Теорија информација **2020**

Ове белешке су настале након вишегодишњег држања вежби за овај предмет од тренутка када је др Марко Обрадовић постао наставник на овом предмету. Ове белешке не би настале без марљивог рада и труда колегиница Бојане Тодић и Тамаре Милић, које су пре мене држале овај курс, на чему им се у потпуности захваљујем.

Трудио сам се да што више и детаљније пишем све што се тиче решења задатака. Надам се да ће постојање овакве скрипте значајно да олакше како слушање тако и учења овог предмета.

Данијел Суботић

Мотивација

На почетку 20. века научници и инжењери су поставили следећа битна питања:

1. Како квантификовати(мерити) информацију?
2. Да ли постоји аналитички математички апарат који би то одрадио?

И размотримо следећа две реченице:

- Жућа је пас.
- Жућа је велики црни пас.

Није тешко закључити да друга реченица нам даје више информације, јер нам преноси и то да је Жућа "велик" и "црн" поред тога што је "пас". Како измерити разлику између ове две реченице? И да ли постоји математичка мера која може да каже колико више информације друга реченица садржи у поређењу са првом?

Научници су се борили са тим питањима. Семантика, домен и облик података је само додавало тежине том задатку, све до појаве Клода Шенона на сцени. Он је први дошао на идеју "неодређености" која је заувек променила начин посматрања нашег света и поставила темеље за почетак "дигитално-информационе ере".

Шенон је предложио да је семантички аспект података заправо небитан и да природа и значење података нису значајни када је реч о информационом садржају. Он је дефинисао квантификацију информацију у терминима вероватносних мера и "неодређености". Ове револуционарне идеје не само да су поставили Теорију информације као засебну грану, већ и отворили огромну могућност напретка области попут вештачке интелигенције. Даље ћемо размотрити неке битне појмове са и интуиције која стоја иза тих идеја.

Неодређеност(Ентропија)

Ентропија нам даје меру неодређености приликом извођења неког експеримента. Размотримо следећа два:

1. Бацамо хомоген новчић и посматрајмо исход, рецимо, писмо
2. Бацамо нехомоген новчић ($P(\text{pismo}) = 0.99$) и посматрајмо исход, рецимо, писмо

Ако упоредимо ова два експеримента, очигледно је да у случају овог другог лакше предвидети исход. Можемо рећи да је први експеримент **значајно неодређенији** него други. И баш ту неодређеност ентропија и има за циљ да квантификује. Баш расподела вероватноћа исхода се користи за рачунање неодреједности.

Детерминистички експеримент, који је у потпуности предвидив, има неодређеност једнаку нули. А експеримент који је у потпуности (бацање хомогеног новчића) насумичан је најтеже предвидив и има највећу неодређеност од свих експеримената тог типа.

Узајамна информација

Узајамна информација је мера узајамне зависности између две вероватносне расподеле или случајних величина. Помоћу ње видимо колико информација о једној променљивој је садржано у другој.

Узајамна информација детектује зависности међу случајним величинама и много је општија него прости коефицијент корелације, који детектује само линеарне зависности.

Кулбак-Лајблерово(КЛ) разилажење

КЛ разилажење је још једна мера сличности између две вероватносне расподеле. Помоћу ње можемо измерити колико једна расподела одступа од друге.

Претпоставимо да имамо податке, који су из неке расподеле P. Међутим у пракси, ми никад не знамо ту праву расподелу P, зато бирамо неку расподелу Q која апроксимира P и одговара добијеним подацима. Како је Q само апроксимација она неће моћи баш идеално да погоди податке као расподела P и створиће се неко информационо **разилажење**. Баш то разилажење зовемо Кулбак-Лајблеровим.

КЛ разилажење између P и Q нам говори колико много информација губимо ако апроксимирамо расподелу P са расподелом Q.

Неке значајне једнакости за решавање задатака:

I.1. $H(X) = -\sum_i P\{X=i\}\log_2(P\{X=i\}) = -\sum_i p(x_i)\log_2 p(x_i)$

I.2. $H(X,Y) = -\sum_i \sum_j p(x_i,y_j)\log_2 p(x_i,y_j)$

I.3. $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$

I.4. $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$

I.5. $H(Y|X) = \sum_i p(x_i)H(Y|X=x_i)$

I.6. $H(X_1,\dots,X_n) = \sum_{i=1}^n H(X_i|X_{i-1},\dots,X_1)$

I.7. $I(X;Y|Z) = H(X|Z) - H(X|Z,Y) = H(Y|Z) - H(Y|Z,X)$

I.8. $I(X_1,\dots,X_n|Y) = \sum_{i=1}^n I(X_i;Y|X_{i-1},\dots,X_1)$

I.9. $KL(p||q) = \sum_i p(x_i)\log_2\left(\frac{p(x_i)}{q(x_i)}\right)$

I.10. $I(X;Y) = \sum_i \sum_j p(x_i,y_j)\log_2 \frac{p(x_i,y_j)}{p(x_i)p(y_j))}$

Неодређеност и Узајамна Информација

1. Баца се фер новчић до прве појаве писма. Нека је X случајна величина која представља број потребних бацања. Наћи неодређеност случајне величине X.

Решење 1. Можемо закључити да X има Геометријску $G(\frac{1}{2})$ расподелу. Неодређеност је, по дефиницији,

$$H(X) = -\sum_{i=1}^{\infty} P\{X=i\}\log_2\left(P\{X=i\}\right).$$

У нашем случају

$$P\{X=i\} = (1-p)^{i-1}p = \frac{1}{2^i},$$

одакле директно добијамо

$$H(X) = -\sum_{i=1}^{\infty} 2^{-i}\log_2(2^{-i}) = \sum_{i=1}^{\infty}\frac{i}{2^i} = E(X) = 2.$$

▲

2. Показати да за дискретну случајну величину X важи неједнакост

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

где је $g(\cdot)$ произвољна неслучајна функција.

Решење 2. Важи формула

$$H(X, g(X)) = H(X) + H(g(X)|X) = H(X),$$

јер $H(g(X)|X) = 0$ - нема неодређености за вредност $g(X)$ ако је позната вредност случајне величине X. Слично

$$H(X, g(X)) = H(g(X)) + H(X|g(X)) \ge H(g(X)),$$

одакле добијамо тврђење из поставке задатка. ▲

3. Струјно коло чине 22 сијалице. Ако једна прегори, остале не могу да сијају, јер је електрично коло прекинуто. На располагању имамо омметар којим можемо да измеримо отпор између сваке две тачке у струјном колу. Колики је минималан број мерења потребан да би пронашли прегорену сијалицу?

Решење 3. За домаћи.

4. Дата је заједничка дводимензиона расподела

	$Y=0$	$Y=1$
$X=0$	$\frac{1}{3}$	$\frac{1}{3}$
$X=1$	0	$\frac{1}{3}$

Наћи $H(X)$, $H(Y)$, $H(X|Y)$, $H(Y|X)$, $H(X,Y)$ и $I(X;Y)$.

Решење 4. Из дводимензионе расподела из поставке задатка добијамо маргиналне расподеле

$$X : \begin{pmatrix} 0 & 1 \\ 2/3 & 1/3 \end{pmatrix}$$

$$Y : \begin{pmatrix} 0 & 1 \\ 1/3 & 2/3 \end{pmatrix}$$

На основу чега даље применом формула наведених у старту фајла добијамо

$$H(X) = -\left(\frac{1}{3}\log_2\frac{1}{3} + \frac{2}{3}\log_2\frac{2}{3}\right) = \log_2 3 - \frac{2}{3} \sim 0.918$$

Приметимо да је $H(Y) = H(X)$.
Даље, према формули $(I.5.)$

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

јер

$$X|Y=0 : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X|Y=1 : \begin{pmatrix} 0 & 1 \\ 1/2 & 1/2 \end{pmatrix}$$

Слично,

$$H(Y|X) = P\{X=0\}H(Y|X=0) + P\{X=1\}H(Y|X=1) = \frac{2}{3}.$$

$$H(X,Y) = H(X) + H(Y|X) = \log_2 3.$$

И на крају

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

▲

5. Коцкица се баца једном. Ако падне број 1, 2, 3 или 4 новчић се баца једном, а иначе два пута. Наћи информацију о броју који је пао на коцкици на основу броја палих глава.

Решење 5. За самосталну вежбу. ▲

6. Нека су X_1 и X_2 дискретне случајне величине које узимају различите вредности и X случајна величина дефинисана као

$$X = \begin{cases} X_1, & \text{са вероватноћом } \alpha \\ X_2, & \text{са вероватноћом } 1-\alpha \end{cases}$$

Наћи неодређеност $H(X)$ у функцији од $H(X_1)$, $H(X_2)$ и α.

Решење 6. Дефинишемо θ као функцију од X на следећи начин

$$\theta = \begin{cases} 1, & X = X_1 \\ 2, & X = X_2 \end{cases}$$

И применом формула $(I.1.)$, $(I.2.)$ и $(I.5.)$ са почетка скрипте добијамо

$$\begin{aligned} H(X) &= H(X,\theta) \\ &= H(\theta) + H(X|\theta) \\ &= -\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha) + \alpha H(X_1) + (1-\alpha)H(X_2). \end{aligned}$$

▲

7. Са вероватноћом $\frac{1}{2}$ у једној од 8 фиока се налази писмо. Редом је отворено 7 фиока и ни у једној нема писма, наћи вероватноћу да је писмо у последњој фиоци.

Решење 7. Замислимо да заправо имамо 16 фиока - од којих је 8 правих, а 8 виртуелних. Са вероватноћом $\dfrac{1}{2}$ имамо да је писмо у првих 8 (правих) фиока или исто са вероватноћом $\dfrac{1}{2}$ у других 8 (виртуелних) фиока. Након што смо отворили 7 фиока преостало је још 9. Вероватноћа да се писмо налази у тој траженој фиоци је $\dfrac{1}{9}$. ▲

8. Од 27 новчића један је фаличан и лакши од осталих. На располагању имамо вагу за мерење са два таса. Колико мерења је потребно да се сигурно одреди фаличан новчић?

Решење 8. У старту су сви подједнако вероватни и вероватноћа је $\frac{1}{27}$.

$$H(\frac{1}{27},\dots,\frac{1}{27}) = \log_2 27 \sim 4.76.$$

У сваком мерењу можемо имати три могућа ишода, стога да извучемо више информација делимо наш почетни скуп на $9-9-9$ новчића. Узмемо две групе и измеримо, након чега тачно знамо у којој од група по 9 новчића се налази тај један фаличан. Ту групу од 9 поново поделимо на три групе $3-3-3$. Након другог мерења преостаће само три новчића, након још једног мерења одмах знамо који је фаличан. Дакле, довољно је 3 мерења. ▲

9. Од 27 новчића један је фаличан, лакши или тежи од осталих. На располагању имамо вагу за мерење са два таса. Колико мерења је потребно да се сигурно одреди фаличан новчић са информацијом да ли је лакши или тежи?

Решење 9. За домаћи.

10. Користећи знања из области вероватноће и статистике показати да важи

$$\int_{-\infty}^{\infty} e^{-x^2}dx = \sqrt{\pi}.$$

Решење 10. Сетимо се да је функција густине нормалне $\mathcal{N}(\mu,\sigma^2)$ расподеле заправо

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \quad x \in \mathbb{R}.$$

И приметимо да за вредности $\mu = 0$ и $\sigma^2 = \frac{1}{2}$ добијамо тражену једнакост. ▲

11. Показати да је неодређеност расподеле вероватноћа $P = (p_1,\dots,p_i,\dots,p_j,\dots,p_m)$ мања или једнака од неодређености расподеле $Q = (p_1,\dots,\frac{p_i+p_j}{2},\dots,\frac{p_i+p_j}{2},\dots,p_m)$, тј.

$$H(P) \leq H(Q).$$

Решење 11.

$$H(Q) - H(P) = -2\frac{p_i+p_j}{2}\log_2\frac{p_i+p_j}{2} + p_i\log_2 p_i + p_j\log_2 p_j$$

Уочимо да је функција $f(x) = x\log_2 x$ конвексна[1], одакле добијамо да важи Јенсенова неједнакост, тј.

$$\frac{f(x)+f(y)}{2} \geq f\left(\frac{x+y}{2}\right).$$

Одакле директно добијамо да је $H(Q) - H(P) \geq 0$. ▲

12. Доказати помоћу Јенсенове неједнакости да је $I(X;Y) \geq 0$.

Решење 12. Узајамна информација се може записати на следећи начин

$$I(X;Y) = -\sum_i\sum_j p(x_i,y_j)\log_2\frac{p(x_i)p(y_j)}{p(x_i,y_j)}$$

Како је функција $f(x) = -\log_2(x)$ конвексна и $\sum_i\sum_j p(x_i,y_j) = 1$ можемо применити Јенсенову неједнакост, тј. добијамо

$$-\sum_i\sum_j p(x_i,y_j)\log_2\frac{p(x_i)p(y_j)}{p(x_i,y_j)} \geq -\log_2\left(\sum_i\sum_j p(x_i,y_j)\frac{p(x_i)p(y_j)}{p(x_i,y_j)}\right) = -\log_2 1 = 0$$

▲

[1]покажите то

13. Доказати да је $ln(x) \leq x-1, \quad x>0$.

Решење 13. Дефинишемо функцију
$$f(x) = ln(x) - x + 1.$$
Ова функција достиже свој максимум за $x=1$ на скупу $(0,\infty)$ и $f(1)=0$. Дакле, важи наведена неједнакост. ▲

14. Користећи неједнакост из претходног задатка показати да је $KL(p||q) \geq 0$.

Решење 14.

$$\begin{aligned}
-KL(p||q) &= -\sum_x p(x)\log_2\frac{p(x)}{q(x)} \\
&= \sum_x p(x)\frac{1}{ln(2)}ln\frac{q(x)}{p(x)} \\
&= /ln(x) \leq x-1/ \\
&\leq \frac{1}{ln(2)}\sum_x p(x)\left(\frac{q(x)}{p(x)}-1\right) \\
&= \frac{1}{ln(2)}\sum_x (q(x)-p(x)) = 0
\end{aligned}$$

▲

15. Показати да за случајне величине X, Y и Z важе следеће неједнакости и наћи услове при којима важе једнакости

(а) $H(X,Y|Z) \geq H(X|Z)$

(б) $I(X,Y;Z) \geq I(X;Z)$

(в) $H(X,Y,Z) - H(X,Y) \leq H(X,Z) - H(X)$

(г) $I(X;Z|Y) \geq I(Z;Y|X) - I(Z;Y) + I(X;Z)$

Решење 15. (а)

$$H(X,Y|Z) = H(X|Z) + H(Y|X,Z) \geq H(X|Z),$$

јер је произвољна неодређеност ненегативна. Једнакост важи ако је Y у функцији од X и Z.

(б)

$$I(X,Y;Z) = I(X;Z) + I(Y;Z|X) \geq I(X:Z),$$

јер је узајамна информација ненегативна. Једнакост важи ако је $Y|X$ независно од $Z|X$.

(в) Можемо другачије да запишемо неједнакост

$$H(X,Y,Z) - H(X,Y) = H(Z|X,Y) \leq H(Z|X) = H(X,Z) - H(X).$$

Даље, применом формуле
$$I(Y;Z|X) = H(Z|X) - H(Z|X,Y) \geq 0$$
добијамо тражено тврђење. Једнакост важи у случају независности $Y|X$ и $Z|X$.

(г) Можемо другачије да запишемо неједнакост

$$I(X;Z|Y) + I(Z;Y) \geq I(Z;Y|X) + I(X;Z)$$

и видимо да заправо са обе стране имамо примену једнакости $(I.8.)$ на израз $I(X,Y;Z)$. У овом случају увек важи једнакост.

▲

16. Наћи пример случајних величина X, Y и Z тако да важи

(а) $I(X;Y|Z) < I(X;Y)$

(б) $I(X;Y|Z) > I(X;Y)$

Решење 16. (а) Нека важи

$$X = Y = Z : \begin{pmatrix} 0 & 1 \\ 1/2 & 1/2 \end{pmatrix}.$$

Тада

$$I(X;Y) = I(X;X) = H(X) - H(X|X) = H(X) - 0 = 1.$$

Док је

$$I(X;Y|Z) = I(X;X|X) = H(X|X) - H(X|X,X) = 0.$$

(б) Нека су X и Y независне једнако расподељене случајне величине са законом расподеле

$$\begin{pmatrix} 0 & 1 \\ 1/2 & 1/2 \end{pmatrix}.$$

А за случајну величину $Z = X + Y$. Тада важи

$$I(X;Y) = 0$$

због независности, док је

$$I(X;Y|Z) = \frac{1}{2}.$$

▲

17. Нека су X и Y случајне величине које узимају вредности $x_1, \ldots, x_r$ и $y_1, \ldots, y_s$ респективно и нека је $Z = X + Y$.

(а) Показати да важи $H(Z|X) = H(Y|X)$;

(б) Ако су X и Y независне, тада важи

$$H(X) \leq H(Z) \quad \text{и} \quad H(Y) \leq H(Z);$$

(в) Наћи пример (зависних) случајних величина за које важе неједнакости

$$H(X) > H(Z) \quad \text{и} \quad H(Y) > H(Z);$$

(г) Под којим условом важи једнакост $H(Z) = H(X) + H(Y)$?

Решење 17. (а) Важи следећи низ једнакости

$$\begin{aligned}
H(Z|X) &= \sum_i p(x_i) H(Z|X = x_i) && (1)\\
&= -\sum_i p(x_i) \sum_k p(z_k|x_i) \log_2 p(z_k|x_i) && (2)\\
&= /P\{Z = z_k|X = x_i\} = P\{Y = z_k - x_i|X = x_i\}/ && (3)\\
&= -\sum_i p(x_i) \sum_k p(y_k|x_i) \log_2 p(z_k|x_i) && (4)\\
&= \sum_i p(x_i) H(Y|X = x_i) && (5)\\
&= H(Y|X). && (6)
\end{aligned}$$

(б) Из задатка 12. знамо да је узајамна информација ненегативна. Стога посматрајмо

$$I(X;Z) = H(Z) - H(Z|X) \geq 0 \implies H(Z) \geq H(Z|X) = H(Y|X) = H(Y), \qquad (7)$$

где последња једнакост важи због услова независности X и Y. Аналогно се показује за случај $H(Z) \geq H(X)$ преко узајамне информације $I(Y;Z)$.

(в) Дефинишемо случајне величине X и Y на следећи начин.

Нека је X произвољна случајна величина са позитивном неодређеношћу, док је $Y \equiv -X$. Тиме добијамо да је $Z \equiv 0$. Пример: $X \sim Unif(2)$ - равномерна дискретна расподела. Тада $H(X) = H(Y) = 1$, док је $H(Z) = 0$.

(г) Из задатка 2. видимо да важи следећа неједнакост

$$H(Z) = H(X+Y) \leq H(X,Y), \tag{8}$$

где је $g(x,y) = x + y$. Такође,

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

а то је једнако $H(X) + H(Y)$ у случају независности случајних величина X и Y. Да бисмо још и неједнакост у (8) претворили у једнакост мора да важи да је $g(x,y)$ $1-1$ функција.[2]

▲

18. Играчи A и B играју карте. Побеђује онај играч који први победи у 4 партије. Нека је X случајна величина која представља исходе ове игре, а Y случајна величина која представља број одиграних партија. Ако претпоставимо да играчи имају једнаке шансе да добију сваку партију и да су партије независне, израчунати $H(X)$, $H(Y)$, $H(Y|X)$, $H(X|Y)$.

Решење 18. Случајна величина Y има следећу расподелу

$$Y : \begin{pmatrix} 4 & 5 & 6 & 7 \\ 1/8 & 1/4 & 5/16 & 5/16 \end{pmatrix}.$$

Одакле директно добијамо

$$H(Y) = -\left(\frac{1}{8}\log_2\frac{1}{8} + \frac{1}{4}\log_2\frac{1}{4} + \frac{5}{16}\log_2\frac{5}{16} + \frac{5}{16}\log_2\frac{5}{16}\right)$$

Случајна величина X има следећу расподелу

$$X : \begin{pmatrix} AAAA & BBBB & AAABA & BBBAB & \dots & AABBAA & \dots & AABBBAA \\ 1/16 & 1/16 & 1/32 & 1/32 & \dots & 1/64 & \dots & 1/128 \end{pmatrix}.$$

Приметимо да ће сви исходи једнаке дужине имати исту вероватноћу. Дакле, само је битно прерачунати колико их има.

- Исхода дужине четири је свега 2
- Исхода дужине пет је свега $8 = 2\binom{4}{1}$
- Исхода дужине шест је свега $20 = 2\binom{5}{2}$
- Исхода дужине седам је свега $40 = 2\binom{6}{3}$

Добијамо на крају

$$\begin{aligned} H(X) &= 2\frac{1}{2^4}\log_2 2^4 + 8\frac{1}{2^5}\log_2 2^5 + 20\frac{1}{2^6}\log_2 2^6 + 40\frac{1}{2^7}\log_2 2^7 \\ &= \frac{1}{2} + \frac{40}{32} + \frac{120}{64} + \frac{280}{128} = 5.8125 \end{aligned}$$

Како је Y заправо функција од X те одмах знамо да је $H(Y|X) = 0$, тиме добијамо из једнакости $(I.3.)$ са почетка скрипте да је $H(X,Y) = H(X) + H(Y|X) = H(X)$.

Док

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

▲

19. У кутији се налази c црвених, b белих и p плавих куглица. Да ли већу неодређеност има извлачење k куглица са понављањем или без понављања?

[2]видети кад је то задовољено у овом задатку

Решење 19. Размотримо сваки случај појединачно.

- Случај са понављањем.

$$H(X_1, X_2, \dots, X_k) = H(X_k|X_{k-1}, \dots, X_1) + H(X_{k-1}|X_{k-2}, \dots, X_1) + \dots + H(X_2|X_1) + H(X_1) = kH(X_1).$$

- Случај без понављања. Са X_i^* обележавамо i-то извлачења без понављања.

$$\begin{aligned} H(X_1, X_2^*, \dots, X_k^*) &= H(X_k^*|X_{k-1}^*, \dots, X_1) + H(X_{k-1}^*|X_{k-2}^*, \dots, X_1) + \dots + H(X_2^*|X_1) + H(X_1) \\ &\le H(X_k^*) + H(X_{k-1}^*) + \dots + H(X_2^*) + H(X_1) \\ &\le H(X_k) + H(X_{k-1}) + \dots + H(X_2) + H(X_1) = kH(X_1). \end{aligned}$$

Видимо да је неоређеност са понављањем већа. ▲

20. Показати да ако је $Z = f(Y)$, онда је $X \to Y \to Z$ ланац Маркова.

Решење 20. За самосталну вежбу. ▲

21. Показати да ако је $X \to Y \to Z$ ланац Маркова, онда важи $I(X;Y) \ge I(X:Z)$.

Решење 21. Кренемо од узајамне информације

$$\begin{aligned} I(X;Y,Z) &= I(X;Z) + I(X;Y|Z) \\ &= I(X;Y) + I(X;Z|Y) = I(X;Y) \end{aligned}$$

Знамо да је узајамна информација ненегативна (тј. $I(X;Y|Z) \ge 0$), још остало да покажемо да је $I(X;Z|Y) = 0$ под претпоставкама задатка. Применимо једнакост $(I.7.)$ са почетка скрипте

$$I(X;Z|Y) = H(X|Y) - H(X|Z,Y) \tag{9}$$

$$= H(Z|Y) - H(Z|X,Y) \tag{10}$$

Даље, како је у питању ланац Маркова, знамо да други сабирак у (10) једнак $H(Z|Y)$ и тиме цела узајамна информација једнака нули. Кад скупимо на једно место овај закључак и то да је узајамна информација ненегативна добијамо и тврђење задатка.

▲

22. Ако је $X_1 \to X_2 \to \dots \to X_n$ ланац Маркова, односно ако важи једнакост

$$p(x_1, x_2, \dots, x_n) = p(x_1)p(x_2|x_1)\dots p(x_n|x_{n_1}),$$

упростити израз $I(X_1; X_2, \dots, X_n)$.

Решење 22. Применом једнакости $(I.10.)$ са почетка скрипте добијамо

$$I(X_1; X_2, \dots, X_n) = -\sum_{(x_1,\dots,x_n)\in\mathbb{X}^n} p(x_1, \dots, x_n) \log_2 \frac{p(x_1)p(x_2, \dots, x_n)}{p(x_1, x_2, \dots, x_n)} \tag{11}$$

$$= -\sum_{(x_1,\dots,x_n)\in\mathbb{X}^n} p(x_1, \dots, x_n) \log_2 \frac{p(x_1)p(x_2)p(x_3|x_2)\dots p(x_n|x_{n-1})}{p(x_1)p(x_2|x_1)p(x_3|x_2)\dots p(x_n|x_{n-1})}. \tag{12}$$

Једнакост (12) важи према услову задатка. У логатирму се пократи све сем $\frac{p(x_1)}{p(x_2|x_1)}$, тј. важи

$$\begin{aligned} I(X_1; X_2, \dots, X_n) &= -\sum_{(x_1,\dots,x_n)\in\mathbb{X}^n} p(x_1, \dots, x_n) \log_2 \frac{p(x_1)}{p(x_2|x_1)} \\ &= H(X_2) - H(X_2|X_1) \\ &= I(X_1; X_2). \end{aligned}$$

▲

23. Доказати да је условна неодређеност $H(X_0|X_n)$ неопадајућа по n за сваки ланац Маркова.

Решење 23. Применом задатка (22) знамо $I(X_0; X_n) \leq I(X_0; X_{n-1})$, тј.

$$H(X_0) - H(X_0|X_n) \leq H(X_0) - H(X_0|X_{n-1})$$
$$\Longrightarrow$$
$$H(X_0|X_n) \geq H(X_0|X_{n-1})$$

Одакле индукцијом видимо да важи тврђење задатка.

▲

24. Нека је $X \to Y \to Z$ ланац Маркова, такав да $X \in \{1, 2, \ldots, n\}$, $Y \in \{1, 2, \ldots, k\}$ и $Z \in \{1, 2, \ldots, m\}$. Показати да је $I(X; Z) \leq \log_2 k$.

Решење 24. Пођимо од следеће узајамне информације

$$I(X; Y, Z) = I(X; Y),$$

једнакост важи према решењу у задатку (22).

$$I(X; Y, Z) = I(X; Y) = H(Y) - H(Y|X) \leq \log_2 k,$$

јер $H(Y) \leq \log_2 k$ (расподела са највећом неодређеношћу са k елемената је униформна), а $H(Y|X) \geq 0$. Одакле добијамо следећи низ неједнакости

$$\log_2 k \geq I(X; Y) \geq I(X; Z),$$

последња неједнакост важи према задатку (22).

▲

25. Ако је $I(X; Z|Y) = 0$, показати да је $I(X; Y) \geq I(X; Z)$. Под којим условима важи једнакост?

Решење 25. Пођимо од узајамне информације

$$I(X; Y, Z) = I(X; Z) + I(X; Y|Z) = I(X; Y) + I(X; Z|Y) = I(X; Y).$$

Одавде се директно види да важи тражена неједнакост због ненегативности узајамне информације.

Једнакост ће да важи у случају да је $I(X; Y|Z) = 0$. ▲

26. Нека случајна величина X узима три могуће вредно сти $\{a\ ,\ b,\ c\}$. Посматрајмо две расподеле вероватноће ове случајне величине

	$p(x)$	$q(x)$
a	1/2	1/3
b	1/4	1/3
c	1/4	1/3

Израчунати $H(p)$, $H(q)$, $KL(p||q)$ и $KL(q||p)$.

Решење 26.

$$H(p) = \frac{1}{2}\log_2(2) + 2\frac{1}{4}\log_2(4) = \frac{1}{2} + 1 = \frac{3}{2}.$$

$$H(q) = 3\frac{1}{3}\log_2(3) = \log_2(3).$$

Даље, применом једнакости $(I.9.)$ са почетка скрипте добијамо

$$\begin{aligned} KL(p||q) &= \sum_i p(x_i)\log_2\frac{p(x_i)}{q(x_i)} \\ &= \frac{1}{2}\log_2\frac{3}{2} + 2\frac{1}{4}\log_2\frac{3}{4} \\ &= \log_2 3 - \frac{3}{2} \\ &\sim 0.085. \end{aligned}$$

Док важи

$$\begin{aligned}
KL(q||p) &= \sum_i q(x_i)\log_2\frac{q(x_i)}{p(x_i)}\\
&= \frac{1}{3}\log_2\frac{2}{3} + 2\frac{1}{3}\log_2\frac{4}{3}\\
&= \frac{5}{3} - \log_2 3\\
&\sim 0.0817.
\end{aligned}$$

▲

27. Претходни задатак говори да је у општем случају $KL(p||q) \neq KL(q||p)$. Наћи пример две расподеле вероватноће p и q тако да у Кулбак-Лајблеровом разилажењу важи једнакост.

Решење 27. За домаћи.

28. Нека су X, Y и Z случајне величине са заједничком расподелом $p(x,y,z)$. Кулбак-Лалблерово разилажење између заједничке расподеле и производа одговарајућих маргиналних је

$$Kl(p(x,y,z)||p(x)p(y)p(z)) = E\left[\log_2\frac{p(x,y,z)}{p(x)p(y)p(z)}\right].$$

Изразити Кулбак-Лајблерово разилажење преко неодређености. Када је ово разилажење једнако нули?

Решење 28. Приметимо да генерално важи следећа једнакост

$$H(X) = -\sum_i p(x_i)\log_2 p(x_i) = E(-\log_2 p(X)).$$

Дакле,

$$\begin{aligned}
Kl(p(x,y,z)||p(x)p(y)p(z)) &= E(\log_2 p(X,Y,Z)) - E(\log_2 p(X)) - E(\log_2 p(Y)) - E(\log_2 p(Z))\\
&= -H(X,Y,Z) + H(X) + H(Y) + H(Z).
\end{aligned}$$

Разилажење једнако нули ако су X, Y и Z независни. ▲

29. Посматрајмо низ од n бинарних случајних величина. Сваки низ са парним бројем јединица има вероватноћу 2^{-n+1} и сваки низ са непарним бројем јединица има вероватноћу нула. Наћи узајамне информације:

$$I(X_1;X_2),\quad I(X_2;X_3|X_1),\quad \ldots,\quad I(X_{n-1};X_n|X_1,\ldots,X_{n-2}).$$

Решење 29. Дакле, низови су дужине n облика $10010101\ldots0101$. Ако је $k \leq n-1$, онда су X_k независни, тј.

$$I(X_1;X_2) = 0,$$

јер X_1 и X_2 независни. И из истог аргумента независности све су нуле, сем $I(X_{n-1};X_n|X_1,X_2,\ldots,X_{n-2}) = 1$, јер тек у случају када знамо све цифре сем једне имамо додатну информацију о парности и тада можемо нешто да закључимо. ▲

30. Нека су X, Y и Z три пар по пар независне случајне величине са Бернулијевом $Ber(\frac{1}{2})$ расподелом.

(а) Одредити минималну вредност неодређености $H(X,Y,Z)$.

(б) Навести пример случајних величина за које се постиже минимум.

Решење 30. (а) Према формули $(I.6.)$ са почетка скрипте важи

$$\begin{aligned}
H(X,Y,Z) &= H(X) + H(Y|X) + H(Z|X,Y) &(13)\\
&= H(X) + H(Y) + H(Z|X,Y) &(14)\\
&\geq H(X) + H(Y) &(15)\\
&= 2\log_2 2 &(16)\\
&= 2, &(17)
\end{aligned}$$

једнакост (14) важи због независности у паровима, док неједнакост (15) јер је $H(Z|X,Y) \geq 0$.

(б) У случају да је $Z = X +_2 Y$.

▲

31. Под којим условима важи следећа једнакост

$$H(X|g(Y)) = H(X|Y)?$$

Решење 31. За домаћи.

32. Одредити узајамну информацију између горње и доње стране хомогеног новчића.

Решење 32. Дефинишемо следеће скупове догађаја: G - горња страна новчића, D - доња страна новчића. Добијамо следеће:

$$I(G;D) = H(G) - H(G|D) = \log_2 2 - 0 = \log_2 2,$$

неодређеност горње стране је униформна расподела са две вредности, док условна неодређеност је једнака нули. ▲

33. Упоредити следеће изразе

(а) $H(X)$ и $H(5X)$;

(б) $I(g(X);Y)$ и $I(X;Y)$;

(в) $\frac{H(X,Y)}{H(X)+H(Y)}$ и 1.

Решење 33. (а) Докажимо општији случај

Теорема 1. Нека је X произвољна дискретна случајна величина, и $a \in \mathbb{R}$ произвољна константа различита од нуле, тада важи

$$H(X) = H(aX).$$

Доказ 1. Случајна величина aX од случајне величине X се разликује само по вредностима које узима. Вероватноће остаје непромењене. Како по дефиницији неодређености само вероватноће играју улогу, то је и $H(X) = H(aX)$. □

Из дате теореме директно добијамо и да су ове две неодређености једнаке.

(б) Како је $Y \to X \to g(X)$ увек ланац Маркова то имамо

$$\begin{aligned} I(X,g(X);Y) &= I(X,Y) + I(g(X);Y|X) &(18)\\ &= I(g(X);Y) + I(X;Y|g(X)) &(19)\\ &\implies I(X;Y) \geq I(g(X);Y), &(20)\end{aligned}$$

јер $I(g(X);Y|X) = 0$, а $I(X;Y|g(X)) \geq 0$.

(в) $H(X,Y) \leq H(X) + H(Y)$, док једнакост важи само у случају независности.

▲

34. Претпоставимо да имамо n новчића међу којима је један фаличан (лакши или тежи од осталих). На располагању имамо теразије које могу имати три исхода. Нека је k најмањи број мерења потребних да се утврди који новчић је фаличан као и да ли је лакши или тежи.

(а) Показати да важи $3^k \geq 2n$;

(б) Нека је $n = 12$ и $k = 3$. Описати та три мерења помоћу којих се може одредити фаличан новчић.

Решење 34. (а) Како теразије имају три могућа исхода те у једном мерењу можемо да добијемо највише $\log_2 3$ битова информације. Неодређеност целог система је $\log_2(2n)$, јер имамо $2n$ могућности n који могу тежи да буду и n који могу лакши. Дакле, добијамо

$$\frac{\log_2(2n)}{\log_2 3} \leq k,$$

коришћењем својства логаритамских функција добијамо

$$\log_3(2n) \leq k \implies 2n \leq 3^k.$$

(б) За самостално решавање.

▲

35. Нека су $X_1, X_2, ..$ независне једнако расподељене случајне величине са функцијом расподеле $p(x)$. Наћи
$$\lim_{n\to\infty} [p(X_1, X_2, \ldots, X_n)]^{\frac{1}{n}}.$$

Решење 35. Како су независне то важи

$$\lim_{n\to\infty} [p(X_1, X_2, \ldots, X_n)]^{\frac{1}{n}} = \lim_{n\to\infty} \left(\prod_{i=1}^{n} p(X_i)\right)^{\frac{1}{n}} = 2^{\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n}\log_2 p(X_i)} \to 2^{\mathbb{E}(\log_2 p(X))} = 2^{-H(X)}$$

што смо добили применом Закона великих бројева и дефиниције неодређености случајне величине. ▲

36. Нека су $X_1, X_2, ..$ независне једнако расподељене случајне величине са функцијом расподеле са расподелом
$$X = \begin{cases} 1, & \text{са вероватноћом } \frac{1}{2} \\ 2, & \text{са вероватноћом } \frac{1}{4} \\ 3, & \text{са вероватноћом } \frac{1}{4} \end{cases}$$
Наћи граничну вредност израза
$$(X_1 X_2 \ldots X_n)^{\frac{1}{n}}$$

Решење 36. Означимо са $A_n = (X_1 X_2 \ldots X_n)^{\frac{1}{n}}$. Тада

$$\log_2 A_n = \frac{1}{n}\sum_{i=1}^{n} \log_2 X_i \to \mathbb{E}(\log_2 X) = \frac{1}{2}\log_2 1 + \frac{1}{4}\log_2 2 + \frac{1}{4}\log_2 3 = \frac{1}{4}(1 + \log_2 3)$$

Одакле директно добијамо

$$\lim_{n\to\infty} (X_1 X_2 \ldots X_n)^{\frac{1}{n}} = 2^{\frac{1}{4}(1+\log_2 3)}$$

▲

37. Нека су (X_i, Y_i) независни једнако расподељени случајни вектори за свако $i \in \mathbb{N}$ са функцијом расподеле $p(x, y)$. Формирамо количник веродостојности за тестирање хипотезе да су X и Y независне. Наћи граничну вредности израза

$$\frac{1}{n}\log_2 \prod_{i=1}^{n} \frac{p(X_i)p(Y_i)}{p(X_i, Y_i)}.$$

Решење 37.

$$\begin{aligned} \frac{1}{n}\log_2 \prod_{i=1}^{n} \frac{p(X_i)p(Y_i)}{p(X_i, Y_i)} &= \frac{1}{n}\sum_{i=1}^{n} [\log_2 p(X_i) + \log_2 p(Y_i) - \log_2 p(X_i, Y_i)] \\ &\to \mathbb{E}(\log_2 p(X)) + \mathbb{E}(\log_2 p(Y)) - \mathbb{E}(\log_2 p(X, Y)) \end{aligned}$$

▲

38. Независно се бацају хомогена коцкица и хомоген новчић. Нека је X вредност на коцкици, а Y је индикатор да је пало писмо. Нека је $Z = X + Y$, наћи $H(Z)$ и $I(Z; X)$.

Решење 38. За домаћи. ▲

39. Дефинисати преко информације довољне статистике. Показати да је статистика $T(X) = \sum_{i=1}^{n} X_i$ довољна за параметар θ ако је узорак $X_1, \ldots, X_n$ из Бернулијеве $Ber(\theta)$ расподеле.

Решење 39. За домаћи. ▲

40. Функција $d(x, y)$ је метрика ако за све x, y важи

1. $d(x, y) \geq 0$
2. $d(x, y) = d(y, x)$

3. $d(x,y) = 0 \iff x = y$
4. $d(x,z) \leq d(x,y) + d(y,z)$

Испитати да ли је $d(X,Y) = H(X|Y) + H(Y|X)$ метрика.

Решење 40. Кренемо корак по корак.

1. $d(x,y) \geq 0$
   Како су неодређености ненегативне то је ово испуњено.
2. $d(x,y) = d(y,x)$
   Симетричност очигледно важи из дефиниције функције $d(X,Y)$.
3. $d(x,y) = 0 \iff x = y$
   Један смер је очигледан (ако важи $X = Y$). Други смер:

   $$d(X,Y) = 0 = H(Y|X) + H(X|Y),$$

   што значи да обе неодређености морају бити једнаке нули, тј.

   $$H(X|Y=y) = 0, \quad \forall y$$

   и

   $$H(Y|X=x) = 0, \quad \forall x$$

   Значи да познавањем једне вредности у потпуности имамо и другу. Међутим то не мора да буде испуњено само за $X = Y$, може да буде и за $X = f(Y)$ где је $f(\cdot)$ нека бијективна функција, која једнозначно одређује X познавањем Y и обратно.

Не морамо ни проверавати неједнакост троугла, већ видимо да није метрика. ▲

41. Показати да важе следеће једнакости

$$H(X) + H(Y) - 2I(X;Y) = H(X,Y) - I(X;Y) = 2H(X,Y) - H(X) - H(Y).$$

Решење 41. Сваки део посебно ћемо да доведемо на облик $H(X|Y) + H(Y|X)$.

$$\begin{aligned}
H(X) + H(Y) - 2I(X;Y) &= H(X) + H(Y) - 2H(Y) + 2H(Y|X) \\
&= H(X) - H(Y) + H(Y|X) + H(Y|X) \\
&= H(X) - I(X;Y) + H(Y|X) \\
&= H(X) - H(X) + H(X|Y) + H(Y|X) \\
&= H(X|Y) + H(Y|X)
\end{aligned}$$

$$\begin{aligned}
H(X,Y) - I(X;Y) &= H(X) + H(Y|X) - H(X) + H(X|Y) \\
&= H(Y|X) + H(X|Y)
\end{aligned}$$

$$\begin{aligned}
2H(X,Y) - H(X) - H(Y) &= (H(X) + H(Y|X)) + (H(Y) + H(X|Y)) - H(X) - H(Y) \\
&= H(Y|X) + H(X|Y)
\end{aligned}$$

▲

42. Јенсен-Шеноново разилажење дефинисано је као

$$JSD(p\|q) = \frac{1}{2}KL(p\|s) + \frac{1}{2}KL(q\|s),$$

где је $s = \frac{1}{2}(p+q)$. Испитати да ли је Јенсен-Шеноново разилажење метрика. А да ли је $\sqrt{JSD(p\|q)}$ метрика?

Решење 42. За домаћи. ▲

43. Нека је

$$X = \begin{cases} Y, & \text{ако је } T = 1 \\ Z, & \text{ако је } T = 0, \end{cases}$$

где Y има расподелу p, а Z расподелу q, док је T индикатор догађаја чија је вероватноћа $\frac{1}{2}$. Показати да је

$$JSD(p||q) = I(X;T).$$

Решење 43. Према поставци задатка видимо да је расподела X заправо нека мешавина расподела p и q и то таква да обе подједнако учествују. Стога, видимо да је расподела за X заправо $r = \frac{p+q}{2}$.

Важи следећи низ једнакосри

$$\begin{aligned}
I(X;T) &= H(X) - H(X|T) \\
&= -\sum_i r(x_i) \log_2 r(x_i) + \frac{1}{2} \sum_j p(y_j) \log_2 p(y_j) + \frac{1}{2} \sum_k q(z_k) \log_2 q(z_k) \\
&= -\sum_i \frac{p(y_i)}{2} \log_2 r(x_i) - \sum_i \frac{q(z_i)}{2} \log_2 r(x_i) + \frac{1}{2} \sum_j p(y_j) \log_2 p(y_j) + \frac{1}{2} \sum_k q(z_k) \log_2 q(z_k) \\
&= \frac{1}{2} \sum_j p(y_j)(\log_2 p(y_j) - \log_2 r_j) + \frac{1}{2} \sum_k q(z_k)(\log_2 q(z_k) - \log_2 r(x_k)) \\
&= \frac{1}{2} \sum_j p(y_j) \log_2 \frac{p(y_j)}{r(x_j)} + \frac{1}{2} \sum_k q(z_k) \log_2 \frac{q(z_k)}{r(x_k)} \\
&= KL(p||r) + KL(q||r) \\
&= JSD(p||q)
\end{aligned}$$

▲

Теорија кодирања

44. Нека је дата случајна величина S са следећим законом расподеле

$$S = \begin{pmatrix} S_1 & S_2 & S_3 & S_4 & S_5 & S_6 \\ p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \end{pmatrix}$$

где су S_i кодиране азбуком која има D симбола. Ако су дужине кодираних речи $(l_1, l_2, l_3, l_4, l_5, l_6) = (1, 1, 2, 3, 2, 3)$ наћи одговарајућу доњу границу за D.

Решење 44. Пробајмо различите бројеве за D:
- Претпоставимо да D има само један симбол, тада не могу да постоје две речи дужине 1.
- Претпоставимо да D има два симбола, тада је могуће следеће кодирање:

$$\{S_1 : 0, S_2 : 1, S_3 : 00, S_4 : 110, S_5 : 01, S_6 : 111\}.$$

Дакле, доња граница за D је 2.
- Уколико још додамо захтев да код мора да буде префиксни (ниједна реч не сме да почиње са неком речју која већ постоји) онда $D > 2$, иначе не могу две речи дужине један да постоје. Пробајмо за $D = 3$

$$\{S_1 : 0, S_2 : 1, S_3 : 20, S_4 : 220, S_5 : 21, S_6 : 221\}.$$

- Уколико на претходни услов још додамо услов да код мора да буде афиксан, онда $D = 4$, и такво једно кодирање је

$$\{S_1 : 0, S_2 : 1, S_3 : 22, S_4 : 202, S_5 : 23, S_6 : 203\}.$$

▲

45. Размотримо случајну величину

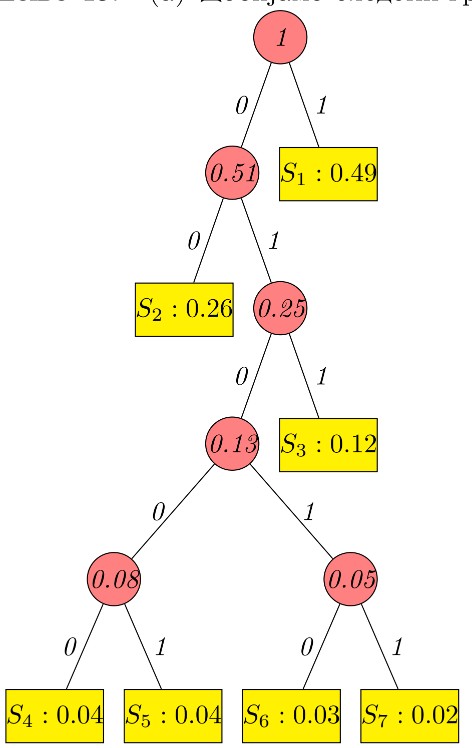
$$S = \begin{pmatrix} S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 \\ 0.49 & 0.26 & 0.12 & 0.04 & 0.04 & 0.03 & 0.02 \end{pmatrix}$$

(а) Наћи бинарни Хафманов код за S.

(б) Наћи средњу дужину речи за то кодирање.

(а) Наћи тројни (тринарни) Хафманов код за S.

Решење 45. (а) Добијамо следећи граф:



Па је добијен код: $\{S_1 : 1, S_2 : 00, S_3 : 011, S_4 : 01000, S_5 : 01001, S_6 : 01010, S_7 : 01011\}$.

(б) Средња дужина кода је

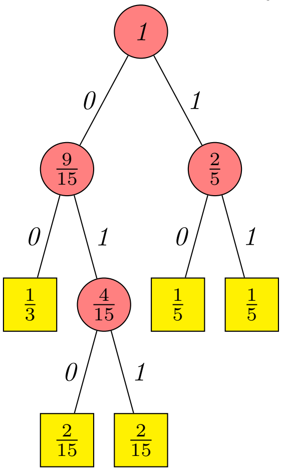
$$\sum_{i=1}^{7} p_i d_i = 0.49 \cdot 1 + 0.26 \cdot 2 + 0.12 \cdot 3 + 0.04 \cdot 5 + 0.04 \cdot 5 + 0.03 \cdot 5 + 0.02 \cdot 5 = 2.02.$$

(в) За домаћи.

▲

46. Наћи бинарни Хафманов код за расподелу $p = (1/3,\ 1/5,\ 1/5,\ 2/15,\ 2/15)$. Показати да је овај код такође оптималан за расподелу $q = (1/5,\ 1/5,\ 1/5,\ 1/5,\ 1/5)$.

Решење 46. Добијамо следећи Хафманов код за расподелу p:



кодирање је следеће $(00, 10, 11, 010, 011)$.
За расподелу q добијамо $(01, 10, 11, 000, 001)$ и видимо да је заправо исто, до на пермутације 0 и 1. Средња дужина је

$$d(K) = \frac{6}{5} + \frac{6}{5} = \frac{12}{5} = 2.4,$$

док је неодређеност овог извора

$$H(q) = \log_2 5 =\sim 2.322,$$

а знамо да важи неједнакост

$$H(q) \le d(K) < H(q) + 1.$$

▲

47. Који од понуђених кодова није бинарни Хафманов ни за једну расподелу вероватноћа?

(а) $\{0,\ 10,\ 11\}$;

(б) $\{00,\ 01,\ 10,\ 110\}$;

(в) $\{10,\ 01\}$.

Решење 47. (а) Јесте Хафманов за произвољну расподелу за коју важи $p_1 \ge p_2 \ge p_3$.

(б) Није Хафманов, јер би две речи са најмањим вероватноћама биле исте дужине и разликовале се само у последњој цифри.

(в) Није Хафманов код ни за једну расподелу вероватноћа, јер би било кодирано са по једним симболом.

▲

48. Наћи бинарни и тројни Хафманов код за случајну величину S чија је расподела вероватноће

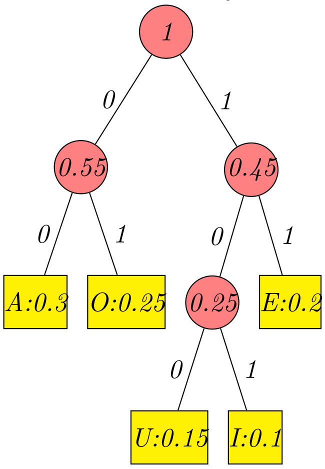
$$p = \left(\frac{1}{21},\ \ \frac{2}{21},\ \ \frac{3}{31},\ \ \frac{4}{21},\ \ \frac{5}{21},\ \ \frac{6}{21} \right).$$

Колика је средња дужина речи у оба случаја?

Решење 48. За самосталну вежбу. ▲

49. Слова $\{A,\ E,\ I,\ O,\ U\}$ јављају се редом у фреквенцијама $\{0.3,\ 0.2,\ 0.1,\ 0.25$ и $0.15\}$. Одредити оптимално бинарно кодирање и средњу дужину кодираних речи.

Решење 49. Добијамо следећи граф Хафмановог кода:



Кодирање је следеће:

- A: 00
- E: 11
- I: 101
- O: 01
- U: 100

Средња дужина:

$$\sum_{i=1}^{5} p_i d_i = 2 \cdot 0.3 + 2 \cdot 0.2 + 3 \cdot 0.1 + 2 \cdot 0.25 + 3 \cdot 0.15 = 2.25,$$

где смо са p_i означили фреквенцију појављивања i-тог слова, а са d_i број цифара i-тог слова у добијеном коду. ▲

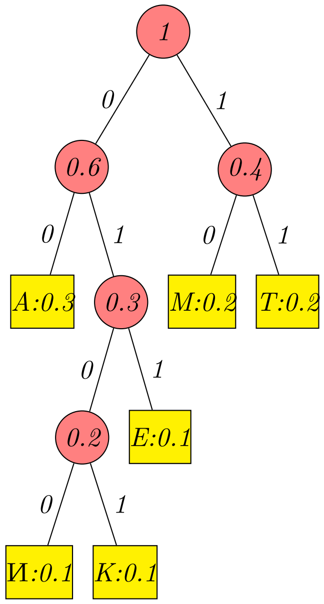
50. Нека је $\mathcal{K}_r$ произвољно $r-$арно Хафманово кодирање.

(а) Колико је потребно битова да би се послала порука "математика" кодирањем $\mathcal{K}_2$? Вероватноће појављивања слова су број појављивања слова у речи "математика" подељен са 10.

(б) Да ли би се разликовао Шенонов бинарни код за реч "математика"?

(в) Колико је потребно битова да се пошаље порука "тематика" истим кодирањем као у делу под (а)? Да ли постоји неко друго тренутно кодирање за које је потребно мање битова?

Решење 50. (а) Издвојимо слова које имамо {М, А, Т, Е, И, К}, њихове одговарајуће фреквенције су $\{\frac{2}{10}, \frac{3}{10}, \frac{2}{10}, \frac{1}{10}, \frac{1}{10}, \frac{1}{10}\}$.



Кодирање је следеће:

- M: 10
- A: 00
- T: 11
- E: 011
- И: 0100
- К: 0101

Да би кодирала порука МАТЕМАТИКА, морамо свако слово да заменимо са неопходним кодом и добијамо да је потребно

$$2 + 2 + 2 + 3 + 2 + 2 + 2 + 4 + 4 + 2 = 25\text{битова}.$$

(б) Нађемо неопходне дужине кодних речи.

- $M: -\log_2(0.2) = 2.32 \implies d = 3$
- $A: -\log_2(0.3) = 1.74 \implies d = 2$
- $T: -\log_2(0.2) = 2.32 \implies d = 3$
- $E: -\log_2(0.1) = 3.32 \implies d = 4$
- И $: -\log_2(0.1) = 3.32 \implies d = 4$
- $K: -\log_2(0.1) = 3.32 \implies d = 4$

А одговарајући низ за развој $\{0, 0.3, 0.5, 0.7, 0.8, 0.9\}$, сад гледамо развоје тих цифара у бинарне бројеве. Дакле развој 0 је 00, јер гледамо до друге цифре (то одговара слову А), развој 0.3 и гледамо прве три децималне цифре 010 (слово М), развој 0.5 је 100 (слово Т), развој 0.7 је 1011 (слово Е), развој 0.8 је 1100 (слово И), развој 0.9 је 1110 (слово К).
На крају добијамо:

- M: 010
- A: 00
- T: 100
- E: 10111
- И: 1100
- К: 1110

Видимо да кодови нису исти.

(в) За реч тематика потребно је

$$2+3+2+2+2+4+4+2 = 21 \text{ битова},$$

што није оптимално. Када бисмо креирали код баш за ту реч добили бисмо оптималан код.

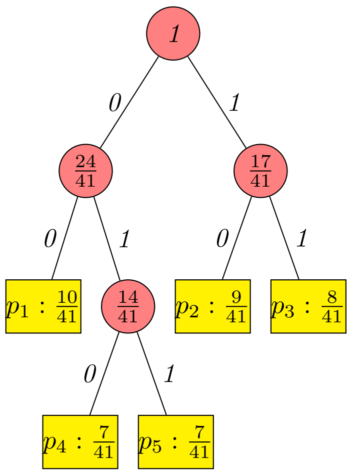
▲

51. Наћи бинарни Хафманов код за следеће расподеле

(а) $p = (\frac{10}{41}, \frac{9}{41}, \frac{8}{41}, \frac{7}{41}, \frac{7}{41});$

(б) $p = (\frac{9}{10}, \frac{9}{10}\frac{1}{10}, \frac{9}{10}\left(\frac{1}{10}\right)^2, \frac{9}{10}\left(\frac{1}{10}\right)^3, \dots);$

Решење 51. (а) Добијамо следећи код:



Па су речи редом: $(00, 10, 11, 010, 011)$.

(б) Кодне речи су редом: $(0, 10, 110, 1110, \dots)$, k-та реч има $k-1$ јединица и нулу на крају.

▲

52. Наћи услов да Хафманов бинарни код са 4 симбола и расподелом $p_1 = p_2 \geq p_3 = p_4$ има све речи дужине 2.

Решење 52. Неопходни услови за то су

$$\begin{aligned} p_1 &< 2p_4 \\ 2p_1 + 2p_4 &= 1 \end{aligned}$$

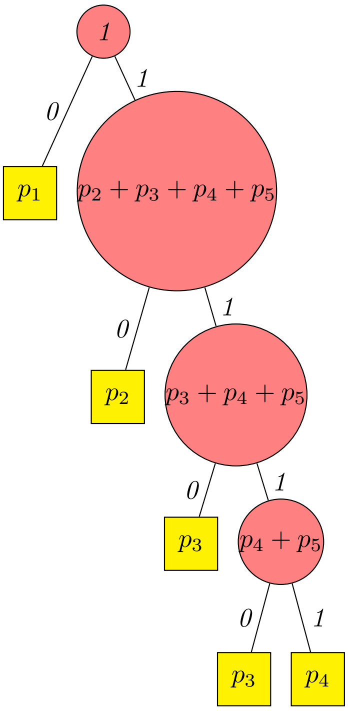
Из ова два услова добијамо да важи

$$\begin{aligned} p_1 &= \frac{1}{2} - p_4 \\ \frac{1}{2} - p_4 &< 2p_4 \\ \frac{1}{6} &< p_4, \end{aligned}$$

последња неједнакост представља тражени услов. ▲

53. Нека Хафманов код има 5 кодних речи над азбуком $\{0, 1\}$ и нека је $p_1 \geq p_2 \geq p_3 \geq p_4 \geq p_5 = q$. Наћи највећу могућу вредност за q, тако да реч која се појављују са вероватноћом q има дужину 4.

Решење 53. Неопходно је да Хафманов граф изгледа овако



Тада реч са вероватноћом $q(p_5)$ има дужину 4. Тј. важе следећи услови:

$$p_1 \geq 3p_5 \tag{21}$$
$$p_2 \geq 2p_5 \tag{22}$$
$$p_1 + p_2 + p_3 + p_4 + p_5 = 1 \tag{23}$$

Убацимо услове (21) и (22) у (23) и добијамо:

$$3p_5 + 2p_5 + p_5 + p_5 + p_5 \leq 1 \tag{24}$$
$$\implies p_5 \leq \frac{1}{8}. \tag{25}$$

Такав код се може добити за следеће вероватноће: $(\frac{3}{8}, \frac{2}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8})$. Највећа вредност за q је $\frac{1}{8}$.

▲

54. Наћи најмању и највећу вредност за q, тако да бинарни Хафманов код са четири кодне речи са вероватноћама $p_1 \geq p_2 \geq p_3 \geq p_4 = q$ има све речи једнаке дужини 2.

Решење 54. Јасно да је $q \leq \frac{1}{4}$, то представља горњу границу за q. Док за доњу важе следећи услови

$$p_2 \leq p_1 \leq p_3 + p_4 \tag{26}$$
$$p_1 + p_2 + p_3 + p_4 = 1 \tag{27}$$

те добијамо:

$$3p_3 + 3p_4 \geq 1 \tag{28}$$
$$\implies p_4 \geq \frac{1}{6}. \tag{29}$$

Дакле доња граница је $\frac{1}{6}$, тако да за произвољне вероватноће p_1, p_2, p_3, p_4 све речи буду дужине 2.

Напомена: иначе постоји и расподела вероватноћа тако да доња граница може бити и нула! Расподела је $\{0.5, 0.25, 0.25, 0\}$. Али то је специјалан случај а према задатку смо агностични према тачним вредностима вероватноћа.

▲

55. Извор има три симбола са вероватноћама $p_1 \geq p_2 \geq p_3$. Показати да бинарни Хафманов код има средњу дужину речи $2 - p_1$. Шта је одговарајући резултат ако извор има четири симбола са вероватноћама $p_1 \geq p_2 \geq p_3 \geq p_4$?

Решење 55. Ако извор има три симбола са задатим условом за вероватноће, онда су спајања у Хафмановом коду увек стриктна! Важе следеће дужине $d_1 = 1$, $d_2 = 2$, $d_3 = 2$.
Рачунамо средњу дужину

$$p_1 + 2p_2 + 2p_3 = 1 + p_2 + p_3 = 2 - p_1,$$

јер $p_1 + p_2 + p_3 = 1$.

У случају са четири симбола пробајте за домаћи. Издвојиће се два случаја. У једном ($p_1 \leq p_3 + p_4$) је средња дужина 2, док у другом ($p_1 \geq p_3 + p_4$) $3 - p_2 - 2p_1$. ▲

Капацитети

56. Нека је $Y = X + Z(mod\ 11) = X +_{11} Z$ дискретан канал без меморије, где је

$$Z = \begin{pmatrix} 1 & 2 & 3 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix},$$

и случајна величина X узима вредности из скупа $\{0, 1, \ldots, 10\}$. Ако претпоставимо да су X и Z независне случајне величине, наћи капацитет датог канала.

Решење 56. Капацитет канала је

$$C = \max_{p_X} I(X; Y),$$

где је максимум по свим могућим расподелама за X. Даље рачунамо

$$\begin{aligned} I(X; Y) &= H(Y) - H(Y|X) \\ &= H(Y) - H(X +_{11} Z|X) \\ &= H(Y) - H(Z), \end{aligned}$$

Неодређеност $H(Z) = \log_2 3$ - према расподели која је дата. А максимум узајамне информације се постиже за $H(Y) = \log_2 11$, тј. за униформну расподелу. Односно капацитет канала је

$$C = \log_2 11 - \log_2 3.$$

▲

Теорема 2. Нека је дат симетричан канал Y са L вредности за Y и m вредности за X. Тада важи

$$C = \log_2 L - H(Y|X = x_i), \quad \forall i \in \{1, \ldots, m\}.$$

57. Наћи капацитет канала са датом матрицом условних вероватноћа

	$Y = 0$	$Y = 1$
$X = 0$	$1/4$	$3/4$
$X = 1$	$3/4$	$1/4$
$X = 2$	$3/4$	$1/4$
$X = 3$	$1/4$	$3/4$

Решење 57. Тражимо $C = \max_{p_X} I(X; Y)$. Приметимо да је канал симетричан, тада важи теорема2. Применом те теореме добијамо

$$\begin{aligned} \max_{p_X} I(X; Y) &= \max_{p_X} (H(Y) - H(Y|X)) \\ &= \max_{p_X} (\log_2 2 - H(Y|X = 0)), \end{aligned}$$

Само израчунамо још ову неодређеност

$$H(Y|X = 0) = \frac{1}{4} \log_2 4 + \frac{3}{4} \log_2 \frac{4}{3},$$

тј капацитет канала је

$$C = \frac{1}{2} - \frac{3}{4} \log_2 \frac{4}{3}.$$

▲

58. Наћи капацитет канала са датом матрицом условних вероватноћа

	$Y = 0$	$Y = 1$	$Y = 2$
$X = 0$	$1/2$	$1/6$	$1/3$
$X = 1$	$1/3$	$1/2$	$1/6$
$X = 2$	$1/6$	$1/3$	$1/2$

Решење 58. Применом Теореме 2 добијамо

$$C = \log_2 3 - \frac{1}{2} \log_2 2 - \frac{1}{6} \log_2 6 - \frac{1}{3} \log_2 3 = \frac{1}{2} \log_2 3 - \frac{2}{3}.$$

▲

59. Наћи капацитет канала и расподелу на улазу за који се он постиже

	$Y=0$	$Y=1$	$Y=2$
$X=0$	$1/4$	0	$3/4$
$X=1$	0	1	0
$X=2$	$3/4$	0	$1/4$

Решење 59. Можемо другачије да поставимо матрица прелаза (пермутацијом да променимо положај)

	$Y=0$	$Y=2$	$Y=1$
$X=0$	$1/4$	$3/4$	0
$X=2$	$3/4$	$1/4$	0
$X=1$	0	0	1

Тако добијамо да је канал "делимично" симетричан. Укупан капацитет добијамо из формуле за матрице која је блок матрица са дисјункним вредностима

$$2^C = 2^{C_1} + 2^{C_2},$$

где је C_1 - капацитет првог канала (прве две врсте и колоне), а C_2 - капацитет другог канала (односно трећа врста и трећа колона).

Одмах видимо да је $C_2 = 0$, док је C_1 симетричан па његову вредности добијамо из теореме 2:

$$C_1 = 1 - \frac{1}{4}\log_2 4 - \frac{3}{4}\log_2\frac{4}{3} = \frac{1}{2} - \frac{3}{4}\log_2\frac{4}{3}.$$

Док је укупна вредност капацитета датог канала у задатку

$$C = \log_2\left(2^{\frac{1}{2}-\frac{3}{4}\log_2\frac{4}{3}} + 1\right).$$

Расподелу на улазу рачунамо на следећи начин. Посматрајмо посебно дисјунктне делове канала везе:

$$X_{C_1} = \begin{pmatrix} 0 & 1 & 2 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}$$

$$X_{C_2} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

Такође, морамо да узмемо у обзир тежине сваког блока.

$$p = \frac{2^{C_1}}{2^{C_1} + 2^{C_2}},$$

што представља тежину првог блока, док $1-p$ другог.

Коначну расподелу добијамо на следећи начин:

$$p \cdot [1/2, 0, 1/2] + (1-p)\cdot[0,1,0] = \left[\frac{p}{2}, 1-p, \frac{p}{2}\right].$$

▲

60. Наћи капацитет канала

	a	b	c	d
0	$\frac{1-p}{2}$	$\frac{1-p}{2}$	$\frac{p}{2}$	$\frac{p}{2}$
1	$\frac{p}{2}$	$\frac{p}{2}$	$\frac{1-p}{2}$	$\frac{1-p}{2}$

Решење 60. Канал је симетричан и има решење у професоровој скрипти. Пробајте сами да изведете.

Решење је:

$$C = 1 - H(p, 1-p),$$

где је $H(p, 1-p)$ - неодређеност случајне величине која узима вероватноће p и $1-p$. ▲

61. Посматрајмо 26 слова на тастатури.

(a) Ако се притисне типка, резултат је одговарајуће слово. Одредити капацитет таквог канала.

(б) Ако се притисне типка, резултат је то слово или слово до њега са једнаким вероватноћама. Према томе: $A \to A$ или $A \to B$, ..., $Z \to Z$ или $Z \to A$. Одредити капацитет таквог канала.

Решење 61. (а) Имамо да је $X \equiv Y$, јер нема никакве случајности у каналу. Капацитет је

$$I(X;Y) = H(Y) - H(Y|X) = H(Y) \leq \log_2 26,$$

што се максимизује наравно за равномерну расподелу па је капацитет

$$C = \log_2 26.$$

(б) У овом случају имамо неке случајности, односно сметње, па добијамо:

$$I(X;Y) = H(Y) - H(Y|X) \leq \log_2 26 - \log_2 2 = \log_2 13 = C.$$

▲

62. Наћи капацитет канала са датом матрицом условних вероватноћа

	$Y=0$	$Y=1$
$X=0$	1	0
$X=1$	1/2	1/2

Решење 62. У овом задатку дата матрица прелаза није симетрична, а није ни блок-дијагонална. У том случају тражимо капацитет директно по дефиницији.

$$C = \max_{P(x)}(H(Y) - H(Y|X)) \tag{30}$$

$$= \max_{P(x)}(-\frac{p}{2}\log_2\frac{p}{2} - (1-\frac{p}{2})\log_2(1-\frac{p}{2}) - H(Y|X=0)P\{X=0\} - H(Y|X=1)P\{X=1\}) \tag{31}$$

$$= \max_{P(x)}(-\frac{p}{2}\log_2\frac{p}{2} - (1-\frac{p}{2}\log_2(1-\frac{p}{2})) - p) \tag{32}$$

Да бисмо даље нашли максимум означимо функцију унутар максимума са $f(p)$ и нађимо извод по p. Максимум се достиже за $p = \frac{2}{5}$.

▲

63. Наћи капацитет канала $C_1 \cdot C_2$ са датом матрицама условних вероватноћа C_1 односно C_2 респективно:

	$Y=0$	$Y=1$
$X=0$	1/3	2/3
$X=1$	2/3	1/3

	$Z=0$	$Z=1$
$Y=0$	5/9	4/9
$Y=1$	4/9	5/9

Решење 63. Нађимо производ ове две матрице:

	$Z=0$	$Z=1$
$X=0$	13/27	14/27
$X=1$	14/27	13/27

Добили смо симетричну матрицу па према теореми 2 налазимо капацитет. ▲

64. Нека је C капацитет канала

	$Y=0$	$Y=1$
$X=0$	1/3	2/3
$X=1$	2/3	1/3

Ако је C_n капацитет n редно везаних канала $C_n = C \cdot C \cdot \cdots \cdot C$, наћи $\lim_{n\to\infty} C_n$.

Решење 64. Налазимо производ матрица помоћу методу дијагонализације.

$$M = TDT^{-1},$$

где је D - дијагонална матрица. Тада

$$M^n = TD^nT^{-1}.$$

Матрицу D налазимо помоћу сопствених вредности матрице прелаза. И добијамо да је то

$$a_1 = 1, \quad a_2 = -\frac{1}{3}$$

И онда матрица D је облика

$$D = \begin{bmatrix} 1 & 0 \\ 0 & -1/3 \end{bmatrix}$$

Степенујемо матрицу

$$D^n = \begin{bmatrix} 1 & 0 \\ 0 & (-1/3)^n \end{bmatrix}$$

И кад пустимо лимес видимо да је капацитет канала заправо 0.

▲

65. Наћи чему тежи капацитет канала C_n ако је $C_n = C \cdot C_{n-1}$, где је $C_1 = C$ а C је канал са следећом матрицом прелаза:

	$Y=0$	$Y=1$	$Y=2$
$X=0$	$1/3$	0	$2/3$
$X=1$	0	1	0
$X=2$	$1/4$	0	$3/4$

Решење 65. Дата је блок дијагонална матрица па капацитет канала налазимо из формуле

$$2^C = 2^{C_1} + 2^{C_2},$$

капацитет канала који садржи само једну вредност је нула. А капацитет другог налазимо слично као у претходном задатку. Сопствене вредности су 1 и $\frac{1}{12}$. Стога је капацитет и овог дела заправо нула у граничној вредности. Укупан капацетет канала је самим тим 1. ▲

66. Наћи капацитет канала

	$Y=0$	$Y=1$	$Y=2$	$Y=3$	$Y=4$	$Y=5$
$X=0$	$1/8$	$1/8$	$1/8$	$1/8$	$1/4$	$1/4$
$X=1$	$1/8$	$1/8$	$1/4$	$1/8$	$1/8$	$1/8$
$X=2$	$1/4$	$1/4$	$1/8$	$1/8$	$1/8$	$1/8$

Решење 66. Канал је симетричан па се све решава применом теореме 2. За самосталну вежбу. ▲

67. Наћи капацитет канала и расподелу на улазу за коју се остварује

	$Y=0$	$Y=1$	$Y=2$	$Y=3$	$Y=4$
$X=0$	$1/4$	$1/4$	$1/2$	0	0
$X=1$	$1/2$	$1/4$	$1/4$	0	0
$X=2$	$1/4$	$1/2$	$1/4$	0	0
$X=3$	0	0	0	$1/4$	$3/4$
$X=4$	0	0	0	$3/4$	$1/4$

Решење 67. Блок дијагонална матрица прелаза је дата у задатку. Сваки од блокова је симетрична матрица прелаза па се оба решавају применом теореме 2.

Коначан капацитет канала је

$$C = \log_2\left(\frac{3}{2^{3/2}} + \frac{3^{3/4}}{2}\right),$$

док је расподела на улазу:

$$\left[\frac{p}{3}, \frac{p}{3}, \frac{p}{3}, \frac{1-p}{2}, \frac{1-p}{2}\right],$$

где је $p = \dfrac{2^{C_1}}{2^{C_1} + 2^{C_2}}$. ▲

68. Дата је расподела на улазу

$$X : \begin{pmatrix} 1 & 2 & 3 \\ 0.3 & 0.2 & 0.5 \end{pmatrix},$$

и канал везе са матрицом прелаза:

	$Y = 1$	$Y = 2$	$Y = 3$
$X = 1$	0.2	0.6	0.2
$X = 2$	0.3	0.3	0.4
$X = 3$	0.1	0.1	0.8

(а) Наћи шему декодирања за идеалног посматрача;

(б) Наћи шему декодирања за посматрача максималне веродостојности (идеалног посматрача при равномерној расподели на улазу).

Решење 68. Шема декодирања идеалног посматрача подразумева узимање у обриз улазних вероватноћа. Док посматрач максималне веродостојности узима у обзир само матрицу преласка.

(а) У случају идеалног посматрача направимо матрицу могућих вредности за њега:

1) Ако смо примили 1 која је вероватноћа да је 1 била послата? То добијамо помоћу:

$$p(1|1) = P\{X = 1|Y = 1\} = \frac{P\{Y = 1|X = 1\}P\{X = 1\}}{P\{Y = 1\}} = \frac{0.2 \cdot 0.3}{P\{Y = 1\}} = \frac{0.06}{P\{Y = 1\}}$$

Ако смо примили 1 која је вероватноћа да је 2 била послата? То добијамо помоћу:

$$p(2|1) = P\{X = 2|Y = 1\} = \frac{P\{Y = 1|X = 2\}P\{X = 2\}}{P\{Y = 1\}} = \frac{0.3 \cdot 0.2}{P\{Y = 1\}} = \frac{0.06}{P\{Y = 1\}}$$

Ако смо примили 1 која је вероватноћа да је 3 била послата? То добијамо помоћу:

$$p(3|1) = P\{X = 3|Y = 1\} = \frac{P\{Y = 1|X = 3\}P\{X = 3\}}{P\{Y = 1\}} = \frac{0.1 \cdot 0.5}{P\{Y = 1\}} = \frac{0.05}{P\{Y = 1\}}$$

Дакле закључак ако смо примили 1 највероватније је послата 1 или 2 па ћемо 1 да декодирамо као 1 или 2, свеједно је.

2) Ако смо примили 2 која је вероватноћа да је 1 била послата? То добијамо помоћу:

$$p(1|2) = P\{X = 1|Y = 2\} = \frac{P\{Y = 2|X = 1\}P\{X = 1\}}{P\{Y = 2\}} = \frac{0.6 \cdot 0.3}{P\{Y = 2\}} = \frac{0.18}{P\{Y = 2\}}$$

Ако смо примили 2 која је вероватноћа да је 2 била послата? То добијамо помоћу:

$$p(2|2) = P\{X = 2|Y = 2\} = \frac{P\{Y = 2|X = 2\}P\{X = 2\}}{P\{Y = 2\}} = \frac{0.3 \cdot 0.2}{P\{Y = 2\}} = \frac{0.06}{P\{Y = 2\}}$$

Ако смо примили 2 која је вероватноћа да је 3 била послата? То добијамо помоћу:

$$p(3|2) = P\{X = 3|Y = 2\} = \frac{P\{Y = 2|X = 3\}P\{X = 3\}}{P\{Y = 2\}} = \frac{0.1 \cdot 0.5}{P\{Y = 2\}} = \frac{0.05}{P\{Y = 2\}}$$

Дакле закључак ако смо примили 2 највероватније је послата 1 па ћемо 2 да декодирамо као 1.

3) Ако смо примили 3 која је вероватноћа да је 1 била послата? То добијамо помоћу:

$$p(1|3) = P\{X = 1|Y = 3\} = \frac{P\{Y = 3|X = 1\}P\{X = 1\}}{P\{Y = 3\}} = \frac{0.2 \cdot 0.3}{P\{Y = 3\}} = \frac{0.06}{P\{Y = 3\}}$$

Ако смо примили 3 која је вероватноћа да је 2 била послата? То добијамо помоћу:

$$p(2|3) = P\{X = 2|Y = 3\} = \frac{P\{Y = 3|X = 2\}P\{X = 2\}}{P\{Y = 3\}} = \frac{0.4 \cdot 0.2}{P\{Y = 3\}} = \frac{0.08}{P\{Y = 3\}}$$

Ако смо примили 3 која је вероватноћа да је 3 била послата? То добијамо помоћу:

$$p(3|3) = P\{X = 3|Y = 3\} = \frac{P\{Y = 3|X = 3\}P\{X = 3\}}{P\{Y = 3\}} = \frac{0.8 \cdot 0.5}{P\{Y = 3\}} = \frac{0.4}{P\{Y = 3\}}$$

Дакле закључак ако смо примили 3 највероватније је послата 3 па ћемо 3 да декодирамо као 3.

(б) У овој шеми све је значајно простије - бирамо максимум по колонама у матрици преласка. Дакле, ако смо примили 1 то декодирамо као 2, ако смо примили 2 то декодирамо као 1 и ако смо примили 3 то декодирамо као 3.

▲

69. Дат је канал C

	$Y=1$	$Y=2$	$Y=3$
$X=1$	1	0	0
$X=2$	0	a	$1-a$
$X=3$	0	b	$1-b$

Који услов треба да задовољавају a и b тако да идеални посматрач за равномерну расподелу на улазу декодира примљену вредност као ону која је послата?

Решење 69. За самосталну вежбу. ▲

70. Нека је Γ канал везе који има капацитет C. Показати да је капацитет канала $\Gamma+\Gamma+\cdots+\Gamma$ (m пута) једнак $C+\log_2 m$.

Решење 70. И у овом случају имамо блок дијагоналне матрице.
Формула је

$$2^{C_{svi}} = \sum_{i=1}^{m} 2^{C_i},$$

за свако i вредност у суми је $2^{C_i}=2^C$. На крају добијамо да је

$$C_{svi} = \log_2(m\cdot 2^C) = \log_2 m + C$$

▲

71. Дат је бинарни понављајући код $\mathcal{K}_n$ непарне дужине $n=2t+1$ којим се кодирају поруке које се преносе кроз бинарни симетрични канал у коме је вероватноћа погрешног преноса једнака $q<\frac{1}{2}$. Наћи правила максималне веродостојности δ и показати да је вероватноћа грешке тог правила

$$p_e \leq \frac{(2t+1)!}{(t!)^2}\,(1-q)^t\,q^{t+1} \tag{33}$$

и да тежи нули.
Због чега ово није добар пример кода са тачке гледишта фундаменталне теореме теорије информације?

Решење 71. Показаћемо на примеру за случај $n=3$ због компактности записа при објашњењу. Све се подједнако уопштава на случај већег n.

Код понављајућег бинарног кода матрица прелаза изгледа овако

	$Y=000$	$Y=001$	$Y=010$	$Y=100$	$Y=011$	$Y=101$	$Y=110$	$Y=111$
$X=0$	$(1-q)^3$	$q(1-q)^2$	$q(1-q)^2$	$q(1-q)^2$	$q^2(1-q)$	$q^2(1-q)$	$q^2(1-q)$	q^3
$X=1$	q^3	$q^2(1-q)$	$q^2(1-q)$	$q^2(1-q)$	$q(1-q)^2$	$q(1-q)^2$	$q(1-q)^2$	$(1-q)^3$

Како је у питању правило максималне веродостојности, то бирамо максимуме по колонама узимајући у обзир да је $q<0.5$. Дакле, шема декодирања је следећа:

- $000\to 0$
- $001\to 0,\ 010\to 0,\ 100\to 0$
- $011\to 1,\ 101\to 1,\ 110\to 1$
- $111\to 1$

Док је вероватноћа грешке у овом случају

$$p_e = \big(q^3+3q^2(1-q)\big) = q^3+3q^2(1-q) \leq \frac{3!}{1}\,(1-q)\,q^2,$$

јер $q\leq 1-q$. Слично се уопштава за произвољно t, односно n.

Код ње добар због екстремно ниске брзине преноса са порастом броја понављања. Замислите да сваки пут некој особи откуцате и пошаљете 100 истих порука уместо 1, јасно да је брзина тиме уништена. ▲

72. Дат је бинарни канал везе својом матрицом прелазних вероватноћа

	$Y=0$	$Y=1$
$X=0$	1	0
$X=1$	q	$1-q$

Због повећања поузданости 0 се кодира као 000, а 1 као 111. Нека је δ_1 правило максималне веродостојности, δ_2 правило којим закључујемо да је послата 0, уколико примљена реч има бар две нуле, а 1 ако има бар две јединице.

(а) Које од ова два правила има већу вероватноћу грешке? Расподела на улазу $p(0)=p$, $p(1)=1-p=w$.

(б) Колика је брзина оваквог преноса?

(в) Шта се са брзином преноса и вероватноћом грешке дешава уколико кодирамо понављајућим кодом дужине n?

Решење 72. Прави се матрица прелаза слично као у претходном задатку само што није симетричан канал у питању.

	$Y=000$	$Y=001$	$Y=010$	$Y=100$	$Y=011$	$Y=101$	$Y=110$	$Y=111$
$X=0$	1	0	0	0	0	0	0	0
$X=1$	q^3	$q^2(1-q)$	$q^2(1-q)$	$q^2(1-q)$	$q(1-q)^2$	$q(1-q)^2$	$q(1-q)^2$	$(1-q)^3$

(а) Са Q означићемо матрицу прелаза. Вероватноћа грешке правила δ_1 налазимо помоћу

$$\begin{aligned} R_{\delta_1} &= \begin{bmatrix} p & 0 \\ 0 & w \end{bmatrix} Q \\ &= \begin{bmatrix} p & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ wq^3 & wq^2(1-q) & wq^2(1-q) & wq^2(1-q) & wq(1-q)^2 & wq(1-q)^2 & wq(1-q)^2 & w(1-q)^3 \end{bmatrix}, \end{aligned}$$

бирамо максимуме по колонама. Дакле декодирање је увек 0, сем у случају да је добијена порука 000. Одакле добијамо грешку:

$$p_{\delta_1} = wq^3 = (1-p)q^3$$

Док за δ_2 је

$$\begin{aligned} R_{\delta_2} &= \begin{bmatrix} p & 0 \\ 0 & w \end{bmatrix} Q \\ &= \begin{bmatrix} p & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ wq^3 & wq^2(1-q) & wq^2(1-q) & wq^2(1-q) & wq(1-q)^2 & wq(1-q)^2 & wq(1-q)^2 & w(1-q)^3 \end{bmatrix}, \end{aligned}$$

бирамо према описаном правилу. Дакле првих 4 (000, 001, 010, 100) декодирамо као 0, док преостале као 1. Одакле добијамо грешку:

$$p_{\delta_2} = wq^3 + 3wq^2(1-q)$$

(б) Брзина понављајућег кода је дефинисана на следећи начин

$$R = \frac{1}{n},$$

где је n број понављања. Па је у овом задатку $R = \frac{1}{3}$.

(в) Брзина се смањује повећањем броја понављања према горе наведеној дефиницији.

▲

Линеарни кодови

73. Нека је

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

матрица провере линеарног кода. Одредити број информационих битова, број битова провере и кодне речи.

Решење 73. Дата је матрица провере а за њу важи $H \cdot v = 0$, где је v-кодна реч.

$$H \cdot v = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{bmatrix} = \begin{bmatrix} v_1 + v_3 + v_5 \\ v_2 + v_3 + v_6 \\ v_1 + v_2 + v_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Из ових једначина и чињенице да важи $-x = x$ *(mod 2)*, добијамо

$$v_5 = v_1 + v_3$$
$$v_6 = v_2 + v_3$$
$$v_4 = v_1 + v_2,$$

тј. знајући вредности прва три знака можемо добити и све остале. Одавде одмах видимо да је број информационих битова заправо

$$k = |\{v_1, v_2, v_3\}| = 3,$$

док је број битова провере $n - k = 3$, тј. такође три. Са прва три бита шаље се порука, док са преостала три проверава да ли је добијена порука тачна.

Број кодних речи је $2^k = 2^3 = 8$ и то су:

редни број	v_1	v_2	v_3	кодна реч
1	0	0	0	000000
2	0	0	1	001011
3	0	1	0	010101
4	1	0	0	100110
5	0	1	1	011110
6	1	0	1	101101
7	1	1	0	110011
8	1	1	1	111000

▲

74. Нека је

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

матрица провере линеарног кода. Одредити број информационих битова, број битова провере и кодне речи. Ако се исправљају обрасци грешака најмање тежине у косету, наћи један начин декодирања.

Решење 74. Слично као и претходном задатку[3] откривамо да су кодне речи

редни број	v_4	v_5	кодна реч
1	0	0	00000
2	0	1	11001
3	1	0	11110
4	1	1	00111

[3] урадите то за вежбу

Број информационих битова је 2, док је број битова провере 3.

Косети:

редни број	грешка(e)	$e+v_2$	$e+v_3$	$e+v_4$
1	00000	11001	11110	00111
2	00001	11000	11111	00110
3	00010	11011	11100	00101
4	00100	11101	11010	00011
5	01000	10001	10110	01111
6	10000	01001	01110	10111
7	01100	10101	10010	01011
8	01010	10011	10100	01101

Помоћу ових косета смо покрили све могуће вредности са 5 бинарних цифара.

Након тога за сваку пристиглу реч гледамо у ком се косету налази и на ту добијену поруку додајемо грешку која се јавља у том реду где смо нашли примљену реч. Тако се врши декодирање и исправљање грешака. ▲

75. Дате су кодне речи 00010, 11001 и 11111. Одредити матрицу провере линеарног кода са највећим могућим бројем битова провере. Колики је број информационих, а колико је број битова провере тог кода?

Решење 75. Дате су нам кодне речи, које су и линеарно независне. Такве кодне речи могу да чине генераторну матрицу.

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

У генераторној матрици G тражимо линеарно независне колоне(!). Колоне означимо редом са c_1, c_2, c_3, c_4, c_5. Линеарно независне колоне су нпр. друга(c_2), трећа(c_3) и четврта(c_4) колоне. Имамо и следеће једнакости

$$c_1 + c_2 = 0 \quad (34)$$
$$c_5 + c_2 = 0, \quad (35)$$

и ово можемо записати у облику матрице провере:

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

односно гледамо која колона из генераторне матрице се јавља у једначини и на њеном редном броју стављамо 1 и 0 уколико се не јавља. Тако у једначини (34) се јављају прва и друга колоне па је први ред у матрици провере 11000, док у (35) се јављају друга и пета колона па је други ред у матрици провере 01001.

Број информационих битова је $k = 3$, док је број битова провере $n - k = 5 - 3 = 2$. Како знамо да је то највећи могући број битова провере? Према задатку видимо да је дужина сваке кодне речи 5, а имамо бар три кодне речи, дакле $k \geq 3$. Стога највећи број битова провере је $n - k \leq 2$, односно 2. А баш то смо и добили у решењу. ▲

76. Дате су кодне речи 0000, 1001, 111 и 0110.

(а) Наћи матрицу провере линеарног кода, број битова провере и број информационих битова.

(б) Ако се исправљају обрасци грешака најмање тежине у косету, наћи један начин декодирања.

Решење 76. За самосталну вежбу. ▲

77. Нека је C бинарни $(5,3)$ код са генераторном матрицом

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

(а) Наћи стандардни облик генераторне матрице.

(а) Наћи матрицу провере.

(б) Наћи кодне речи дуалног кода $G^{\top}$.

Решење 77. (а) Стандардни облик је

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix},$$

тако што смо прву колону сабрали са другом и петом, трећу колону сабрали са четвртом и све пермутовали на овај облик.

(б) Наша генераторна матрица је

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix},$$

дакле тражимо линеарно независне колоне, то су c_1, c_2 и c_3. Једначине су

$$c_2 + c_3 + c_4 = 0 \tag{36}$$
$$c_1 + c_2 + c_5 = 0, \tag{37}$$

Одакле директно добијамо и матрицу провере:

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

(в) Дуални код се добија када матрицу провере поставимо да буде генераторна матрица. Тј. генераторна матрица дуалног кода је

$$G^{\top} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Његова матрица провере је

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

А све кодне речи овог кода су

редни број	v_1	v_3	кодна реч
1	0	0	000 00
2	0	1	011 10
3	1	0	110 01
4	1	1	101 11

▲

78. Матрица провере линеарног кода над азбуком је

$$H = \begin{bmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{bmatrix}$$

Наћи кодне речи и генераторну матрицу. Колико има информационих, а колико битова провере. Како се зове овакав код?

Решење 78.

$$H \cdot v = \begin{bmatrix} 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{bmatrix} = \begin{bmatrix} v_1 + 2v_2 \\ v_2 + 2v_3 \\ v_3 + 2v_4 \\ v_4 + 2v_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Важе једнакости

$$v_1 + 2v_2 = 0$$
$$v_2 + 2v_3 = 0$$
$$v_3 + 2v_4 = 0$$
$$v_4 + 2v_5 = 0$$

И видимо да су ове све једнакости заправо зависне. Ако је $v_1 = 1$ онда и сви остали битови морају да буду 1, ако је $v_1 = 0$ такође и сви остали су 0, а ако је $v_1 = 2$ и сви остали су два. Одатле следи да имамо само један информациони бит

$$k = 1$$

док су преосталих $n - k = 4$ битови провере. Кодне речи су

$$00000,$$
$$11111,$$
$$22222.$$

Овај код је понављајући код где је број понављања 5. ▲

Хамингова и Гилберт-Варшамова границе

Теорема 3. **[Хамингова граница]** Нека је C q-арни код и исправља t грешака, n је дужина речи, а M број кодних речи. Тада важи

$$M\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right)\leq q^n, \tag{38}$$

или другачије

$$\frac{\log_q\left(M\left(1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{t}(q-1)^t\right)\right)}{n}\leq\frac{\log_q q^n}{n}=1. \tag{39}$$

А са R означавамо брзину преноса дефинисану као

$$R=\frac{\log_q M}{n} \tag{40}$$

79. Нека је азбука бинарна ($q=2$), а $t=1$. Колики је највећи могући број кодних речи таквог кода?

Решење 79. Према теореми 3

$$M(1+n(2-1))\leq 2^n, \tag{41}$$

односно одавде добијамо број број кодних речи таквог кода

$$M=\left[\frac{2^n}{1+n}\right],$$

узимамо цео део, јер број кодних речи мора да буде цео број.

▲

80. За сваки линеарни код ЛК(n,k) који исправља t грешака над пољем F_q важи

$$\sum_{i=0}^{t}\binom{n}{i}(n-i)^i\leq q^{n-k}$$

Решење 80. Како је код линеаран са k информационих битова, то је број кодних речи $M=q^k$. Убацимо ово у теорему 3 и добијамо директно тврђење задатка. ▲

Дефиниција 1. Кажемо да је код C савршен уколико важи једнакост у (38) у теореми 3.

81. Показати да је линеарни код савршен ако и само ако исправља све грешке тежине t и ништа више.

Решење 81. За самосталну вежбу. ▲

82. Нека је $\mathcal{K}$ бинарни понављајући код дужине n (непарне), тј ЛК$(n,1)$, $q=2$ и $t=\frac{n-1}{2}$. Да ли је такав код савршен?

Решење 82. Према теореми 3 важи

$$\sum_{i=0}^{t}\binom{n}{i}=\frac{1}{2}\sum_{i=0}^{n}\binom{n}{i}=2^{n-1}$$

где једнакост важи због $t=\frac{n-1}{2}$ и чињеници да је $\binom{n}{i}=\binom{n}{n-i}$. ▲

Дефиниција 2. Линеаран код ЛК(n, k) је Хамингов ако важи $n = 2^r - 1$ и $k = 2^r - r - 1$ за неко $r \in \mathbb{N}$.

83. Показати да је ЛК$(7, 4)$ Хамингов и савршен.

Решење 83. Директно применом теореме 3 добијамо да је тај код савршен:

$$\sum_{i=0}^{1} \binom{7}{i}(2-1)^i = \binom{7}{0} + \binom{7}{1} = 8 = 2^{7-4} = 2^3.$$

А како је $n = 7 = 2^3 - 1$ и $k = 4 = 2^3 - 3 - 1$ то је код и Хамингов. ▲

84. Наћи Хамингове кодове.

Решење 84. Неки други Хамингови кодови су

- ЛК(7, 4)
- ЛК(15, 11)
- ...

▲

Теорема 4. [Гилберт-Варшамова граница] Нека је $A_q(n, d)$ број кодних речи q-арног кода C дужине n и Хаминговим растојањем d, такво да $n \geq d \geq 1$. Тада важи

$$A_q(n,d)\left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{d-1}(q-1)^{d-1}\right) \geq q^n. \tag{42}$$

85. Нека је дат код C за који важи над бинарном азбуком и Хаминговим растојањем 3. Наћи минималан и максималан број речи овог кода ако

(а) $n = 3$

(б) $n = 4$

(в) $n = 5$

(г) $n = 8$

Решење 85. Како је Хамингово растојање $d = 3$ то одмах можемо добити и t, односно број колико грешака исправља.

$$t = \frac{d-1}{2} = 1.$$

Одакле важи да је максималан број кодних речи према теореми 3

$$A_2(n, 3) = M \leq \frac{2^n}{1+n} \tag{43}$$

Док је доња граница из теореме 4

$$A_2(n, 3) \geq \frac{2^n}{1 + n + \frac{n(n-1)}{2}} \tag{44}$$

Наравно у случају горње границе узимамо цео део, док у случају доње границе заокружујемо на горњи цео део

(а) $2 \leq A_2(3, 3) \leq 2$

(б) $2 \leq A_2(4,3) \leq 3$

(в) $2 \leq A_2(5,3) \leq 5$

(г) $7 \leq A_2(8,3) \leq 28$

▲

86. Дат је бинарни код C. Свака кодна реч је дужине 4, минимално Хамингово растојање кода је 3. Наћи такав код да важи да је његов број кодних речи 2.

Решење 86. Како је Хамингово растојање овог кода 3 то је $t = 1$ (број грешака које исправља). Из претходног задатка видимо да је број кодних речи таквог кода 2 или 3.
Дакле, потребан нам је код где свака кодна реч има дужину 4 а свега их имамо 2, где је притом минимално Хамингово растојање 3. Такве кодне речи могу бити 1110 и 0000. Генераторна матрица таквог кода је

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Односно матрица провере

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

И заиста добијамо да су кодне речи 1110 и 0000. ▲

87. Дат је тринарни код C. Свака кодна реч је дужине n, минимално Хамингово растојање је 3. Наћи доњу границу за број речи таквог кода.

Решење 87. Према теореми 4

$$A_3(n,3) \geq \frac{3^n}{1 + 2n + 2n(n-1)} \tag{45}$$

▲

88. Наћи генераторну матрицу и матрицу провере за Хамингов ЛК(7, 4) код.

Решење 88. За самосталну вежбу. ▲

Теорема 5. Нека је C линеаран ЛК(n,k) код са миниманлним Хаминговим растојањем d. Тада је број линеарно независних колона у матрици провере баш d.

89. Испитати да ли је бинарни линеарни ЛК(23, 12) код савршен ако му је минимално Хамингово растојање 7.

Решење 89. За самосталну вежбу. ▲

90. Нека је

$$G = \begin{bmatrix} J+I & I & -I \\ 0 & H & -H \end{bmatrix}$$

генераторна матрица кода, где је I јединична матрица $4x4$, J матрица која се састоји само од јединица димензије $4x4$, а H је

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}$$

Показати да је G генераторна матрица за тернарни ЛК(12, 6) са минималним Хаминговим растојањем 6. Тај код је Голајев G_{12} код.

Решење 90. ▲

Други задаци

91. У белој кутији налазе се 2 беле, 3 црвене и 3 плаве куглице, у црвеној 6 белих, 3 црвене и 1 плава, а у плавој 2 беле и 2 црвене куглице. Случајно се бира кутија, а онда из ње куглица. Затим се та куглица ставља у кутију исто обојену као та куглица. Наћи узајамну информацију боје извучене куглице и броја куглица у белој кутији на крају експеримента.

92. Дате су дискретне случајне величине X, Y и Z.

(а) Доказати да за свако $k \in \mathbb{N}$ важи

$$\mathrm{H}(Z^{2k+1}) - \mathrm{H}(Z|Z^{2k}) = \mathrm{H}(Z^2).$$

(б) Доказати да важи

$$\frac{1}{2}\left[\mathrm{H}(X,Y) + \mathrm{H}(X,Z) + \mathrm{H}(Y,Z)\right] \geq \mathrm{H}(X,Y,Z).$$

(в) Ако важи $\mathrm{H}(X) \leq \mathrm{H}(Y) \leq \mathrm{H}(Z)$, наћи доњу и горњу границу израза $\mathrm{H}(X,Y,Z)$, као и услове под којим се те границе достижу.

93. Дата је изворна азбука A која има шест слова, а вероватноће њихових појављивања су: $p(a_1) = 0.33$, $p(a_2) = 0.25$, $p(a_3) = 0.22$, $p(a_4) = 0.08$, $p(a_5) = 0.07$, $p(a_6) = 0.05$. Наћи средње дужине Хафманових и Шенонових бинарних и тернарних кодова азбуке A.

94. Одредити минималан природан број n тако да постоји тренутни бинарни код чије су речи редом дужина n, n, $n+1$, $n+1$, $n+1$, $n+2$, $n+2$, $n+2$.

95. Одредити неодређеност $\mathrm{H}(X)$ случајне величине X чији је закон расподеле

$$p(x) = \frac{1}{C \cdot x \log_2^2 x}, \quad x = 2, 3, \ldots,$$

где је $C = \sum_{x=2}^{\infty} \frac{1}{x \log_2^2 x}$.

96. Нека код $\mathcal{K} \subset A^n$, где је A азбука од s слова, исправља t грешака.

а) Формулисати и доказати Хамингову границу за код $\mathcal{K}$.

б) Одредити максималну брзину кода $\mathcal{K}$.

в) Написати дефиницију савршеног линеарног кода преко Хамингове границе.

г) Која од следећих факторизација може бити факторизација Хамингове границе линеарног бинарног савршеног кода? Ако јесте написати ког тачно.

1) $1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}$;
2) $1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 2^2$;
3) $1 + \binom{90}{1} + \binom{90}{2}$.

97. Нека је X_0, X_1, $X_2, \ldots$ случајно лутање по целобројним вредностима дефинисано на следећи начин. Полази се из тачке $X_0 = 0$, први корак има једнаку вероватноћу у обе стране ($X_1 = \pm 1$ с једнаким вероватноћама), а сваки следећи има вероватноћу од 0.9 да буде у смеру претходног корака, а 0.1 да буде у супротном смеру. Израчунати неодређеност $\mathrm{H}(X_1, \ldots, X_n)$.

98. Нека је $\mathcal{K}$ бинарни линеарни код дат својом генераторном матрицом

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

а) Наћи матрицу провере H кода $\mathcal{K}$.

б) Одредити укупан број кодних речи и брзину кода. Образложити одговор.

в) Наћи $\Delta(\mathcal{K})$, минимално растојање кода $\mathcal{K}$. Објаснити како уклањање неких координата утиче на минимално растојање и брзину кода.

г) Колико има косета датог кода чија је Хамингова тежина једнака 1? Постоји ли неки косет чија је Хамингова тежина једнака 2?

д) Конструишите табелу синдрома а затим помоћу ње декодирајте примљене речи 100010, 010001, 001100. Да ли бисте декодирањем добили друге кодне речи да сте узели неке друге представнике косета?

99. Дата је матрица провере линеарног кода $\mathcal{K}$

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

а) Одредити број кодних речи, број цифара провере и генераторну матрицу кода $\mathcal{K}$.

б) Одредити минимално растојање кода $\mathcal{K}$. Колико простих грешака он исправља?

в) Нека је примљена реч 1101001. Наћи њен синдром и декодирати поруку.

100. Извор информације емитује следеће симболе: 0, 1, -1, 2 и -2. Међутим, приликом слања поруке додају се сметње, које узимају вредности: -1, 0 и 1, са једнаким вероватноћама.

а) Одредити капацитет таквог канала.

б) Показати да важи

$$I(X;Y|Z) = \sum_z I(X;Y|Z=z)P\{Z=z\}.$$

в) Претпоставимо да је познато $Z = |E|$, где је E сметња из поставке задатка. Одредити капацитет канала у овом случају.

101. Нека је азбука дужине n и $p_1 \geq p_2 \geq \cdots \geq p_n$. Доказати да ако је $p_1 \geq \frac{4}{10}$, тада је најкраћа реч у бинарном Хафмановом коду дужине 1.

102. Ако је матрица преласка блок-дијагонална облика

$$\begin{array}{|c|c|} Q_1 & 0 \\ 0 & Q_2 \\ \hline \end{array}$$

тада важи да је укупан капацитет канала $\log_2(2^{C_1} + 2^{C_2})$, где су C_1 и C_2 капацитети Q_1 и Q_2, респективно. Доказати.