15 + 4 \cdot 0.14) \cdot 3 + 0.09 \cdot 4 + 0.05 \cdot 5 = 3.19$$

A bináris Shannon-Fano-kód hatásfoka:

$$\text{Eff}(\mathcal{K}_2) = \frac{2.9383}{3.19 \cdot 1} = 0.9211 \quad (92.11 \%)$$



Megoldás

2. Trináris kód: $s = 3$.

Eloszlás:

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$$

Trináris Shannon-Fano-kód:

$$\mathcal{K}_3 = \{02, 10, 00, 212, 12, 221, 20, 01\}$$

Kódszóhosszak:

$$\mathcal{L}_3 = \{2, 2, 2, 3, 2, 3, 2, 2\}$$

Entrópia:

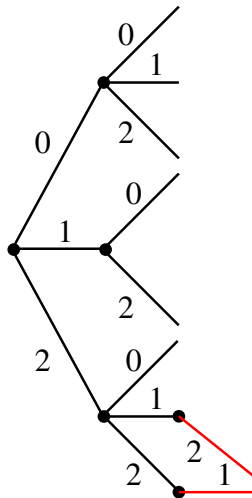
$$H(\mathcal{X}) = 2.9383$$

Átlagos kódszóhossz:

$$E(\mathcal{K}_3) = (2 \cdot 0.15 + 4 \cdot 0.14) \cdot 2 + (0.09 + 0.05) \cdot 3 = 2.14$$

A trináris Shannon-Fano-kód hatásfoka:

$$\text{Eff}(\mathcal{K}_2) = \frac{2.9383}{2.14 \cdot \log_2 3} = 0.8663 \quad (86.63 \%)$$



Gilbert-kód

Shannon-Fano-kód: az első lépésnél még mindig szükség van egy rendezésre. n forrásbetű esetén ez n^2 nagyságrendű művelet, míg a kódolás maga n nagyságrendű.

Lehetséges megoldás: **Gilbert-kód.** $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$: az adott forrásábécé. Legyen

$$L_i := \lceil -\log_s p(x_i) \rceil + 1, \quad \text{ahol} \quad \lceil a \rceil := \min\{n \in \mathbb{Z}, n \geq a\},$$

s pedig a kódábécé elemszáma, és

$$w_1 := \frac{1}{s}p(x_1), \quad w_i := \frac{1}{s}p(x_i) + \sum_{\ell=1}^{i-1} p(x_\ell), \quad i = 2, 3, \dots, n.$$

Az x_i forrásbetű $f(x_i)$ kódja legyen $\lfloor s^{L_i} w_i \rfloor$ s -adikus (s alapú számrendszerbeli) alakja L_i hosszon ábrázolva, ahol $\lfloor a \rfloor := \max\{n \in \mathbb{Z}, n \leq a\}$.

Tétel. *A Gilbert-kód prefix és az átlagos kódszóhosszára teljesül*

$$\frac{H(\mathcal{X})}{\log_2 s} + 1 \leq E(f) < \frac{H(\mathcal{X})}{\log_2 s} + 2.$$

Példa

Határozza meg

$$\mathcal{P} = \{0.07, 0.02, 0.49, 0.14, 0.01, 0.14, 0.07, 0.04, 0.02\}$$

eloszlású $\mathcal{X} = \{a, b, c, d, e, f, g, h, i\}$ forrásábécé bináris Gilbert-kódját és adja meg a kód hatásfokát.

Megoldás. $s = 2$ eset.

x_i	$p(x_i)$	L_i	w_i	$\lfloor 2^{L_i} w_i \rfloor$	$K_i = f(x_i)$
a	0.07	5	0.035	1	00001
b	0.02	7	0.080	10	0001010
c	0.49	3	0.335	2	010
d	0.14	4	0.650	10	1010
e	0.01	8	0.725	185	10111001
f	0.14	4	0.800	12	1100
g	0.07	5	0.905	28	11100
h	0.04	6	0.960	61	111101
i	0.02	7	0.990	126	1111110

Kódszóhosszak: $L_i := \lceil -\log_2 p(x_i) \rceil + 1$

Súlyok: $w_1 = \frac{1}{2}p(x_1)$, $w_i = \frac{1}{2}p(x_i) + \sum_{\ell=1}^{i-1} p(x_\ell)$

Entrópia: $H(\mathcal{X}) = 2.3136$

Átlagos kódszóhossz: $E(\mathcal{K}) = 3.89$

Bináris Gilbert-kód: $\mathcal{K} = \{00001, 0001010, 010, 1010, 10111001, 1100, 11100, 111101, 111110\}$

A bináris Gilbert-kód hatásfoka:

$$\text{Eff}(\mathcal{K}) = \frac{H(\mathcal{X})}{E(\mathcal{K}) \cdot \log_2 s} = \frac{2.3136}{3.89 \cdot 1} = 0.5947 \quad (59.47 \%)$$



Példa

Határozza meg

$$\mathcal{P} = \{0.07, 0.02, 0.49, 0.14, 0.01, 0.14, 0.07, 0.04, 0.02\}$$

eloszlású $\mathcal{X} = \{a, b, c, d, e, f, g, h, i\}$ forrásábécé trináris Gilbert-kódját és adja meg a kód hatásfokát.

Megoldás. $s = 3$ eset.

x_i	$p(x_i)$	L_i	w_i	$\lfloor 3^{L_i} w_i \rfloor$	$K_i = f(x_i)$
a	0.07	4	0.02(3)	1	0001
b	0.02	5	0.07(6)	18	00200
c	0.49	2	0.25(3)	2	02
d	0.14	3	0.62(6)	16	121
e	0.01	6	0.73(3)	527	201112
f	0.14	3	0.77(6)	20	202
g	0.07	4	0.89(3)	72	2200
h	0.04	4	0.95(3)	77	2212
i	0.02	5	0.98(6)	239	22212

Kódszóhosszak: $L_i := \lceil -\log_3 p(x_i) \rceil + 1$

Súlyok: $w_1 = \frac{1}{3}p(x_1)$, $w_i = \frac{1}{3}p(x_i) + \sum_{\ell=1}^{i-1} p(x_\ell)$

Entrópia: $H(\mathcal{X}) = 2.3136$

Átlagos kódszóhossz: $E(\mathcal{K}) = 2.8$

Trináris Gilbert-kód: $\mathcal{K} = \{0001, 00200, 02, 121, 201112, 202, 2200, 2212, 22212\}$

A trináris Gilbert-kód hatásfoka:

$$\text{Eff}(\mathcal{K}) = \frac{H(\mathcal{X})}{E(\mathcal{K}) \cdot \log_2 s} = \frac{2.3136}{2.8 \cdot \log_2 3} = 0.5213 \quad (52.13\%)$$



A kódok összehasonlítása

Forrásábécé \mathcal{X}	Eloszlás \mathcal{P}	Bináris kódok			Trináris kódok		
		Huffman	Shannon-Fano	Gilbert	Huffman	Shannon-Fano	Gilbert
a	0.07	1011	1100	00001	10	202	0001
b	0.02	10010	111100	0001010	012	2211	00200
c	0.49	0	00	010	2	0	02
d	0.14	111	011	1010	12	11	121
e	0.01	100110	1111110	10111001	010	22220	201112
f	0.14	110	101	1100	11	12	202
g	0.07	1010	1101	11100	02	211	2200
h	0.04	1000	11101	111101	00	220	2212
i	0.02	100111	111110	1111110	011	2220	22212
Átlagos kódszóhossz		2.33	2.89	3.89	1.56	1.80	2.80
Hatásfok		99.29 %	80.05 %	59.47 %	93.57 %	81.09 %	52.13 %

A forrásábécé entrópiája: $H(\mathcal{X}) = 2.3136$

Példa

Egy nyolcelemű forrásábécé betűinek eloszlása

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}.$$

1. Határozza meg a forrásábécé bináris Gilbert-kódját, rajzolja fel a megfelelő kódfát és adja meg a kód hatásfokát.
2. Határozza meg a forrásábécé trináris Gilbert-kódját, rajzolja fel a megfelelő kódfát és adja meg a kód hatásfokát.

Megoldás.

1. Bináris kód: $s = 2$, $L_i := \lceil -\log_2 p(x_i) \rceil + 1$.

$p(x_i)$	L_i	w_i	$2^{L_i} w_i$	K_i
0.14	4	0.070	1	0001
0.14	4	0.210	3	0011
0.15	4	0.355	5	0101
0.09	5	0.475	15	01111
0.14	4	0.590	9	1001
0.05	6	0.685	43	101011
0.14	4	0.780	12	1100
0.15	4	0.925	14	1110

2. Trináris kód: $s = 3$, $L_i := \lceil -\log_3 p(x_i) \rceil + 1$.

$p(x_i)$	L_i	w_i	$3^{L_i} w_i$	K_i
0.14	3	0.04(6)	1	001
0.14	3	0.18(6)	5	012
0.15	3	0.330	8	022
0.09	4	0.460	37	1101
0.14	3	0.56(6)	15	120
0.05	4	0.67(6)	54	2000
0.14	3	0.75(6)	20	202
0.15	3	0.900	24	220

Megoldás

1. Bináris kód: $s = 2$.

Eloszlás:

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$$

Bináris Gilbert-kód:

$$\mathcal{K}_2 = \{0001, 0011, 0101, 01111, 1001, 101011, 1100, 1110\}$$

Kódszóhosszak:

$$\mathcal{L}_2 = \{4, 4, 4, 5, 4, 6, 4, 4\}$$

Entrópia:

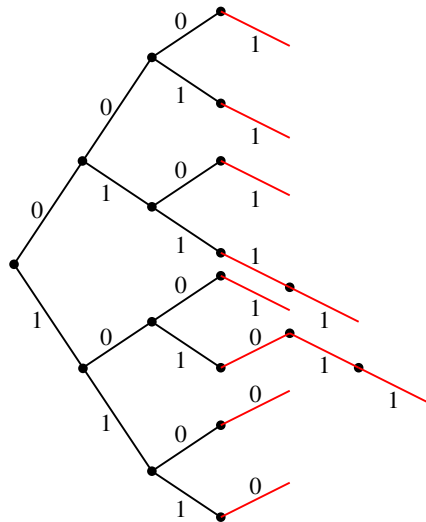
$$H(\mathcal{X}) = 2.9383$$

Átlagos kódszóhossz:

$$E(\mathcal{K}_2) = (2 \cdot 0.15 + 4 \cdot 0.14) \cdot 4 + 0.09 \cdot 5 + 0.05 \cdot 6 = 4.19$$

A bináris Gilbert-kód hatásfoka:

$$\text{Eff}(\mathcal{K}_2) = \frac{2.9383}{4.19 \cdot 1} = 0.7013 \quad (70.13 \%)$$



Megoldás

2. Trináris kód: $s = 3$.

Eloszlás:

$$\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$$

Trináris Gilbert-kód:

$$\mathcal{K}_3 = \{001, 012, 022, 1101, 120, 2000, 202, 220\}$$

Kódszóhosszak:

$$\mathcal{L}_3 = \{3, 3, 3, 4, 3, 4, 3, 3\}$$

Entrópia:

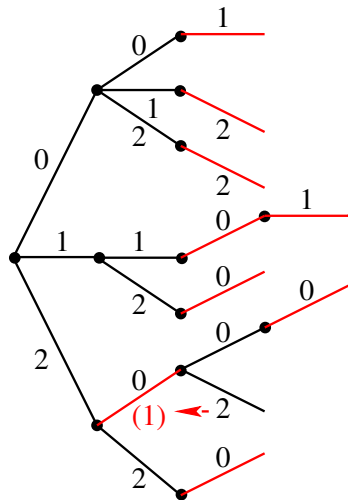
$$H(\mathcal{X}) = 2.9383$$

Átlagos kódszóhossz:

$$E(\mathcal{K}_3) = (2 \cdot 0.15 + 4 \cdot 0.14) \cdot 3 + (0.09 + 0.05) \cdot 4 = 3.14$$

A trináris Gilbert-kód hatásfoka:

$$\text{Eff}(\mathcal{K}_2) = \frac{2.9383}{3.14 \cdot \log_2 3} = 0.5904 \quad (59.04 \%)$$

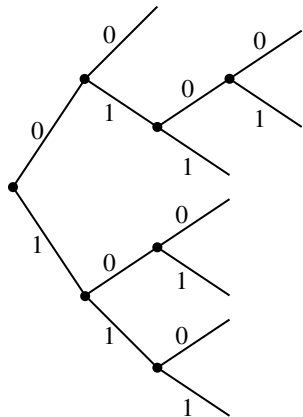


Bináris kódok összehasonlítása

Eloszlás: $\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$.

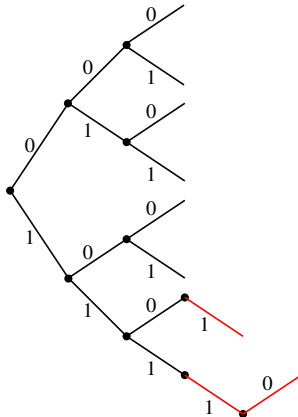
Entrópia: 2.9383

Huffman-kód



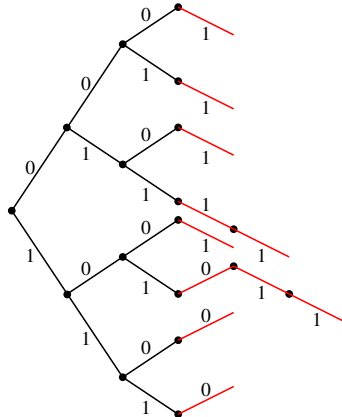
Átlagos kódszóhossz: 2.99
Hatásfok: 98.27 %

Shannon-Fano-kód



Átlagos kódszóhossz: 3.19
Hatásfok: 92.11 %

Gilbert-kód



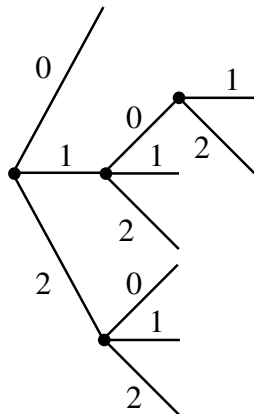
Átlagos kódszóhossz: 4.19
Hatásfok: 70.13 %

Trináris kódok összehasonlítása

Eloszlás: $\mathcal{P} = \{0.14, 0.14, 0.15, 0.09, 0.14, 0.05, 0.14, 0.15\}$.

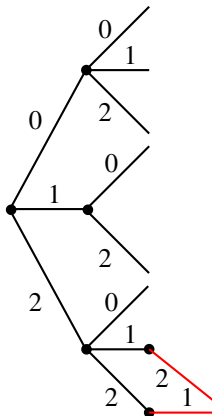
Entrópia: 2.9383

Huffman-kód



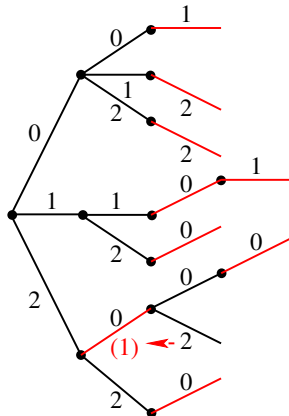
Átlagos kódszóhossz: 1.99
Hatásfok: 93.16 %

Shannon-Fano-kód



Átlagos kódszóhossz: 2.14
Hatásfok: 86.67 %

Gilbert-kód



Átlagos kódszóhossz: 3.14
Hatásfok: 59.04 %

Univerzális forráskódolás

Adatátvitel költségei az eddig vizsgált (blokk)kódoknál:

- Állandó költség: pl. a forrásszimbólumok gyakoriságai.
- Változó költség: az üzenet kódszavai.

Elméletileg végtelen hosszú forrásokat vizsgálunk. Az állandó költség ekkor fajlagosan nullához tart.

A gyakorlatban a források véges hosszúságúak. Az állandó költség esetleg magasabb lehet, mint az üzenet kódszavainak összhossza.

Adaptív kód: az aktuális forrásszimbólumot az azt megelőző szimbólumok alapján kódoljuk.

Példák:

- Adaptív Huffman-kód;
- Lempel-Ziv algoritmusok (LZ77, LZ78, LZW).

Az LZ77 algoritmus

Abraham Lempel és Jakov Ziv (1977)

A forrásszimbólumokon egy h_a hosszúságú csúszóablakot mozgatunk.

A csúszóablak részei:

- keresőpuffer: a legutóbb kódolt h_k darab forrásszimbólumot tartalmazza;
- előretekintő puffer: a következő h_e darab kódolandó szimbólumot tartalmazza.

Példa. Forrásszöveg

... cabracadabrarrarrad ...

Csúszóablak: $h_a := 13$, $h_k := 7$, $h_e := 6$.

c a b r a c a	d a b r a r
---------------	-------------

r a r r a d

Az LZ77 algoritmus

Kódolás:

- 1 Egy hátrafelé mutató mutatóval a kódoló megkeresi a keresőpufferben az előretekintő puffer első szimbólumával megegyező szimbólumokat.
- 2 Megvizsgálja, a kapott pozíciókkal kezdődően a keresőpufferben lévő szimbólumok milyen hosszan egyeznek meg az előretekintő puffer szimbólumaival.
- 3 A talált szimbólumok közül kiválasztja azt, ahol a leghosszabb az egyezés.
- 4 Átküldi a $\langle t, h, c \rangle$ hármast.

t : a keresőpufferben megtalált szimbólum távolsága az előretekintő puffertől. Ha nincs találat a keresőpufferben, $t = 0$.

h : a kereső- és az előretekintő puffer egyező szimbólumainak legnagyobb hosszúsága. Ha nincs találat a keresőpufferben, $h = 0$.

c : az első, az előretekintő pufferben levő nem egyező karakter kódszáva.

Példa

Csúszóablak: $h_a := 13$, $h_k := 7$, $h_e := 6$.

c a b r a c a	d a b r a r
---------------	-------------

 r a r r a d

d nincs a keresőpufferben. Átküldendő: $\langle 0, 0, f(d) \rangle$.

c

a b r a c a d	a b r a r r
---------------	-------------

 a r r a d

a a keresőpufferben: $t = 2$, $h = 1$; $t = 4$, $h = 1$ és $t = 7$, $h = 4$.

Leghosszabb egyezés: $t = 7$, $h = 4$. Átküldendő: $\langle 7, 4, f(r) \rangle$.

c a b r a c

a d a b r a r	r a r r a d
---------------	-------------

r a keresőpufferben: $t = 1$, $h = 1$ és $t = 3$, $h = 5$.

Leghosszabb egyezés: $t = 3$, $h = 5$. Átküldendő: $\langle 3, 5, f(d) \rangle$.

Jellemzők

A $\langle t, h, c \rangle$ kódolásához állandó kódhosszú kód esetén

$$\lceil \log_2 h_k \rceil + \lceil \log_2 h_e \rceil + \lceil \log_2 n \rceil$$

bit szükséges, ahol n a forrásábécé mérete.

Az eljárás hatékonysága aszimptotikusan ($h_k, h_e \rightarrow \infty$) tart az optimális algoritmuséhoz, amihez viszont kell a forrás eloszlása is.

Hatékonyságot növelő módosítások, például

- Változó hosszúságú kódok $\langle t, h, c \rangle$ tömörítéséhez. Pl. adaptív Huffman kódolás.
- Duál formátum: $\langle t, h \rangle$ vagy $\langle c \rangle$ továbbítódik. Jelzőbittel azonosítja a formátumokat.
LZSS – Lempel-Ziv-Storer-Szymanski
- Változtatható méretű pufferek.

Alkalmazások: pkzip, arj

Az LZ78 algoritmus

A kódoló és a dekódoló szótárt épít az előzőleg előfordult sorozatokból.

- 1 A kódoló megkeresi a forrásszimbólumok aktuális pozíciójától kezdődő leghosszabb egyezést a szótárban.
- 2 Átküldi az $\langle i, c \rangle$ párt.
 i : az egyező karaktersorozat szótárbeli indexe;
 c : az első nem egyező karakter kódja.
Ha nem talál egyezést a szótárban, a $\langle 0, c \rangle$ párt küldi át.
- 3 A szótárba felveszi az i indexű karaktersorozat és a c konkatenációjával kapott string-et. Van **eof** szimbólum is.

Probléma: a szótár folyamatosan, korlát nélkül növekszik.

Megoldás: egy idő után fix szótár használata, vagy a ritkán használt, illetve felesleges bejegyzések eltávolítása.

Kódolandó szöveg:

dabbacdabbacdabbacdabbacdeecdeecdee

Szótár		A kódoló kimenete	Szótár		A kódoló kimenete
index	bejegyzés		index	bejegyzés	
1	<i>d</i>	$\langle 0, f(d) \rangle$	10	<i>bac</i>	$\langle 4, f(c) \rangle$
2	<i>a</i>	$\langle 0, f(a) \rangle$	11	<i>dabb</i>	$\langle 9, f(b) \rangle$
3	<i>b</i>	$\langle 0, f(b) \rangle$	12	<i>acd</i>	$\langle 8, f(d) \rangle$
4	<i>ba</i>	$\langle 3, f(a) \rangle$	13	<i>e</i>	$\langle 0, f(e) \rangle$
5	<i>c</i>	$\langle 0, f(c) \rangle$	14	<i>ec</i>	$\langle 13, f(c) \rangle$
6	<i>da</i>	$\langle 1, f(a) \rangle$	15	<i>de</i>	$\langle 1, f(e) \rangle$
7	<i>bb</i>	$\langle 3, f(b) \rangle$	16	<i>ecd</i>	$\langle 14, f(d) \rangle$
8	<i>ac</i>	$\langle 2, f(c) \rangle$	17	<i>ee</i>	$\langle 13, f(e) \rangle$
9	<i>dab</i>	$\langle 6, f(b) \rangle$			

Az LZW algoritmus

Az LZ78 továbbfejlesztése. Terry Welch (1984)

Az LZ78 $\langle i, c \rangle$ párjából csak az i indexet kell átküldeni. A szótárban szerepelnie kell a teljes forrásábécének.

- 1 A kódoló az aktuális pozíciótól addig olvassa be a forrásszimbólumokat egy p pufferbe, míg a beolvasott sorozat szerepel a szótárban.
Legyen c az első karakter, amelyre pc nincs a szótárban.
- 2 Átküldi a p sorozat indexét.
- 3 Felveszi a szótárba a pc sorozatot és a c karaktertől folytatja az eljárást.

Alkalmazások: a Unix rendszer `compress` parancsa, a GIF formátum.

Adaptív szótárméret. Compress esetén 512 bejegyzés, ha megtelik 1024, stb. A felső határ beállítható, maximum 2^{16} bejegyzésig.

Példa

Kódolandó szöveg:

dabbacdabbacdabbacdabbacdeecdeecdee

Szótár		A kódoló kimenete	Szótár		A kódoló kimenete
index	bejegyzés		index	bejegyzés	
1	<i>a</i>		14	<i>acd</i>	10
2	<i>b</i>		15	<i>dabb</i>	12
3	<i>c</i>		16	<i>bac</i>	9
4	<i>d</i>		17	<i>cda</i>	11
5	<i>e</i>		18	<i>abb</i>	7
6	<i>da</i>	4	19	<i>bacd</i>	16
7	<i>ab</i>	1	20	<i>de</i>	4
8	<i>bb</i>	2	21	<i>ee</i>	5
9	<i>ba</i>	2	22	<i>ec</i>	5
10	<i>ac</i>	1	23	<i>cde</i>	11
11	<i>cd</i>	3	24	<i>eec</i>	21
12	<i>dab</i>	6	25	<i>cdee</i>	23
13	<i>bba</i>	8			5

Példa

Kódoljuk az

abbabbabbbaababa

szöveget

- ❶ LZ77 algoritmussal $h_k = 7$, $h_e = 6$ paraméterekkel;
- ❷ LZ78 algoritmussal;
- ❸ LZW algoritmussal.

Megoldás.

1. LZ77 algoritmus

Ablakok	t	h	A kódoló kimenete
a b b a b b a b b b a a b a b a	0	0	$\langle 0, 0, f(a) \rangle$
a b b a b b a b b b a a b a b a	0	0	$\langle 0, 0, f(b) \rangle$
a b b a b b a b b b a a b a b a	1	1	$\langle 1, 1, f(a) \rangle$
a b b a b b a b b b a a b a b a	3	5	$\langle 3, 5, f(b) \rangle$
a b b a b b a b b b a a b a b a	4	1	$\langle 4, 1, f(a) \rangle$
a b b a b b a b b b a a b a b a	7	3	$\langle 7, 3, f(a) \rangle$

Megoldás

Kódolandó szöveg: *abbabbabbbaababa*

2. LZ78 algoritmus

Szótár		A kódoló kimenete
index	bejegyzés	
1	<i>a</i>	$\langle 0, f(a) \rangle$
2	<i>b</i>	$\langle 0, f(b) \rangle$
3	<i>ba</i>	$\langle 2, f(a) \rangle$
4	<i>bb</i>	$\langle 2, f(b) \rangle$
5	<i>ab</i>	$\langle 1, f(b) \rangle$
6	<i>bba</i>	$\langle 4, f(a) \rangle$
7	<i>aba</i>	$\langle 5, f(a) \rangle$
		$\langle 3, \text{eof} \rangle$

3. LZW algoritmus

Szótár		A kódoló kimenete
index	bejegyzés	
1	<i>a</i>	
2	<i>b</i>	
3	<i>ab</i>	1
4	<i>bb</i>	2
5	<i>ba</i>	2
6	<i>abb</i>	3
7	<i>bab</i>	5
8	<i>bbb</i>	4
9	<i>baa</i>	5
10	<i>aba</i>	3
		10



Feladat. Kódolja mindhárom algoritmussal az alábbi szövegeket:

- a) „bed spreaders spread spreads on beds”. A **space** és az **eof** külön karakter.
- b) „az ipafai papnak fapipaja van a papi fapipa” A **space** és az **eof** külön karakter.

Az entrópia

Definíció. Az $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ értékkészletű X valószínűségi változó (Shannon) entrópiája

$$H(X) := - \sum_{i=1}^n p(x_i) \log_2 p(x_i),$$

ahol $p(x_i) = P(X = x_i)$, $i = 1, 2, \dots, n$, és $0 \log_2 0 := 0$.

Megjegyzés. Amint az korábban szerepelt, \mathcal{X} felfogható úgy is, mint egy forrásábécé. Ennek $H(\mathcal{X})$ entrópiája az egy forrásbetűre jutó átlagos információmennyiség.

Az entrópia definíciója ugyanígy néz ki, ha $\mathbf{X} = (X_1, X_2, \dots, X_r)^\top$ egy véletlen vektor aminek értékkészlete $\mathcal{X} = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n\}$:

$$H(\mathbf{X}) := - \sum_{i=1}^n p(\mathbf{x}_i) \log_2 p(\mathbf{x}_i).$$

Az entrópia tulajdonságai

Tétel

- a) *Az entrópia csak az eloszlástól függ, azaz ha X és Y eloszlása megegyezik, akkor $H(X) = H(Y)$.*
- b) *Ha az X valószínűségi változó n különböző értéket $(\{x_1, x_2, \dots, x_n\})$ vehet fel pozitív valószínűséggel, akkor*

$$0 \leq H(X) \leq \log_2 n.$$

A bal oldalon egyenlőség pontosan akkor áll fenn, ha X egy valószínűséggel konstans, a jobb oldalon pedig pontosan akkor, ha X eloszlása egyenletes, azaz

$$p(x_i) = P(X = x_i) = \frac{1}{n}, \quad i = 1, 2, \dots, n.$$

- c) $H(X, X) = H(X)$.

Az entrópia tulajdonságai

- d) Az X és Y véges értékészletű diszkrét valószínűségi változókra

$$H(X, Y) \leq H(X) + H(Y),$$

az egyenlőség pedig pontosan akkor teljesül, ha X és Y független.

Általánosan: az X_1, X_2, \dots, X_k véges értékészletű diszkrét valószínűségi változókra

$$H(X_1, X_2, \dots, X_k) \leq H(X_1) + H(X_2) + \dots + H(X_k),$$

egyenlőség pedig pontosan akkor teljesül, ha X_1, X_2, \dots, X_k teljesen függetlenek.

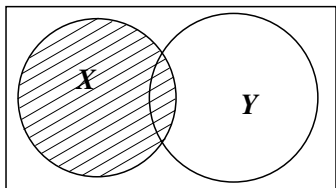
- e) Az X tetszőleges $g(X)$ függvényére

$$H(g(X)) \leq H(X),$$

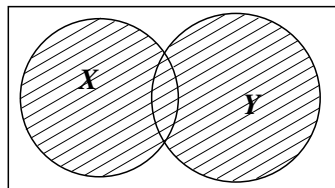
az egyenlőség szükséges és elégséges feltétele pedig a g invertálhatósága.

Grafikus reprezentáció

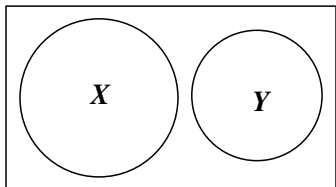
A valószínűségi változókat halmazok reprezentálják.



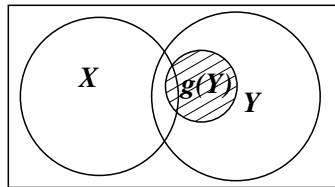
$H(X)$: az X halmaz területe.



$H(X, Y)$: az $X \cup Y$ halmaz területe.



X és Y független: diszjunkt halmazok.



$g(Y)$: az Y részhalmaza

Példa

Feldobunk egy szabályos dobókockát. Ha az eredmény páros, akkor egy, ha páratlan, akkor két szabályos érmét dobunk fel utána. Legyen X a kockadobás eredménye, nevezetesen $X = 1$ ha a kocka páros, és $X = -1$, ha páratlan számot mutat, Y pedig jelentse a dobott fejek számát (0, 1 vagy 2).

- 1 Határozzuk meg az X és Y entrópiáját, valamint az (X, Y) együttes entrópiáját.
- 2 Határozzuk meg az X^2 és Y^2 entrópiáját.
- 3 Határozzuk meg az X^3 és Y^3 entrópiáját.

Megoldás. Az X és Y együttes eloszlása:

$$\begin{aligned} P(Y=0, X=-1) &= \frac{1}{8}, & P(Y=1, X=-1) &= \frac{1}{4}, & P(Y=2, X=-1) &= \frac{1}{8}, \\ P(Y=0, X=1) &= \frac{1}{4}, & P(Y=1, X=1) &= \frac{1}{4}, & P(Y=2, X=1) &= 0. \end{aligned}$$

Peremeloszlások:

$$P(X=-1) = P(X=1) = \frac{1}{2} \quad \text{és} \quad P(Y=0) = \frac{3}{8}, \quad P(Y=1) = \frac{4}{8}, \quad P(Y=2) = \frac{1}{8}.$$

Megoldás

Az X és Y együttes eloszlása és peremeloszlásai (kontingencia tábla):

$X \backslash Y$	0	1	2	Σ
-1	$1/8$	$1/4$	$1/8$	$1/2$
1	$1/4$	$1/4$	0	$1/2$
Σ	$3/8$	$4/8$	$1/8$	1

1. Az X és Y entrópiája:

$$H(X) = \frac{1}{2} \log_2 2 + \frac{1}{2} \log_2 2 = 1, \quad H(Y) = \frac{3}{8} \log_2 \frac{8}{3} + \frac{1}{2} \log_2 2 + \frac{1}{8} \log_2 8 = 2 - \frac{3}{8} \log_2 3 = 1.4056.$$

Az (X, Y) entrópiája:

$$H(X, Y) = 2 \cdot \frac{1}{8} \log_2 8 + 3 \cdot \frac{1}{4} \log_2 4 + 0 = \frac{9}{4} = 2.25 < 2.4056 = H(X) + H(Y).$$

2. $P(X^2 = 1) = 1$, így $H(X^2) = 0$.

Az Y^2 eloszlása: $P(Y^2 = 0) = \frac{3}{8}$, $P(Y^2 = 1) = \frac{4}{8}$, $P(Y^2 = 4) = \frac{1}{8}$. Így $H(Y^2) = H(Y) = 2 - \frac{3}{8} \log_2 3$.

3. Mivel X^3 eloszlása megegyezik X eloszlásával, valamint Y^3 eloszlása megegyezik Y eloszlásával, $H(X^3) = H(X)$ és $H(Y^3) = H(Y)$.

□

Feltételes entrópia

X : diszkrét valószínűségi változó. Értékek: $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$. Eloszlás: $p_i := P(X = x_i)$.

Y : diszkrét valószínűségi változó. Értékek: $\mathcal{Y} = \{y_1, y_2, \dots, y_m\}$. Eloszlás: $q_j := P(Y = y_j)$.

Az (X, Y) **együttes eloszlása**: $p_{ij} := P(X = x_i, Y = y_j)$, $i = 1, 2, \dots, n$, $j = 1, 2, \dots, m$.

Feltételes eloszlások:

$$p_{i|j} := P(X = x_i | Y = y_j) = \frac{p_{ij}}{q_j}; \quad q_{j|i} := P(Y = y_j | X = x_i) = \frac{p_{ij}}{p_i}.$$

Definíció. Az X -nek az $\{Y = y_j\}$ ($j = 1, 2, \dots, m$) feltétellel vett **feltételes entrópiája**

$$H(X|Y = y_j) := \sum_{i=1}^n p_{i|j} \log_2 \left(\frac{1}{p_{i|j}} \right) = - \sum_{i=1}^n p_{i|j} \log_2 p_{i|j}.$$

Az X -nek az Y -ra vonatkozó **feltételes entrópiája**

$$H(X|Y) := \sum_{j=1}^m P(Y = y_j) H(X|Y = y_j) = - \sum_{j=1}^m \sum_{i=1}^n q_j p_{i|j} \log_2 p_{i|j} = - \sum_{j=1}^m \sum_{i=1}^n p_{ij} \log_2 p_{i|j}.$$

A feltételes entrópia tulajdonságai

Tétel. Legyenek X , Y , Z véges értékészletű valószínűségi változók. Ekkor

a)

$$H(X, Y) = H(Y) + H(X|Y) = H(X) + H(Y|X).$$

b)

$$0 \leq H(X|Y) \leq H(X).$$

A bal oldalon egyenlőség pontosan akkor áll fenn, ha X egy valószínűséggel az Y függvénye, a jobb oldalon pedig pontosan akkor, ha X és Y független.

c)

$$H(X|Z, Y) \leq H(X|Z),$$

egyenlőség pedig akkor és csak akkor áll fenn, ha

$$P(X = x \mid Z = z, Y = y) = P(X = x \mid Z = z)$$

minden olyan x, y, z -re, amelyre $P(X = x, Y = y, Z = z) > 0$.

A feltételes entrópia tulajdonságai

- d) Az Y valószínűségi változó minden f függvényére

$$H(X|Y) \leq H(X|f(Y)),$$

egyenlőség pedig pontosan akkor áll fenn, ha minden rögzített z -re

$$P(X = x | Y = y) = P(X = x | f(Y) = z)$$

minden olyan x -re és y -ra, amelyre $f(y) = z$ és $P(Y = y) > 0$.

- e) Az X_1, X_2, \dots, X_k valószínűségi változók együttes entrópiájára

$$\begin{aligned} H(X_1, X_2, \dots, X_k) &= H(X_1) + H(X_2|X_1) + H(X_3|X_2, X_1) + \dots \\ &\quad \dots + H(X_k|X_{k-1}, \dots, X_1). \end{aligned}$$

Példa

Feldobunk egy szabályos dobókockát. Ha az eredmény páros, akkor egy, ha páratlan, akkor két szabályos érmét dobunk fel utána. Legyen X a kockadobás eredménye, nevezetesen $X = 1$ ha a kocka páros, és $X = -1$, ha páratlan számot mutat, Y pedig jelentse a dobott fejek számát (0, 1 vagy 2). Határozzuk meg a $H(Y|X)$ és $H(X|Y)$ feltételes entrópiákat

- 1 a definíció alapján;
- 2 az X és Y entrópiája, valamint az (X, Y) együttes entrópiája segítségével.

Megoldás. Az X és Y együttes eloszlása és peremeloszlásai:

$X \backslash Y$	0	1	2	Σ
-1	1/8	1/4	1/8	1/2
1	1/4	1/4	0	1/2
Σ	3/8	4/8	1/8	1

1. Az Y feltételes eloszlása az X értékeire:

$$\begin{aligned} P(Y = 0|X = -1) &= \frac{1}{4}, & P(Y = 1|X = -1) &= \frac{1}{2}, & P(Y = 2|X = -1) &= \frac{1}{4}, \\ P(Y = 0|X = 1) &= \frac{1}{2}, & P(Y = 1|X = 1) &= \frac{1}{2}, & P(Y = 2|X = 1) &= 0. \end{aligned}$$

Megoldás

Feltételes entrópiák:

$$H(Y|X = -1) = 2 \cdot \frac{1}{4} \log_2 4 + \frac{1}{2} \log_2 2 = \frac{3}{2}, \quad H(Y|X = 1) = 2 \cdot \frac{1}{2} \log_2 2 = 1;$$

$$H(Y|X) = H(Y|X = -1) \cdot P(X = -1) + H(Y|X = 1) \cdot P(X = 1) = \frac{3}{2} \cdot \frac{1}{2} + 1 \cdot \frac{1}{2} = \frac{5}{4}.$$

Az X feltételes eloszlása az Y értékeire:

$$\begin{aligned} P(X = -1|Y = 0) &= \frac{1}{3}, & P(X = -1|Y = 1) &= \frac{1}{2}, & P(X = -1|Y = 2) &= 1, \\ P(X = 1|Y = 0) &= \frac{2}{3}, & P(X = 1|Y = 1) &= \frac{1}{2}, & P(X = 1|Y = 2) &= 0. \end{aligned}$$

Feltételes entrópiák:

$$H(X|Y = 0) = \frac{1}{3} \log_2 3 + \frac{2}{3} \log_2 \frac{3}{2} = \log_2 3 - \frac{2}{3}, \quad H(X|Y = 1) = 2 \cdot \frac{1}{2} \log_2 2 = 1, \quad H(X|Y = 2) = 0;$$

$$\begin{aligned} H(X|Y) &= H(X|Y = 0) \cdot P(Y = 0) + H(X|Y = 1) \cdot P(Y = 1) + H(X|Y = 2) \cdot P(Y = 2) \\ &= \left[\log_2 3 - \frac{2}{3} \right] \cdot \frac{3}{8} + 1 \cdot \frac{1}{2} + 0 \cdot \frac{1}{8} = \frac{3}{8} \log_2 3 + \frac{1}{4} = 0.8844. \end{aligned}$$

2. Összefüggés az entrópia és feltételes entrópia között: $H(X, Y) = H(Y) + H(X|Y) = H(X) + H(Y|X)$.

Korábban kiszámolt értékek:

$$H(X) = 1, \quad H(Y) = 2 - \frac{3}{8} \log_2 3, \quad H(X, Y) = \frac{9}{4}.$$

Feltételes entrópiák:

$$H(Y|X) = H(X, Y) - H(X) = \frac{9}{4} - 1 = \frac{5}{4},$$
$$H(X|Y) = H(X, Y) - H(Y) = \frac{9}{4} - 2 + \frac{3}{8} \log_2 3 = \frac{1}{4} + \frac{3}{8} \log_2 3.$$

□

Kölcsönös információ

Definíció. Az X és Y diszkrét valószínűségi változók *kölcsönös információján* az

$$I(X; Y) := H(X) + H(Y) - H(X, Y)$$

mennyiséget értjük.

Megjegyzés. A kölcsönös információ szimmetrikus, és

$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y; X).$$

Megjegyzés. Legyen $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ és $\mathcal{Y} = \{y_1, y_2, \dots, y_m\}$ az X , illetve Y értékkészlete.

$$\begin{aligned} I(X; Y) &= \sum_{i=1}^n \sum_{j=1}^m P(X = x_i, Y = y_j) \log_2 \frac{P(X = x_i, Y = y_j)}{P(X = x_i)P(Y = y_j)} = \sum_{i=1}^n \sum_{j=1}^m p_{ij} \log_2 \frac{p_{ij}}{p_i q_j} \\ &= \sum_{i=1}^n \sum_{j=1}^m p_{ij} \log_2 \frac{p_{i|j}}{p_i} = \sum_{i=1}^n \sum_{j=1}^m p_{ij} \log_2 \frac{q_{j|i}}{q_j}. \end{aligned}$$

A kölcsönös információ tulajdonságai

Tétel. Legyenek X és Y diszkrét valószínűségi változók.

- a) $I(X; Y) \geq 0$ és $I(X; Y)$ pontosan akkor 0, ha X és Y független.
- b) $I(X; X) = H(X)$.
- c) $I(X; Y) \leq H(X)$ és $I(X, Y) \leq H(Y)$.
- d) Az X és Y bármely g és h függvényére

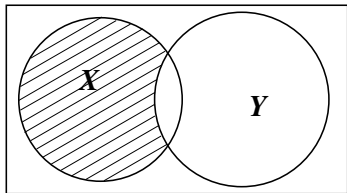
$$I(X; Y) \geq I(g(X); h(Y)).$$

e) A következő három állítás ekvivalens:

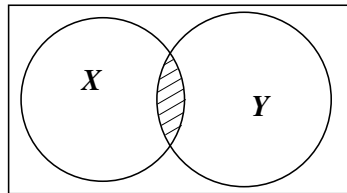
- i) $I(X; Y) = H(X)$;
- ii) $H(X|Y) = 0$;
- iii) létezik olyan $g : \mathbb{R} \rightarrow \mathbb{R}$, hogy $P(X = g(Y)) = 1$.

Grafikus reprezentáció

- A valószínűségi változókat halmazok reprezentálják. $H(X)$ az X területe.
- Független valószínűségi változóknak diszjunkt halmazok felelnek meg.
- Tetszőleges g függvényre $g(X)$ az X részhalmazaként jelenik meg.



$H(X|Y)$: az $X \setminus Y$ halmaz területe.



$I(X; Y)$: az $X \cap Y$ halmaz területe.

Példa

Feldobunk egy szabályos dobókockát. Ha az eredmény páros, akkor egy, ha páratlan, akkor két szabályos érmét dobunk fel utána. Legyen X a kockadobás eredménye, nevezetesen $X = 1$ ha a kocka páros, és $X = -1$, ha páratlan számot mutat, Y pedig jelentse a dobott fejek számát (0, 1 vagy 2). Határozzuk meg az X és Y kölcsönös információját

- 1 a definíció alapján;
- 2 a feltételes entrópiák segítségével.

Megoldás. Korábban kiszámolt értékek:

$$H(X) = 1, \quad H(Y) = 2 - \frac{3}{8} \log_2 3, \quad H(X, Y) = \frac{9}{4}; \quad H(Y|X) = \frac{5}{4}, \quad H(X|Y) = \frac{1}{4} + \frac{3}{8} \log_2 3.$$

1. Definíció alapján:

$$I(X; Y) := H(X) + H(Y) - H(X, Y) = 1 + 2 - \frac{3}{8} \log_2 3 - \frac{9}{4} = \frac{3}{4} - \frac{3}{8} \log_2 3 = 0.1556.$$

2. A feltételes entrópiák segítségével:

$$I(X; Y) = H(X) - H(X|Y) = 1 - \frac{1}{4} - \frac{3}{8} \log_2 3 = \frac{3}{4} - \frac{3}{8} \log_2 3;$$

$$I(X; Y) = H(Y) - H(Y|X) = 2 - \frac{3}{8} \log_2 3 - \frac{5}{4} = \frac{3}{4} - \frac{3}{8} \log_2 3.$$



Az X és Y véletlen változók együttes eloszlása:

$$\begin{aligned} P(X=1, Y=-1) &= \frac{1}{2}, & P(X=1, Y=0) &= \frac{1}{4}, & P(X=1, Y=1) &= \frac{1}{8} \\ P(X=2, Y=-1) &= \frac{1}{16}, & P(X=2, Y=0) &= \frac{1}{32}, & P(X=2, Y=1) &= \frac{1}{32}. \end{aligned}$$

- ➊ Határozzuk meg az X és Y entrópiáját, valamint az (X, Y) együttes entrópiáját.
- ➋ Határozzuk meg az X^2 és Y^2 entrópiáját, valamint az (X^2, Y^2) együttes entrópiáját.
- ➌ Határozzuk meg az X és Y kölcsönös információját.
- ➍ Határozzuk meg az X^2 és Y^2 kölcsönös információját és vizsgáljuk meg a kapcsolatát az előző pontban kapott értékkel.
- ➎ Határozzuk meg a $H(X|Y)$ és $H(Y|X)$ feltételes entrópiákat.
- ➏ Határozzuk meg a $H(X|Y^2)$ és $H(Y|X^2)$ feltételes entrópiákat és vizsgáljuk meg a kapcsolatukat az előző pontban kapott értékekkel.

Megoldás

Az X és Y , valamint az X^2 és Y^2 együttes eloszlása és peremeloszlásai rendre:

$X \backslash Y$	-1	0	1	Σ
1	1/2	1/4	1/8	7/8
2	1/16	1/32	1/32	1/8
Σ	9/16	9/32	5/32	1

és

$X^2 \backslash Y^2$	0	1	Σ
1	1/4	5/8	7/8
4	1/32	3/32	1/8
Σ	9/32	23/32	1

1. Az X és Y entrópiája, valamint az (X, Y) együttes entrópiája:

$$H(X) = \frac{7}{8} \log_2 \left(\frac{8}{7} \right) + \frac{1}{8} \log_2 8 = 3 - \frac{7}{8} \log_2 7 = 0.5436 \text{ bit};$$

$$H(Y) = \frac{9}{16} \log_2 \left(\frac{16}{9} \right) + \frac{9}{32} \log_2 \left(\frac{32}{9} \right) + \frac{5}{32} \log_2 \left(\frac{32}{5} \right) = \frac{71}{16} - \frac{27}{16} \log_2 3 - \frac{5}{32} \log_2 5 = 1.4001 \text{ bit};$$

$$H(X, Y) = \frac{1}{2} \log_2 2 + \frac{1}{4} \log_2 4 + \frac{1}{8} \log_2 8 + \frac{1}{16} \log_2 16 + 2 \cdot \frac{1}{32} \log_2 32 = \frac{31}{16} = 1.9375 \text{ bit}.$$

Megoldás

2. Az X és X^2 eloszlása megegyezik, így $H(X^2) = H(X)$. Az Y^2 entrópiája, valamint az (X^2, Y^2) együttes entrópiája:

$$H(Y^2) = \frac{9}{32} \log_2 \left(\frac{32}{9} \right) + \frac{23}{32} \log_2 \left(\frac{32}{23} \right) = 5 - \frac{9}{16} \log_2 3 - \frac{23}{32} \log_2 23 = 0.8571 \text{ bit};$$

$$H(X^2, Y^2) = \frac{1}{4} \log_2 4 + \frac{5}{8} \log_2 \left(\frac{8}{5} \right) + \frac{1}{32} \log_2 32 + \frac{3}{32} \log_2 \left(\frac{32}{3} \right) = 3 - \frac{5}{8} \log_2 5 - \frac{3}{32} \log_2 32 = 1.4002 \text{ bit}.$$

3. Az X és Y kölcsönös információja:

$$I(X; Y) = H(X) + H(Y) - H(X, Y) = 3 - \frac{7}{8} \log_2 7 + \frac{71}{16} - \frac{27}{16} \log_2 3 - \frac{5}{32} \log_2 5 - \frac{31}{16} = 0.0061 \text{ bit}.$$

4. Az X^2 és Y^2 kölcsönös információja:

$$\begin{aligned} I(X^2; Y^2) &= H(X^2) + H(Y^2) - H(X^2, Y^2) \\ &= 3 - \frac{7}{8} \log_2 7 + 5 - \frac{9}{16} \log_2 3 - \frac{23}{32} \log_2 23 - 3 + \frac{5}{8} \log_2 5 + \frac{3}{32} \log_2 32 = 0.0005 \text{ bit}. \end{aligned}$$

$I(X; Y) > I(X^2; Y^2)$, ami természetes, mert az X és Y bármely g és h függvényére

$$I(X; Y) \geq I(g(X); h(Y)).$$

Megoldás

5. A $H(X|Y)$ és $H(Y|X)$ feltételes entrópiák meghatározásához használjuk ki az alábbiakat:

$$H(X, Y) = H(Y) + H(X|Y) = H(X) + H(Y|X).$$

Ezek alapján:

$$H(X|Y) = H(X, Y) - H(Y) = \frac{31}{16} - \frac{71}{16} + \frac{27}{16} \log_2 3 + \frac{5}{32} \log_2 5 = 0.5374 \text{ bit.}$$

$$H(Y|X) = H(X, Y) - H(X) = \frac{31}{16} - 3 + \frac{7}{8} \log_2 7 = 1.3939 \text{ bit.}$$

6. A $H(X|Y^2)$ és $H(Y|X^2)$ feltételes entrópiák meghatározásához szükség van a $H(X, Y^2)$ és $H(X^2, Y)$ értékére. Mivel esetünkben könnyen látható, hogy (X, Y^2) eloszlása megegyezik (X^2, Y^2) eloszlásával, (X^2, Y) eloszlása pedig megegyezik (X, Y) eloszlásával, $H(X, Y^2) = H(X^2, Y^2)$ és $H(X^2, Y) = H(X, Y)$.

$$\begin{aligned} H(X|Y^2) &= H(X, Y^2) - H(Y^2) = H(X^2, Y^2) - H(Y^2) \\ &= 3 - \frac{5}{8} \log_2 5 - \frac{3}{32} \log_2 32 - 5 + \frac{9}{16} \log_2 3 + \frac{23}{32} \log_2 23 = 0.5431 \text{ bit.} \end{aligned}$$

$$H(Y|X^2) = H(X^2, Y) - H(X^2) = H(X, Y) - H(X) = \frac{31}{16} - 3 + \frac{7}{8} \log_2 7 = 1.3939 \text{ bit.}$$

$H(X|Y^2) > H(X|Y)$, míg $H(Y|X^2) = H(Y|X)$, mivel az $f(x) = x^2$ függvény az X értékészletén kölcsönösen egyértelmű, az Y értékészletén viszont nem.



Példa

Feldobunk egy szabályos érmét. Mennyi az érme felső és alsó lapja által mutatott kép kölcsönös információjája?

Megoldás. Legyen X és Y az érme felső, illetve alsó lapján lévő képet jellemző valószínűségi változó, lehetséges értékeik \mathcal{F} (fej) és \mathcal{I} (írás).

Az X és Y együttes eloszlása és peremeloszlásai:

$X \backslash Y$	\mathcal{F}	\mathcal{I}	Σ
\mathcal{F}	0	$1/2$	$1/2$
\mathcal{I}	$1/2$	0	$1/2$
Σ	$1/2$	$1/2$	1

Ezek alapján az X és Y entrópiája, valamint az (X, Y) együttes entrópiája:

$$H(X) = H(Y) = 2 \cdot \frac{1}{2} \log_2 2 = 1 \text{ bit}, \quad H(X, Y) = 2 \cdot \frac{1}{2} \log_2 2 = 1 \text{ bit}.$$

A keresett kölcsönös információ:

$$I(X; Y) = H(X) + H(Y) - H(X, Y) = 1 \text{ bit}.$$



Példa

Feldobunk egy szabályos dobókockát. Mennyi a kocka felső lapján és a hozzánk legközelebbi elülső lapján mutatott szám kölcsönös információja?

Megoldás. Legyen X a kocka felső lapján, Y pedig az elülső lapján mutatott szám. Az X és Y eloszlása egyenletes az $\{1, 2, 3, 4, 5, 6\}$ halmazon, azaz $P(X = k) = P(Y = k) = 1/6$, $k = 1, 2, 3, 4, 5, 6$.

Az X entrópiája: $H(X) = \log_2 6$.

Ha adott az Y értéke, akkor az X csak 4 tőle különböző értéket vehet fel, mindegyiket azonos eséllyel.
Például:

$$P(X = 2|Y = 1) = P(X = 3|Y = 1) = P(X = 4|Y = 1) = P(X = 5|Y = 1) = \frac{1}{4}, \quad \text{vagy}$$

$$P(X = 1|Y = 2) = P(X = 3|Y = 2) = P(X = 6|Y = 2) = P(X = 4|Y = 2) = \frac{1}{4}.$$

Ezek alapján

$$H(X|Y = k) = \log_2 4 = 2 \text{ bit}, \quad k = 1, 2, 3, 4, 5, 6.$$

$$H(X|Y) = \sum_{k=1}^6 H(X|Y = k)P(Y = k) = 2 \text{ bit}, \quad \text{így}$$

$$I(X; Y) = H(X) - H(X|Y) = \log_2 6 - 2 = 2(\log_2 3 - 1) = 0.5850 \text{ bit}.$$



Egy amerikai kisvárosban a végzős diákok 75%-a átment az érettségi vizsgán, a többiek megbuktak. A sikeres vizsgázók 10%-ának van saját személygépkocsija, a bukottak esetén ez az arány 50%.

- 1 Mennyi információt nyerünk egy diák vizsgájának az eredményéről, ha tudjuk, hogy van saját személygépkocsija?
- 2 Mennyi információt nyerünk egy diák vizsgájának az eredményéről, ha tudjuk, hogy nincs saját személygépkocsija?
- 3 Mennyi információt nyerünk egy diák vizsgájának az eredményéről, ha tudjuk, hogy van-e saját személygépkocsija?

Megoldás. Egy véletlenszerűen kiválasztott diák adatait a következő két valószínűségi változóval írhatjuk le.

X : a vizsga eredménye. $X = 1$: sikeres; $X = 0$: sikertelen.
 Y : saját személygépkocsi. $Y = 1$: van; $Y = 0$: nincs.

Megoldás

A feladat szövege alapján a következő valószínűségek és feltételes valószínűségek adottak:

$$\begin{aligned}P(X = 1) &= \frac{3}{4}, & P(X = 0) &= \frac{1}{4}; \\P(Y = 1|X = 1) &= \frac{1}{10}, & P(Y = 0|X = 1) &= \frac{9}{10}; \\P(Y = 1|X = 0) &= \frac{1}{2}, & P(Y = 0|X = 0) &= \frac{1}{2}.\end{aligned}$$

A vizsga eredményének meghatározásához szükséges információ mennyisége:

$$H(X) = \frac{3}{4} \log_2 \left(\frac{4}{3} \right) + \frac{1}{4} \log_2 4 = \log_2 4 - \frac{3}{4} \log_2 3 = 2 - \frac{3}{4} \log_2 3 = 0.8113.$$

1. A vizsga eredményének meghatározásához szükséges információ mennyisége, ha tudjuk, hogy a diáknak van saját személygépkocsija: $H(X|Y = 1)$. Információnyereség: $H(X) - H(X|Y = 1)$.
2. A vizsga eredményének meghatározásához szükséges információ mennyisége, ha tudjuk, hogy a diáknak nincs saját személygépkocsija: $H(X|Y = 0)$. Információnyereség: $H(X) - H(X|Y = 0)$.
3. A vizsga eredményének meghatározásához szükséges információ mennyisége, ha tudjuk, hogy a diáknak van-e saját személygépkocsija: $H(X|Y)$. Információnyereség: $H(X) - H(X|Y)$.

Megoldás

Az Y eloszlása a teljes valószínűség tételével határozható meg:

$$P(Y = 1) = P(Y = 1|X = 1)P(X = 1) + P(Y = 1|X = 0)P(X = 0) = \frac{1}{10} \cdot \frac{3}{4} + \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{5},$$

$$P(Y = 0) = 1 - P(Y = 1) = \frac{4}{5}.$$

1. A $H(X|Y = 1)$ meghatározásához szükségünk van az X feltételes eloszlására az $Y = 1$ feltétel mellett, amit a Bayes formula segítségével számolhatunk ki.

$$P(X = 1|Y = 1) = \frac{P(Y = 1|X = 1)P(X = 1)}{P(Y = 1)} = \frac{\frac{1}{10} \cdot \frac{3}{4}}{\frac{1}{5}} = \frac{3}{8},$$

$$P(X = 0|Y = 1) = 1 - P(X = 1|Y = 1) = \frac{5}{8}.$$

$$\begin{aligned} H(X|Y = 1) &= \frac{3}{8} \log_2 \left(\frac{8}{3} \right) + \frac{5}{8} \log_2 \left(\frac{8}{5} \right) = \frac{3}{8} (\log_2 8 - \log_2 3) + \frac{5}{8} (\log_2 8 - \log_2 5) \\ &= \log_2 8 - \frac{3}{8} \log_2 3 - \frac{5}{8} \log_2 5 = 3 - \frac{3}{8} \log_2 3 - \frac{5}{8} \log_2 5 = 0.9544. \end{aligned}$$

Információnyereség:

$$H(X) - H(X|Y = 1) = 2 - \frac{3}{4} \log_2 3 - \left[3 - \frac{3}{8} \log_2 3 - \frac{5}{8} \log_2 5 \right] = \frac{5}{8} \log_2 5 - \frac{3}{8} \log_2 3 - 1 = -0.1432.$$

Megoldás

2. Az 1. pont megoldásához hasonlóan a $H(X|Y=0)$ meghatározásához szükségünk van az X feltételes eloszlására az $Y=0$ feltétel mellett.

$$P(X=1|Y=0) = \frac{P(Y=0|X=1)P(X=1)}{P(Y=0)} = \frac{\frac{9}{10} \cdot \frac{3}{4}}{\frac{4}{5}} = \frac{27}{32},$$

$$P(X=0|Y=0) = 1 - P(X=1|Y=0) = \frac{5}{32}.$$

Így

$$\begin{aligned} H(X|Y=0) &= \frac{27}{32} \log_2 \left(\frac{32}{27} \right) + \frac{5}{32} \log_2 \left(\frac{32}{5} \right) = \frac{27}{32} (\log_2 32 - \log_2 27) + \frac{5}{32} (\log_2 32 - \log_2 5) \\ &= 5 - \frac{27}{32} \log_2 27 - \frac{5}{32} \log_2 5 = 5 - \frac{81}{32} \log_2 3 - \frac{5}{32} \log_2 5 = 0.6253. \end{aligned}$$

Információnyereség:

$$\begin{aligned} H(X) - H(X|Y=0) &= 2 - \frac{3}{4} \log_2 3 - \left[5 - \frac{81}{32} \log_2 3 - \frac{5}{32} \log_2 5 \right] \\ &= \frac{57}{32} \log_2 3 + \frac{5}{32} \log_2 5 - 3 = 0.1860. \end{aligned}$$

3. Az X feltételes entrópiája az Y -ra nézve:

$$\begin{aligned} H(X|Y) &= H(X|Y=1)P(Y=1) + H(X|Y=0)P(Y=0) \\ &= \left[3 - \frac{3}{8} \log_2 3 - \frac{5}{8} \log_2 5 \right] \cdot \frac{1}{5} + \left[5 - \frac{81}{32} \log_2 3 - \frac{5}{32} \log_2 5 \right] \cdot \frac{4}{5} \\ &= \frac{23}{5} - \frac{21}{10} \log_2 3 - \frac{1}{4} \log_2 5 = 0.6911. \end{aligned}$$

Információnyereség (X és Y kölcsönös információja):

$$\begin{aligned} I(X; Y) &= H(X) - H(X|Y) = 2 - \frac{3}{4} \log_2 3 - \left[\frac{23}{5} - \frac{21}{10} \log_2 3 - \frac{1}{4} \log_2 5 \right] \\ &= \frac{27}{20} \log_2 3 + \frac{1}{4} \log_2 5 - \frac{13}{5} = 0.1202. \end{aligned}$$

□

Egy város lakosai két területben laknak, Alsóvárosban és Felsővárosban. Alsóváros lakói az összlakosság p -ed részét adják ($0 < p < 1$). Az itt élők az esetek felében igazat mondanak, 30 %-ában hazudnak, egyébként pedig nem válaszolnak a kérdésre. Felsővárosban ezek az arányok rendre 30 %, 50 % és 20 %.

- ❶ Mennyi információt szolgáltat egy megkérdezett lakos lakhelyére vonatkozóan az, hogy egy feltett kérdésre nem válaszol?
- ❷ Határozza meg azt az átlagos információmennyiséget, amit egy kérdésre adott válasz a lakhelyre vonatkozóan tartalmaz.
- ❸ A p mely értéke mellett lesz ez az információ a maximális?

Megoldás. Egy véletlenszerűen kiválasztott lakos adatait a következő két valószínűségi változóval írhatjuk le.

X : lakhely. $X = 1$: Alsóváros; $X = 0$: Felsőváros.

Y : válasz. $Y = 1$: igaz; $Y = 0$: nincs; $Y = -1$: hamis.

Megoldás

A feladat szövege alapján a következő valószínűségek és feltételes valószínűségek adottak:

$$\begin{aligned}P(X = 1) &= p, & P(Y = 1|X = 1) &= 0.5, & P(Y = 0|X = 1) &= 0.2, & P(Y = -1|X = 1) &= 0.3; \\P(X = 0) &= 1 - p, & P(Y = 1|X = 0) &= 0.3, & P(Y = 0|X = 0) &= 0.2, & P(Y = -1|X = 0) &= 0.5.\end{aligned}$$

A lakhely meghatározásához szükséges információ mennyisége:

$$H(X) = p \log_2 \left(\frac{1}{p} \right) + (1 - p) \log_2 \left(\frac{1}{1 - p} \right) = -p \log_2 p - (1 - p) \log_2 (1 - p) =: H_2(p).$$

$H_2(p)$: **bináris entrópia függvény**.

1. A lakhely meghatározásához szükséges információ mennyisége, feltéve, hogy a kérdezett nem válaszol: $H(X|Y = 0)$. Az információnyereség a válasz megtagadása esetén: $H(X) - H(X|Y = 0)$.

Az Y eloszlása a teljes valószínűség tételével határozható meg:

$$P(Y = 1) = P(Y = 1|X = 1)P(X = 1) + P(Y = 1|X = 0)P(X = 0) = 0.5p + 0.3(1 - p) = 0.3 + 0.2p,$$

$$P(Y = 0) = P(Y = 0|X = 1)P(X = 1) + P(Y = 0|X = 0)P(X = 0) = 0.2p + 0.2(1 - p) = 0.2,$$

$$P(Y = -1) = 1 - P(Y = 1) - P(Y = 0) = 0.5 - 0.2p.$$

Megoldás

A $H(X|Y=0)$ meghatározásához szükségünk van az X feltételes eloszlására az $Y=0$ feltétel mellett, amit a Bayes formula segítségével számolhatunk ki.

$$P(X=1|Y=0) = \frac{P(Y=0|X=1)P(X=1)}{P(Y=0)} = \frac{0.2p}{0.2} = p = P(X=1),$$

$$P(X=0|Y=0) = 1 - P(X=1|Y=0) = 1 - p = P(X=0).$$

$$H(X|Y=0) = -p \log_2 p - (1-p) \log_2 (1-p) = H_2(p) = H(X).$$

Információnyereség: $H(X) - H(X|Y=0) = 0$.

2. Az átlagos információmennyiséget, amit egy kérdésre adott válasz a lakhelyre vonatkozóan tartalmaz az X és Y kölcsönös információja: $I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$.

A megadott feltételes eloszlások és az Y korábban meghatározott eloszlása alapján:

$$H(Y) = -(0.3 + 0.2p) \log_2 (0.3 + 0.2p) - (0.5 - 0.2p) \log_2 (0.5 - 0.2p) - 0.2 \log_2 0.2;$$

$$H(Y|X=1) = -0.5 \log_2 0.5 - 0.2 \log_2 0.2 - 0.3 \log_2 0.3 = 1.4855;$$

$$H(Y|X=0) = -0.3 \log_2 0.3 - 0.2 \log_2 0.2 - 0.5 \log_2 0.5 = H(Y|X=1).$$

$$H(Y|X) = H(Y|X=1)P(X=1) + H(Y|X=0)P(X=0) = H(Y|X=1)p + H(Y|X=1)(1-p) = H(Y|X=1).$$

Megoldás

Az X és Y kölcsönös információja:

$$\begin{aligned} I(X; Y) &= H(Y) - H(Y|X) = H(Y) - H(Y|X = 1) \\ &= -(0.3 + 0.2p) \log_2(0.3 + 0.2p) - (0.5 - 0.2p) \log_2(0.5 - 0.2p) + 0.5 \log_2 0.5 + 0.3 \log_2 0.3 =: I(p). \end{aligned}$$

3. Az $I(p)$ függvény szélsőértékhelye megoldja az $I'(p) = 0$ egyenletet.

$$\begin{aligned} I'(p) &= -0.2 \log_2(0.3 + 0.2p) - \frac{(0.3 + 0.2p) 0.2}{(0.3 + 0.2p) \ln 2} + 0.2 \log_2(0.5 - 0.2p) - \frac{(0.5 - 0.2p)(-0.2)}{(0.5 - 0.2p) \ln 2} \\ &= 0.2 (\log_2(0.5 - 0.2p) - \log_2(0.3 + 0.2p)) = 0.2 \log_2 \left(\frac{0.5 - 0.2p}{0.3 + 0.2p} \right) = 0.2 \log_2 \left(\frac{0.8}{0.3 + 0.2p} - 1 \right). \end{aligned}$$

$$I'(p) = 0 \iff \frac{0.8}{0.3 + 0.2p} - 1 = 1 \iff p = 0.5$$

$p^* = 0.5$ az $I(p)$ függvény szélsőértékhelye. Rövid számolás után:

$$I''(p) = \frac{-0.032}{(0.5 - 0.2p)(0.3 + 0.2p) \ln 2}, \quad \text{így} \quad I''(p^*) = -\frac{0.2}{\ln 2} < 0.$$

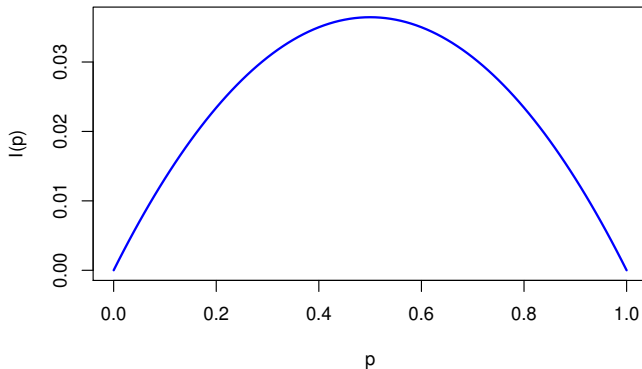
$p^* = 0.5$ az $I(p)$ függvény maximumhelye. A maximális információ:

$$I(p^*) = -0.8 \log_2 0.4 + 0.5 \log_2 0.5 + 0.3 \log_2 0.3 = 0.0365 \text{ bit.}$$

Megoldás

Az X és Y kölcsönös információját:

$$I(p) = -(0.3 + 0.2p) \log_2(0.3 + 0.2p) - (0.5 - 0.2p) \log_2(0.5 - 0.2p) + 0.5 \log_2 0.5 + 0.3 \log_2 0.3.$$



Maximumhely: $p^* = 0.5$. A maximum értéke: $I(0.5) = 0.0365$.



Zajmentes távközlési csatornák

Adott egy távközlési csatorna, ami az $\mathcal{Y} = \{y_1, y_2, \dots, y_s\}$ csatornaábécé jeleit tudja továbbítani.

X : a csatorna bemeneténél leadott jel.

Y : a csatorna kimeneténél vett, az X -nek megfelelő jel.

Feltesszük, hogy a csatorna **emlékezet nélküli**, azaz Y csak az X -től függ.

Az Y kimenő kódjel az X bemenő kódjelről $I(X; Y)$ információt tartalmaz.

Zajmentes csatorna: $X = Y$, ekkor $I(X; Y) = H(X)$.

$H(X)$ meghatározásához szükség van az X eloszlására. Ez megadható a forrás eloszlásának és a kódolási eljárásnak az ismeretében.

A csatorna bemenő jelének eloszlása

$\mathcal{X} = \{x_1, x_2, \dots, x_n\}$: forrásábécé $\mathcal{P} = \{p_1, p_2, \dots, p_n\}$ eloszlással.

$\mathcal{K} = \{K_1, K_2, \dots, K_n\}$: az \mathcal{X} forrásábécének az \mathcal{Y} elemeiből alkotott egyértelműen dekódolható kódja.

$\mathcal{L} = \{L_1, L_2, \dots, L_n\}$: a \mathcal{K} kód kódszóhosszai.

N_{ij} : az y_j kódjel gyakorisága az L_i hosszú K_i kódszóban.

$$P(X = y_j) = \sum_{i=1}^n P(X = y_j | y_j \text{ az } x_i \text{ kódjának eleme}) P(y_j \text{ az } x_i \text{ kódjának eleme}) = \sum_{i=1}^n \frac{N_{ij}}{L_i} p_i.$$

Példa. Legyen $\mathcal{X} = \{A, B, C\}$, $\mathcal{P} = \{1/2, 1/4, 1/4\}$, $\mathcal{Y} = \{0, 1\}$, $\mathcal{K} = \{0, 10, 11\}$, azaz $\mathcal{L} = \{1, 2, 2\}$.

$$N_{11} = 1, \quad N_{21} = 1, \quad N_{31} = 0, \quad N_{12} = 0, \quad N_{22} = 1, \quad N_{32} = 2.$$

Ezek alapján

$$P(X = 0) = \frac{1}{1} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} + \frac{0}{2} \cdot \frac{1}{4} = \frac{5}{8}; \quad P(X = 1) = \frac{0}{1} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{4} + \frac{2}{2} \cdot \frac{1}{4} = \frac{3}{8}.$$

Zajmentes csatorna kapacitása

X : a csatorna bemeneténél leadott jel;

Y : a csatorna kimeneténél vett, az X -nek megfelelő jel.

Az Y kimenő kódjel az X bemenő kódjelről $I(X; Y)$ információt tartalmaz.

Zajmentes csatorna: $X = Y$, ekkor $I(X; Y) = H(X)$.

$H(X)$ maximális értéke $\log_2 s$, azaz egy kódjel maximálisan ennyi információt tartalmazhat. Ez az információmennyiség maradéktalanul továbbítható a csatornán. A zajmentes csatorna maximálisan $C = \log_2 s$ információt tud továbbítani, ennyi a kapacitása.

A p_i valószínűségű x_i forrásbetű L_i hosszúságú K_i kódjának továbbításával maximum $L_i \log_2 s$ bit információt továbbítunk. Egy forrásbetű átvitelével továbbított átlagos információ maximuma:

$$\log_2 s \sum_{i=1}^n p_i L_i = \log_2 s E(\mathcal{K}) = C E(\mathcal{K}) \geq H(\mathcal{X}),$$

ahol $E(\mathcal{K})$ az átlagos kódszóhossz.

Csatornakapacitás

Zajos csatorna: $X \neq Y$, ekkor $I(X, Y) < H(X)$.

Az egy kódjellel továbbítható információ maximuma kevesebb, mint $\log_2 s$.

A csatorna viselkedését a

$$p_{i|j} := P\{Y = y_i | X = y_j\}, \quad i, j = 1, 2, \dots, s,$$

átmenetvalószínűségek írják le.

Az X bemenő jel eloszlása: $q_j := P(X = y_j)$, $j = 1, 2, \dots, s$.

Egy emlékezet nélküli távközlési csatorna **kapacitása**

$$C := \sup I(X; Y),$$

ahol az supremum az X összes lehetséges eloszlása felett értendő.

Kapacitás: az egy kódjellel átvihető átlagos információmennyiség pontos felső korlátja. C kapacitású csatornán egy $E(\mathcal{K})$ az átlagos kódszóhosszú kód felhasználásával csak akkor továbbíthatjuk a forrásközleményeket, ha $H(\mathcal{X}) \leq C E(\mathcal{K})$.

A csatornakapacitás meghatározása

Átmenetvalószínűségek: $p_{i|j} := P\{Y = y_i | X = y_j\}$, $i, j = 1, 2, \dots, s$.

Bemeneti eloszlás: $q_j := P(X = y_j)$, $j = 1, 2, \dots, s$.

Kapacitás: $C := \sup I(X; Y)$.

Példa. Zajmentes csatorna:

$$p_{i|j} = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

$I(X; Y) = H(X) \leq \log_2 s$ és az egyenlőség teljesül, ha X egyenletes eloszlású, azaz $q_j = 1/s$, $j = 1, 2, \dots, s$.
Kapacitás:

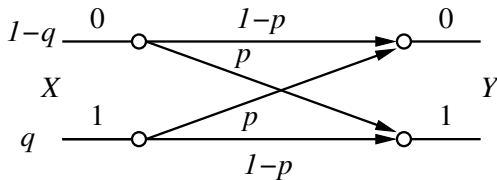
$$C = \log_2 s.$$

Általánosan: keressük a

$$I(X; Y) = G(q_1, \dots, q_s) := \sum_{i=1}^s \sum_{j=1}^s p_{i|j} q_j \log_2 \left(\frac{p_{i|j}}{\sum_{k=1}^s p_{i|k} q_k} \right)$$

maximumát a $q_1 + q_2 + \dots + q_s = 1$, $0 \leq q_i \leq 1$, $i = 1, 2, \dots, s$, feltétel mellett.

Példa. Emlékezet nélküli szimmetrikus bináris X-csatorna



$\mathcal{Y} = \{0, 1\}$, azaz $s = 2$.

Legyenek $p, q \in [0, 1]$.

A bemenő jel eloszlása:

$$P(X = 1) = q, \quad P(X = 0) = 1 - q.$$

Átmenetvalószínűségek:

$$\begin{aligned} p_{0|0} &:= P(Y = 0 \mid X = 0) = 1 - p, & p_{1|0} &:= P(Y = 1 \mid X = 0) = p, \\ p_{1|1} &:= P(Y = 1 \mid X = 1) = 1 - p, & p_{0|1} &:= P(Y = 0 \mid X = 1) = p. \end{aligned}$$

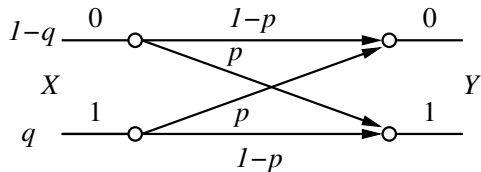
Feltételes entrópiák:

$$H(Y|X = 0) = H(Y|X = 1) = H_2(p), \quad \text{ahol} \quad H_2(p) := -p \log_2 p - (1 - p) \log_2 (1 - p).$$

$$H(Y|X) = H(Y|X = 0)P(X = 0) + H(Y|X = 1)P(X = 1) = H_2(p)(1 - q) + H_2(p)q = H_2(p).$$

$H_2(p)$: bináris entrópia függvény.

Példa. Emlékezet nélküli szimmetrikus bináris X-csatorna



Kölcsönös információ:

$$I(X; Y) = H(Y) - H(Y|X) = H(Y) - H_2(p),$$

$$\text{ahol } H_2(p) := -p \log_2 p - (1-p) \log_2(1-p).$$

$H(Y) \leq \log_2 2 = 1$ és $H(Y) = 1$ pontosan akkor, ha $P(Y=0) = P(Y=1) = \frac{1}{2}$.

$$P(Y=0) = (1-p)P(X=0) + pP(X=1), \quad P(Y=1) = pP(X=0) + (1-p)P(X=1).$$

$$P(Y=0) = P(Y=1) = 1/2 \iff P(X=0) = P(X=1) = 1/2 \iff q = 1/2.$$

$$I(X; Y) = H(Y) - H(Y|X) = H(Y) - H_2(p) \leq 1 - H_2(p) \text{ és } I(X; Y) = 1 - H_2(p), \text{ ha } q = 1/2.$$

Az emlékezet nélküli szimmetrikus bináris X-csatorna (BSC_p) kapacitása: $C = 1 - H_2(p)$.

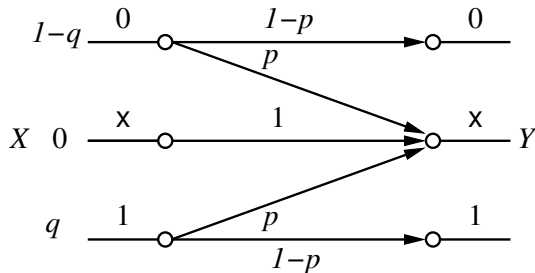
Speciális esetek:

- $C = 1 \iff H_2(p) = 0 \iff p = 0 \text{ vagy } p = 1.$

$p = 0$: zajmentes csatorna; $p = 1$: bináris fordító csatorna.

- $C = 0 \iff H_2(p) = 1 \iff p = 1/2$: véletlen csatorna.

Példa. Emlékezet nélküli szimmetrikus bináris törléses csatorna



$\mathcal{Y} = \{0, 1, x\}$; x : elveszett a jel.

Legyenek $p, q \in [0, 1]$.

A bemenő jel eloszlása:

$$P(X=1) = q, \quad P(X=0) = 1-q, \quad P(X=x) = 0.$$

Átmenetvalószínűségek:

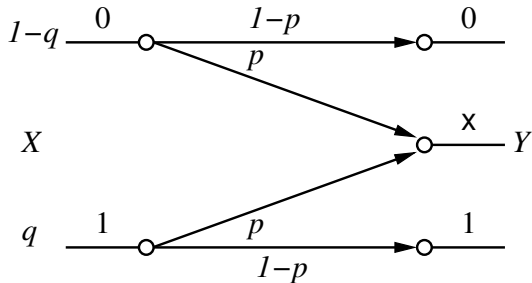
$$\begin{aligned} p_{0|0} &:= P(Y=0 | X=0) = 1-p, & p_{x|0} &:= P(Y=x | X=0) = p, & p_{1|0} &:= P(Y=1 | X=0) = 0; \\ p_{1|1} &:= P(Y=1 | X=1) = 1-p, & p_{x|1} &:= P(Y=x | X=1) = p, & p_{0|1} &:= P(Y=0 | X=1) = 0; \\ p_{1|x} &:= P(Y=1 | X=x) = 0, & p_{x|x} &:= P(Y=x | X=x) = 1, & p_{0|x} &:= P(Y=0 | X=x) = 0. \end{aligned}$$

Feltételes entrópiák:

$$H(Y|X=0) = H(Y|X=1) = H_2(p), \quad \text{ahol} \quad H_2(p) := -p \log_2 p - (1-p) \log_2 (1-p).$$

$$H(Y|X) = H(Y|X=0)P(X=0) + H(Y|X=1)P(X=1) = H_2(p)(1-q) + H_2(p)q = H_2(p).$$

Példa. Emlékezet nélküli szimmetrikus bináris törléses csatorna



Kölcsönös információ:

$$I(X; Y) = H(Y) - H(X|Y) = H(Y) - H_2(p),$$

ahol $H_2(p) := -p \log_2 p - (1-p) \log_2 (1-p)$.

$$P(Y = 0) = (1-q)(1-p), \quad P(Y = 1) = q(1-p),$$

$$P(Y = x) = (1-q)p + qp = p.$$

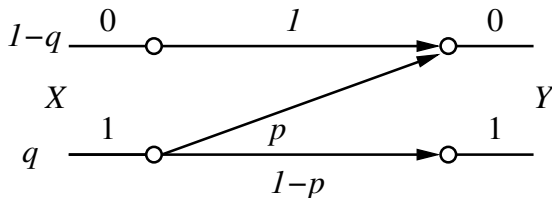
$$\begin{aligned} H(Y) &= -(1-q)(1-p) \log_2 [(1-q)(1-p)] - q(1-p) \log_2 [q(1-p)] - p \log_2 p \\ &= -(1-q)(1-p) [\log_2 (1-q) + \log_2 (1-p)] - q(1-p) [\log_2 q + \log_2 (1-p)] - p \log_2 p \\ &= (1-p)H_2(q) - (1-q)[(1-p) \log_2 (1-p)] - q[(1-p) \log_2 (1-p)] - p \log_2 p = (1-p)H_2(q) + H_2(p). \end{aligned}$$

$$I(X; Y) = H(Y) - H(X|Y) = (1-p)H_2(q) \leq 1-p \text{ és } I(X; Y) = 1-p, \text{ ha } q = 1/2.$$

Az emlékezet nélküli szimmetrikus bináris törléses csatorna (BEC) kapacitása: $C = 1-p$.

A leadott jelek p -edrésze vesz el.

Példa. Emlékezet nélküli bináris Z-csatorna



$\mathcal{Y} = \{0, 1\}$, azaz $s = 2$.

Legyenek $p, q \in]0, 1[$.

A bemenő jel eloszlása:

$$P(X = 1) = q, \quad P(X = 0) = 1 - q.$$

Átmenetvalószínűségek:

$$p_{0|0} := P(Y = 0 \mid X = 0) = 1,$$

$$p_{1|0} := P(Y = 1 \mid X = 0) = 0,$$

$$p_{1|1} := P(Y = 1 \mid X = 1) = 1 - p,$$

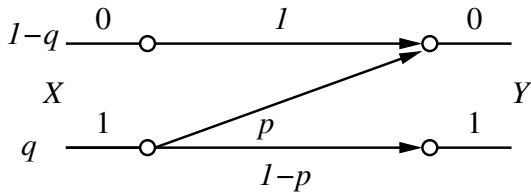
$$p_{0|1} := P(Y = 0 \mid X = 1) = p.$$

Feltételes entrópiák:

$$H(Y|X = 0) = 0, \quad H(Y|X = 1) = H_2(p), \quad \text{ahol} \quad H_2(p) := -p \log_2 p - (1 - p) \log_2 (1 - p).$$

$$H(Y|X) = H(Y|X = 0)P(X = 0) + H(Y|X = 1)P(X = 1) = H_2(p)q.$$

Példa. Emlékezet nélküli bináris Z-csatorna



Kölcsönös információ:

$$I(X; Y) = H(Y) - H(Y|X) = H(Y) - H_2(p) q,$$

ahol $H_2(p) := -p \log_2 p - (1-p) \log_2 (1-p)$.

$$P(Y = 0) = P(X = 0) + p P(X = 1) = (1 - q) + pq, \quad P(Y = 1) = (1 - p)P(X = 1) = (1 - p)q.$$

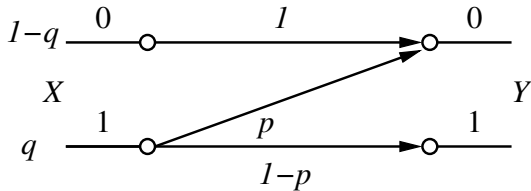
$$H(Y) = -[(1 - q) + pq] \log_2 [(1 - q) + pq] - [(1 - p)q] \log_2 [(1 - p)q] = H_2((1 - p)q).$$

Kölcsönös információ

$$I(q) := I(X; Y) = H(Y) - H(Y|X) = H_2((1 - p)q) - H_2(p) q.$$

A csatornakapacitás meghatározásához meg kell keresni az $I(q)$ maximumát a $[0, 1]$ intervallumon.

Példa. Emlékezet nélküli bináris Z-csatorna



Kölcsönös információ:

$$I(q) := I(X; Y) = H_2((1-p)q) - H_2(p)q,$$

ahol $H_2(p) := -p \log_2 p - (1-p) \log_2(1-p)$.

$$I(q) = -[(1-q) + pq] \log_2 [(1-q) + pq] - [(1-p)q] \log_2 [(1-p)q] - H_2(p)q.$$

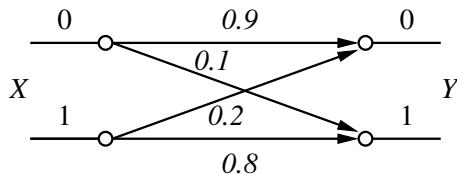
$$I'(q) = (1-p) \log_2 \left[\frac{1 - (1-p)q}{(1-p)q} \right] - H_2(p) = 0 \iff q = \frac{1}{(1-p) \left(2^{\frac{H_2(p)}{1-p}} + 1 \right)}.$$

$$I''(q) = -\frac{1-p}{(1 - (1-p)q) \ln 2} < 0, \quad p, q \in]0, 1[, \quad \text{így} \quad q^* = \frac{1}{(1-p) \left(2^{\frac{H_2(p)}{1-p}} + 1 \right)} \quad \text{maximumhely.}$$

Az emlékezet nélküli bináris Z-csatorna kapacitása:

$$C = I(q^*) = \log_2 \left[1 + 2^{-\frac{H_2(p)}{1-p}} \right].$$

Példa



Számítsa ki az ábrán látható bináris csatorna kapacitását.

Megoldás. Legyen a bemenő jel eloszlása $P(X = 1) = q$, $P(X = 0) = 1 - q$. Ekkor

$$P(Y = 1) = 0.8q + 0.1(1 - q) = 0.1 + 0.7q, \quad P(Y = 0) = 0.9(1 - q) + 0.2q = 0.9 - 0.7q, \quad \text{így}$$

$$H(Y) = H_2(0.1 + 0.7q) = -(0.1 + 0.7q) \log_2(0.1 + 0.7q) - (0.9 - 0.7q) \log_2(0.9 - 0.7q).$$

Feltételes entrópiák:

$$H(Y|X = 0) = H_2(0.1) = -0.1 \log_2(0.1) - 0.9 \log_2 0.9 = 0.4690,$$

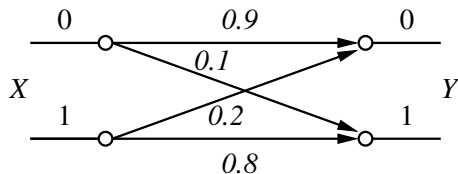
$$H(Y|X = 1) = H_2(0.2) = -0.2 \log_2(0.2) - 0.8 \log_2 0.8 = 0.7219;$$

$$H(Y|X) = H(Y|X = 0)P(X = 0) + H(Y|X = 1)P(X = 1) = H_2(0.1)(1 - q) + H_2(0.2)q.$$

Kölcsönös információ:

$$I(q) := I(X; Y) = H(Y) - H(Y|X) = H_2(0.1 + 0.7q) - H_2(0.1)(1 - q) - H_2(0.2)q.$$

Megoldás



A bemenő jel eloszlása

$$P(X = 1) = q, \quad P(X = 0) = 1 - q.$$

Kölcsönös információ:

$$I(q) = I(X; Y) = H_2(0.1 + 0.7q) - H_2(0.1)(1 - q) - H_2(0.2)q,$$

$$\text{ahol } H_2(p) = -p \log_2 p - (1 - p) \log_2 (1 - p).$$

Kölcsönös információ:

$$I(q) = -(0.1 + 0.7q) \log_2 (0.1 + 0.7q) - (0.9 - 0.7q) \log_2 (0.9 - 0.7q) - H_2(0.1)(1 - q) - H_2(0.2)q,$$

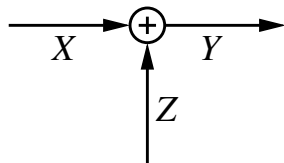
$$I'(q) = 0.7 \log_2 \left[\frac{0.9 - 0.7q}{0.1 + 0.7q} \right] + H_2(0.1) - H_2(0.2) = 0 \iff q = \frac{0.9 - 0.1 \cdot 2^{\frac{H_2(0.2) - H_2(0.1)}{0.7}}}{0.7 \left[1 + 2^{\frac{H_2(0.2) - H_2(0.1)}{0.7}} \right]}.$$

$$I''(q) = -\frac{0.7^2}{(0.1 + 0.7q)(0.9 - 0.7q) \ln 2} < 0, \quad q \in [0, 1], \quad \text{így } q^* = \frac{0.9 - 0.1 \cdot 2^{\frac{H_2(0.2) - H_2(0.1)}{0.7}}}{0.7 \left[1 + 2^{\frac{H_2(0.2) - H_2(0.1)}{0.7}} \right]}$$

maximumhely. A csatorna kapacitása:

$$C = I(q^*) = 0.4081 \text{ bit.}$$





Határozza meg az ábrán látható blokkсémával leírt bináris csatorna kapacitását, ahol $Y = X + Z$, a Z zaj és az X bemenet egymástól független és

$$P(Z = 1) = p, \quad P(Z = 0) = 1 - p.$$

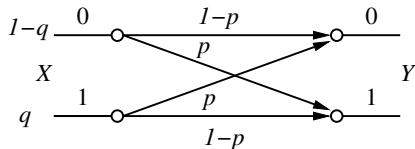
Megoldás. Legyen $X = 0$. Ekkor $Y = X + Z = 1$, ha $Z = 1$ és $Y = 0$, ha $Z = 0$. Az előbbi eseménynek p , az utóbbinak $1 - p$ a valószínűsége. Hasonlóan, ha $X = 1$, akkor p valószínűséggel $Y = 0$ ($Z = 1$) és $1 - p$ valószínűséggel $Y = 1$ ($Z = 0$). Átmenetvalószínűségek:

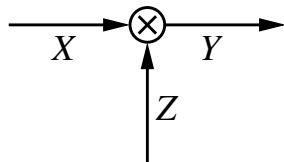
$$p_{0|0} := P(Y = 0 | X = 0) = 1 - p, \quad p_{1|0} := P(Y = 1 | X = 0) = p,$$

$$p_{1|1} := P(Y = 1 | X = 1) = 1 - p, \quad p_{0|1} := P(Y = 0 | X = 1) = p.$$

Az blokkсéma egy szimmetrikus bináris X-csatornát ad meg. Ennek kapacitása:

$$C = 1 - H_2(p), \text{ ahol } H_2(p) := -p \log_2 p - (1-p) \log_2 (1-p).$$





Határozza meg az ábrán látható blokkсémával leírt bináris csatorna kapacitását, ahol $Y = X \times Z$, a Z zaj és az X bemenet egymástól független és

$$P(Z = 0) = p, \quad P(Z = 1) = 1 - p.$$

Megoldás. Legyen $X = 0$. Ekkor $Y = X \times Z = 0$, függetlenül a Z értékétől. Ha $X = 1$, akkor p valószínűséggel $Y = 0$ ($Z = 0$) és $1 - p$ valószínűséggel $Y = 1$ ($Z = 1$). Átmenetvalószínűségek:

$$p_{0|0} := P(Y = 0 \mid X = 0) = 1,$$

$$p_{1|0} := P(Y = 1 \mid X = 0) = 0,$$

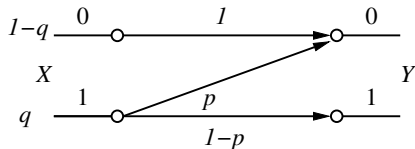
$$p_{1|1} := P(Y = 1 \mid X = 1) = 1 - p,$$

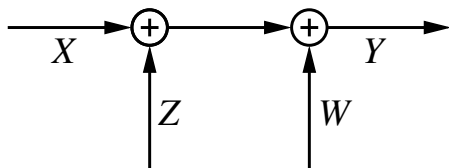
$$p_{0|1} := P(Y = 0 \mid X = 1) = p.$$

Az blokkсéma egy bináris Z-csatornát ad meg. Ennek kapacitása:

$$C = \log_2 \left[1 + 2^{-\frac{H_2(p)}{1-p}} \right],$$

ahol $H_2(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)$.





Az ábrán látható blokkképe egy olyan bináris csatornát ad meg, ahol $Y = X + Z + W$, a Z és W zajok és az X bemenet egymástól teljesen függetlenek és

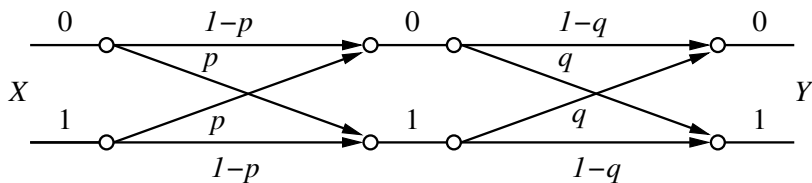
$$P(Z = 1) = p, \quad P(Z = 0) = 1 - p,$$

$$P(W = 1) = q, \quad P(W = 0) = 1 - q.$$

- 1 Számítsa ki fenti a csatorna kapacitását.
- 2 Az első bináris összeadást cseréljük ki a bináris *vagy* műveletre, a másodikat pedig a bináris *és* műveletre. Mennyi az így kapott csatorna kapacitása $p = 1/3$ és $q = 3/4$ esetén?

Megoldás

1. A korábbi feladat alapján a bináris additív zaj egy szimmetrikus bináris X-csatornát határoz meg. Az itt megadott blokséma így két egymás után kapcsolt szimmetrikus bináris X-csatornát ír le, ahol az elsőnél p , a másodiknál pedig q a tévesztés valószínűsége.



Átmenetvalószínűségek:

$$p_{1|0} = p(1-q) + q(1-p) = p + q - 2pq =: \varrho = p_{0|1},$$

$$p_{0|0} = (1-p)(1-q) + pq = 1 - p - q + 2pq = 1 - \varrho = p_{1|1}.$$

A két szimmetrikus bináris X-csatorna összekapcsolása egy olyan szimmetrikus bináris X-csatornát eredményez, ahol a tévesztés valószínűsége $\varrho = p + q - 2pq$. Ennek a kapacitása:

$$C = 1 - H_2(\varrho) = 1 + \varrho \log_2 \varrho + (1 - \varrho) \log_2 (1 - \varrho).$$

Megoldás

2. Az egyes komponensek a következő csatornákat írják le.

- **Bináris vagy:** $U = X \vee Z$, ahol $P(Z = 1) = p$, $P(Z = 0) = 1 - p$. Átmenetvalószínűségek:

$$p_{0|0} := P(U = 0 \mid X = 0) = 1 - p, \quad p_{1|0} := P(U = 1 \mid X = 0) = p,$$

$$p_{1|1} := P(U = 1 \mid X = 1) = 1, \quad p_{0|1} := P(U = 0 \mid X = 1) = 0.$$

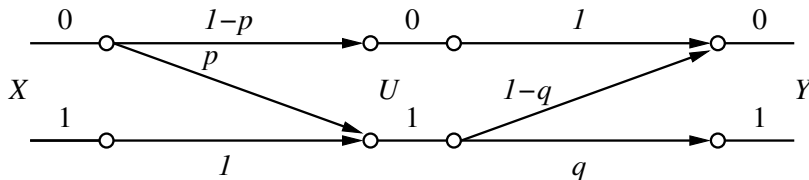
- **Bináris és:** $Y = U \wedge W$, ahol $P(W = 1) = q$, $P(W = 0) = 1 - q$. Átmenetvalószínűségek:

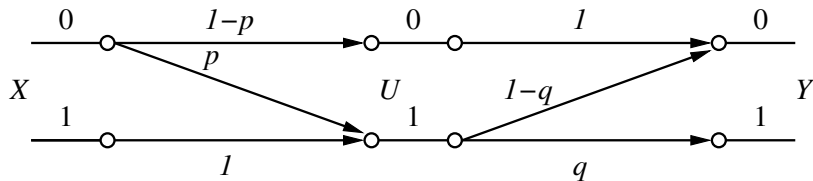
$$p_{0|0} := P(Y = 0 \mid U = 0) = 1, \quad p_{1|0} := P(Y = 1 \mid U = 0) = 0,$$

$$p_{1|1} := P(Y = 1 \mid U = 1) = q, \quad p_{0|1} := P(Y = 0 \mid U = 1) = 1 - q.$$

Megegyezik a bináris szorzás által leírt csatornával.

A két csatorna összekapcsolása az alábbi csatornát eredményezi:





Átmenetvalószínűségek:

$$\begin{aligned}
 p_{0|0} &:= P(Y = 0 \mid X = 0) = 1 - p + p(1 - q) = 1 - pq, & p_{1|0} &:= P(Y = 1 \mid X = 0) = pq, \\
 p_{1|1} &:= P(Y = 1 \mid X = 1) = q, & p_{0|1} &:= P(Y = 0 \mid X = 1) = 1 - q.
 \end{aligned}$$

Legyen $p = 1/3$, $q = 3/4$. Ekkor

$$p_{0|0} = 3/4 = p_{1|1} \quad \text{és} \quad p_{1|0} = 1/4 = p_{0|1}$$

azaz egy olyan szimmetrikus bináris X-csatorna, ahol a tévesztés valószínűsége $1/4$. Kapacitása:

$$C = 1 - H_2(1/4) = 1 - \frac{1}{4} \log_2 4 - \frac{3}{4} \log_2 \left(\frac{4}{3} \right) = \frac{3}{4} \log_2 3 - 1 = 0.1887 \text{ bit.}$$

Példa

Kapcsoljunk egymás után n darab szimmetrikus bináris csatornát. Mutassuk meg, hogy ha a csatornák mindegyike azonos p valószínűséggel hibázik, akkor az összekapcsolt csatorna ekvivalens egy olyan szimmetrikus bináris csatornával, ahol a hiba valószínűsége

$$q_n = \frac{1}{2}(1 - (1 - 2p)^n), \quad n = 1, 2, \dots$$

Megoldás. Teljes indukció.

- Legyen $n = 1$. Ekkor $q_1 = p$, azaz teljesül az állítás.
- Tegyük fel, hogy az állítás igaz az $n = k$ esetben, azaz k darab szimmetrikus bináris csatorna összekapcsolása egy olyan szimmetrikus bináris csatornát eredményez, ahol a hiba valószínűsége

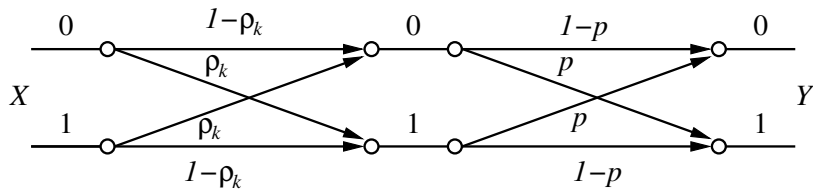
$$q_k = \frac{1}{2}(1 - (1 - 2p)^k).$$

- Legyen most $n = k + 1$. Az indukciós feltétel alapján a vizsgálandó csatorna egy q_k és egy p valószínűséggel hibázó szimmetrikus bináris csatorna összekapcsolásával áll elő.

Megoldás

Indukciós feltétel: Az $n = k$ eset egy olyan szimmetrikus bináris csatornát eredményez, ahol a hiba valószínűsége $\varrho_k = \frac{1}{2}(1 - (1 - 2p)^k)$.

Indukciós lépés: $n = k + 1$ eset.



Átmenetvalószínűségek:

$$\begin{aligned} p_{1|0} &= (1 - \varrho_k)p + \varrho_k(1 - p) = \left[1 - \frac{1}{2}(1 - (1 - 2p)^k)\right]p + \frac{1}{2}(1 - (1 - 2p)^k)(1 - p) \\ &= p - \frac{1}{2}(1 - (1 - 2p)^k)p + \frac{1}{2}(1 - (1 - 2p)^k)(1 - p) = p + \frac{1}{2}(1 - (1 - 2p)^k)(1 - 2p) \\ &= p + \frac{1}{2} - p - \frac{1}{2}(1 - 2p)^{k+1} = \frac{1}{2}(1 - (1 - 2p)^{k+1}) = \varrho_{k+1}. \end{aligned}$$

A szimmetria miatt $p_{1|0} = p_{0|1} = \varrho_{k+1}$ és $p_{0|0} = p_{1|1} = 1 - \varrho_{k+1}$, azaz az $n = k + 1$ eset egy ϱ_{k+1} eséllyel hibázó szimmetrikus bináris csatornát eredményez. \square

Keresési probléma

Feladat. 9 darab azonos kinézetű pénzérme közül az egyik hamis, könnyebb mint a többi. Egy kétkarú mérleg segítségével legkevesebb hány méréssel található meg a hamis érme?

Matematikai átfogalmazás. Számozzuk meg az érméket 1-től 9-ig.

X : a hamis érme sorszáma; egyenletes eloszlású, azaz $P(X = k) = 1/9$, $k = 1, 2, \dots, 9$.

A hamis érme megtalálásához szükséges információmennyiség: $H(X) = \log_2 9 = 2 \log_2 3$ bit.

Mérlegelés: a mérleg serpenyőibe azonos számú érmét kell tennünk. Azt tudjuk eldönteni, fent van-e a mérlegen a hamis érme és ha igen, melyik serpenyőn.

A_1 : a mérleg bal serpenyőjében lévő érmék halmaza;

A_2 : a mérleg jobb serpenyőjében lévő érmék halmaza;

A_0 : a mérlegre fel nem került érmék halmaza.

Y : a mérlegelés eredménye. Megadja, egy adott mérésnél a három halmaz közül melyikben van a hamis érme. Értékei: $\{0, 1, 2\}$.

A hamis érme sorszámaról egy méréssel megszerezhető információ: $I(X; Y)$.

Optimális stratégia

$X \in \{1, 2, \dots, 9\}$: a hamis érme sorszáma; egyenletes eloszlású.

A hamis érme megtalálásához szükséges információmennyiség: $H(X) = \log_2 9 = 2 \log_2 3$ bit.

$Y \in \{0, 1, 2\}$: a mérlegelés eredménye. Megadja, hogy egy adott mérésnél az A_1 (bal serpenyő), az A_2 (jobb serpenyő), vagy az A_0 (nincs a mérlegen) halmazban van a hamis érme.

A hamis érme sorszámaról egy méréssel megszerezhető információ: $I(X; Y)$.

X értéke meghatározza az Y értékét: létezik $f: \mathbb{R} \rightarrow \mathbb{R}$, hogy $Y = f(X)$.

$$I(X; Y) = H(Y), \quad \text{ahol} \quad H(Y) \leq \log_2 3; \quad H(Y) = \log_2 3 \iff P(Y = k) = \frac{1}{3}, \quad k = 0, 1, 2.$$

Egy mérés akkor adja a maximális információmennyiséget, ha mindhárom halmaz ugyanannyi érmét tartalmaz.

Optimális stratégia:

① 3 – 3 érme a mérleg serpenyőibe. Nyert információmennyiség: $\log_2 3$ bit.

② 1 – 1 érme a mérleg serpenyőibe. Nyert információmennyiség: $\log_2 3$ bit.

Két mérés elegendő a $2 \log_2 3$ bit információ megszerzéséhez.

Stratégiaiák összehasonlítása

Az első mérés lehetséges stratégiái:

Mérlegre tett érmék száma	Az Y eloszlása			Az első mérés által nyert információ mennyisége, $H(Y)$
	$P(Y=0)$	$P(Y=1)$	$P(Y=2)$	
1 – 1	7/9	1/9	1/9	$2 \log_2 3 - \frac{7}{9} \log_2 7 = 0.9864$
2 – 2	5/9	2/9	2/9	$2 \log_2 3 - \frac{5}{9} \log_2 5 - \frac{4}{9} = 1.4355$
3 – 3	1/3	1/3	1/3	$\log_2 3 = \mathbf{1.5850}$
4 – 4	1/9	4/9	4/9	$2 \log_2 3 - 16/9 = 1.3921$

Egyes mérési stratégiák várható mérésszámai:

1. mérés	2. mérés	3. mérés	Várható mérésszám
1 – 1	2 – 2	1 – 1	$1 \cdot 2/9 + 3 \cdot 7/9 = 23/9 > 2$
1 – 1	3 – 3	1 – 1	$1 \cdot 2/9 + 2 \cdot 1/9 + 3 \cdot 6/9 = 22/9 > 2$
2 – 2	1 – 1	1 – 1	$2 \cdot 6/9 + 3 \cdot 3/9 = 21/9 > 2$
3 – 3	1 – 1	–	2
4 – 4	1 – 1	1 – 1	$1 \cdot 1/9 + 2 \cdot 4/9 + 3 \cdot 4/9 = 21/9 > 2$

Mérési stratégiák ábrázolása

Trináris fa: minden csomópontból legfeljebb 3 ág indul ki. Megad egy trináris prefix kódot.

Levelek: az egyes pénzérmék.

Csomópontok: az egyes méréseket jelentik.

Kimenő ágak indexei: az egyes halmazok (1: bal serpenyő; 2: jobb serpenyő; 0: kimarad).

Példa. 3 – 3; 1 – 1 stratégia. Trináris prefix kód:

$$\mathcal{K} = \{00, 01, 02, 10, 11, 12, 20, 21, 22\}.$$

Eloszlás:

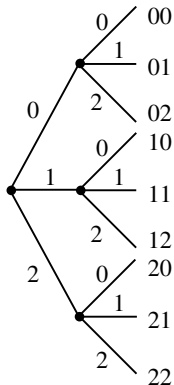
$$\mathcal{P} = \{1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9\}.$$

Kódszóhosszak:

$$\mathcal{L} = \{2, 2, 2, 2, 2, 2, 2, 2, 2\}.$$

Átlagos kódszóhossz (várható mérésszám):

$$E(\mathcal{K}) = 2 = \frac{2 \log_2 3}{\log_2 3} = \frac{H(X)}{\log_2 3} \implies \text{optimális kód.}$$



Példa. 1 – 1; 3 – 3; 1 – 1 stratégia

Trináris prefix kód:

$$\mathcal{K} = \{00, 010, 011, 012, 020, 021, 022, 1, 2\}.$$

Eloszlás:

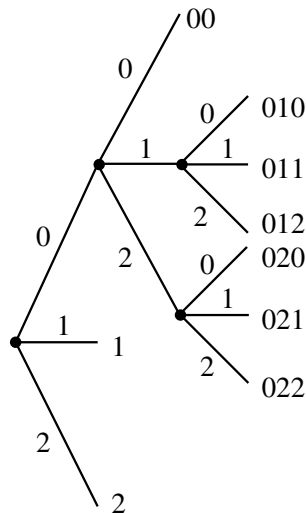
$$\mathcal{P} = \{1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9\}.$$

Kódszóhosszak:

$$\mathcal{L} = \{2, 3, 3, 3, 3, 3, 3, 1, 1\}.$$

Átlagos kódszóhossz (várható mérésszám):

$$E(\mathcal{K}) = 2 \cdot \frac{1}{9} + 3 \cdot 6 \cdot \frac{1}{9} + 2 \cdot 1 \cdot \frac{1}{9} = \frac{22}{9} > \frac{H(X)}{\log_2 3}.$$



Példa

7 darab azonos kinézetű pénzérme közül az egyik hamis, könnyebb mint a többi. A hamis érme megtalálására ismét egy kétkarú mérleg áll rendelkezésre. Adjon optimális keresési stratégiát, ha az egyik érme gyanús, háromszor akkora eséllyel hamis, mint a többi.

Megoldás. Számozzuk meg az érmeket 1-től 7-ig, legyen 1 a gyanús érme sorszáma.

X : a hamis érme sorszáma. Eloszlása: $\mathcal{P} = \{1/3, 1/9, 1/9, 1/9, 1/9, 1/9, 1/9\}$.

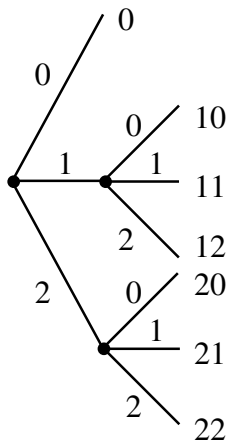
Optimális trináris prefix kód (Huffman-kód): $\mathcal{K} = \{0, 10, 11, 12, 20, 21, 22\}$.

Kódszóhosszak: $\mathcal{L} = \{1, 2, 2, 2, 2, 2, 2\}$.

Átlagos kódszóhossz (várható mérésszám):

$$E(\mathcal{K}) = 1 \cdot \frac{1}{3} + 2 \cdot 6 \cdot \frac{1}{9} = \frac{15}{9} = \frac{5}{3} = \frac{H(X)}{\log_2 3}.$$

A kód optimális. **Az optimális stratégia:** 3 – 3, 1 – 1.



Példa

Legyen ismét 9 számozott érménk és legyen újra X a hamis érme sorszáma, melynek eloszlása.

$$\mathcal{P} = \{1/3, 1/9, 1/9, 1/9, 1/9, 1/9, 1/27, 1/27, 1/27\}.$$

Optimális trináris prefix kód (Huffman-kód):

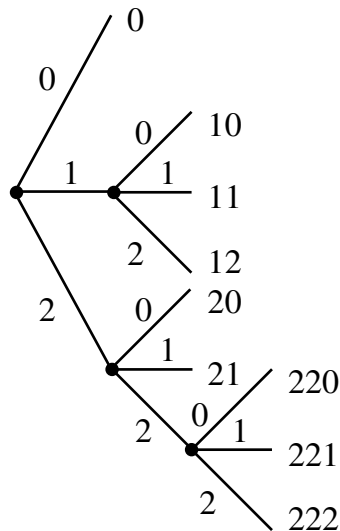
$$\mathcal{K} = \{0, 10, 11, 12, 20, 21, 220, 221, 222\}.$$

Kódszóhosszak: $\mathcal{L} = \{1, 2, 2, 2, 2, 2, 3, 3, 3\}.$

Átlagos kódszóhossz (várható mérésszám):

$$E(\mathcal{K}) = 1 \cdot \frac{1}{3} + 2 \cdot 5 \cdot \frac{1}{9} + 3 \cdot 3 \cdot \frac{1}{27} = \frac{16}{9} = \frac{H(X)}{\log_2 3}.$$

Probléma. Az optimális prefix kód nem ad **megengedett** keresési stratégiát. Az első csomópontnál nincs két olyan ág, amin egyenlő számú levél van, azaz a mérleg serpenyőire **nem** egyenlő számú érme kerül.



n darab azonos kinézetű pénzérme közül az egyik hamis, könnyebb mint a többi. Egy kétkarú mérleg segítségével keressük meg a hamis érmét, átlagosan a lehető legkevesebb mérést végezve.

Megoldás. Az érméket minden mérésnél három csoportba kell osztanunk (A_0, A_1, A_2) , amiből kettő (A_1, A_2) azonos számosságú (az ezekben levő érmék kerülnek a mérleg serpenyőibe).

$Y \in \{0, 1, 2\}$: a mérlegelés eredménye. Megadja, hogy a három halmaz közül melyikben van a hamis érme.

A mérés által szolgáltatott információmennyiség $H(Y)$, ami akkor a maximális, ha Y egyenletes eloszlású. Elegendő egy mérést vizsgálni, utána rekurzívan haladhatunk tovább.

Három esetet különböztetünk meg: $n = 3k$, $n = 3k + 1$, vagy $n = 3k - 1$.

1. $n = 3k$: mindhárom csoportba k darab érme kerül. $H(Y) = \log_2 3$, ami a $H(Y)$ maximuma.

Megoldás

2. $n = 3k + 1$: az egyenleteshez legközelebbi megoszlások: k és k a mérlegre, $k + 1$ kimarad, vagy $k + 1$ és $k + 1$ a mérlegre, $k - 1$ kimarad.

Entrópia a k és k esetben:

$$H_1(k) := \frac{2k}{3k+1} \log_2 \left(\frac{3k+1}{k} \right) + \frac{k+1}{3k+1} \log_2 \left(\frac{3k+1}{k+1} \right) = \log_2(3k+1) - \frac{2k}{3k+1} \log_2 k - \frac{k+1}{3k+1} \log_2(k+1).$$

Entrópia a $k + 1$ és $k + 1$ esetben:

$$H_2(k) := \frac{2(k+1)}{3k+1} \log_2 \left(\frac{3k+1}{k+1} \right) + \frac{k-1}{3k+1} \log_2 \left(\frac{3k+1}{k-1} \right) = \log_2(3k+1) - \frac{2(k+1)}{3k+1} \log_2(k+1) - \frac{k-1}{3k+1} \log_2(k-1).$$

Igazolandó: tetszőleges $k \in \mathbb{N}$ esetén $H_1(k) > H_2(k)$.

$$H_1(k) > H_2(k) \quad \Longleftrightarrow \quad 2k \log_2 k < (k+1) \log_2(k+1) + (k-1) \log_2(k-1).$$

Legyen $f(x) := x \log_2 x$, $x > 0$. Ekkor $f'(x) = \log_2 x + (\ln 2)^{-1}$, $f''(x) = (x \ln 2)^{-1} > 0$, azaz f szigorúan konvex. Emiatt

$$k \log_2 k = f(k) = f\left(\frac{1}{2}(k+1) + \frac{1}{2}(k-1)\right) < \frac{1}{2}f(k+1) + \frac{1}{2}f(k-1) = \frac{1}{2}[(k+1) \log_2(k+1) + (k-1) \log_2(k-1)].$$

Megoldás

3. $n = 3k - 1$: k és k a mérlegre, $k - 1$ kimarad, vagy $k - 1$ és $k - 1$ a mérlegre, $k + 1$ kimarad.

Entrópia a k és k esetben:

$$H_1(k) := \log_2(3k - 1) - \frac{2k}{3k - 1} \log_2 k - \frac{k - 1}{3k - 1} \log_2(k - 1).$$

Entrópia a $k - 1$ és $k - 1$ esetben:

$$H_2(k) := \log_2(3k - 1) - \frac{2(k - 1)}{3k - 1} \log_2(k - 1) - \frac{k + 1}{3k - 1} \log_2(k + 1).$$

Igazolandó: tetszőleges $k \in \mathbb{N}$ esetén $H_1(k) > H_2(k)$.

$$H_1(k) > H_2(k) \iff 2k \log_2 k < (k - 1) \log_2(k - 1) + (k + 1) \log_2(k + 1),$$

ami teljesül, mivel $f(x) = x \log_2 x$, szigorúan konvex, ha $x > 0$.

Mindhárom vizsgált esetben ($n = 3k$, $n = 3k + 1$, $n = 3k - 1$) a mérleg serpenyőibe $k - k$ érmét kell tennünk. □

Van n darab egyforma pénzérménk, melyek közül az egyik hamis. A hamis érme azonos eséllyel könnyebb vagy nehezebb, mint a többi. Ha egy kétkarú mérleg segítségével szeretnénk megtalálni a hamis érmét, mennyi érmét kell egyszerre a mérlegre tennünk, hogy a mérés a lehető legtöbb információt szolgáltatassa?

Megoldás. Legyen X a hamis érme sorszáma, ami egyenletes eloszlású. Az X értékének meghatározásához $H(X) = \log_2 n$ bit információra van szükség.

Tegyük $k - k$ érmét a mérlegre. Y : a mérlegelés eredménye. Értékei:

-1 : a **bal** serpenyő a könnyebb; 0 : a mérleg **egyensúly**ban van; 1 : a **jobb** serpenyő a könnyebb.

$$P(Y = 1|X = \ell) = P(Y = -1|X = \ell) = \begin{cases} \frac{1}{2}, & \text{ha az } \ell \text{ indexű érme a mérlegen van,} \\ 0, & \text{egyébként;} \end{cases}$$

$$P(Y = 0|X = \ell) = \begin{cases} 0, & \text{ha az } \ell \text{ indexű érme a mérlegen van,} \\ 1, & \text{egyébként.} \end{cases}$$

Ezek alapján:

$$H(Y|X = \ell) = \begin{cases} 2 \cdot \frac{1}{2} \log_2 2 = 1, & \text{ha az } \ell \text{ indexű érme a mérlegen van,} \\ 0, & \text{egyébként.} \end{cases}$$

Megoldás

X : a hamis érme sorszáma. $P(X = \ell) = \frac{1}{n}$, $\ell = 1, 2, \dots, n$.

$k - k$ érme a mérlegen. $Y \in \{-1, 0, 1\}$: a mérlegelés eredménye.

$$H(Y|X = \ell) = \begin{cases} 1, & \text{ha az } \ell \text{ indexű érme a mérlegen van,} \\ 0, & \text{egyébként.} \end{cases}$$

Feltételes entrópia:

$$H(Y|X) = \sum_{\ell=1}^n H(Y|X = \ell)P(X = \ell) = \frac{2k}{n}.$$

Y eloszlása:

$$P(Y = 1) = \sum_{\ell=1}^n P(Y = 1|X = \ell)P(X = \ell) = \frac{1}{2} \cdot \frac{2k}{n} = \frac{k}{n} = P(Y = -1), \quad P(Y = 0) = \frac{n - 2k}{n}.$$

Y entrópiája:

$$H(Y) = 2 \cdot \frac{k}{n} \log_2 \frac{n}{k} + \frac{n - 2k}{n} \log_2 \frac{n}{n - 2k}.$$

Megoldás

X : a hamis érme sorszáma. $Y \in \{-1, 0, 1\}$: a mérlegelés eredménye. $k - k$ érme a mérlegen.

$$H(Y|X) = \frac{2k}{n}, \quad H(Y) = \frac{2k}{n} \log_2 \frac{n}{k} - \frac{n-2k}{n} \log_2 \frac{n}{n-2k}.$$

Kölcsönös információ:

$$I(X; Y) = H(Y) - H(Y|X) = \frac{2k}{n} \log_2 \frac{n}{k} + \frac{n-2k}{n} \log_2 \frac{n}{n-2k} - \frac{2k}{n} = \frac{2k}{n} \log_2 \frac{n}{2k} + \frac{n-2k}{n} \log_2 \frac{n}{n-2k} = H_2\left(\frac{2k}{n}\right),$$

ahol $H_2(p) := -p \log_2 p - (1-p) \log_2 (1-p)$.

$$H_2(p) \leq 1 \quad \text{és} \quad H_2(p) = 1 \iff p = \frac{1}{2}.$$

Egy mérés pontosan akkor adja a lehető legtöbb információt, ha

$$\frac{2k}{n} = \frac{1}{2} \iff k = \frac{n}{4}.$$

Egy ilyen méréssel, ami 1 bit információt szolgáltat, megfelezzük a vizsgálandó érmék mennyiségét. Ha $n = 2^m$, akkor m lépésben megtaláljuk a hamis érmét; megkapjuk a szükséges $\log_2 n = m$ bit információt. \square

Hibakeresés

Feladat. Egy Európát Észak-Amerikával összekötő kábel víz alatti szakaszán 7 automata erősítőállomás van, melyek közül az egyik meghibásodott. A hibás erősítőt úgy lokalizálják, hogy valahol rácsatlakoznak a kábelre, majd mindkét irányba elindítanak egy jelet. Amelyik irányba nem megy át, arra keresnek tovább. Adjon meg egy a legkisebb átlagos mérésszámot biztosító optimális keresési stratégiát, ha az A, B, C, D, E, F és G erősítők meghibásodási valószínűségei rendre $\frac{1}{4}$, $\frac{1}{16}$, $\frac{1}{16}$, $\frac{1}{4}$, $\frac{1}{16}$, $\frac{1}{16}$, $\frac{1}{4}$.

A keresési stratégia reprezentálható egy bináris fagráffal, azaz egy bináris prefix kóddal.

Csomópontok: az egyes mérések.

A kódjelek jelentése

- 0: a hibás erősítő balra van;
- 1: a hibás erősítő jobbra van.

A kapott bináris kód átlagos kódszóhossza megadja az átlagos mérésszámot.

Megoldás.

Forrásábécé:

$$\mathcal{X} = \{A, B, C, D, E, F, G\}.$$

A forrásábécé eloszlása:

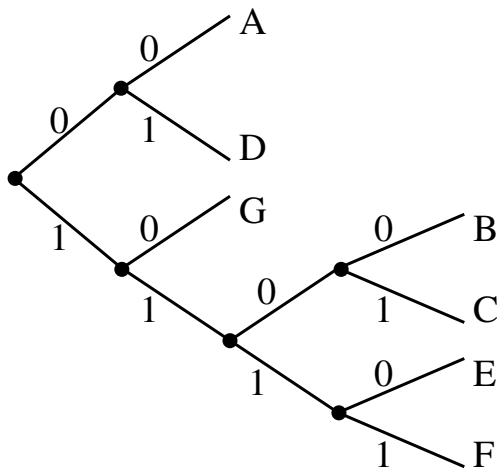
$$\mathcal{P} = \left\{ \frac{1}{4}, \frac{1}{16}, \frac{1}{16}, \frac{1}{4}, \frac{1}{16}, \frac{1}{16}, \frac{1}{4} \right\}.$$

Optimális bináris prefix kód (Huffman-kód):

$$\mathcal{K} = \{00, 1100, 1101, 01, 1110, 1111, 10\}.$$

Probléma. Az optimális prefix kód nem ad [megengedett](#) keresési stratégiát. Az első lépésben a D és G erősítő között kellene a kábelre csatlakozni, mely erősítők nem szomszédosak.

A gondot a Huffman-kódoláshoz szükséges sorbarendeázés okozza. Javaslat: [Gilbert-féle kód](#).



Megoldás.

Gilbert-féle kód:

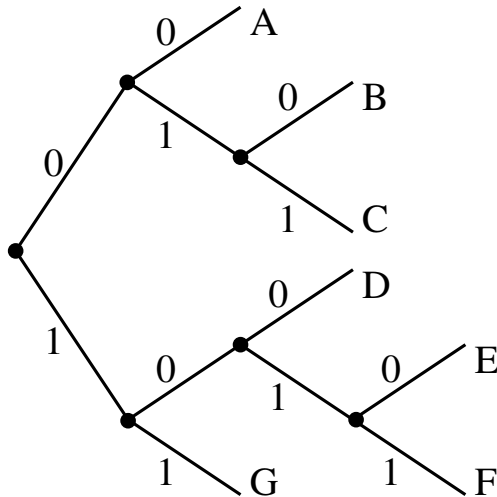
Erősítő	p	L	r	$2^L r$	Kód	Opt. kód
A	1/4	3	1/8	1	00 1	00
B	1/16	5	9/32	9	0100 1	010
C	1/16	5	11/32	11	010 1 1	011
D	1/4	3	1/2	4	100	100
E	1/16	5	21/32	21	1010 1	1010
F	1/16	5	23/32	23	1011 1	1011
G	1/4	3	7/8	7	11 1	11

Keresési stratégia:

- 1 Mérés C és D között;
- 2 Mérés A és B között, vagy F és G között.
- ...

Az optimalizált kód átlagos kódszóhossza: $21/8$.

Átlagos mérésszám: $21/8$.



Programot akarunk írni, mely az $1 - 100$ természetes számokat besorolja az

$$1 - 10, 11 - 20, 21 - 30, 31 - 50, 51 - 90, 91 - 100$$

osztályokba oly módon, hogy a bemenetül megadott számot összehasonlítja a $10, 20, 30, 50, 90$ osztályhatárok valamelyikével, majd újabb összehasonlítások segítségével meghatározza az alkalmas csoportot. Adjon meg egy optimális, azaz átlagosan a legkevesebb összehasonlítást igénylő algoritmust, ha minden szám egyformán valószínű.

Megoldás. Az összehasonlítások egy bináris fa csomópontjainak felelnek meg, aminek megfeleltethető egy az egyes osztályokat leíró bináris kód. Keressük azt az osztályok sorrendjét megőrző bináris kódot, melynek a legkisebb az átlagos kódszóhossza. Az egyes csoportok valószínűségei: $\mathcal{P} = \{0.1, 0.1, 0.1, 0.2, 0.4, 0.1\}$.

Meg kell határoznunk a fenti eloszláshoz tartozó Gilbert-féle kódot, majd a kapott kódot optimalizálnunk kell.

Megoldás.

Gilbert-féle kód:

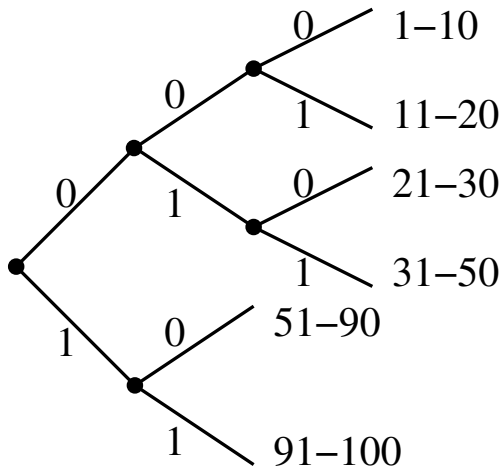
Osztály	p	L	r	$2^L r$	Kód	Opt. kód
1-10	0.1	5	0.05	1	000 01	000
11-20	0.1	5	0.15	4	001 00	001
21-30	0.1	5	0.25	8	010 00	010
31-50	0.2	4	0.4	6	011 0	011
51-90	0.4	3	0.7	5	10 1	10
91-100	0.1	5	0.95	30	11 110	11

Keresési stratégia:

- 1 Összehasonlítás 50-nel;
- 2 Összehasonlítás 20-szal, vagy 90-nel;
- ⋮

Az optimalizált kód átlagos kódszóhossza: 2.5.

Átlagos összehasonlítószám: 2.5.

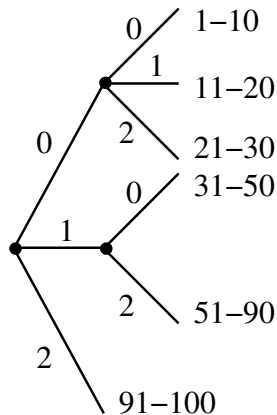


Példa

Oldjuk meg az előző feladatot arra az esetre is, ha az algoritmus a bemenetül megadott számot a 10, 20, 30, 50, 90 osztályhatárok közül kettővel hasonlítja össze.

Megoldás. Jelölje LB és UB egy adott összehasonlításnál az alsó, illetve felső határt, X pedig legyen a bemenetül megadott szám. Az összehasonlításnak három kimenete lehet: $X \leq LB$, $LB < X \leq UB$, vagy $X > UB$. Ez leírható egy trináris kóddal, ahol rendre 0, 1, illetve 2 jelöli az egyes kimeneteket. Gilbert-féle trináris kód:

Osztály	p	L	r	$3^L r$	Kód	Opt. kód
1-10	0.1	4	0.0(3)	2	00 02	00
11-20	0.1	4	0.1(3)	10	01 01	01
21-30	0.1	4	0.2(3)	18	02 00	02
31-50	0.2	3	0.3(6)	9	1 00	10
51-90	0.4	2	0.6(3)	5	12	12
91-100	0.1	4	0.9(3)	75	2 210	2



Keresési stratégia:

- ❶ $LB = 30$ és $UB = 90$;
- ❷ $LB = 10$ és $UB = 20$ vagy $LB = 50$;

Átlagos összehasonlításszám: 1.9.

Infomációforrások

\mathbb{X} : **információforrás**, az X_1, X_2, \dots valószínűségi változók végtelen sorozata. A forrás az i -edik időpontban az X_i értéket veszi fel. Mindegyik valószínűségi változó ugyanazon $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ forrásábécéből veszi fel az értékeit.

Az \mathbb{X} forrás **emlékezet nélküli**, ha az X_1, X_2, \dots változók függetlenek.

Az \mathbb{X} forrás **stacionárius**, ha az X_1, X_2, \dots sorozat stacionárius, azaz minden $n, k \in \mathbb{N}$ esetén az X_1, X_2, \dots, X_n véletlen vektor és az eltolt $X_{k+1}, X_{k+2}, \dots, X_{k+n}$ vektor együttes eloszlása megegyezik.

$\mathcal{Y} = \{y_1, y_2, \dots, y_s\}$: csatornaábécé. \mathcal{Y}^* : az \mathcal{Y} elemeiből álló véges sorozatok halmaza.

Betűnkénti kódolás: egy közlemény kódját az egyes forrásbetűk kódjainak egymás után írásával kapjuk.

Blokk kódolás: a forrásüzenetet k hosszúságú blokkokra bontjuk és a blokkokat kódoljuk. Formálisan egy $f : \mathcal{X}^k \rightarrow \mathcal{Y}^*$ kód, ahol \mathcal{X}^k az új forrásábécé.

Infomációforrások változó szóhosszú kódolása

Egyértelműen dekódolható blokk kódolás $k \geq 1$ blokkhosszal: $f : \mathcal{X}^k \rightarrow \mathcal{Y}^*$.

Cél: az egy forrásbetűre jutó L átlagos kódszóhossz minimalizálása.

\mathbb{X} emlékezet nélküli és stacionárius, betűnkénti kódolás. Egy k hosszúságú üzenet kódjára

$$L = \frac{1}{k} \mathbb{E}(|f(X_1)| + \dots + |f(X_k)|) = \mathbb{E}|f(X_1)|.$$

Shannon tétel: $\mathbb{E}|f(X_1)| \geq \frac{H(X_1)}{\log_2 s}$ és létezik f^* prefix kód, melyre $\mathbb{E}|f^*(X_1)| < \frac{H(X_1)}{\log_2 s} + 1$.

Blokkonkénti kódolás $f : \mathcal{X}^k \rightarrow \mathcal{Y}^*$ kódolóval.

$$L = \frac{1}{k} \mathbb{E}(|f(X_1, \dots, X_k)|) \geq \frac{1}{k} \frac{H(X_1, \dots, X_k)}{\log_2 s} \underset{\text{függetlenség}}{=} \frac{H(X_1)}{\log_2 s}.$$

Minden k -re létezik olyan L betűnkénti átlagos kódszóhosszú $f : \mathcal{X}^k \rightarrow \mathcal{Y}^*$ prefix kód, melyre

$$L < \frac{H(X_1)}{\log_2 s} + \frac{1}{k}.$$

Általánosabb információforrások kódolása

Definíció. Az $\mathbb{X} = X_1, X_2, \dots$ forrás *forrásentrópiája* a

$$H(\mathbb{X}) = \lim_{n \rightarrow \infty} n^{-1} H(X_1, X_2, \dots, X_n)$$

menyiség, amennyiben a határérték létezik.

Tétel. Ha az $\mathbb{X} = X_1, X_2, \dots$ forrás stacionárius, akkor létezik a forrásentrópiája, és

$$H(\mathbb{X}) = \lim_{n \rightarrow \infty} H(X_n | X_1, X_2, \dots, X_{n-1}).$$

Megjegyzés. Stacionárius forrásra $H(\mathbb{X}) \leq H(X_1)$, egyenlőség pedig pontosan akkor teljesül, ha a forrás emlékezet nélküli.

Tétel. Ha az $\mathbb{X} = X_1, X_2, \dots$ stacionárius forrást blokkonként kódoljuk az $f : \mathcal{X}^k \rightarrow \mathcal{Y}^*$ egyértelműen dekódolható kóddal, akkor a kód L betűnkénti átlagos kódszóhosszára teljesül az

$$L \geq H(\mathbb{X}) / \log_2 s$$

egyenlőtlenség. A k blokhosszt elég nagyra választva létezik olyan kód, amelynek L betűnkénti átlagos kódszóhossza tetszőlegesen megközelíti a fenti alsó korlátot.

Állandó hosszúságú blokk-kódok

Változó szóhosszú forráskódolás problémája: ha egy kódszó meghibásodik, gond lehet az utána következő összes további kódszó dekódolásával. Fix hosszú kódoknál nincs ilyen probléma.

\mathcal{X} , \mathcal{Y} : n -elemű forrás-, illetve s -elemű csatornaábéce.

Az $f : \mathcal{X}^k \rightarrow \mathcal{Y}^m$ kód egyértelműen dekódolható, ha

$$n^k \leq s^m.$$

Betűnkénti átlagos kódszóhossz:

$$L = \frac{m}{k} \geq \frac{\log_2 n}{\log_2 s}.$$

A feltétel elégséges is az egyértelműen dekódolható $f : \mathcal{X}^k \rightarrow \mathcal{Y}^m$ kód létezésére.

A forrás entrópiája csak akkor $\log_2 n$, ha emlékezet nélküli, stacionárius és egyenletes eloszlású. Állandó hosszú kódszavakkal nem tudjuk tetszőlegesen közelíteni a forrásentrópiát, bár-mekkora is a k blokkhossz.

Forráskódolás előírt hibavalószínűséggel

$\mathbb{X} = X_1, X_2, \dots$: stacionárius forrás.

k hosszúságú üzenetek egy $B \in \mathcal{X}^k$ halmazának valószínűsége:

$$P(B) := P((X_1, X_2, \dots, X_k) \in B) = \sum_{\mathbf{x} \in B} p(\mathbf{x}),$$

ahol

$$p(\mathbf{x}) := P(X_1 = x_1, X_2 = x_2, \dots, X_k = x_k), \quad \mathbf{x} = (x_1, x_2, \dots, x_k) \in \mathcal{X}^k.$$

Stacionaritás:

$$P(B) = P((X_{n+1}, X_{n+2}, \dots, X_{n+k}) \in B), \quad n = 1, 2, \dots$$

Definíció. Az \mathbb{X} stacionárius forrás $f : \mathcal{X}^k \rightarrow \mathcal{Y}^m$ kódját akkor nevezzük ε -hibával dekódolhatónak ($0 < \varepsilon < 1$), ha létezik olyan $f' : \mathcal{Y}^m \rightarrow \mathcal{X}^k$ dekódoló függvény, hogy a hibás dekódolás valószínűsége legfeljebb ε , azaz

$$P\left(f'(f(X_1, X_2, \dots, X_k)) \neq (X_1, X_2, \dots, X_k)\right) \leq \varepsilon.$$

Az ε -hibával való dekódolhatóság feltétele

Megjegyzés. Az $f : \mathcal{X}^k \rightarrow \mathcal{Y}^m$ pontosan akkor dekódolható ε -hibával, ha f a \mathcal{X}^k egy $1 - \varepsilon$ -nál nagyobb valószínűségű B részhalmazát invertálhatóan képezi le. Így akkor és csak akkor létezik $f : \mathcal{X}^k \rightarrow \mathcal{Y}^m$ ε -hibával dekódolható kód, ha létezik olyan $B \subset \mathcal{X}^k$, melyre $P(B) > 1 - \varepsilon$ és $|B| \leq s^m$ ($|B|$: a B halmaz számossága).

Keresendő egy olyan minimális számosságú $B \subset \mathcal{X}^k$ üzenethalmaz, amelyre $P(B) > 1 - \varepsilon$. Feltétel az m kódszóhosszra: $s^{m-1} < |B| \leq s^m$.

B üzeneteit kölcsönösen egyértelműen kódolhatjuk m hosszú kódszavakkal, a többi üzenetet meg akárhogyan. A kapott ε -hibával dekódolható $f : \mathcal{X}^k \rightarrow \mathcal{Y}^m$ kód optimális, azaz, ha $g : \mathcal{X}^k \rightarrow \mathcal{Y}^{m'}$ ε -hibával dekódolható, akkor $m \leq m'$.

Indexeljük \mathcal{X}^k üzeneteit csökkenő valószínűségek szerint: $p(\mathbf{x}_1) \geq p(\mathbf{x}_2) \geq \dots \geq p(\mathbf{x}_{n^k})$.

$N(k, \varepsilon)$: az az index, melyre

$$\sum_{i=1}^{N(k, \varepsilon)} p(\mathbf{x}_i) > 1 - \varepsilon, \quad \sum_{i=1}^{N(k, \varepsilon)-1} p(\mathbf{x}_i) \leq 1 - \varepsilon.$$

A keresett minimális elemszámú üzenethalmaz: $B_{k, \varepsilon} := \bigcup_{i=1}^{N(k, \varepsilon)} \{\mathbf{x}_i\}$.

Információstabilis források

$f : \mathcal{X}^k \rightarrow \mathcal{Y}^m$: ε -hibával dekódolható kód.

$N(k, \varepsilon)$: az egyértelműen dekódolható üzenetek száma.

$$N(k, \varepsilon) \leq s^m.$$

Betűnkénti átlagos kódszóhossz:

$$L = \frac{m}{k} \geq \frac{\frac{1}{k} \log_2 N(k, \varepsilon)}{\log_2 s}.$$

Keresendő: $\lim_{k \rightarrow \infty} \frac{1}{k} \log_2 N(k, \varepsilon)$.

Definíció. Az $\mathbb{X} = X_1, X_2, \dots$ *stacionárius forrást* **információstabilisnak** nevezzük, ha minden $\delta > 0$ esetén

$$\lim_{k \rightarrow \infty} \mathbb{P} \left(\left| -\frac{1}{k} \log_2 p(X_1, X_2, \dots, X_k) - H(\mathbb{X}) \right| > \delta \right) = 0,$$

azaz az $Y_k := -\frac{1}{k} \log_2 p(X_1, X_2, \dots, X_k)$, $k = 1, 2, \dots$, sorozat sztochasztikusan tart a $H(\mathbb{X})$ forrásentrópiához, ha $k \rightarrow \infty$.

Tipikus halmazok

$\mathbb{X} = X_1, X_2, \dots$: információstabilis forrás, forrásentrópiája $H(\mathbb{X})$.

Megjegyzés. Stacionárius és emlékezet nélküli források információstabilisak.

Tétel. Ha az \mathbb{X} stacionárius forrás információstabilis, akkor minden $0 < \varepsilon < 1$ esetén

$$\lim_{k \rightarrow \infty} \frac{1}{k} \log_2 N(k, \varepsilon) = H(\mathbb{X}).$$

Definíció. Legyen $\varepsilon > 0$. k hosszúságú üzenetek egy $A_{k,\varepsilon}$ halmazát *tipikus halmaznak* nevezzük, ha tetszőleges $\mathbf{x} \in A_{k,\varepsilon}$ esetén

$$2^{-k(H(\mathbb{X})+\varepsilon)} \leq p(\mathbf{x}) \leq 2^{-k(H(\mathbb{X})-\varepsilon)}.$$

- a) tetszőleges $\mathbf{x} \in A_{k,\varepsilon}$ üzenetre $H(\mathbb{X}) - \varepsilon \leq -\frac{1}{k} \log_2 p(\mathbf{x}) \leq H(\mathbb{X}) + \varepsilon$, azaz $p(\mathbf{x}) \approx 2^{-kH(\mathbb{X})}$;
- b) $P(A_{k,\varepsilon}) \geq 1 - \varepsilon$, azaz $P(A_{k,\varepsilon}) \approx 1$;
- c) $|A_{k,\varepsilon}| \leq 2^{k(H(\mathbb{X})+\varepsilon)}$;
- d) ha k elég nagy, akkor $|A_{k,\varepsilon}| \geq (1 - \varepsilon)2^{k(H(\mathbb{X})-\varepsilon)}$, azaz $|A_{k,\varepsilon}| \approx 2^{kH(\mathbb{X})}$.

Az ε -hibavalószínűségű kódolás tétele

Tétel. Legyen az \mathbb{X} stacionárius forrás információstabilis. Ekkor, ha az \mathbb{X} forrás k -hosszú blokkjait ε -hibával ($0 < \varepsilon < 1$) kódoljuk állandó m_k hosszú kódszavakkal, akkor a kódok bármely ilyen tulajdonságú sorozatára

$$\liminf_{k \rightarrow \infty} \frac{m_k}{k} \geq \frac{H(\mathbb{X})}{\log_2 s}.$$

Másrészt, tetszőleges $0 < \varepsilon < 1$ hibavalószínűséghez és $\delta > 0$ számhoz elég nagy k esetén mindig létezik olyan $f : \mathcal{X}^k \rightarrow \mathcal{Y}^{m_k}$ ε -hibával dekódolható kód, hogy

$$L = \frac{m_k}{k} < \frac{H(\mathbb{X})}{\log_2 s} + \delta.$$

$\frac{H(\mathbb{X})}{\log_2 s}$ a betűnkénti átlagos kódszóhossza alsó határa, amit elég nagy k blokkhossz esetén tetszőlegesen meg tudunk közelíteni.

Példa

Tekintsünk egy emlékezet nélküli $\mathbb{X} = X_1, X_2, \dots$ bináris forrást, ahol $P(X_i = 1) = 0.6$ és $P(X_i = 0) = 0.4$, $i = 1, 2, \dots$.

- 1 Adja meg, hogy $k = 25$ hosszúságú blokkok és $\varepsilon = 0.1$ esetén hány elemet tartalmaz az ε -hibával de-kódolható kód $B_{k,\varepsilon}$ minimális elemszámú üzenethalmaza.
- 2 Számítsa ki a forrásentrópiát.
- 3 Adja meg, $\varepsilon = 0.1$ tolerancia mellett milyen sorozatok tartoznak az $A_{k,\varepsilon}$ tipikus halmazba. Mennyi a tipikus halmaz valószínűsége és mekkora a számossága?

Megoldás. Ha $P(X_i = 1) = p$, $P(X_i = 0) = 1 - p$, akkor az (X_1, X_2, \dots, X_k) blokk értékei k -hosszúságú bináris sorozatok.

Azon k -hosszúságú bináris sorozatok száma, amiben ℓ darab 1 van: $\binom{k}{\ell}$, $\ell = 0, 1, 2, \dots, k$.

Egy ilyen x sorozat valószínűsége: $p(x) = p^\ell (1 - p)^{k-\ell}$, $\ell = 0, 1, 2, \dots, k$.

Az egyes x sorozatok darabszáma és valószínűsége, valamint az egy szimbólumra jutó $-\frac{1}{k} \log_2 p(x)$ információmennyiség $p = 0.6$ és $k = 25$ esetén.

ℓ	$\binom{k}{\ell}$	$p(x) = p^\ell (1-p)^{k-\ell}$	$-\frac{1}{k} \log_2 p(x)$	ℓ	$\binom{k}{\ell}$	$p(x) = p^\ell (1-p)^{k-\ell}$	$-\frac{1}{k} \log_2 p(x)$
0	1	1.126×10^{-10}	1.3219281	13	5200300	2.191×10^{-8}	1.0177476
1	25	1.689×10^{-10}	1.2985296	14	4457400	3.287×10^{-8}	0.9943491
2	300	2.533×10^{-10}	1.2751311	15	3268760	4.930×10^{-8}	0.9709506
3	2300	3.800×10^{-10}	1.2517326	16	2042975	7.395×10^{-8}	0.9475521
4	12650	5.700×10^{-10}	1.2283341	17	1081575	1.109×10^{-7}	0.9241536
5	53130	8.555×10^{-10}	1.2049356	18	480700	1.664×10^{-7}	0.9007551
6	177100	1.282×10^{-9}	1.1815371	19	177100	2.496×10^{-7}	0.8773566
7	480700	1.924×10^{-9}	1.1581386	20	530130	3.744×10^{-7}	0.8539581
8	1081575	2.886×10^{-9}	1.1347401	21	12650	5.616×10^{-7}	0.8305596
9	2042975	4.328×10^{-9}	1.1113416	22	2300	8.424×10^{-7}	0.8071611
10	3268760	6.493×10^{-9}	1.0879431	23	300	1.264×10^{-6}	0.7837626
11	4457400	9.739×10^{-9}	1.0645446	24	25	1.895×10^{-6}	0.7603641
12	5200300	1.461×10^{-8}	1.0411461	25	1	2.843×10^{-6}	0.7369656

Megoldás

1. A $B_{k,\varepsilon}$ minimális elemszámú üzenethalmazt úgy lehet elképzelni, mint egy zsákot, amit úgy kell adott súlyúra tölteni, hogy a lehető legkevesebb elem legyen benne. Ezt úgy érhetjük el, ha a legnagyobb valószínűségű üzeneteket használjuk.

A táblázat alapján látható, hogy az egyes sorozatok valószínűsége az ℓ monoton növekvő függvénye. Így elindulva a legnagyobb valószínűségű üzenetektől addig kell az üzeneteket a halmazba rakni, míg el nem érjük a kívánt $\varepsilon = 0.9$ valószínűséget. Az

$$S_K := \sum_{\ell=K}^{25} \binom{25}{\ell} 0.6^\ell 0.4^{25-\ell}$$

kumulatív összegek értékei:

K	25	24	23	...	14	13	12
S_K	2.843×10^{-6}	5.023×10^{-5}	4.2933×10^{-4}	...	0.7322822	0.8462322	0.9221989

Az $\ell \geq 13$ esethez tartozó sorozatok mindegyike kell, valamint néhány, ahol $\ell = 12$, hogy lefedjék a hiányzó 0.05376777 valószínűséget. Ezek száma: $0.05376777 / 1.460814 \times 10^{-8} = 3680672$

A $B_{25,0.1}$ teljes elemszáma: $\sum_{\ell=13}^{25} \binom{25}{\ell} + 3680672 = 16777216 + 3680672 = 20457888.$

Ez rögzített, viszont maga a $B_{25,0.1}$ nem egyértelmű: az 5200300 darab 12 darab egyest tartalmazó üzenetből tetszőlegesen választhatunk ki 3680672 darabot.

Megoldás

2. A $\mathbb{X} = X_1, X_2, \dots$ bináris forrás emlékezet nélküli és stacionárius, azaz

$$H(\mathbb{X}) = H(X_1) = H_2(0.6) = -0.6 \log_2 0.6 - 0.4 \log_2 0.4 = 0.97095 \text{ bit.}$$

3. Az $A_{k,\varepsilon}$ tipikus halmazba azok az x sorozatok tartoznak, melyekre

$$-\frac{1}{k} \log_2 p(x) \in [H(\mathbb{X}) - \varepsilon, H(\mathbb{X}) + \varepsilon].$$

$\varepsilon = 0.1$ és $H(\mathbb{X}) = 0.97095$ esetén ez az intervallum $[0.87095, 1.07095]$.

A táblázat alapján a $11 \leq \ell \leq 19$ esetekhez tartozó összes sorozat tipikus. Ezek együttes valószínűsége

$$\sum_{\ell=11}^{19} \binom{25}{\ell} 0.6^\ell 0.4^{25-\ell} = S_{19} - S_{10} = 0.9362463,$$

számossága pedig

$$\sum_{\ell=11}^{19} \binom{25}{\ell} = 26366510.$$

□

Differenciális entrópia

X : diszkrét valószínűségi változó $\{p_1, p_2, \dots, p_n\}$ eloszlással. X entrópiája:

$$H(X) = - \sum_{i=1}^n p_i \log_2 p_i.$$

Analóg források jellemzése: abszolút folytonos valószínűségi változók.

Definíció. Legyen X egy abszolút folytonos valószínűségi változó $f(x)$ sűrűségfüggvénnyel, melynek tartója $\mathcal{S} \subseteq \mathbb{R}$, azaz $f(x) = 0$, ha $x \notin \mathcal{S}$. Ekkor az X (vagy f) **differenciális entrópiája**

$$H(X) = H(f) := - \int_{\mathcal{S}} f(x) \ln f(x) dx,$$

amennyiben az integrál létezik. Hasonlóan, ha $\mathbf{X} = (X_1, X_2, \dots, X_k)^\top$ egy véletlen vektor $f(\mathbf{x}) = f(x_1, x_2, \dots, x_k)$ együttes sűrűségfüggvénnyel, melynek tartója $\mathcal{S} \subseteq \mathbb{R}^k$, akkor

$$H(\mathbf{X}) = H(X_1, X_2, \dots, X_k) := \int \cdots \int_{\mathcal{S}} f(x_1, x_2, \dots, x_k) \ln f(x_1, x_2, \dots, x_k) dx_1 dx_2 \cdots dx_k,$$

amennyiben az integrál létezik.

Példa. Egyenletes eloszlás

Legyen X egyenletes eloszlású az $[a, b]$ intervallumon, $a \leq b$. Jelölés: $X \sim U(a, b)$. Ekkor

$$f(x) = (b - a)^{-1}, \quad \text{ha } x \in [a, b], \quad \text{és} \quad f(x) = 0, \quad \text{egyébként.}$$

Differenciális entrópia:

$$H(X) = - \int_a^b \frac{1}{b-a} \ln \left(\frac{1}{b-a} \right) dx = \frac{1}{b-a} \ln(b-a) \int_a^b dx = \ln(b-a).$$

$H(X)$ tetszőleges valós értéket felvehet, **negatív is**.

Példa. Normális eloszlás

Legyen X normális eloszlású μ várható értékkel és σ^2 szórásnégyzettel. Jelölés: $\mathcal{N}(\mu, \sigma^2)$. Ekkor

$$f(x) = (2\pi\sigma^2)^{-1/2} \exp \left\{ - (x - \mu)^2 / (2\sigma^2) \right\}, \quad x \in \mathbb{R}.$$

Differenciális entrópia:

$$\begin{aligned} H(X) &= - \int_{\mathbb{R}} f(x) \ln f(x) dx = - \int_{\mathbb{R}} f(x) \left[-\frac{1}{2} \ln(2\pi\sigma^2) - \frac{1}{2\sigma^2} (x - \mu)^2 \right] dx \\ &= \frac{1}{2} \ln(2\pi\sigma^2) \underbrace{\int_{\mathbb{R}} f(x) dx}_1 + \frac{1}{2\sigma^2} \underbrace{\int_{\mathbb{R}} (x - \mu)^2 f(x) dx}_{\text{Var}(X)=\sigma^2} = \frac{1}{2} \left(\ln(2\pi\sigma^2) + 1 \right) = \frac{1}{2} \ln(2\pi e \sigma^2). \end{aligned}$$

A differenciális entrópia tulajdonságai

Tétel.

- a) $-\infty \leq H(X) \leq \infty$.
- b) Tetszőleges c konstans esetén $H(X + c) = H(X)$, azaz a differenciális entrópia eltolásinvariáns.
- c) Tetszőleges abszolút folytonos X valószínűségi változó és $a \in \mathbb{R}$ konstans esetén
$$H(aX) = H(X) + \ln |a|.$$
- d) Ha (X, Y) együttes eloszlása abszolút folytonos, valamint $H(X)$ és $H(Y)$ véges, akkor $H(X, Y)$ létezik és véges,

$$H(X, Y) \leq H(X) + H(Y),$$

az egyenlőség pedig pontosan akkor teljesül, ha X és Y független.

Általánosan: ha X_1, X_2, \dots, X_k együttes eloszlása abszolút folytonos és mindegyik változó differenciális entrópiája véges, akkor $H(X_1, X_2, \dots, X_k)$ létezik és véges,

$$H(X_1, X_2, \dots, X_k) \leq H(X_1) + H(X_2) + \dots + H(X_k),$$

egyenlőség pedig pontosan akkor teljesül, ha X_1, X_2, \dots, X_k teljesen függetlenek.

Példa

Határozza meg az alábbi eloszlások differenciális entrópiáját.

- 1 $\lambda > 0$ paraméterű exponenciális eloszlás.
- 2 $\lambda > 0$ paraméterű Laplace eloszlás, melynek sűrűségfüggvénye $f(x) = \frac{1}{2}\lambda e^{-\lambda|x|}$, $x \in \mathbb{R}$.

Megoldás. 1. Ha X exponenciális eloszlású $\lambda > 0$ paraméterrel, akkor sűrűségfüggvénye

$$f(x) = \lambda e^{-\lambda x}, \quad \text{ha } x \geq 0, \quad \text{és} \quad f(x) = 0, \quad \text{egyébként.}$$

Differenciális entrópia:

$$H(X) = - \int_0^{\infty} f(x) \ln f(x) dx = - \int_0^{\infty} f(x) [\ln \lambda - \lambda x] dx = - \ln \lambda \underbrace{\int_0^{\infty} f(x) dx}_1 + \lambda \underbrace{\int_0^{\infty} x f(x) dx}_{EX=1/\lambda} = 1 - \ln \lambda.$$

2. Az Y Laplace eloszlású valószínűségi változó differenciális entrópiája:

$$H(Y) = - \int_{-\infty}^{\infty} f(x) \left[\ln \frac{\lambda}{2} - \lambda|x| \right] dx = - \ln \frac{\lambda}{2} + \lambda \int_{-\infty}^{\infty} |x| \frac{1}{2} \lambda e^{-\lambda|x|} dx = - \ln \frac{\lambda}{2} + \lambda \underbrace{\int_0^{\infty} x \lambda e^{-\lambda x} dx}_{1/\lambda} = 1 - \ln \frac{\lambda}{2}.$$



Példa

Határozza meg az X valószínűségi változó differenciális entrópiáját, ha sűrűségfüggvénye

$$f(x) = \frac{1}{x(\ln x)^2}, \quad \text{ha } x \geq e, \quad \text{és} \quad f(x) = 0, \quad \text{egyébként.}$$

Megoldás. Az $f(x)$ függvény tényleg sűrűségfüggvényt határoz meg:

$$\int_e^\infty \frac{1}{x(\ln x)^2} dx = \int_e^\infty \frac{(\ln x)'}{(\ln x)^2} dx = \int_1^\infty \frac{1}{y^2} dy = \left[-\frac{1}{y} \right]_{y=1}^{y=\infty} = 1.$$

Differenciális entrópia:

$$\begin{aligned} H(X) &= - \int_e^\infty \frac{1}{x(\ln x)^2} \ln \left(\frac{1}{x(\ln x)^2} \right) dx = \int_e^\infty \frac{1}{x(\ln x)^2} \left[\ln x + \underbrace{\ln(\ln x)^2}_{\geq 0} \right] dx \geq \int_e^\infty \frac{1}{x(\ln x)^2} \ln x dx \\ &= \int_e^\infty \frac{1}{x \ln x} dx = \int_e^\infty \frac{(\ln x)'}{\ln x} dx = \int_1^\infty \frac{1}{y} dy = [\ln y]_{y=1}^{y=\infty} = \infty. \end{aligned}$$

□

Maximális differenciális entrópiájú eloszlások

X : diszkrét valószínűségi változó $\{p_1, p_2, \dots, p_n\}$ eloszlással. Ekkor $H(X) \leq \log_2 n$ és egyenlőség pontosan akkor teljesül, ha $p_i = 1/n$, $i = 1, 2, \dots, n$.

Tétel. Legyen X egyenletes eloszlású az $[a, b]$ intervallumon. Ekkor $H(X) = \ln(b - a)$, és tetszőleges $[a, b]$ tartójú abszolút folytonos Y valószínűségi változó esetén (azaz $P(Y \in [a, b]) = 1$) teljesül, hogy $H(Y) \leq H(X)$.

Tétel. Legyen X exponenciális eloszlású $\lambda > 0$ paraméterrel. Ekkor $H(X) = 1 - \ln \lambda$, és tetszőleges nemnegatív abszolút folytonos Y valószínűségi változó esetén, melyre $EY \leq \frac{1}{\lambda} = EX$, teljesül, hogy $H(Y) \leq H(X)$.

Tétel. Legyen X normális eloszlású μ várható értékkel és σ^2 szórásnégyzettel. Ekkor $H(X) = \frac{1}{2} \ln(2\pi e \sigma^2)$ és tetszőleges abszolút folytonos Y valószínűségi változó esetén, melyre $\text{Var}(Y) \leq \sigma^2 = \text{Var}(X)$, teljesül, hogy $H(Y) \leq H(X)$.

Feltételes sűrűségfüggvények

X, Y : diszkrét valószínűségi változók p_{ij} együttes eloszlással, valamint p_i és q_j peremeloszlásokkal ($i = 1, 2, \dots, n, j = 1, 2, \dots, m$).

X -nek az Y -ra vonatkozó feltételes eloszlása: $p_{i|j} = p_{ij}/q_j, \quad i = 1, 2, \dots, n, j = 1, 2, \dots, m.$

X -nek az Y -ra vonatkozó feltételes entrópiája:

$$H(X|Y) = - \sum_{j=1}^m \sum_{i=1}^n q_j p_{i|j} \log_2 p_{i|j} = - \sum_{j=1}^m \sum_{i=1}^n p_{ij} \log_2 p_{i|j}.$$

X, Y : abszolút folytonos valószínűségi változók $f(x, y)$ együttes sűrűségfüggvénnyel, melynek tartója $\mathcal{S} \subseteq \mathbb{R}^2$ ($f(x, y) = 0$, ha $(x, y) \notin \mathcal{S}$) valamint $f(x)$ és $g(y)$ perem-sűrűségfüggvényekkel.

X -nek az Y -ra [Y -nak az X -re] vonatkozó feltételes sűrűségfüggvénye:

$$f(x|y) := \frac{f(x, y)}{g(y)} \quad \left[f(y|x) := \frac{f(x, y)}{f(x)} \right], \quad (x, y) \in \mathcal{S}.$$

Feltételes differenciális entrópia

Definíció. Az X -nek az $\{Y = y\}$ feltétellel vett *feltételes differenciális entrópiája*

$$H(X|Y = y) := - \int f(x|y) \log f(x|y) dx,$$

az X -nek az Y -ra vonatkozó *feltételes differenciális entrópiája* pedig

$$\begin{aligned} H(X|Y) &:= \int H(X|Y = y)g(y)dy = - \iint_S [f(x|y) \log f(x|y)] g(y) dx dy \\ &= - \iint_S f(x, y) \log f(x|y) dx dy, \end{aligned}$$

amennyiben a fenti integrálok léteznek.

Példa. Legyen az (X, Y) eloszlása egyenletes az $(1, 1)$, $(1, 0)$ és $(0, 0)$ pontok által határolt háromszögön. Határozza meg a $H(X|Y)$ feltételes differenciális entrópiát.

Megoldás. Az (X, Y) együttes sűrűségfüggvénye:

$$f(x, y) = \begin{cases} 2, & \text{ha } 0 \leq x \leq 1, 0 \leq y \leq x, \\ 0, & \text{egyébként;} \end{cases} \quad \text{másik alak: } f(x, y) = \begin{cases} 2, & \text{ha } 0 \leq y \leq 1, y \leq x \leq 1, \\ 0, & \text{egyébként.} \end{cases}$$

Megoldás

A perem-sűrűségfüggvények:

$$f(x) = \int_0^x 2dy = 2x, \quad \text{ha } 0 \leq x \leq 1, \quad \text{és} \quad g(y) = \int_y^1 2dx = 2 - 2y, \quad \text{ha } 0 \leq y \leq 1.$$

Feltételes sűrűségfüggvények:

$$f(y|x) = \begin{cases} 1/x, & \text{ha } 0 \leq x \leq 1, 0 \leq y \leq x, \\ 0, & \text{egyébként,} \end{cases} \quad \text{és} \quad f(x|y) = \begin{cases} 1/(1-y), & \text{ha } 0 \leq y \leq 1, y \leq x \leq 1, \\ 0, & \text{egyébként.} \end{cases}$$

Az X -nek az $\{Y = y\}$ feltétellel vett feltételes differenciális entrópiája:

$$H(X|Y = y) = - \int_y^1 \frac{1}{1-y} \ln\left(\frac{1}{1-y}\right) dx = \frac{1}{1-y} \ln(1-y) \int_y^1 dx = \ln(1-y), \quad 0 \leq y \leq 1.$$

Az X -nek az Y -ra vonatkozó feltételes differenciális entrópiája:

$$H(X|Y) = \int_0^1 H(X|Y = y)g(y)dy = \int_0^1 \ln(1-y)(2-2y)dy = -2 \int_1^0 z \ln z dz = -\frac{1}{2}.$$

□

A feltételes differenciális entrópia tulajdonságai

Tétel.

- a) Ha (X, Y) együttes eloszlása abszolút folytonos, valamint $H(X)$ és $H(Y)$ véges, akkor $H(X|Y)$ és $H(Y|X)$ is létezik és véges, valamint

$$H(X, Y) = H(Y) + H(X|Y) = H(X) + H(Y|X).$$

- b) $H(X|Y) \leq H(X)$, és egyenlőség pontosan akkor áll fenn, ha X és Y független.
- c) Ha X_1, X_2, \dots, X_k együttes eloszlása abszolút folytonos és mindegyik változó differenciális entrópiája véges, akkor

$$H(X_1, X_2, \dots, X_k) = H(X_1) + H(X_2|X_1) + H(X_3|X_2, X_1) + \dots + H(X_k|X_{k-1}, \dots, X_1).$$

Kölcsönös információ és tulajdonságai

Definíció. Az X és Y együttesen abszolút folytonos valószínűségi változók *kölcsönös információja*

$$I(X; Y) := H(X) + H(Y) - H(X, Y).$$

Megjegyzés. Ha (X, Y) együttes eloszlása abszolút folytonos $f(x, y)$ együttes sűrűségfüggvénnyel, melynek tartója $\mathcal{S} \subseteq \mathbb{R}^2$, $f(x)$ és $g(y)$ pedig rendre az X és Y perem-sűrűségfüggvényei, akkor

$$I(X; Y) = \iint_{\mathcal{S}} f(x, y) \ln \frac{f(x, y)}{f(x)g(y)} dx dy = \iint_{\mathcal{S}} f(x, y) \ln \frac{f(x|y)}{f(x)} dx dy = \iint_{\mathcal{S}} f(x, y) \ln \frac{f(y|x)}{g(y)} dx dy.$$

Megjegyzés. A kölcsönös információ tulajdonságai megegyeznek a diszkrét esetben kimondottakkal.

- a) Szimmetrikus, és $I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y; X)$.
- b) $I(X; Y) \geq 0$ és $I(X; Y)$ pontosan akkor 0, ha X és Y független.

Példa

Legyen az (X, Y) eloszlása egyenletes az $(1, 1)$, $(1, 0)$ és $(0, 0)$ pontok által határolt háromszögön. Határozza meg az $I(X; Y)$ kölcsönös információt.

Megoldás. Az (X, Y) együttes sűrűségfüggvénye:

$$f(x, y) = \begin{cases} 2, & \text{ha } 0 \leq x \leq 1, 0 \leq y \leq x, \\ 0, & \text{egyébként;} \end{cases} \quad \text{másik alak: } f(x, y) = \begin{cases} 2, & \text{ha } 0 \leq y \leq 1, y \leq x \leq 1, \\ 0, & \text{egyébként.} \end{cases}$$

A perem-sűrűségfüggvények:

$$f(x) = 2x, \quad \text{ha } 0 \leq x \leq 1, \quad \text{és} \quad g(y) = 2 - 2y, \quad \text{ha } 0 \leq y \leq 1.$$

Az X -nek az Y -ra vonatkozó feltételes differenciális entrópiája: $H(X|Y) = -1/2$.

$$H(X) = - \int_0^1 2x \ln(2x) dx = - \frac{1}{2} \int_0^2 z \ln z dz = \frac{1}{2} - \ln 2.$$

Kölcsönös információ: $I(X; Y) = H(X) - H(X|Y) = \frac{1}{2} - \ln 2 + \frac{1}{2} = 1 - \ln 2$.

□

Példa

Legyen az (X, Y) eloszlása egyenletes az $(0, 0)$, $(1, 0)$ és $(0, 2)$ pontok által határolt háromszögön.

- 1 Határozza meg az (X, Y) differenciális entrópiáját.
- 2 Határozza meg a $H(X|Y)$ és $H(Y|X)$ feltételes differenciális entrópiákat.
- 3 Határozza meg az $I(X; Y)$ kölcsönös információt.

Megoldás. Az (X, Y) együttes sűrűségfüggvénye:

$$f(x, y) = \begin{cases} 1, & \text{ha } 0 \leq x \leq 1, 0 \leq y \leq 2(1-x), \\ 0, & \text{egyébként;} \end{cases} \quad \text{másik alak: } f(x, y) = \begin{cases} 1, & \text{ha } 0 \leq y \leq 2, 0 \leq x \leq 1-y/2, \\ 0, & \text{egyébként.} \end{cases}$$

A perem-sűrűségfüggvények:

$$f(x) = \int_0^{2(1-x)} 1 dy = 2(1-x), \quad \text{ha } 0 \leq x \leq 1, \quad \text{és} \quad g(y) = \int_1^{1-y/2} 1 dx = 1-y/2, \quad \text{ha } 0 \leq y \leq 2.$$

Feltételes sűrűségfüggvények:

$$f(y|x) = \begin{cases} \frac{1}{2(1-x)}, & \text{ha } 0 \leq x \leq 1, 0 \leq y \leq 2(1-x), \\ 0, & \text{egyébként;} \end{cases} \quad \text{és} \quad f(x|y) = \begin{cases} \frac{1}{1-y/2}, & \text{ha } 0 \leq y \leq 2, 0 \leq x \leq 1-y/2, \\ 0, & \text{egyébként.} \end{cases}$$

Megoldás.

1. Az (X, Y) differenciális entrópiája:

$$H(X, Y) = - \int_0^1 \int_0^{2(1-x)} 1 \ln 1 \, dy \, dx = 0.$$

2. Az X -nek az $\{Y = y\}$ feltétellel vett feltételes differenciális entrópiája:

$$H(X|Y = y) = - \int_0^{1-y/2} \frac{1}{1-y/2} \ln \left(\frac{1}{1-y/2} \right) dx = \frac{1}{1-y/2} \ln(1-y/2) \int_0^{1-y/2} dx = \ln(1-y/2), \quad 0 \leq y \leq 2.$$

Az X -nek az Y -ra vonatkozó feltételes differenciális entrópiája:

$$H(X|Y) = \int_0^2 H(X|Y = y)g(y)dy = \int_0^2 \ln(1-y/2)(1-y/2)dy = -2 \int_1^0 z \ln z \, dz = -\frac{1}{2}.$$

Az Y -nak az $\{X = x\}$ feltétellel vett feltételes differenciális entrópiája:

$$H(Y|X = x) = - \int_0^{2-2x} \frac{1}{2-2x} \ln \left(\frac{1}{2-2x} \right) dy = \frac{1}{2-2x} \ln(2-2x) \int_0^{2-2x} dy = \ln(2-2x), \quad 0 \leq x \leq 1.$$

Az Y -nak az X -re vonatkozó feltételes differenciális entrópiája:

$$H(Y|X) = \int_0^1 H(Y|X = x)f(x)dx = \int_0^1 \ln(2-2x)(2-2x)dx = -\frac{1}{2} \int_2^0 z \ln z \, dz = \ln 2 - \frac{1}{2}.$$

Megoldás.

3. Az (X, Y) differenciális entrópiája: $H(X, Y) = 0$.

Feltételes differenciális entrópiák: $H(X|Y) = -1/2$, $H(Y|X) = \ln 2 - 1/2$.

A perem-sűrűségfüggvények:

$$f(x) = \int_0^{2(1-x)} 1dy = 2(1-x), \quad \text{ha } 0 \leq x \leq 1, \quad \text{és} \quad g(y) = \int_1^{1-y/2} 1dx = 1 - y/2, \quad \text{ha } 0 \leq y \leq 2.$$

Az X és Y entrópiája:

$$H(X) = - \int_0^1 (2-2x) \ln(2-2x) dx = \frac{1}{2} - \ln 2,$$

$$H(Y) = - \int_0^2 (1-y/2) \ln(1-y/2) dy = \frac{1}{2}.$$

Kölcsönös információ:

$$I(X; Y) = H(X) + H(Y) - H(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = 1 - \ln 2 = 0.3069.$$



Példa. Zajos csatorna additív Gauss zajjal

Adott egy emlékezet nélküli analóg csatorna, aminek a bemeneti jele egy abszolút folytonos X valószínűségi változó, melynek véges a differenciális entrópiája. Határozza meg a csatorna kapacitását, ha az X bemeneti jelhez tartozó kimeneti jel $Y = X + Z$, ahol a Z zaj normális eloszlású nulla várható értékkel és σ_Z^2 szórásnégyzettel, valamint független az X bemenettől.

Megoldás. Jelölje $f(x, y)$ az (X, Y) együttes sűrűségfüggvényét, $f(x)$, $g(y)$ és $h(z)$ pedig az X , Y , illetve Z sűrűségfüggvényét. Ha rögzítjük az $X = x$ értéket, akkor $Y = x + Z$, azaz az Y feltételes eloszlása az $\{X = x\}$ feltétel mellett tulajdonképpen a Z eloszlása eltolva az x értékkel. Ez azt jelenti, hogy az Y -nak az X -re vonatkozó feltételes sűrűségfüggvénye

$$f(y|x) = h(y - x), \quad \text{azaz} \quad f(x, y) = f(y|x)f(x) = h(y - x)f(x).$$

A feltételes differenciális entrópia:

$$\begin{aligned} H(Y|X) &= - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} h(y - x)f(x) \ln h(y - x) dx dy = - \int_{-\infty}^{\infty} \left(\int_{-\infty}^{\infty} h(y - x) \ln h(y - x) dy \right) f(x) dx \\ &= \int_{-\infty}^{\infty} \left(- \int_{-\infty}^{\infty} h(z) \ln h(z) dz \right) f(x) dx = \int_{-\infty}^{\infty} H(Z)f(x) dx = H(Z) \int_{-\infty}^{\infty} f(x) dx = H(Z). \end{aligned}$$

Megoldás

Kölcsönös információ:

$$I(X; Y) = H(Y) - H(Y|X) = H(Y) - H(Z) = H(Y) - \frac{1}{2} \ln(2\pi e \sigma_Z^2).$$

Feltehetjük, hogy az X bemenő jel szórása nem halad meg egy adott $\sigma > 0$ szintet, azaz

$$\text{Var}(Y) = \text{Var}(X) + \text{Var}(Z) \leq \sigma^2 + \sigma_Z^2.$$

Azon valószínűségi változók közül, melyek szórásnégyzete legfeljebb $\sigma^2 + \sigma_Z^2$, a $\sigma^2 + \sigma_Z^2$ szórásnégyzetű normális eloszlásnak a legnagyobb az entrópiája, ami $\frac{1}{2} \ln(2\pi e(\sigma^2 + \sigma_Z^2))$. Ezek alapján

$$I(X; Y) \leq \frac{1}{2} \ln(2\pi e(\sigma^2 + \sigma_Z^2)) - \frac{1}{2} \ln(2\pi e \sigma_Z^2) = \frac{1}{2} \ln\left(\frac{\sigma^2 + \sigma_Z^2}{\sigma_Z^2}\right).$$

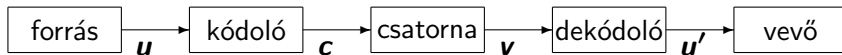
Amennyiben megadható olyan X bemenő jel, melyre a kimenő jel $\sigma^2 + \sigma_Z^2$ szórásnégyzetű normális, akkor az $I(X; Y)$ felső korlátja elérhető és így ez a korlát csatorna kapacitása.

Legyen $X \sim \mathcal{N}(0, \sigma^2)$. Ekkor $Y = X + Z \sim \mathcal{N}(0, \sigma^2 + \sigma_Z^2)$, tehát a kapacitás

$$C = \frac{1}{2} \ln\left(\frac{\sigma^2 + \sigma_Z^2}{\sigma_Z^2}\right).$$



Hamming-távolság



u, u' : egy \mathcal{X} forrásábécé betűiből alkotott k hosszúságú vektorok.

c, v : egy \mathcal{Y} kódábécé betűiből alkotott n hosszúságú vektorok.

Kódoló: $f: \mathcal{X}^k \rightarrow \mathcal{C} \subseteq \mathcal{Y}^n$ invertálható függvény. Az $u \in \mathcal{X}^k$ **üzenet**et a $c \in \mathcal{C}$ **kódszó**ba képezi le. \mathcal{C} az \mathcal{X}^k **kódja**.

Egy $c = (c_1, c_2, \dots, c_n)$ bemeneti és $v = (v_1, v_2, \dots, v_n)$ kimeneti sorozat esetén az m -edik pozíciónál a csatorna hibázott, ha $c_m \neq v_m$.

$d(c, v)$: azon i pozíciók száma, ahol $c_i \neq v_i$. A c és v vektorok **Hamming-távolsága**. A csatorna hibáinak száma: $t = d(c, v)$. Ez **egyszerű hibázás**, mert sem a hiba helye, sem az értéke nem ismert.

Megjegyzés. A $d(c, v)$ Hamming-távolság metrika, azaz

- a) $d(c, v) \geq 0$ és $d(c, v) = 0$ pontosan akkor, ha $c = v$;
- b) $d(c, v) = d(v, c)$;
- c) $d(c, v) \leq d(c, w) + d(w, v)$ (háromszög-egyenlőtlenség).

Algebrai dekódolás

Dekódolás: egy $g : \mathcal{Y}^n \rightarrow \mathcal{C}$ és az $f^{-1} : \mathcal{C} \rightarrow \mathcal{X}^k$ egymás utáni alkalmazása. A csatorna kimeneti jeléhez rendel egy forrásüzenetet.

Az f kódoló egyértelműen meghatározza az f^{-1} függvényt. A továbbiakban dekódoló alatt a g függvényt értjük.

Algebrai dekódoló:

$$g(\mathbf{v}) = \mathbf{c}', \quad \text{ha} \quad d(\mathbf{c}', \mathbf{v}) = \min_{\mathbf{c} \in \mathcal{C}} d(\mathbf{c}, \mathbf{v}).$$

Ha a minimum feltétel több kódszóra is teljesül, akkor tetszőlegesen válasszuk ki az egyiket.

Cél: minden lehetséges \mathbf{v} kimenő jelsorozat esetén a hozzá legközelebbi \mathbf{c} kódszó meghatározása anélkül, hogy az összes $d(\mathbf{c}, \mathbf{v})$ távolságot kiszámítanánk.

Definíció. Egy \mathcal{C} kód *kódtávolsága*

$$d_{\min} := \min_{\substack{\mathbf{c} \neq \mathbf{c}' \\ \mathbf{c}, \mathbf{c}' \in \mathcal{C}}} d(\mathbf{c}, \mathbf{c}').$$

Definíció. Egy \mathbf{c} vektor $w(\mathbf{c})$ *súlya* a koordinátái között levő nem nulla elemek száma.

Példa

Határozza meg a következő bináris vektorok súlyát és Hamming távolságait:

$$\mathbf{v}_1 = 1001010, \quad \mathbf{v}_2 = 0110101, \quad \mathbf{v}_3 = 0011110, \quad \mathbf{v}_4 = \mathbf{v}_2 + \mathbf{v}_3.$$

Megoldás. Súlyok:

$$w(\mathbf{v}_1) = 3, \quad w(\mathbf{v}_2) = 4, \quad w(\mathbf{v}_3) = 4, \quad \mathbf{v}_4 = 0101011 \implies w(\mathbf{v}_4) = 4.$$

Hamming távolságok:

$$\begin{aligned} d(\mathbf{v}_1, \mathbf{v}_2) &= 7, & d(\mathbf{v}_1, \mathbf{v}_3) &= 3, & d(\mathbf{v}_1, \mathbf{v}_4) &= 3, \\ d(\mathbf{v}_2, \mathbf{v}_3) &= 4, & d(\mathbf{v}_2, \mathbf{v}_4) &= 4, & d(\mathbf{v}_3, \mathbf{v}_4) &= 4. \end{aligned}$$



Hibajelzés, hibajavítás

Hibajelzés: a vevőnél csupán detektálni akarjuk a hibázás tényét.

Tétel. Egy d_{\min} kódtávolságú kód minden legfeljebb $d_{\min} - 1$ számú egyszerű hibát jelezni tud.

Magyarázat. Egy \mathbf{v} vett kódjelsorozat esetén akkor tudjuk a hibázást észrevenni, ha \mathbf{v} nem kódszó. Ez biztosan teljesül, ha a \mathbf{c} küldött kódszó esetén

$$d_{\min} > d(\mathbf{v}, \mathbf{c}),$$

azaz a hibák t számára $d_{\min} > t$. □

Hibajavítás: t egyszerű hiba esetén a vett \mathbf{v} szóból egyértelműen visszaállítható a küldött \mathbf{c} kódszó.

Tétel. Egy d_{\min} kódtávolságú kód $\lfloor \frac{d_{\min}-1}{2} \rfloor$ hibát tud javítani.

Magyarázat. A \mathbf{c} küldött kódszó pontosan akkor állítható egyértelműen vissza, ha tetszőleges \mathbf{c}' kódszó esetén

$$d(\mathbf{v}, \mathbf{c}') > d(\mathbf{v}, \mathbf{c}). \quad (1)$$

A háromszög-egyenlőtlenség miatt $d(\mathbf{v}, \mathbf{c}') \geq d(\mathbf{c}, \mathbf{c}') - d(\mathbf{v}, \mathbf{c})$. Az (1) egyenlőtlenség biztosan teljesül, ha $d(\mathbf{c}, \mathbf{c}') - d(\mathbf{v}, \mathbf{c}) > d(\mathbf{v}, \mathbf{c})$, azaz minden $\mathbf{c} \neq \mathbf{c}'$ esetén $d(\mathbf{v}, \mathbf{c}') > d(\mathbf{v}, \mathbf{c})$, tehát $d_{\min}/2 > d(\mathbf{v}, \mathbf{c})$. □

Példa

$\mathcal{X} = \mathcal{Y} = \{0, 1\}$, $k = 2$, $n = 5$. Kódoló (f):

$$00 \xrightarrow{f} \mathbf{c}_1 = 00000 \quad 01 \xrightarrow{f} \mathbf{c}_2 = 01101 \quad 10 \xrightarrow{f} \mathbf{c}_3 = 10110 \quad 11 \xrightarrow{f} \mathbf{c}_4 = 11011$$

Dekódoló (g és f^{-1}):

$$\begin{array}{ccc} \left. \begin{array}{l} 00000 \\ 10000 \\ 01000 \\ 00100 \\ 00010 \\ 00001 \end{array} \right\} \xrightarrow{g} 00000 \xrightarrow{f^{-1}} 00 & \left. \begin{array}{l} 01101 \\ 11101 \\ 00101 \\ 01001 \\ 01111 \\ 01100 \end{array} \right\} \xrightarrow{g} 01101 \xrightarrow{f^{-1}} 01 & \left. \begin{array}{l} 10110 \\ 00110 \\ 11110 \\ 10010 \\ 10100 \\ 10111 \end{array} \right\} \xrightarrow{g} 10110 \xrightarrow{f^{-1}} 10 \\ \\ \left. \begin{array}{l} 11011 \\ 01011 \\ 10011 \\ 11111 \\ 11001 \\ 11010 \end{array} \right\} \xrightarrow{g} 11011 \xrightarrow{f^{-1}} 11 & \left. \begin{array}{l} 00011 \\ 01010 \\ 10001 \\ 11000 \end{array} \right\} \xrightarrow{g} 00000 \xrightarrow{f^{-1}} 00 & \left. \begin{array}{l} 00111 \\ 01110 \\ 10101 \\ 11100 \end{array} \right\} \xrightarrow{g} 01101 \xrightarrow{f^{-1}} 01 \end{array}$$

Első négy blokk esetén a távolság 1, utolsó kettőnél 2.

Kódtávolság: $d_{\min} = 3$. 2 hibát tud jelezni, 1 hibát tud javítani.

Példa

$\mathcal{X} = \mathcal{Y} = \{0, 1\}$, $k = 2$, $n = 3$. Kódoló (f):

$u_1 u_2$		$c_1 c_2 c_3$	
0 0	\mapsto	0 0 0	c_1
0 1	\mapsto	0 1 1	c_2
1 0	\mapsto	1 0 1	c_3
1 1	\mapsto	1 1 0	c_4

Az $u_1 u_2$ forrásüzenet egy paritásbittel lett kiegészítve.

Ha $\mathbf{v} = v_1 v_2 v_3 \in \mathcal{Y}^3$ nem kódszó, akkor három kódszóból is megkapható 1 bit megváltoztatásával (1 hibával).

Kódtávolság: $d_{\min} = 2$. 1 hibát tud jelezni, 0 hibát tud javítani.

Törléses hiba

A hiba helyét ismerjük, de az értékén nem.

Tétel. Egy d_{\min} kódtávolságú kód $d_{\min} - 1$ törléses hibát tud javítani.

Magyarázat. Mivel a kódszavak legalább d_{\min} pozícióban különböznek, nem fordulhat elő, hogy a \mathbf{c} és \mathbf{c}' kódszavak ugyanazon, legfeljebb $d_{\min} - 1$ pozíciójának törlésével ugyanazt a szót kapjuk. □

Singleton-korlát

$A_s(n, d_{\min})$: egy s elemű kódábécé elemeiből alkotott d_{\min} kódtávolságú n hosszú blokk kód kódszavainak maximális száma.

Singleton-korlát:

$$A_s(n, d_{\min}) \leq s^{n-d_{\min}+1}.$$

Magyarázat. Legyen \mathcal{C} egy tetszőleges n hosszú kódszavakból álló d_{\min} kódtávolságú blokk kód. Ha minden kódszavának töröljük az első $d_{\min} - 1$ betűjét, akkor $n - d_{\min} + 1$ hosszúságú új, egymástól különböző kódszavakat kapunk. Ezek maximális száma $s^{n-d_{\min}+1}$. Mivel a \mathcal{C} kódot tetszőlegesen választottuk,

$$|\mathcal{C}| \leq A_s(n, d_{\min}) \leq s^{n-d_{\min}+1}. \quad \square$$

(n, k) paraméterű kód: a kódoló k hosszú forrásszegmensekhez rendel n hosszú vektorokat. Ekkor $|\mathcal{C}| = s^k$, a Singleton-korlát:

$$d_{\min} \leq n - k + 1.$$

Definíció. Azt a kódot, melyre a Singleton-korlátban egyenlőség áll, *maximális távolságú*, vagy *MDS* (maximum distance separable) kódnak nevezzük.

Hamming-korlát

t : a kód által javítható hibák száma.

Hamming-korlát:

$$A_s(n, d_{\min}) \leq \frac{s^n}{\sum_{i=0}^t \binom{n}{i} (s-1)^i}, \quad \text{ahol} \quad t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor.$$

Magyarázat. Minden egyes kódszó esetén tekintsünk egy t sugarú gömböt, vagyis azokat az n hosszú kódjel-sorozatokat, amik legfeljebb t hibával keletkeznek (**Hamming-gömb**). $(s-1)^i$ darab olyan sorozat van, ami pontosan i pozícióban tér el egy adott kódszótól, így egy gömb $\sum_{i=0}^t \binom{n}{i} (s-1)^i$ sorozatot tartalmaz. A kód akkor tud t hibát javítani, ha a gömbök diszjunktak. A gömbökben lévő sorozatok teljes száma legfeljebb s^n , azaz

$$A_s(n, d_{\min}) \times \sum_{i=0}^t \binom{n}{i} (s-1)^i \leq s^n. \quad \square$$

Megjegyzés. (n, k) paraméterű kód esetén a Hamming-korlát:

$$\sum_{i=0}^t \binom{n}{i} (s-1)^i \leq s^{n-k}.$$

Perfekt kódok

Bináris (n, k) típusú kódok esetén a Hamming korlát:

$$\sum_{i=0}^t \binom{n}{i} \leq 2^{n-k}.$$

Definíció. Az olyan kódokat, ahol a Hamming-korlátban egyenlőség áll, *perfekt kódoknak* nevezzük.

Egy bináris (n, k) típusú 1 hibát javítani képes kód perfekt, ha

$$1 + n = 2^{n-k}.$$

Példák.

1. Bináris $(5, 2)$ típusú kód, $d_{\min} = 3$. Nem MDS és nem perfekt.
2. Bináris $(3, 2)$ típusú kód, $d_{\min} = 2$. MDS, de nem perfekt.

Vizsgálja meg, az alábbi \mathcal{C} kódok detektálják-e a megadott hibamintákat. Adja meg a kódtávolságokat is.

1 $\mathcal{C} = \{00000, 10101, 00111, 11100\}$

(a) $e = 10101$

(b) $e = 01010$

(c) $e = 11011$

2 $\mathcal{C} = \{1101, 0110, 1100\}$

(a) $e = 0010$

(b) $e = 0011$

(c) $e = 1010$

3 $\mathcal{C} = \{1000, 0100, 0010, 0001\}$

(a) $e = 1001$

(b) $e = 1110$

(c) $e = 0110$

1. Kód: $\mathcal{C} = \{00000, 10101, 00111, 11100\}$. Kódtávolság: $d_{\min} = 2$.

(a) Hibaminta: $\mathbf{e} = 10101$. Mivel $00000 + \mathbf{e} = 10101 \in \mathcal{C}$, a hibaminta **nem** detektálható.

(b) Hibaminta: $\mathbf{e} = 01010$. Mivel

$$00000 + \mathbf{e} = 01010 \notin \mathcal{C}, \quad 10101 + \mathbf{e} = 11111 \notin \mathcal{C}, \quad 00111 + \mathbf{e} = 01101 \notin \mathcal{C}, \quad 11100 + \mathbf{e} = 10110 \notin \mathcal{C},$$

a hibaminta detektálható.

(c) Hibaminta: $\mathbf{e} = 11011$. Mivel $00111 + \mathbf{e} = 11100 \in \mathcal{C}$, a hibaminta **nem** detektálható.

2. Kód: $\mathcal{C} = \{1101, 0110, 1100\}$. Kódtávolság: $d_{\min} = 1$.

(a) Hibaminta: $\mathbf{e} = 0010$. Mivel

$$1101 + \mathbf{e} = 1111 \notin \mathcal{C}, \quad 0110 + \mathbf{e} = 0100 \notin \mathcal{C}, \quad 1100 + \mathbf{e} = 1110 \notin \mathcal{C},$$

a hibaminta detektálható.

Megoldás

2. Kód: $\mathcal{C} = \{1101, 0110, 1100\}$

(b) Hibaminta: $\mathbf{e} = 0011$. Mivel

$$1101 + \mathbf{e} = 1110 \notin \mathcal{C}, \quad 0110 + \mathbf{e} = 0101 \notin \mathcal{C}, \quad 1100 + \mathbf{e} = 1111 \notin \mathcal{C},$$

a hibaminta detektálható.

(c) Hibaminta: $\mathbf{e} = 1010$. Mivel $0110 + \mathbf{e} = 1100 \in \mathcal{C}$, a hibaminta **nem** detektálható.

3. Kód: $\mathcal{C} = \{1000, 0100, 0010, 0001\}$. Kódtávolság: $d_{\min} = 2$.

(a) Hibaminta: $\mathbf{e} = 1001$. Mivel $1000 + \mathbf{e} = 0001 \in \mathcal{C}$, a hibaminta **nem** detektálható.

(b) Hibaminta: $\mathbf{e} = 1110$. Mivel

$$1000 + \mathbf{e} = 0110 \notin \mathcal{C}, \quad 0100 + \mathbf{e} = 1010 \notin \mathcal{C}, \quad 0010 + \mathbf{e} = 1100 \notin \mathcal{C}, \quad 0001 + \mathbf{e} = 1111 \notin \mathcal{C},$$

a hibaminta detektálható.

(c) Hibaminta: $\mathbf{e} = 0110$. Mivel $0100 + \mathbf{e} = 0010 \in \mathcal{C}$, a hibaminta **nem** detektálható.

□

Példa

Vizsgálja meg, az alábbi bináris \mathcal{C} kódok javítják-e a megadott hibamintákat. Adja meg a kódtávolságokat, valamint vizsgálja meg, hogy az adott kód MDS, illetve perfekt kód-e.

❶ $\mathcal{C} = \{000000, 100101, 010110, 001111, 110011, 101010, 011001, 111100\}$

(a) $e = 001000$

(b) $e = 000010$

(c) $e = 100100$

❷ $\mathcal{C} = \{1001011, 0110101, 1110010, 1111111\}$

(a) $e = 0100000$

(b) $e = 0101000$

(c) $e = 1100000$

Megoldás.

1. Kód: $\mathcal{C} = \{000000, 100101, 010110, 001111, 110011, 101010, 011001, 111100\}$.

Kódtávolság: $d_{\min} = 3$. A kód így $t = 1$ hibát tud javítani, azaz ha a hibaminta súlya egy, az javítható.

Paraméterek: $n = 6$, $k = 3$.

$n - k + 1 = 4 > 3 = d_{\min}$: **nem** MDS; $1 + n = 7 < 8 = 2^{6-3}$: **nem** perfekt.

Megoldás

1. Kód: $\mathcal{C} = \{000000, 100101, 010110, 001111, 110011, 101010, 011001, 111100\}$. Kódtávolság: $d_{\min} = 3$.

(a) Hibaminta: $\mathbf{e} = 001000$. $w(\mathbf{e}) = 1$, így javítható.

(b) Hibaminta: $\mathbf{e} = 000010$. $w(\mathbf{e}) = 1$, így javítható.

(c) Hibaminta: $\mathbf{e} = 100100$. $w(\mathbf{e}) = 2$. Legyen $\mathbf{v} = 000000 + \mathbf{e} = \mathbf{e} = 100100$.

$$d(\mathbf{v}, 000000) = 2 > 1 = d(\mathbf{v}, 100101),$$

azaz a hibaminta **nem** javítható.

2. Kód: $\mathcal{C} = \{1001011, 0110101, 1110010, 1111111\}$.

Kódtávolság: $d_{\min} = 3$. A kód így egy hibát tud javítani, azaz ha a hibaminta súlya egy, az javítható.

Paraméterek: $n = 7$, $k = 2$.

$n - k + 1 = 6 > 3 = d_{\min}$: **nem** MDS; $1 + 7 = 8 < 32 = 2^{7-2}$: **nem** perfekt.

Megoldás.

2. Kód: $\mathcal{C} = \{1001011, 0110101, 1110010, 1111111\} = \{c_1, c_2, c_3, c_4\}$. Kódtávolság: $d_{\min} = 3$.

(a) Hibaminta: $e = 0100000$. $w(e) = 1$, így javítható.

(b) Hibaminta: $e = 0101000$. $w(e) = 2$. Legyen $v = 1001011 + e = 1100011$.

$$d(v, 1001011) = 2 = d(v, 1110010),$$

azaz a hibaminta **nem** javítható.

(c) Hibaminta: $e = 1100000$. $w(e) = 2$.

Legyenek $v_1 = c_1 + e = 0101011$, $v_2 = c_2 + e = 1010101$, $v_3 = c_4 + e = 0010010$, $v_4 = c_4 + e = 0011111$.

Mivel $w(e) = 2$, $d(v_1, c_1) = d(v_2, c_2) = d(v_3, c_4) = d(v_4, c_4) = 2$.

$$\begin{array}{lll} d(v_1, c_2) = 4, & d(v_1, c_3) = 4, & d(v_1, c_4) = 3; \\ d(v_2, c_1) = 4, & d(v_2, c_3) = 4, & d(v_2, c_4) = 3; \\ d(v_3, c_1) = 4, & d(v_3, c_2) = 4, & d(v_3, c_4) = 5; \\ d(v_4, c_1) = 3, & d(v_4, c_2) = 3, & d(v_4, c_3) = 5. \end{array}$$

A hibaminta javítható.



Bináris lineáris kódok

Definíció. Egy \mathcal{C} bináris kód *lineáris*, ha \mathcal{C} lineáris tér, azaz minden $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ esetén $\mathbf{c} + \mathbf{c}' \in \mathcal{C}$.

Megjegyzés. Ha a \mathcal{C} kód lineáris, akkor $\mathbf{0} \in \mathcal{C}$.

$\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in \mathcal{C}$: a \mathcal{C} kód egy bázisa, ahol $\mathbf{g}_i = (g_{i1}, g_{i2}, \dots, g_{in})$.

\mathbf{G} : a $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k$ sorvektorokból álló $k \times n$ méretű mátrix.

Tetszőleges $\mathbf{c} = (c_1, c_2, \dots, c_n) \in \mathcal{C}$ esetén egyértelműen létezik $\mathbf{u} = (u_1, u_2, \dots, u_k)$, hogy

$$\mathbf{c} = \sum_{i=1}^k u_i \mathbf{g}_i, \quad \text{azaz} \quad \mathbf{c} = \mathbf{uG}.$$

Definíció. A \mathbf{G} mátrixot a \mathcal{C} kód *generátormátrixának* nevezzük.

Megjegyzés. A generátormátrix nem egyértelmű.

Definíció. Egy (n, k) paraméterű lineáris kód *szisztematikus*, ha minden kódszavára igaz, hogy annak utolsó $n - k$ kódjelét elhagyva éppen a neki megfelelő üzenetet kapjuk.

Szisztematikus kódok

Szisztematikus kód generátormátrixa egyértelmű (standard alakú): $\mathbf{G} = (\mathbf{I}_k, \mathbf{B})$.

\mathbf{I}_k : $k \times k$ méretű egységmátrix.

\mathbf{B} : $k \times (n - k)$ méretű mátrix.

A kódszavak alakja: $\mathbf{c} = (u_1, \dots, u_k, c_{k+1}, \dots, c_n)$.

Első k tag: **üzenetszegmens**; utolsó $n - k$ tag: **paritásszegmens**.

Példák.

1. $00 \mapsto 00000$, $01 \mapsto 01101$, $10 \mapsto 10110$, $11 \mapsto 11011$.

Lineáris kód, $n = 5$, $k = 2$. Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \quad \text{szisztematikus kód.}$$

2. $00 \mapsto 000$, $01 \mapsto 011$, $10 \mapsto 101$, $11 \mapsto 110$.

Lineáris kód, $n = 3$, $k = 2$. Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \text{szisztematikus kód.}$$

Példa

Vizsgálja meg, az alábbi \mathcal{C} kódok közül melyek lineárisak. A lineáris kódoknak adja meg a kódtávolságát és egy generátormátrixát.

1 $\mathcal{C} = \{101, 111, 011\}$

2 $\mathcal{C} = \{000, 001, 010, 011\}$

3 $\mathcal{C} = \{0000, 0001, 1110\}$

4 $\mathcal{C} = \{0000, 1001, 0110, 1111\}$

5 $\mathcal{C} = \{00000, 11111\}$

6 $\mathcal{C} = \{00000, 11100, 00111, 11011\}$

7 $\mathcal{C} = \{00000, 11110, 01111, 10001\}$

8 $\mathcal{C} = \{000000, 101010, 010101, 111111\}$

Megoldás

1. Kód: $\mathcal{C} = \{101, 111, 011\}$. Mivel $101 + 111 = 010 \notin \mathcal{C}$, a kód **nem** lineáris.

Megjegyzés. Ha a \mathcal{C} kód lineáris, akkor $\mathbf{0} \in \mathcal{C}$.

2. Kód: $\mathcal{C} = \{000, 001, 010, 011\}$. Bármelyik két kódszó összege kódszó, így a kód lineáris.

Kódtávolság: $d_{\min} = w_{\min} = 1$. Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

3. Kód: $\mathcal{C} = \{0000, 0001, 1110\}$. Mivel $0001 + 1110 = 1111 \notin \mathcal{C}$, a kód **nem** lineáris.

4. Kód: $\mathcal{C} = \{0000, 1001, 0110, 1111\}$. Bármelyik két kódszó összege kódszó, így a kód lineáris.

Kódtávolság: $d_{\min} = w_{\min} = 2$. Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad (\text{standard alakú}).$$

5. Kód: $\mathcal{C} = \{00000, 11111\}$. A két kódszó összege kódszó, így a kód lineáris.

Kódtávolság: $d_{\min} = w_{\min} = 5$. Generátormátrix:

$$\mathbf{G} = (1 \ 1 \ 1 \ 1 \ 1) \quad (\text{standard alakú}).$$

Megoldás

6. Kód: $\mathcal{C} = \{00000, 11100, 00111, 11011\}$. Bármelyik két kódszó összege kódszó, így a kód lineáris.

Kódtávolság: $d_{\min} = w_{\min} = 3$. Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

7. Kód: $\mathcal{C} = \{00000, 11110, 01111, 10001\}$. Bármelyik két kódszó összege kódszó, így a kód lineáris.

Kódtávolság: $d_{\min} = w_{\min} = 2$. Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (\text{standard alakú}).$$

8. Kód: $\mathcal{C} = \{000000, 101010, 010101, 111111\}$. Bármelyik két kódszó összege kódszó, így a kód lineáris.

Kódtávolság: $d_{\min} = w_{\min} = 3$. Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad (\text{standard alakú}).$$



Példa

A \mathcal{C} kód generátormátrixa:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Az angol ábécé 16 betűjének a következő forráskódok felelnek meg:

0000	1000	0100	0010	0001	1100	1010	1001
A	B	C	D	E	F	G	H
0110	0101	0011	1110	1101	1011	0111	1111
I	J	K	L	M	N	O	P

- 1 Kódolja a *HELP* üzenetet.
- 2 A *HELP* üzenet hibajavító kódját egy zajos csatornán továbbítják, ami az első kódszó esetén az első pozíciónál hibázik, a második kódszó hibátlanul továbbítódik, a harmadik kódszónál a hetedik, míg a negyedik kódszónál az ötödik és hatodik pozíciónál lép fel hiba. Dekódolja a kapott üzenetet.

Megoldás

Az egyes betűk hibajavító kódjai (a \mathcal{C} kód):

0000000	1000111	0100110	0010101	0001011	1100001	1010010	1001100
A	B	C	D	E	F	G	H
0110011	0101101	0011110	1110100	1101010	1011001	0111000	1111111
I	J	K	L	M	N	O	P

Kódtávolság: $d_{\min} = w_{\min} = 3$.

1. A *HELP* üzenet kódja: 1001100 0001011 1110100 1111111.
2. A csatorna kimeneténél vett jelsorozat: 0001100 0001011 1110101 1111001.

Mivel a kódtávolság 3, a kód egy hibát biztosan javítani tud. Ezek alapján az első három vett kód szó hibátlanul dekódolható a *H*, *E* és *L* betűkké. Az utolsó vektor távolsága az egyes betűk kódszavaitól:

A: 5; B: 5; C: 6; D: 4; E: 4; F: 2; G: 4; H: 4; I: 3; J: 3; K: 5; L: 3; M: 3; N: 1; O: 2; P: 2

Ezek alapján az utolsó vektor *N* betűvé dekódolódik, azaz a dekódolt üzenet *HELN*.



Paritásellenőrző mátrix

Definíció. Ha egy $(n - k) \times n$ méretű \mathbf{H} mátrixra

$$\mathbf{H}\mathbf{c}^\top = \mathbf{0}$$

akkor és csak akkor, ha $\mathbf{c} \in \mathcal{C}$, akkor a \mathbf{H} mátrixot a \mathcal{C} kód *paritásellenőrző mátrixának* (röviden *paritásmátrixának*) nevezzük.

Tétel. Ha \mathbf{G} és \mathbf{H} ugyanazon \mathcal{C} kód generátormátrixa, illetve paritásmátrixa, akkor

$$\mathbf{H}\mathbf{G}^\top = \mathbf{0}.$$

Minden lineáris kódnak van paritásmátrixa.

Szisztematikus kód esetén a generátormátrix alakja: $\mathbf{G} = (\mathbf{I}_k, \mathbf{B})$.

A megfelelő paritásmátrix: $\mathbf{H} = (\mathbf{B}^\top, \mathbf{I}_{n-k})$.

Nem szisztematikus generátormátrixot Gauss-eliminációval olyan alakra hozhatunk, aminél léteznek i_1, i_2, \dots, i_k egészek, hogy az i_j oszlop a j -edik helyen 1, másutt 0. Ez oszlopcserével már szisztematikussá tehető.

Példák

1. $00 \mapsto 00000$, $01 \mapsto 01101$, $10 \mapsto 10110$, $11 \mapsto 11011$.

Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \quad \text{szisztematikus kód.}$$

Paritásmátrix:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

2. $00 \mapsto 000$, $01 \mapsto 011$, $10 \mapsto 101$, $11 \mapsto 110$.

Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \text{szisztematikus kód.}$$

Paritásmátrix:

$$\mathbf{H} = (1 \quad 1 \quad 1).$$

Adja meg az alábbi \mathcal{C} lineáris kódok egy paritásellenőrző mátrixát. Használja a korábban kiszámolt generátormátrixokat.

1 $\mathcal{C} = \{000, 001, 010, 011\}$

2 $\mathcal{C} = \{0000, 1001, 0110, 1111\}$

3 $\mathcal{C} = \{00000, 11111\}$

4 $\mathcal{C} = \{00000, 11100, 00111, 11011\}$

5 $\mathcal{C} = \{00000, 11110, 01111, 10001\}$

6 $\mathcal{C} = \{000000, 101010, 010101, 111111\}$

Megoldás

1. Kód: $\mathcal{C} = \{000, 001, 010, 011\}$.

Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \quad \text{Nem standard alakú: oszlopcserével azzá tehető} \quad \tilde{\mathbf{G}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

A $\tilde{\mathbf{G}}$ standard alakú mátrixhoz tartozó paritásellenőrző mátrix:

$$\tilde{\mathbf{H}} = (0 \ 0 \ 1). \quad \text{Ellenkező irányú oszlopcsere:} \quad \mathbf{H} = (1 \ 0 \ 0).$$

2. Kód: $\mathcal{C} = \{0000, 1001, 0110, 1111\}$.

Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad (\text{standard alakú}).$$

Paritásellenőrző mátrix:

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Megoldás

3. Kód: $\mathcal{C} = \{00000, 11111\}$.

Generátormátrix:

$$\mathbf{G} = (1 \ 1 \ 1 \ 1 \ 1) \quad (\text{standard alakú}).$$

Paritásellenőrző mátrix:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

4. Kód: $\mathcal{C} = \{00000, 11100, 00111, 11011\}$.

Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}. \quad \text{Nem standard alakú: oszlopcsere.} \quad \tilde{\mathbf{G}} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

A $\tilde{\mathbf{G}}$ standard alakú mátrixhoz tartozó paritásellenőrző mátrix:

$$\tilde{\mathbf{H}} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad \text{Ellenkező irányú oszlopcsere:} \quad \mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Megoldás

5. Kód: $\mathcal{C} = \{00000, 11110, 01111, 10001\}$.

Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (\text{standard alakú}).$$

Paritásellenőrző mátrix:

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

6. Kód: $\mathcal{C} = \{000000, 101010, 010101, 111111\}$.

Generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad (\text{standard alakú}).$$

Paritásellenőrző mátrix:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$



Példa

Egy bináris lineáris (n, k) kód paritásellenőrző mátrixa:

$$H = (1 \ 1 \ 1 \ 1 \ 1).$$

- 1 Adja meg az n és k értékét.
- 2 Határozza meg a kód generátormátrixát, a kódtávolságot és a kódszavak számát.
- 3 Mennyi egyszerű hibát képes a fenti kód detektálni, illetve javítani?
- 4 Vizsgálja meg, maximális távolságú szeparábilis-e, illetve perfekt-e a kód.

Megoldás.

1. A paritásellenőrző mátrix dimenziója $(n - k) \times n$, így $n = 5$, $k = 4$.

2. A

$$\mathbf{H} = (1 \ 1 \ 1 \ 1 \ 1)$$

paritásellenőrző mátrixhoz megadható egy standard alakú generátormátrix:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

A kód a $k = 4$ hosszúságú forrásüzeneteket egy paritásbittel egészíti ki. Emiatt $d_{\min} = 2$, a kódszavak száma pedig $2^k = 16$.

3. Mivel $d_{\min} = 2$, a kód egy egyszerű hibát képes detektálni, javítani viszont egyetlen egyszerű hibát sem tud.

4. $n - k + 1 = 2 = d_{\min}$: MDS; $1 < 2 = 2^{5-4}$: **nem** perfekt.

□

Kód minimális súlya

Egy \mathbf{c} vektor $w(\mathbf{c})$ súlya a koordinátái között levő nem nulla elemek száma.

Definíció. Egy \mathcal{C} kód *minimális súlyán* a

$$w_{\min} := \min_{\substack{\mathbf{c} \in \mathcal{C} \\ \mathbf{c} \neq \mathbf{0}}} w(\mathbf{c})$$

számot értjük.

Tétel. Ha \mathcal{C} egy lineáris kód, akkor a kódtávolsága megegyezik a minimális súlyával, azaz

$$d_{\min} = w_{\min}.$$

Magyarázat.

$$d_{\min} = \min_{\mathbf{c} \neq \mathbf{c}'} d(\mathbf{c}, \mathbf{c}') = \min_{\mathbf{c} \neq \mathbf{c}'} w(\mathbf{c} - \mathbf{c}') = \min_{\mathbf{c}'' \neq \mathbf{0}} w(\mathbf{c}'') = w_{\min}.$$

□

Egy $|\mathcal{C}|$ elemszámú \mathcal{C} kód esetén d_{\min} kiszámításához $|\mathcal{C}|(|\mathcal{C}| - 1)/2$, w_{\min} kiszámításához $|\mathcal{C}| - 1$ művelet szükséges.

Szindróma dekódolás

\mathbf{H} : egy \mathcal{C} kód paritásmátrixa.

Definíció. Az $\mathbf{s} = \mathbf{e}\mathbf{H}^\top$ mennyiséget *szindrómának* nevezzük.

\mathbf{c} : leadott kódszó; \mathbf{v} vett szó; $\mathbf{e} = \mathbf{v} - \mathbf{c}$: hibavektor.

$$\mathbf{H}\mathbf{v}^\top = \mathbf{H}(\mathbf{c} + \mathbf{e})^\top = \mathbf{H}\mathbf{c}^\top + \mathbf{H}\mathbf{e}^\top = \mathbf{H}\mathbf{e}^\top.$$

$\mathbf{H}\mathbf{v}^\top$ értéke nem függ az adott kódszótól, csak a hibavektortól.

Szindróma dekódolás:

- A vett \mathbf{v} szóból kiszámítjuk az $\mathbf{s}^\top = \mathbf{H}\mathbf{v}^\top = \mathbf{H}\mathbf{e}^\top$ szindrómát.
- A szindróma alapján megbecsüljük a hibavektort.
- A becsült hibavektort \mathbf{v} -ből kivonva megkapjuk a kódszóra vonatkozó becslést.

Egy \mathbf{e} hibaminta által generált *mellékosztály*: $\mathcal{C}_{\mathbf{e}} := \{\mathbf{e} + \mathbf{c} \mid \mathbf{c} \in \mathcal{C}\}$.

Egy adott mellékosztály elemeihez azonos szindróma tartozik.


Ha $\mathbf{e} = \mathbf{e}' + \mathbf{c}$, akkor $\mathcal{C}_{\mathbf{e}} = \mathcal{C}_{\mathbf{e}'}$. $\mathcal{C}_{\mathbf{0}} = \mathcal{C}$.

Mellékosztály-vezető: azonos mellékosztályba tartozó hibaminták közül a legkisebb súlyú.

Standard elrendezési táblázat

$\mathcal{C}(n, k)$: egy (n, k) típusú kód.

szindróma	mellékosztály- vezető			
$\mathbf{s}^{(0)}$	$\mathbf{e}^{(0)} = \mathbf{0}$	$\mathbf{c}^{(1)}$	\dots	$\mathbf{c}^{(s^k-1)}$
$\mathbf{s}^{(1)}$	$\mathbf{e}^{(1)}$	$\mathbf{c}^{(1)} + \mathbf{e}^{(1)}$	\dots	$\mathbf{c}^{(s^k-1)} + \mathbf{e}^{(1)}$
\vdots	\vdots	\vdots	\ddots	\vdots
$\mathbf{s}^{(s^{n-k}-1)}$	$\mathbf{e}^{(s^{n-k}-1)}$	$\mathbf{c}^{(1)} + \mathbf{e}^{(s^{n-k}-1)}$	\dots	$\mathbf{c}^{(s^k-1)} + \mathbf{e}^{(s^{n-k}-1)}$



mellékosztály elemek

Sorrend: $w(\mathbf{e}^{(i+1)}) \geq w(\mathbf{e}^{(i)})$, $\mathbf{e}^{(0)} = \mathbf{0}$, $i = 0, 1, \dots, s^{n-k} - 2$. A táblázat elemei mind különbözőek.

Definíció. Az $\mathbf{e}^{(i)}$, $i = 1, 2, \dots, s^{n-k} - 1$ mellékosztály-vezetőket *javítható hibamintáknak* nevezzük.

Vett \mathbf{v} szó szindrómája $\mathbf{s}^{(i)}$: a választott kódszó $\hat{\mathbf{c}} = \mathbf{v} - \mathbf{e}^{(i)}$.

Bináris eset: 2^{n-k} javítható hibavektor a szindrómával címezve.

Példa

$00 \mapsto 00000$, $01 \mapsto 01101$, $10 \mapsto 10110$, $11 \mapsto 11011$.

Paritásmátrix:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Dekódolási táblázat:

szindróma	javítható hibaminta
000	00000
001	00001
010	00010
011	00011
100	00100
101	01000
110	10000
111	01010

Az egyszeres hibák és a 00011, 01010 hibaminták javíthatóak.



Példa

Tekintsük a $\mathcal{C} = \{00000, 11100, 00111, 11011\}$ $(5, 2)$ bináris kódot, melynek egy paritásellenőrző mátrixa:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Adja meg a szindrómákat és a hozzájuk tartozó javítható hibamintákat.

Megoldás. Az egyes szindrómákhoz tartozó mellékosztályokat táblázatba rendezzük úgy, hogy a mellékosztály-vezetők (javítható hibaminták) súlyai nem csökkenő sorrendben vannak: [standard elrendezési táblázat](#).

szindróma	javítható hibaminta				
000	00000	11100	00111	11011	
110	00001	11101	00110	11010	
010	00010	11110	00101	11001	
100	00100	11000	00011	11111	
001	01000	10100	01111	10011	
101	10000	01100	10111	01011	
111	01001	10101	01110	10010	
011	01010	10110	01101	10001	



Bináris Hamming-kód

Egy hibát javítani képes lineáris, bináris kód. A hibajavításra r bit használható, azaz $n - k = r$.

Cél: rögzített n és r esetén a legnagyobb k elérése.

Paritásmátrix:

$$\mathbf{H} = (\mathbf{a}_1^\top, \mathbf{a}_2^\top, \dots, \mathbf{a}_n^\top).$$

Legfeljebb egy hiba esetén a javítható \mathbf{e} hibavektor: $\mathbf{e} = \mathbf{0}$ vagy $\mathbf{e} = \mathbf{e}_i$, $i = 1, 2, \dots, n$ (az i -edik pozíción 1, egyébként 0).

Az $\mathbf{s} = \mathbf{e}\mathbf{H}^\top$ **szindróma**: $\mathbf{0}$ vagy \mathbf{a}_i , $i = 1, 2, \dots, n$.

Az \mathbf{e} hiba (és így a \mathbf{c} kódszó) pontosan akkor adható meg egyértelműen, ha az \mathbf{a}_i vektorok mind különbözőek és egyik sem $\mathbf{0}$.

\mathbf{H} sorainak száma $n - k = r$: legfeljebb $2^r - 1$ különböző $\mathbf{a}_i \neq \mathbf{0}$ lehet.

Rögzített r esetén mind a $2^r - 1$ darab különböző bináris $\mathbf{a}_i \neq \mathbf{0}$ vektort kihasználjuk, ezek lesznek a \mathbf{H} oszlopai.

Kódszavak: a $\mathbf{H}\mathbf{c}^\top = \mathbf{0}$ egyenletrendszer megoldásai.

A bináris Hamming-kód tulajdonságai

Megjegyzés. Az (n, k) paraméterű bináris Hamming-kód esetén $n = 2^{n-k} - 1$, azaz a kód perfekt.

Néhány lehetséges számpár:

$$\begin{array}{rcccccc} n = & 3 & 7 & 15 & 31 & 63 & 127 \\ k = & 1 & 4 & 11 & 26 & 57 & 120 \end{array}$$

Tétel. *Nincs olyan egy hibát javító bináris kód, amely egy Hamming-kóddal azonos szóhosszúságú, és a hozzá tartozó kódszavak száma nagyobb, mint a megfelelő Hamming-kód kódszavainak száma.*

Példa. $(7, 4)$ paraméterű bináris Hamming kód:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Teletext metaadatainak kódolása (European Telecommunications Standards Institute: ETS 300 706 szabvány):
 $(7, 4)$ paraméterű Hamming-kód paritásbittel kiegészítve.