Klaidas taisančių kodų teorija

Paskaitų konspektai

Gintaras Skersys
VU MIF

2008 m. pavasaris

Dėkoju Justui Kranauskui ir Andriui Unguriui už pradinio konspektų varianto surinkimą.

I dalis
Pagrindinės sąvokos

1 Įvadas

Panagrinėkime tokią schemą. Kažkokį pranešimą M norime kažkam perduoti. Perduodant pranešimą, galimas jo iškraipymas. Tai galima pavaizduoti grafiškai šitaip:

$$M \longrightarrow \boxed{\text{kanalas}} \longrightarrow M'(\text{galbūt} \neq M)$$

Pranešimas M perduodamas nepatikimu ryšio kanalu, t.y. kanale jį gali iškraipyti triukšmas. Iš kanalo išėjęs pranešimas M' gali skirtis nuo M. Ką daryti, kad iškraipymo tikimybė būtų kuo mažesnė?

Keli kanalų pavyzdžiai:

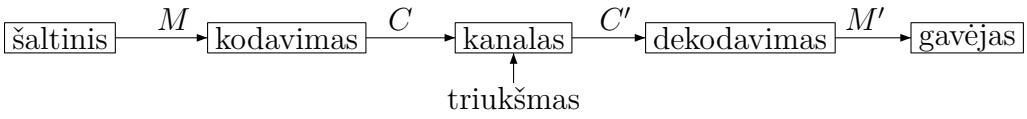
1. Telefono linija (informacija gali būti iškraipyta dėl triukšmo ir t.t.).
2. Kosminis zondas siunčia Marso nuotraukas į Žemę.
3. Ląstelių dalijimasis — motininės ląstelės DNR perduoda informaciją dukterinės ląstelės DNR (dėl radiacijos ir kt. poveikio gali mutuoti).
4. Informacijos laikmena, pavyzdžiui, kietas diskas — informacija užrašoma, o po kurio laiko nuskaitoma.

Paskutinis pavyzdys rodo, kad „kanalas“ nebūtinai reiškia, kad informacija perkeliama iš vienos vietos į kitą. Mes užrašome failą į diską ir jį nuskaitome paprastai toje pačioje vietoje, bet skirtingu laiku. O per tą laiką jis galėjo būti iškraipytas.

Visi šie ryšio kanalai yra *nepatikimi*, t. y. gali iškraipyti[1] informaciją. Norėtųsi turėti tokį ryšio kanalą, kuriame informacijos iškraipymo tikimybė būtų lygi nuliui, arba bent jau tokia artima nuliui, kad praktikoje ją galėtume laikyti lygia nuliui. Ką daryti?

Fizinis sprendimas būtų bandyti pagerinti kanalo fizines charakteristikas, tačiau tada išauga perdavimo kaštai.

Kodavimo teorijos siūlomas sprendimas — priimame kanalą tokį, koks jis yra, bet, perduodami juo informaciją, naudojame tam tikrus metodus, padedančius aptikti ir ištaisyti kanale padarytas klaidas. Tam informacija prieš siunčiant į kanalą yra koduojama, o išėjusi iš kanalo — dekoduojama:



Kodavimo metu prie pradinio pranešimo M prijungiama papildoma informacija, leisianti aptikti ir ištaisyti tam tikrą skaičių kanale padarytų klaidų. Gaunamas užkoduotas pranešimas C, kuris yra didesnės apimties nei M. Pranešimas C siunčiamas ryšio kanalu, kur galbūt yra kažkiek iškraipomas. Dekodavimo metu iš kanalo gautame pranešime C', naudojantis kodavimo metu pridėta informacija, yra ištaisomos klaidos ir gaunamas pradinis pranešimas M'. Paprastai, naudojant tokią sistemą, tikimybė, kad M' skirsis nuo M, žymiai sumažėja, užtat išauga informacijos kiekis, siunčiamas kanalu.

Taigi, fiziškai didinant kanalo patikimumą, jo kaina išauga, o naudojant kodavimą, vieninteliai kaštai yra papildomi skaičiavimai koduojant ir dekoduojant bei didesnis kanalo apkrovimas.

Informacijos teorija nagrinėja tokių sistemų teorines ribas ir galimybes.

Klaidas taisančių kodų teorija (trumpiau dažnai vadinama *kodavimo teorija*), kurios pradmenys ir bus pateikti šiame kurse, kuria praktinius kodavimo ir dekodavimo būdus.

2 Paprasti klaidas aptinkančių ir taisančių kodų pavyzdžiai

Ką galima pridėti prie pradinio pranešimo, kad būtų galima aptikti ir ištaisyti kanalo padarytas klaidas? Šiame skyriuje pateiksime kelis paprastus pavyzdžius. Tarkime, pradinis pranešimas M yra dvinaris vektorius (0 ir 1 seka).

2.1 Pakartojimo kodas R_n

Tarkime, $n \geqslant 1$ — sveikasis skaičius. Paprasčiausias kodavimo būdas - pakartoti kiekvieną siunčiamą ženklą (0 arba 1) n kartų.

Pavyzdys. $n = 3, M = (1\ 0\ 1\ 1)$ — pradinis pranešimas;

$C = (1\ 1\ 1\ \ 0\ 0\ 0\ \ 1\ 1\ 1\ \ 1\ 1\ 1)$ — siunčiamas pranešimas;

$C' = (1\ 0\ 1\ \ 0\ 0\ 1\ \ 0\ 1\ 0\ \ 1\ 1\ 1)$ — gautas pranešimas (kanale padarytos 4 klaidos);

$E = C' - C \pmod 2 = (0\ 1\ 0\ \ 0\ 0\ 1\ \ 1\ 0\ 1\ \ 0\ 0\ 0)$ — skirtumas tarp gauto ir išsiųsto vektorių, vadinamas *klaidų vektoriumi*. Jei kuri nors klaidų vektoriaus koordinatė nelygi nuliui, reiškia, toje

[1] Čia turima omenyje, kad iškraipymai įvyksta ne dėl kieno nors piktos valios, o dėl gamtinių sąlygų, technikos netobulumo ir pan. atsiradusio kanalo triukšmo. Piktavalius iškraipymus nagrinėja *kriptografija*.

pozicijoje įvyko klaida; jei lygi nuliui — klaidos ten nėra. Čia „(mod 2)“ reiškia, kad skaičiavimas vyksta moduliu 2, t.y., skirtumo $C' - C$ koordinatės dalinamos iš 2 ir imama liekana. Pastebėsime, kad, skaičiuojant moduliu 2, -1=1 ir 2=0.

Dekoduodami ženklų seką išskaidome į blokus po $n = 3$ simbolius. Kiekvieną bloką keičiame ženklu, kuris dažniausiai kartojasi tame bloke.

$M' = (1\ 0\ 0\ 1)$ - dekoduotas pranešimas ($M' \neq M$). □

Bendru atveju, kiekviename bloke galime ištaisyti $\left\lfloor \frac{n-1}{2} \right\rfloor$ klaidų, kur $\lfloor x \rfloor$ yra skaičiaus x sveikoji dalis (didžiausias sveikasis skaičius, mažesnis už x). Pavyzdžiui, kai $n = 3$, kiekviename bloke galime ištaisyti $\left\lfloor \frac{3-1}{2} \right\rfloor = \lfloor 1 \rfloor = 1$ klaidą, o kai $n = 4$, tai irgi $\left\lfloor \frac{4-1}{2} \right\rfloor = \lfloor 1.5 \rfloor = 1$ klaidą (jei įvyktų dvi klaidos, nulių ir vienetų gautume po lygiai, todėl negalėtume pasakyti, ar užkoduotas nulis, ar vienetas). Tai reiškia, kad naudodami pavyzdyje nurodytą dekodavimo procedūrą mes *tikrai* galėsime ištaisyti visas padarytas klaidas, jei jų skaičius neviršija $\left\lfloor \frac{n-1}{2} \right\rfloor$. Jei šis skaičius viršytas, tai galime dekoduoti klaidingai (bet galime ir teisingai).

Šis kodas yra $n - 1$ klaidą aptinkantis kodas. Iš tikro, jei padaroma $n - 1$ ar mažiau klaidų, iš kanalo gausime bloką, kuriame ne visi simboliai bus vienodi, iš ko ir nuspręsime, kad buvo klaidų. Bet jei klaidų buvo n, tai gausime bloką, kur vėl visi simboliai bus vienodi, ir negalėsime nuspręsti, ar klaidų buvo.

Kodo koeficientu vadinsime pradinio ir persiunčiamo pranešimų ilgių santykį. Jis parodo, kuri į kanalą pasiųstų simbolių dalis yra naudinga informacija, o kuri tik pridėta klaidų aptikimui ir ištaisymui. Kuo jis didesnis, tuo geriau, nes tuo daugiau naudingos informacijos yra siunčiamame pranešime.

Pakartojimo kodo R_n koeficientas yra mažas, tik $\frac{1}{n}$ (iš n kanalu persiųstų simbolių tik vienas yra pradinio pranešimo simbolis). Užtat klaidų jis ištaiso daug — beveik pusė simbolių gali būti klaidingi, vistiek kodas dekoduos teisingai.

2.2 Kontrolinio simbolio kodas (lyginių svorių kodas)

Šis kodas skirtas ne ištaisyti, o kuo greičiau ir paprasčiau surasti perdavimo klaidą.

Pradinį pranešimą $M = (m_1, m_2, \ldots, m_k)$ užkoduojame vektoriumi $C = (m_1, \ldots, m_k, m_{k+1})$, kur *kontrolinis simbolis* m_{k+1} prirašomas taip, kad vektoriuje C būtų lyginis vienetų skaičius. Nesunku pastebėti, kad m_{k+1} tenkina tokią formulę:

$$m_{k+1} = \sum_{i=1}^{k} m_i \ (mod\ 2) = \begin{cases} 0, \text{ jei vienetų skaičius vektoriuje } M \text{ lyginis;} \\ 1, \text{ jei vienetų skaičius vektoriuje } M \text{ nelyginis.} \end{cases}$$

Pavyzdys. Jei $M = (1\ 0\ 1\ 1\ )$, tai $C = (1\ 0\ 1\ 1\ 1)$. □

Vektorius C turi tenkinti lygybę:

$$\sum_{i=1}^{k+1} m_i \equiv 0 \ (mod\ 2)$$

Dekodavimas:

patikriname gautame kode vienetų skaičių, jei vienetų skaičius lyginis, tai padarome išvadą, kad klaidų nėra, jei nelyginis - yra. Šis kodas klaidų neištaiso, jis tik aptinka jas, jei jų skaičius - nelyginis.

Kodo koeficientas yra labai aukštas, $\frac{k}{k+1} = 1 - \frac{1}{k+1}$, bet kodas labai silpnas, nes neištaiso klaidų.

2.3 Knygų numeracijos sistema ISBN (International Standard Book Numbering)

Kiekviena dabar leidžiama knyga turi unikalų ISBN numerį, nurodantį šalį, leidyklą ir knygos numerį. ISBN numeris sudarytas iš devynių dešimtainių skaitmenų $a_1, \ldots, a_9$ bei dešimtojo kontrolinio a_{10}. Šis kodas aptinka dažniausias renkant skaičius pasitaikančias klaidas, kai

- vietoje vieno skaitmens įvedamas kitas,
- du gretimi skaitmenys sukeičiami vietomis.

Kontrolinis simbolis a_{10} pridedamas pagal tokią taisyklę:

$$a_{10} \equiv \sum_{i=1}^{9} i a_i \pmod{11}. \tag{1}$$

Jei gauname $a_{10} = 10$, tai kontrolinis simbolis a_{10} žymimas ženklu X.

Pavyzdys. ISBN $1 - 56592 - 127 - 5$. Daugiau pavyzdžių rasite pavartę knygas. □

2.1 teiginys. *(1) lygybė nebegalioja, jei padaroma viena klaida arba transpozicija (greta stovinčių skaitmenų sukeitimas vietomis). Jei padaromos dvi klaidos, (1) lygybė gali išlikti teisinga.*

Užduotis. Įrodyti teiginį.

Užduotis. Paimkite bet kurią knygą ir patikrinkite, ar tikrai jos ISBN tenkina (1) lygybę.

2.4 Asmens kodas

Lietuvos gyventojų asmens kodo struktūra:

$$\underbrace{L}_{\text{Lytis}}\ \underbrace{Y_1Y_2M_1M_2D_1D_2}_{\text{Gimimo data}}\ \underbrace{X_1X_2X_3}_{\text{Asmens eilės nr.}}\ \underbrace{K}_{\text{Kontrolinis simbolis}}$$

L gali įgyti reikšmę nuo 1 iki 6:

1 — vyras, gimęs XIX a.,

2 — moteris, gimusi XIX a.,

3 — vyras, gimęs XX a.,

4 — moteris, gimusi XX a.,

5 — vyras, gimęs XXI a.,

6 — moteris, gimusi XXI a.

Kontrolinis skaičius K apskaičiuojamas taip:

$$S = L \cdot 1 + Y_1 \cdot 2 + Y_2 \cdot 3 + M_1 \cdot 4 + M_2 \cdot 5 + D_1 \cdot 6 + D_2 \cdot 7 + X_1 \cdot 8 + X_2 \cdot 9 + X_3 \cdot 1 \pmod{11}.$$

Jei $S \neq 10$, tai $K = S$. Jei $S = 10$, tai skaičiuojame taip:

$$S = L \cdot 3 + Y_1 \cdot 4 + Y_2 \cdot 5 + M_1 \cdot 6 + M_2 \cdot 7 + D_1 \cdot 8 + D_2 \cdot 9 + X_1 \cdot 1 + X_2 \cdot 2 + X_3 \cdot 3 \pmod{11}.$$

Jei $S \neq 10$, tai $K = S$, jei $S = 10$, tai $K = 0$.

Užduotis. Patikrinkite, ar tikrai jūsų asmens kodas tenkina šias lygybes.

2.5 Kodas $[t^2 + 2t, t^2]$

Grįžkime vėl prie bitų sekos. Tarkime, turime bitų seką, kurią reikia perduoti. Ją skaidome į t^2 ilgio vektorius, kur $t \geqslant 1$ yra sveikasis skaičius — kodo parametras. Surašome į $t \times t$ lentelę. Tada užkoduojame taip: kiekvienai eilutei ir kiekvienam stulpeliui prirašome papildomą bitą tokiu būdu, kad vienetų skaičius kiekvienoje eilutėje ir kiekviename stulpelyje pasidarytų lyginis. Gautą lentelę užrašome vektoriumi-eilute.

Pavyzdys. Pavyzdžiui, $t = 2$ ir $M = (1\ 1\ 0\ 1)$.

1	1	0
0	1	1
1	0	

$C = (1\ 1\ 0\ \ 0\ 1\ 1\ \ 1\ 0)$ □

Bendru atveju vektorius, kurį koduojame turi t^2 simbolių, o C ilgis $t^2 + 2t$. Kodo koeficientas $\frac{t^2}{t^2+2t}$. Pavyzdžiui, kai $t = 2$, tai kodo koeficientas $\frac{4}{8}$.

Dekodavimo algoritmas toks. Iš kanalo gautą vektorių C' surašome į lentelę ir patikriname vienetų skaičių. Jei padaryta viena klaida, tame stulpelyje ir eilutėje, kur padaryta klaida, vienetų skaičius yra nelyginis, taip nustatome, kur padaryta klaida.

Pavyzdys. Jei klaida buvo antroj pozicijoj, pirmoje eilutėje ir antrame stulpelyje vienetų skaičius bus nelyginis:

1	$\boxed{0}$	0
0	1	1
1	0	

□

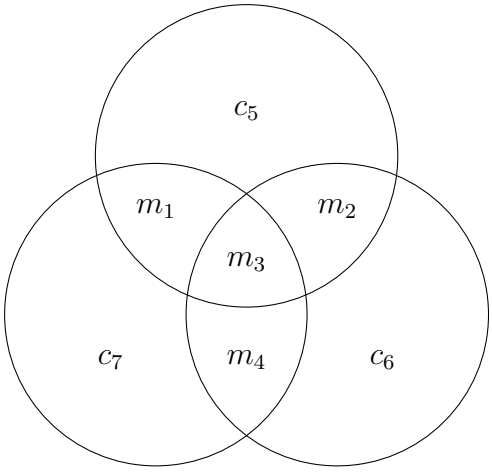
2.2 pastaba. Jei padarytos dvi klaidos, tai dekoduojant tokiu būdu arba dekoduojama neteisingai, arba dekodavimas nėra vienareikšmiškas.

Užduotis. Įrodyti, kad pastaba yra teisinga.

Užduotis. Nustatyti, kiek klaidų toks kodas aptinka.

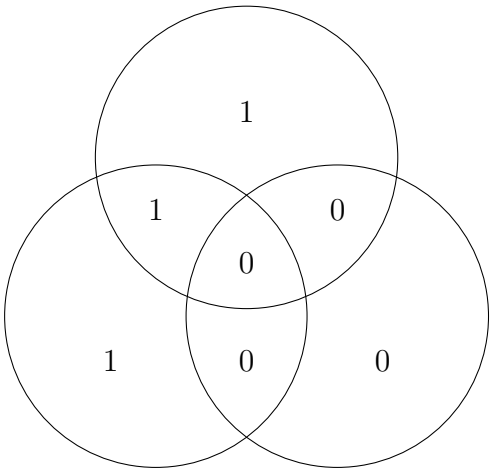
2.6 [7,4] Hemingo (Hamming) kodas

Vėl kalbėsime apie dvinarių vektorių kodavimą. Kodavimą [7,4] Hemingo kodu galima pavaizduoti grafiškai taip.



Informacijos vektorių $m = (m_1, m_2, m_3, m_4)$ užkoduojame vektoriumi $c = (m_1, m_2, m_3, m_4, c_5, c_6, c_7)$, kur c_5, c_6 ir c_7 yra tokie, kad kiekviename skritulyje vienetų skaičius būtų lyginis.

Pavyzdys. Tegu $m = (1, 0, 0, 0)$.



Tada užkoduotas vektorius $c = (1, 0, 0, 0,\ 1, 0, 1)$. □

Dekodavimas. Tarkime, padaryta viena klaida. Tarkime, klaida įvyko pozicijoje, priklausančioje tik vienam skrituliui, pavyzdžiui, klaidinga šešta pozicija, t.y. $c_6 = 1$. Matome, kad tokiu atveju vienetų skaičius nelyginis tik viename apskritime (dešiniajame), todėl nuspręsime, kad klaida padaryta būtent toje vietoje, kuri priklauso dešiniajam apskritimui, bet nepriklauso kitiems apskritimams. Tokia vieta tėra viena, todėl klaidą aptinkame.

Tarkime, kad padaryta klaida pozicijoje, priklausančioje lygiai dviems skrituliams, pavyzdžiui, $m_2 = 1$. Tada vienetų skaičius bus nelyginis dviejuose skrituliuose (viršutiniame ir dešiniajame), todėl nuspręsime, kad klaida įvyko toje vietoje, kuri priklauso tiems dviems skrituliams ir nepriklauso trečiajam. Tokia vieta tėra viena, todėl klaidą galėsime rasti ir ištaisyti.

Taip pat klaidą galėsime ištaisyti ir tuo atveju, jei ji yra pozicijoje, kuri priklauso visiems trims skrituliams ($m_3 = 1$).

Dabar tarkime, kad padarytos dvi klaidos, pavyzdžiui, $c_5 = 0,\ m_4 = 1$. Tada manome, kad reikia taisyti m_3 ir taip padarome dar vieną klaidą.

2.3 teiginys. *Įvykus dviems klaidoms, [7,4] Hemingo kodas, naudojantis šį dekodavimo metodą, visada dekoduos klaidingai.*

Užduotis. Įrodyti teiginį.

Kodo koeficientas $\frac{4}{7}$.

3 Kanalai ir Šenono teorema

3.1 Kanalų modelių pavyzdžiai

Šiame poskyryje susipažinsime su paprasčiausiais naudojamais kanalų modeliais.

3.1 apibrėžimas. Diskretus be atminties kanalas — *tai trejetas* (A, B, Π)*, kur*

- A *yra aibė, vadinama* įėjimo abėcėle*,* $A = \{a_1, \ldots, a_s\}$*,*
- B *yra aibė, vadinama* išėjimo abecėle*,* $B = \{b_1, \ldots, b_t\}$*,*
- $\Pi = \begin{pmatrix} p_{11} & \cdots & p_{1t} \\ \vdots & \ddots & \vdots \\ p_{s1} & \cdots & p_{st} \end{pmatrix}$ *yra* $s \times t$ *matrica, tenkinanti savybes:*

  1) $p_{ij} \geqslant 0$, $\forall\ 1 \leqslant i \leqslant s$, $\forall\ 1 \leqslant j \leqslant t$,

  2) $\sum_{j=1}^{t} p_{ij} = 1$, $\forall\ 1 \leqslant i \leqslant s$.

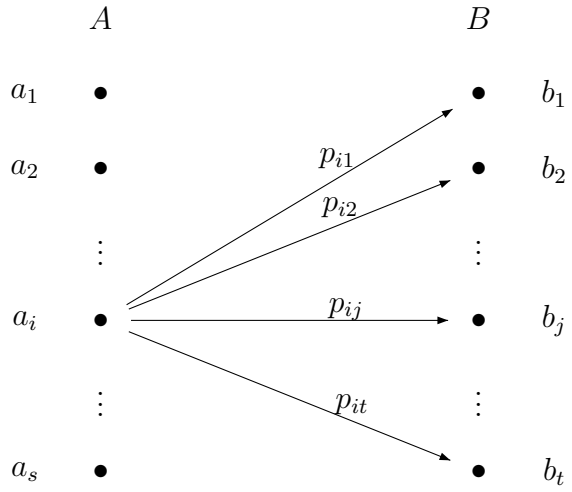
Šias savybes tenkinanti matrica Π vadinama *tikimybine matrica*.

Pastaba. Diskretaus be atminties kanalo apibrėžimas interpretuojamas taip. Laikome, kad kanalu siunčiami simboliai iš įėjimo abėcėlės A, o iš kanalo išėję simboliai priklauso išėjimo abėcėlei B. Dažniausiai laikysime, kad $A = B$.

Matrica Π interpretuojama taip. Siuntėją sutapatiname su atsitiktiniu dydžiu X, įgyjančiu reikšmes iš abėcėlės A, o gavėją su atsitiktiniu dydžiu Y, įgyjančiu reikšmes iš abėcėlės B. Tada matricos elementą p_{ij} interpretuojame kaip tikimybę, kad jei į kanalą pasiųstas simbolis a_i (t.y. jei X įgyja reikšmę a_i), tai iš kanalo išėjo simbolis b_j (t.y. Y įgijo reikšmę b_j), t.y. p_{ij} — tai sąlyginė tikimybė $p_{ij} = P(Y = b_j | X = a_i)$. Trumpiau ją žymėsime $P(b_j|a_i)$ — tikimybė, kad iš kanalo išeis b_j, jei į kanalą įėjo a_i.

Apibrėžime „be atminties“ reiškia, kad Π yra nekintamas dydis (nekinta laikui bėgant). „Diskretus“ reiškia, kad įėjimo ir išėjimo aibės yra diskrečios.

Diskretų be atminties kanalą galima pavaizduoti grafiškai taip:



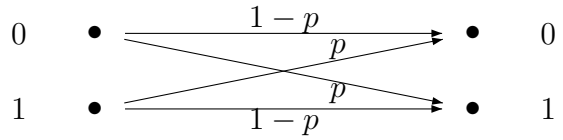
Dabar panagrinėsime kelis diskretaus be atminties kanalo pavyzdžius.

3.2 apibrėžimas. *Tegu* $0 \leqslant p \leqslant 1$. Dvinaris simetrinis kanalas su iškraipymo tikimybe p — *tai diskretus be atminties kanalas, kuriame* $A = B = \{0, 1\}$ *ir*
$P(1|0) = P(0|1) = p$,
$P(0|0) = P(1|1) = 1 - p$.

Iš apibrėžimo matome, kad dvinario simetrinio kanalo tikimybinė matrica yra tokia:

$$\Pi = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}.$$

Dvinarį simetrinį kanalą grafiškai galima pavaizduoti taip:



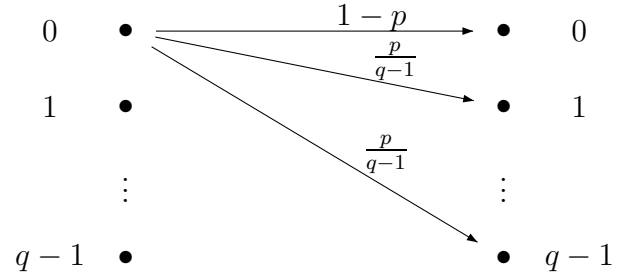
3.3 apibrėžimas. *Tegu* $0 \leqslant p \leqslant 1$, $q \geqslant 2$. q-naris simetrinis kanalas su iškraipymo tikimybe p — *tai diskretus be atminties kanalas, kuriame* $A = B$, $|A| = q$ *ir*

$$P(b|a) = \begin{cases} 1-p & , \textit{jei } a = b; \\ \frac{p}{q-1} & , \textit{jei } a \neq b. \end{cases}$$

Taigi, q-nario simetrinio kanalo tikimybinė matrica yra tokia:

$$\Pi = \begin{pmatrix} 1-p & \frac{p}{q-1} & \frac{p}{q-1} & \cdots & \frac{p}{q-1} \\ \frac{p}{q-1} & 1-p & \frac{p}{q-1} & \cdots & \frac{p}{q-1} \\ \frac{p}{q-1} & \frac{p}{q-1} & 1-p & \cdots & \frac{p}{q-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{p}{q-1} & \frac{p}{q-1} & \frac{p}{q-1} & \cdots & 1-p \end{pmatrix}.$$

Jei $A = \{0, 1, \ldots, q-1\}$, tai q-narį simetrinį kanalą grafiškai galima pavaizduoti taip:



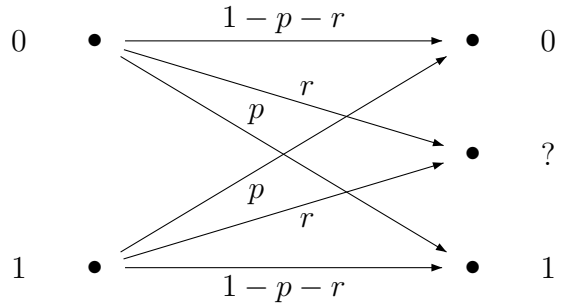
3.4 apibrėžimas. *Tegu* $0 \leqslant p \leqslant 1$, $0 \leqslant r \leqslant 1$. Dvinaris simetrinis trinantis kanalas su iškraipymo tikimybe p ir ištrynimo tikimybe r — *tai diskretus be atminties kanalas, kuriame* $A = \{0, 1\}$, $B = \{0, 1, ?\}$ *ir*
$P(0|0) = P(1|1) = 1 - p - r$,
$P(1|0) = P(0|1) = p$,
$P(?|0) = P(?|1) = r$.

Čia klaustukas žymi tai, kad pasiųstas ženklas išsitrynė. Yra tik žinoma, kad toje vietoje buvo kažkoks ženklas, o kuris — ar nulis, ar vienetas, — neaišku.

Dvinario simetrinio trinančio kanalo tikimybinė matrica yra tokia:

$$\Pi = \begin{pmatrix} 1-p-r & p & r \\ p & 1-p-r & r \end{pmatrix}.$$

Dvinarį simetrinį trinantį kanalą grafiškai galima pavaizduoti taip:



3.2 Adityvus kanalas

Kartais naudinga mokėti elementus sudėti, atimti, o ir neutralus elementas — nulis — būna ne pro šalį. Tam mes aprūpinkime kanalo abėcėles Abelio grupės struktūra.

3.5 apibrėžimas. *Kanalą vadinsime* adityviu*, jei $A = B$ ir A — baigtinė Abelio grupė sudėties atžvilgiu, t.y. $\forall a, b, c \in A$:*

$a + b \in A$,
$a + b = b + a$,
$(a + b) + c = a + (b + c)$,
$\exists\ 0 \in A:\ a + 0 = 0 + a = a$,
$\exists (-a):\ a + (-a) = 0$.

Nuo šiol laikysime, kad kanalas adityvus.

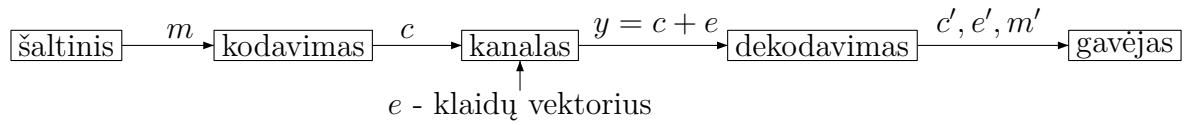
3.6 apibrėžimas. *Tarkime, į adityvų kanalą įeina vektorius $x \in A^n$, o išeina vektorius $y \in A^n$. Tada vektorių $e = y - x$ vadinsime* klaidų vektoriumi. Klaidų padėtimis *vadinsime klaidų vektoriaus nenulinių koordinačių pozicijas.* Klaidų reikšmės *yra klaidų vektoriaus koordinatės.*

Pavyzdys. Tarkime, adityvaus trinario kanalo abėcėlė yra $A = \{0, 1, 2\}$, kur veiksmai atliekami moduliu 3. Tarkime, kad į kanalą įeina vektorius $x = 12010$, o išeina vektorius $y = 10210$. Tada klaidų vektorius yra $e = y - x = 01200$, klaidų pozicijos yra 2 ir 3, o klaidų reikšmės yra tokios: pirmoje pozicijoje įvykusios klaidos reikšmė yra 0 (klaidos nebuvo), antroje — 1, trečioje — 2 ir t. t. Paprastai nulinės klaidų reikšmės nevardijamos, todėl užtenka pasakyti, kad antroje pozicijoje įvykusios klaidos reikšmė yra 1, o trečioje — 2. □

Tarkime, į adityvų kanalą įeina vektorius $x \in A^n$, o išeina vektorius $y \in A^n$. Pagal klaidų vektoriaus e apibrėžimą, $e = y - x$, todėl $y = x + e$. Taigi, adityvaus kanalo atliekamus iškraipymus matematiškai galima užrašyti taip: prie į kanalą pasiųsto vektoriaus x pridedamas klaidų vektorius e, ir iš kanalo išeina rezultatas $y = x + e$.

3.3 Šenono teorema

Prisiminkime, kad kodavimas vyksta pagal tokią schemą:



Norimą perduoti informaciją verčiame k ilgio vektoriais iš abėcėlės A simbolių. Kiekvieną tokį vektorių m užkoduojame, pridėdami papildomų simbolių — gauname n ilgio užkoduotą vektorių c. Jį siunčiame kanalu, kur galimi iškraipymai. Iš kanalo išeina n ilgio vektorius $y = c + e$. Dekoduojant paprastai randami 3 dydžiai: klaidų vektorius e', pataisyti užkoduotas vektorius c' ir pradinis pranešimas m'.

Taigi, norėdami perduoti k informacijos simbolių, iš tikro perduodame n simbolių. Santykį k/n vadiname *kodo koeficientu*. Kuo daugiau koduodami pridedame papildomų simbolių, t.y. kuo kodo koeficientas mažesnis, tuo labiau galime sumažinti klaidingo dekodavimo tikimybę, bet tuo pačiu tuo labiau apkrauname kanalą (reikia persiųsti daugiau simbolių). Taigi, norime sumažinti tą tikimybę, tuo pačiu išlaikydami kodo koeficientą pakankamai aukštą. 1948 m. Šenonas (Shannon) įrodė, kad kiekvienam diskrečiam be atminties kanalui egzistuoja tokia konstanta C, vadinama *kanalo talpa*, kad:

1. $\forall \varepsilon > 0$ ir $\forall R < C$ egzistuoja tokios kodavimo ir dekodavimo taisyklės, kad kodo koeficientas $\frac{k}{n} \geqslant R$ ir dekodavimo klaidos tikimybė yra mažesnė už ε;

2. Tegu $R > C$, tada $\exists \varepsilon > 0$ toks, kad kokias bepaimtume kodavimo ir dekodavimo taisykles, kurių kodo koeficientas $\frac{k}{n} \geqslant R$, dekodavimo klaidos tikimybė bus nemažesnė už ε.

Šenono teorema rodo, kad klaidingo dekodavimo tikimybę galime padaryti kiek norime mažą, tuo pačiu išlaikydami kodo koeficientą gana aukštą — artimą kanalo talpai.

Deja, šios teoremos įrodymas nėra konstruktyvus, jis neparodo, kaip sudaryti tuos „gerus“ kodus. Juos gauti ir yra klaidas taisančių kodų teorijos tikslas.