Információelmélet példatár

Összeállította: Györfi László

1. feladat. (Egyértelmű dekódolhatóság alternatív definíciója) *Nevezzünk egy $f : \mathcal{X} \to \mathcal{Y}^*$ kódot egyértelműen dekódolhatónak, ha az $\mathbf{u} = u_1 \cdots u_k$ és $\mathbf{v} = v_1 \cdots v_k$ üzenetekre (itt $u_1, v_i, \dots, u_k, v_k \in \mathcal{X}$)*

$$f(u_1)f(u_2)\cdots f(u_k) = f(v_1)f(v_2)\cdots f(v_k)$$

esetén $u_i = v_i$ minden i-re. Tehát, az órán elhangzott definícióval ellentétben most azt is megköveteljük, hogy bármely két különböző, azonos hosszúságú üzenet kódja is különbözzön. Bizonyítsd be, hogy a két definíció ekvivalens!

2. feladat. (Az optimális kód átlagos szóhossza) *Mutasd meg, hogy az optimális bináris kód átlagos szóhossza tetszőlegesen közel lehet $H(X) + 1$-hez. (Aminél azonban, ahogy azt órán léttuk, mindig kisebb.) Pontosabban, bármely kis $\epsilon > 0$ számhoz adj meg egy olyan eloszlást az $\mathcal{X}$ forrásábécén, hogy az optimális bináris kód átlagos szóhosszára*

$$\mathbf{E}|f(X)| > H(X) + 1 - \epsilon$$

teljesüljön.

3. feladat.* (Egyenlőség a Kraft egyenlőtlenségben) *Nevezzünk egy f prefix kódot teljesnek, ha bármely új kódszó hozzáadásával a kód elveszti prefix tulajdonságát. Egy $\mathbf{x}$ stringet dekódolhatatlannak nevezünk, ha nem lehet kódszavak egymás után írásával olyan stringet kapni, amelynek $\mathbf{x}$ a prefixe. Mutasd meg, hogy a következő három állítás ekvivalens:*

(a) *f teljes,*

(b) *nem létezik f-re nézve dekódolhatatlan string,*

(c) $\sum_{i=1}^{n} s^{-l_i} = 1$, *ahol s a kódábécé elemszáma, l_i az i-edik kódszó hossza, és n a kódszavak száma.*

4. feladat. (Rossz kódok) *A következő bináris kódok melyike nem lehet semmilyen eloszlás Huffmann kódja? Mindegyik válaszod indokold meg, azaz ha nincs ilyen eloszlás, akkor magyarázd meg, miért, ha pedig van, akkor adj meg egy olyat!*

(a) *0, 10, 111, 101*

(b) *00, 010, 011, 10, 110*

(c) *1, 000, 001, 010, 011*

5. feladat. *Legyen az $\mathcal{X}$ forrásábécé ötelemű, a következő valószínűségekkel:* $0.4; 0.35; 0.1; 0.1; 0.05$. *Mennyi az eloszlás entrópiája? Konstruáld meg az előző feladatban szereplő bináris Shannon-Fano kódot, illetve konstruálj bináris prefix kódot az $l_i = \lceil -\log p(x_i) \rceil$ kódhosszúságokkal az órán bemutatott módon (a kód bináris fával való reprezentálásával). Mennyi az átlagos kódszóhossz?*

6. feladat.* (A Shannon-Fano kód majdnem optimális) *Legyen* $l(x) = \left\lceil \log \frac{1}{p(x)} \right\rceil$ *a bináris Shannon-Fano kódban a forrásábécé* $x \in \mathcal{X}$ *eleméhez tartozó kódszavának hosszúsága, ahol* $p(x) = \mathbf{P}\{X = x\}$*. Legyen* $l'(x)$ *egy tetszőleges egyértelműen dekódolható kód* x*-hez rendelt kódszavának hosszúsága. Bizonyítsd be, hogy bármely* $c > 1$ *számra*

$$\mathbf{P}\{l(X) \geq l'(X) + c\} \leq \frac{1}{2^{c-1}},$$

tehát például annak a valószínűsége, hogy egy véletlenszerűen választott forrásszimbólum l' *kódszava öttel rövidebb, mint a megfelelő Shannon-Fano kódszó, kisebb, mint* $1/16$.

7. feladat. *Egy kétforintost addig dobunk fel, amíg írást nem kapunk. Jelölje az* X *valószínűségi változó a dobások számát. Mennyi az* X *entrópiája?*

8. feladat. (Egyenletesebb eloszlás entrópiája nagyobb) *Mutasd meg, hogy a*

$$(p_1, \ldots, p_i, \ldots, p_j \ldots, p_n)$$

eloszlás entrópiája nem lehet nagyobb, mint a

$$(p_1, \ldots, \frac{p_i + p_j}{2}, \ldots, \frac{p_i + p_j}{2} \ldots, p_n)$$

eloszlás entrópiája.

9. feladat.* (Egyenletesebb eloszlás optimális kódja rosszabb) *Tekintsük a*

$$\mathbf{p} = (p_1, \ldots, p_i, \ldots, p_j \ldots, p_n) \quad \textit{illetve} \quad \mathbf{q} = (p_1, \ldots, \frac{p_i + p_j}{2}, \ldots, \frac{p_i + p_j}{2} \ldots, p_n)$$

eloszlásokat. Mutasd meg, hogy a $\mathbf{q}$ *eloszláshoz tartozó optimális (minimális átlagos szóhosszúságú) kód átlagos szóhosszúsága (*$\mathbf{q}$ *szerint) nem lehet kisebb, mint a* $\mathbf{p}$ *eloszláshoz tartozó optimális kód átlagos szóhosszúsága (*$\mathbf{p}$ *szerint).*

10. feladat. (Információs divergencia) *Legyen* $\mathbf{p} = (p_1, \ldots, p_n)$ *és* $\mathbf{q} = (q_1, \ldots, q_n)$ *két valószínűség eloszlás, és definiáljuk a két eloszlás közötti „információs távolságot” a*

$$D(\mathbf{p}|\mathbf{q}) = \sum_{i=1}^{n} p_i \log \frac{p_i}{q_i}$$

kifejezéssel. (A mennyiséget gyakran információs divergenciának, relatív entrópiának, vagy Kullback-Leibler távolságnak nevezik.) Lássuk be a következő tulajdonságokat:

- *Bármely két eloszlásra* $D(\mathbf{p}|\mathbf{q}) \geq 0$*, és egyenlőség pontosan akkor teljesül, ha* $\mathbf{p} = \mathbf{q}$.
- $H(\mathbf{p}) = \log n - D(\mathbf{p}|\mathbf{u})$*, ahol* $H(\mathbf{p})$ *jelöli a* $\mathbf{p}$ *eloszlás entrópiáját,* $\mathbf{u}$ *pedig az egyenletes eloszlást az* $\{1, \ldots, n\}$ *halmazon.*

11. feladat. (Rosszul ismert eloszlás) *Tegyük fel, hogy az* X *valószínűségi változó eloszlása* $\mathbf{p} = (p_1, \ldots, p_n)$*, de ez az eloszlás nem pontosan ismert, helyette a* $\mathbf{q} = (q_1, \ldots, q_n)$ *eloszlás adott, és ennek ismeretében készítünk Shannon-Fano kódot, melynek kódszóhosszúságai tehát* $l_i = \left\lceil \log \frac{1}{q_i} \right\rceil$, $i = 1, \ldots, n$*. Mutasd meg, hogy a kapott kód átlagos kódszóhosszúságára*

$$H(\mathbf{p}) + D(\mathbf{p}|\mathbf{q}) \leq \sum_{i=1}^{n} p_i l_i < H(\mathbf{p}) + D(\mathbf{p}|\mathbf{q}) + 1$$

teljesül. Ez azt jelenti, hogy az ár, amelyet az eloszlás pontatlan ismeretéért fizetünk körülbelül az információs divergenciával egyezik meg (ami sohasem lehet negatív, tehát semmiképpen sem nyerhetünk!).

12. feladat.* (ÜGETŐ) *Egy lóversenyen n ló fut, és az i-edik $p(i)$ valószínűséggel nyer. A bukméker az i-edik lóra tett pénz $o(i)$-szeresét fizeti vissza (ahol $o(i) > 0$), ha az nyer, minden más helyezésnél elvész a fogadott pénz. A versenyt k-szor futják le, minden futamban változatlanok az esélyek és az oddszok. Jelöljék az $X_1, \ldots, X_k$ valószínűségi változók az egyes futamok nyertes lovainak sorszámait. Tegyük fel, hogy egységnyi pénzzel indulunk, minden körben "befektetjük" az összes pénzünket, és minden körben ugyanolyan arányban osztjuk el az egyes lovak között: az i-edik lóra pénzünk $b(i)$-szeresét tesszük ($\sum_{i=1}^{n} b(i) = 1$). Világos, hogy a k futam után*

$$S_k = \prod_{i=1}^{k} b(X_i) o(X_i)$$

pénzünk van. Egy adott $\mathbf{p} = (p(1), \ldots, p(n))$ eloszlásra és $\mathbf{b} = (b(1), \ldots, b(n))$ fogadási stratégiára legyen

$$W(\mathbf{b}, \mathbf{p}) = \mathbf{E} \log(b(X_1) o(X_1)) = \sum_{i=1}^{n} p(i) \log(b(i) o(i)).$$

Mutasd meg, hogy

$$S_k \approx 2^{kW(\mathbf{b},\mathbf{p})},$$

ahol $a_k \approx b_k$ jelentése $\lim_{k\to\infty} \frac{1}{k} \log \frac{a_k}{b_k} = 0$, és a fenti konvergenciát valószínűségben (sztochasztikusan) értjuk. Látszik tehát, hogy hosszú távon $W(\mathbf{b}, \mathbf{p})$ maximalizálása eredményezi a legnagyobb jövedelmet. Bizonyítsd be, hogy $\mathbf{b}$ optimális értéke $\mathbf{b} = \mathbf{p}$, tehát pénzünket a valószínűségek arányában kell elosztani, függetlenül az oddszok értékétől (!!!).

13. feladat. (SHANNON-FANO ÉS HUFFMAN KÓD) *Legyen az X valószínűségi változó eloszlása*

$$(1/3; 1/3; 1/4; 1/12).$$

Konstruálj Huffmann kódot ehhez az eloszláshoz. Mutasd meg, hogy két különböző optimális kód is van, azaz, hogy az $(1; 2; 3, 3)$, és a $(2; 2; 2; 2)$ kódszóhosszúságokkal adott mindkét kód optimális. Vond le a következtetést, hogy létezik olyan optimális kód, amelynek van a megfelelő Shannon-Fano kódénál hosszabb kódszava is.

14. feladat.* *Egy X valószínűségi változó eloszlásából egymástól függetlenül sorsolt szimbólumokat betűnként optimálisan (Huffmann kóddal) kódolták. Egy hat hosszúságú üzenet kódolásának eredménye az 10110000101 string. Azt tudjuk, hogy a forrásábécé öt elemű, a forrás eloszlásáról azonban csak az ismert, hogy az egyes szimbólumok valószínűségeit a $\{0,4; 0,3; 0,2; 0,05; 0,05\}$, és $\{0,3; 0,25; 0,2; 0,2; 0,05\}$ eloszlások egyike adja meg. Állapítsuk meg a forrás eloszlását!*

15. feladat. (TITKOSÍTÁS) *Legyenek X és Z bináris (0-1 értékű) független valószínűségi változók. Eloszlásukat $\mathbf{P}\{X = 1\} = p$ és $\mathbf{P}\{Z = 1\} = 1/2$ adja meg. Legyen $Y = X \oplus Z$, ahol $\oplus$ modulo 2 összeadást jelöl. X felfogható, mint titkosítandó üzenet, Z a titkos kulcs, és Y a rejtjelezett üzenet. Számold ki a következő mennyiségeket: $H(X), H(X|Z), H(X|Y), H(X|Y, Z), I(X;Y), I(X;Z), I(X;(Y, Z))$. Értelmezd a kapott eredményeket, például azt, hogy mit jelent az $I(X;Y)$-ra kapott szám.*

16. feladat. (EGYENLŐTLENSÉGEK) *Legyenek X, Y és Z tetszőleges (véges értékkészletű) valószínűségi változók. Bizonyítsd be a következő egyenlőtlenségeket:*

- $H(X, Y|Z) \geq H(X|Z)$,

- $I((X,Y);Z) \geq I(X;Z)$,
- $H(X,Y,Z) - H(X,Y) \leq H(X,Z) - H(X)$.

17. feladat.* (Kártyapakli keverése növeli a rendezetlenséget) *Legyen X egy tetszőleges valószínűségi változó , amely értékeit az $\{1,2,\ldots,52\}$ halmazból veszi fel. Legyen T az $1,2,\ldots,52$ számok egy véletlen permutációja, azaz $T(1),T(2),\ldots,T(52)$ a $\{1,2,\ldots,52\}$ halmaz elemeinek egy véletlen átrendezése. (Feltesszük, hogy T független X-től.) Bizonyítsd be, hogy*

$$H(T(X)) \geq H(X).$$

18. feladat. (Futamhossz kódolás) *Legyenek $X_1,\ldots,X_n$ bináris valószínűségi változók. Jelölje $\mathbf{R} = (R_1,R_2,\ldots)$ az egyes szimbólumok előfordulásainak futamhosszait. Tehát például az 1110010001111 sorozathoz $\mathbf{R} = (3,2,1,3,4)$ tartozik. Hogyan viszonyul egymáshoz $H(X_1,\ldots,X_n), H(\mathbf{R})$ és $H(\mathbf{R},X_n)$?*

19. feladat. (Markov-lánc entrópiája) *Legyen $\mathbf{X} = X_1,X_2,\ldots$ egy bináris, stacionárius Markov lánc, amely állapotátmenetei a következők:*

$$\mathbf{P}\{X_2=0|X_1=0\}=p,\ \mathbf{P}\{X_2=1|X_1=0\}=1-p,\ \mathbf{P}\{X_2=0|X_1=1\}=\frac{1-p}{2},\ \mathbf{P}\{X_2=1|X_1=1\}=\frac{1+p}{2}.$$

Mennyi $\mathbf{P}\{X_1=0\}$? Mennyi a forrás entrópiája?

20. feladat.* (A termodinamika második főtétele) *Legyen $\mathbf{X} = X_1,X_2,\ldots$ egy stacionárius Markov-lánc. Mutasd meg, hogy $H(X_n|X_1)$ monoton nő, ahogy n növekszik. (Annak ellenére, hogy a stacionaritás miatt nyilván $H(X_n)$ nem változik.)*

21. feladat. (Bináris entrópiafüggvény tulajdonságai) *Legyen a $[0,1]$ intervallumon értelmezett h függvény értéke $h(x) = -x\log x - (1-x)\log(1-x)$, ha $x \in (0,1)$, és $h(0) = h(1) = 0$. Mutassuk meg, hogy h rendelkezik a következő tulajdonságokkal:*

- $1/2$ *körül szimmetrikus;*
- $[0,1]$ *minden pontjában folytonos;*
- $[0,1/2]$*-ben szigorúan monoton növekvő;*
- *szigorúan konkáv.*

22. feladat. (Vissza a jövőbe) *Legyen $\ldots,X_{-2},X_{-1},X_0,X_1,X_2,\ldots$ valószínűségi változók egy stacionárius sorozata. Mutasd meg, hogy*

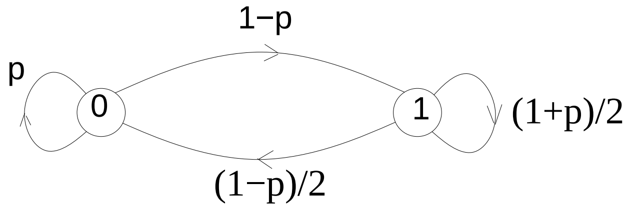
$$H(X_0|X_{-1},X_{-2},\ldots,X_{-n}) = H(X_0|X_1,X_2,\ldots,X_n),$$

azaz, a jelen feltételes entrópiája a múlttal, és jövővel, mint feltétellel megegyezik.

23. feladat. *Legyenek a $\mathbf{Z}$ stacionárius Markov-lánc állapotai a $0,1,\ldots,255$ számok. Legyenek az állapotátmenet valószínűségek az alábbi 256×256-os mátrix-szal adottak. (A mátrix i-edik sorának j-edik* *oszlopában a $\mathbf{P}\{Z_2 = j | Z_1 = i\}$ valószínűség található.) Mi a Markov-lánc stacionárius eloszlása? Mennyi a forrás entrópiája? Készíts jó egyértelműen dekódolható, változó szóhosszúságú blokk-kódot!*

$$\begin{bmatrix} 1/2 & 1/4 & 1/4 & 0 & 0 & 0 & \cdots & & & 0 \\ 0 & 1/2 & 1/4 & 1/4 & 0 & 0 & \cdots & & & 0 \\ 0 & 0 & 1/2 & 1/4 & 1/4 & 0 & \cdots & & & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \cdots & & & & 0 & 1/2 & 1/4 & 1/4 \\ 1/4 & 0 & 0 & \cdots & & & & 0 & 1/2 & 1/4 \\ 1/4 & 1/4 & 0 & \cdots & & & & 0 & 0 & 1/2 \end{bmatrix}$$

24. feladat. *Az alábbi ábra egy $\mathbf{Z} = Z_1, Z_2, \ldots$ Markov-lánc működését írja le. Tegyük fel, hogy a láncot a stacionárius eloszlásból indítjuk.*



Legyen továbbá $Y_1, Y_2, \ldots$ független, azonos eloszlású bináris valószínűségi változók sorozata, ahol $P(Y_i = 0) = \frac{1}{3}$. Definiáljuk az $\mathbf{X} = X_1, X_2, \ldots$ forrást az $X_i = 2Z_i + Y_i$ egyenlettel. Mennyi az $\mathbf{X}$ forrás entrópiája feltéve, hogy $Z_1, Z_2, \ldots$ független $Y_1, Y_2, \ldots$-től?

25. feladat. (Ismétléses kód) *Két üzenet (0 és 1) egyikét szeretnénk egy p hibavalószínűségű bináris szimmetrikus csatornán továbbítani. Álljon a csatornakód a (000) és (111) kódszavakból, vagyis az üzenetbitet egyszerűen háromszor küldjük át a csatornán. Dekódoláskor többségi döntést hozunk, azaz azt a szimbólumot választjuk, amely legalább kétszer szerepel a csatorna kimenetén megjelenő három bit közül. Mutasd meg, hogy a dekódolás hibavalószínűsége $P_e = P_{e,1} = P_{e,2} = 3p^2 - 2p^3$.*

26. feladat. (Paritásbit használata visszacsatolásos csatornán) *A gyakorlatban rendkívül gyakran használt kódolási módszer az, hogy az üzenet bináris stringet egy bittel meghosszabbítjuk, és ez a bit éppen a string bitjeinek bináris összege (paritásbit). Ez a kód természetesen hibajavításra nem alkalmas, azonban, ha páratlan számú hiba történik átvitel során, akkor azt a dekódoló észreveszi, és ha van visszacsatolás a csatornán, akkor az üzenet ismételt küldését kérheti. A legegyszerűbb eset a következő: Tekintsünk egy bináris szimmetrikus csatornát p hibavalószínűséggel. Csakúgy, mint az előző példában, az üzenet a 0 és 1 szimbólumok valamelyike. A kódolási szabály szerint, ha az üzenet 0, akkor a (00) kódszót küldjük át a csatornán, míg 1 esetén az (11) kódszót. Dekódoláskor, ha a két vett bit megegyezik, akkor annak megfelelően döntünk, ha pedig nem, akkor újabb küldést igénylünk. Bizonyítsd be, hogy ekkor a dekódolás hibavalószínűsége*

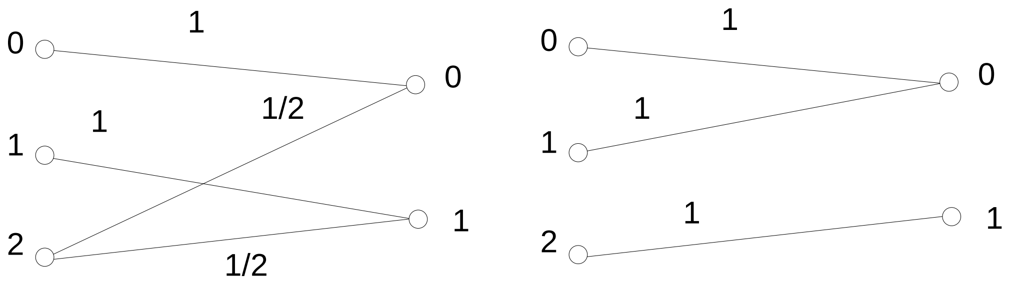
$$P_e = P_{e,1} = P_{e,2} = \frac{p^2}{1 - 2p + 2p^2},$$

továbbá, hogy egy üzenetbit továbbításához átlagosan

$$\frac{2}{1 - 2p + 2p^2}$$

bitet kell a csatornán átküldeni. Hasonlítsd össze ezeket a számokat az előző példa eredményével! Látszik, hogy ha p kicsi (kisebb, mint $(1 - 1/\sqrt{3})/2$), akkor kevesebb bit továbbításával kisebb hibavalószínűséget tudtunk elérni a visszacsatolásnak köszönhetően. Másrészt azonban meglepő, de bebizonyítható, hogy a visszacsatolás nem növeli a csatornakapacitást, azaz, visszacsatolás nélkül is mindig elérhető ugyanaz a jelsebesség és hibavalószínűség, legfeljebb hosszabb blokkokat kell használni.

27. feladat. *Mennyi az ábrán látható két csatorna kapacitása?*



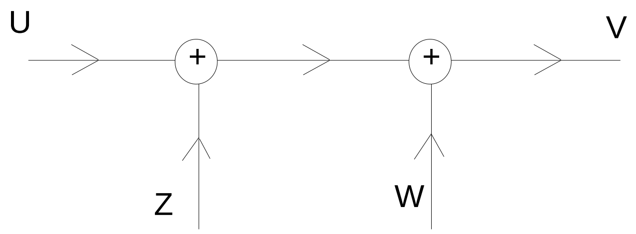
Tegyük fel most, hogy a két csatornát egyszerre használjuk, azaz a bemeneti 0,1, vagy 2 szimbólumot mindkét csatornán továbbítjuk. Így egy olyan csatornához jutottunk, amelynek három lehetséges bemenete, és négy kimenete van. Mennyi az új csatorna kapacitása? Mutasd meg, hogy mindhárom csatorna esetén van olyan $R = C$ jelsebességű kód, amely nulla hibavalószínűséggel dekódolható.

28. feladat. (MOD 11 CSATORNA) *Legyen egy diszkrét memóriamentes csatorna bemenete $U \in \{0, 1, \dots, 10\}$. A csatorna kimenetét, V-t a $V = U + Z \pmod{11}$ egyenlet határozza meg, ahol Z független U-tól és*

$$P\{Z = 1\} = P\{Z = 2\} = P\{Z = 3\} = \frac{1}{3}.$$

a, Határozd meg a csatorna kapacitását!
b, Adj maximális jelsebességű, egy-hosszú blokkokat kódoló csatornakódot, melyet 0 hibavalószínűséggel lehet dekódolni! Mekkora az így elérhető legnagyobb jelsebesség?

29. feladat. *Az ábrán látható blokksémán U, Z és W független bináris valószínűségi változók , $\oplus$ pedig modulo 2 összeadást jelöl. Az elrendezés meghatároz egy bináris csatornát, melynek bemenete U, kimenete V.*
(a) Mennyi a csatorna kapacitása, ha $\mathbf{P}\{Z = 1\} = p$ és $\mathbf{P}\{W = 1\} = q$?
(b) Ha az első $\oplus$ műveletet kicseréljük bináris „vagy” műveletre, a másodikat bináris „és” műveletre, akkor $p = 1/3$ és $q = 3/4$ esetén mi a csatorna kapacitása?



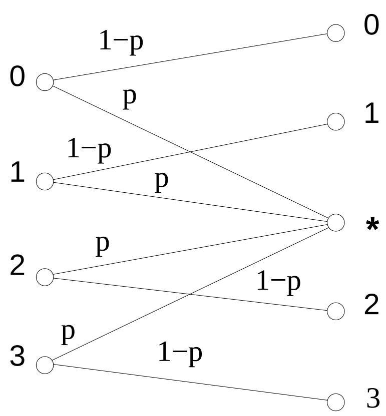
30. feladat. (BSC-K KASZKÁDJA) *Kapcsoljunk egymás után k darab bináris szimmetrikus csatornát, melyek mindegyikének hibavalószínűsége p. Mutasd meg, hogy a kapott csatorna ekvivalens egy bináris* *szimmetrikus csatornával, amely hibavalószínűsége* $\frac{1}{2}(1-(1-2p)^k)$*, azaz, a csatorna kapacitása nullához tart, ahogy* k *tart végtelenhez. (Az információelmélet megszületésekor az jelentette az egyik legnagyobb meglepetést, hogy ha az egyes csatornák közé kódolókat és dekódolókat teszünk, akkor az egyes elemi csatornák kapacitásának megfelelő jelsebesség mellett tetszőlegesen kis hibavalószínűség érhető el. Más szóval, az átvitel tulajdonságai megjavíthatóak az átvivő közegbe iktatott kódolók és dekódolók segítségével, anélkül, hogy a közeg fizikai tulajdonságait megváltoztatnánk.)*

31. feladat. (Törléses csatorna kapacitása) *Bizonyítsd be, hogy a* p *hibavalószínűségű bináris törléses csatorna kapacitása* $C = 1 - p$.

32. feladat.* (Gyengén szimmetrikus csatornák kapacitása) *A csatornamátrix a* $p(v|u)$ *átmeneti valószínűségeket tartalmazza* ($u \in \mathcal{U}, v \in \mathcal{V}$)*, mégpedig úgy, hogy az* i*-edik sor* j*-edik oszlopában a* $p(v_j|u_i)$ *valószínűség áll. Egy diszkrét memóriamentes csatornát gyengén szimmetrikusnak nevezünk, ha csatornamátrixa minden sora ugyanannak a* $\mathbf{p}$ *valószínűség vektornak egy permutációja, továbbá az oszlopokban álló valószínűségek összege állandó. Mutasd meg, hogy egy ilyen csatorna kapacitása*

$$C = \log|\mathcal{V}| - H(\mathbf{p}).$$

33. feladat. *(a) Mennyi az ábrán látható csatorna kapacitása?*



(b) Az előző csatornánál legyen $p = \frac{1}{4}$*! Tegyük fel, hogy a csatornát összesen 30-szor használhatjuk. Közelítőleg hány bites bináris üzenetek átvitelét valósíthatjuk így meg, ha az üzenet meghibásodásának valószínűségét kis szinten akarjuk tartani?*

34. feladat. (Kapacitás fölötti jelsebesség) *Tegyük fel, hogy egyenletes eloszlással véletlenszerűen sorsolt* n *hosszúságú bináris stringeket kódolás nélkül továbbítunk egy* p *hibavalószínűségű bináris szimmetrikus csatornán. Világos, hogy ekkor a jelsebesség nagyobb, mint a csatornakapacitás. Mekkora a dekódolás hibavalószínűsége? Mekkorára érdemes az* n *blokkhosszat választani?*

35. feladat. (MAP és ML dekódolás) *Vegyünk egy bináris szimmetrikus csatornát* p *hibavalószínűséggel. Tegyük fel, hogy két üzenet egyikét akarjuk továbbítani, és* n *hosszúságú ismétléses kódot alkalmazunk. Azaz, az első üzenet esetén az* n *darab nullából, míg a második esetén az* n *darab egyesből álló kódszót küldjük át a csatornán. Órán láttuk, hogy a maximum likelihood dekódolás azt a kódszót választja ki, amelynek a csatorna kimenetén vett sorozattól mért Hamming távolsága kisebb. Tudjuk, hogy a legkisebb hibavalószínűségű dekódolás a maximum a posteriori dekódolás. Tegyük most fel, hogy a két* *üzenet küldésének valószínűsége q, illetve $1-q$. Állapítsd meg a maximum a posteriori dekódolás szabályát! Például $p = 1/3$ és $q = 0,1$ esetén határozd meg a dekódolási szabályt n több értékére, pl. $n = 3, 10, 100$ esetén.*

36. feladat. (ML dekódolás törléses csatornán) *Állapítsd meg a maximum likelihood dekódolás szabályát bináris törléses csatornán!*

37. feladat. (Időjóslás) *Tegyük fel, hogy az esős és napsütéses napok stacionárius Markov lánc szerint követik egymást a következő eloszlás szerint:*

$$\mathbf{P}\{\textit{ma esni fog}|\textit{tegnap esett}\} = 0,5; \qquad \mathbf{P}\{\textit{ma esni fog}|\textit{tegnap sütött a nap}\} = 0,3.$$

Arra próbálok meg reggel dönteni a tegnapi időjárás ismeretében, hogy vigyek-e esernyőt. A költségeim a következők: Ha viszek esernyőt, akkor akár esik, akár nem, 100 Ft a költségem (ez abból adódik, hogy gyakran elvesztem az esernyőmet). Ha nem viszek esernyőt, és süt a nap, akkor nincs költségem. Ha viszont esik, és nincs nálam ernyő, akkor tönkremegy a frizurám, ami 150 forintomba kerül. Mi az optimális döntés, ha tegnap esett, illetve, ha tegnap sütött a nap? Mi a helyzet akkor, ha drága, 200 forintos frizurám van? Mennyi optimális döntés esetén a várható költségem a két esetben?

38. feladat. (Detekció additív Gauss zajban) *Tekintsük az órán tárgyalt detekciós feladatot, azaz, amikor bináris szimbólumokat továbbítunk additív Gauss zajjal terhelt analóg csatornán. Hogyan alakul a Bayes (maximum a posteriori) döntés, ha a nullák és egyesek valószínűsége most nem egyenletes, hanem q és $1-q$? Számold ki $n = 1$ esetén (azaz vételkor egyszer veszünk mintát a vett jelalakból) a döntés hibavalószínűségét! Hogyan írható fel egyszerűen a Bayes döntés „fehér zaj” esetén, azaz, ha az egyes mintavételi időpontokban a jelhez adódó normális eloszlású valószínűségi változók egymástól függetlenek? (Itt persze $n > 1$.)*