

Kodavimo teorija. A5 užduoties realizacijos ataskaita

1. Realizuotos užduoties dalys:

- 1.1. Realizuotas pirmasis scenarijus: Vartotojas užrašo programos nurodyto ilgio vektorių iš kūno F_q elementų. Programa patikrina, ar vektoriaus ilgis korektiškas (išimtis: jei naudojamas sąsūkos kodas, pranešimo ilgis gali būti bet koks, todėl tuo atveju programa neturi nurodyti ilgio ir tikrinti jo korektiškumo), jį užkoduoja kodu C, parodo užkoduotą vektorių, siunčia jį kanalu, parodo iš kanalo išėjusį vektorių, praneša, kiek ir kuriose pozicijose įvyko klaidų, dekoduoja gautą vektorių ir parodo rezultatą. Vartotojas turi turėti galimybę prieš dekodavimą redaguoti iš kanalo išėjusį vektorių, kad galėtų pats nurodyti klaidas ten, kur jam reikia, ir tiek, kiek reikia.
- 1.2. Nerealizuotas antrasis ir trečiasis scenarijai.

2. Trečiųjų šalių funkcijų bibliotekos

Trečiųjų šalių funkcijų bibliotekos nebuvo naudojamos. Buvo naudojama tik standartiniai python bibliotekų moduliai tokie kaip “**random**” skirtas generuoti atsitiktinius skaičius. Grafinei vartotojo sąsajai buvo naudota “**Tkinter**” biblioteka.

3. Programos paleidimas

Programą paleisti galima pagrindinėje direktorijoje esančiame “**main.exe**” faile. Failo paleidimas nereikalauja išankstinės Python aplinkos sukonfigūravimo.

4. Programos failai:

Failo vieta/pavadinimas:	Failo turinys ir paskirtis:
encoder.py	Užkoduojama pradinė žinutė pagal Rydo-Miulerio kodą $RM(1, m)$. Realizuota generatoriaus matricos kūrimo logika.
channel.py	Realizuotas vektoriaus siuntimas kanalu, įvedant klaidas pagal nustatytą tikimybę
decoder.py	Dekoduojama gauta žinutė, naudojant greitąją Hadamardo transformaciją, klaidos pozicijos nustatomos ir žinutė atkuriamą.

main.py	Realizuojama GUI su trimis puslapiais: parametrų įvedimas, pranešimo užkodavimas ir siuntimas, bei rezultatų peržiūra.
---------	--

5. Vartotojo sąsajos aprašymas

5.1. Pradinis puslapis (HomePage)

Pradiniame puslapyje vartotojas įveda pagrindinius parametrus:

m – natūralusis skaičius, kuris nurodo Rydo-Miulerio kodo parametą. Leidžiama įvesti tik natūraliuosius skaičius, ($m > 0$).

p – reikšmė, kuri nurodo klaidos tikimybę siunčiant pranešimą per kanalą. Galima įvesti bet kokį realų skaičių tarp ($0 \leq p \leq 1$).

Suvedę m ir p , spaudžiame mygtuką „Toliau“, kad pereitumėme į sekantį vartotojo sąsajos langą, kuris skirtas pranešimo įvedimui.

5.2. Pranešimo įvedimo langas (InputMessagePage)

Pranešimo įvedimo lange vartotojas įveda žinutę, kurią nori užkoduoti ir siunčia ją per kanalą.

Teksto lauke galima įvesti tik dvejetaines reikšmes (0 ir 1), nes programos baigtinis kūnas $q=2$.

Pranešimas turi būti ilgio $m + 1$ (pagal ankstesniame puslapyje įvestą m). Jeigu įvedamas netinkamo ilgio pranešimas, vartotojui išvedama klaida ir prašoma įvesti pranešimą iš naujo.

Suvedus pranešimą, spaudžiant mygtuką „Encode“, užkoduojama įvesta žinutė naudojant Rydo-Miulerio kodą. Užkoduotos žinutės ilgis yra 2^m . Užkoduota žinutė yra išvedama vartotojui programoje. Užkoduotą žinutę galima siųsti kanalu paspaudus mygtuką „Send“.

5.3. Rezultatų peržiūra (ResultPage)

Rezultatų peržiūros puslapyje vartotojas gali peržiūrėti siųstos žinutės kanalu rezultatus, žinutėje padarytų klaidų pozicijas, redaguoti kanalu siųstos žinutės reikšmę ir ją dekoduoti.

Pačiame viršuje yra parodoma kanalo žinutė, kuri buvo gauta iš kanalo. Klaidos parodo klaidų skaičių ir jų pozicijas. Spaudžiant mygtuką „Edit“, galima vartotojui rankiniu būdu redaguoti kanalo žinutę įvedant naują bitų seką atitinkamo ilgio. „Decode“ mygtukas atlieka esamos kanalo žinutės dekodavimą naudojant greitąją Hadamardo transformaciją, rezultatas išvedamas vartotojui po Dekoduota žinutė tekstu. Galiausiai, paskutinis „Home“ mygtukas leidžia vartotojui grįžti į pradinį programos puslapį bei pradėti viską iš naujo pradiniame puslapyje.

6. Programiniai sprendimai

6.1. Pradinio teksto pavertimas vektoriais

Tekstas neapdorojamas tiesiogiai, o vartotojas įveda dvejetainį pranešimą kaip eilutę (0 ir 1 bitų forma). Jei vartotojas įveda neteisingo formato pranešimą (pvz., naudodamas simbolius, kurie nėra 0 ar 1) arba žinutės ilgis neatitinka reikalavimų, sistema iš karto rodo klaidos pranešimą. Jei įvestis būtų per trumpa, palyginti su reikalavimu, programa pateikia klaidą ir neleidžia tęsti užkodavimo proceso.

6.2. Kodavimas

Kodavimo procesas prasideda nuo RM kodo generatoriaus matricos kūrimo taikant rekursinį algoritmą, kuris sudeda matricas horizontaliai ir vertikaliai, kol gaunama pilna $RM(1, m)$ matrica. Užkoduotas vektorius apskaičiuojamas dauginant generatoriaus matricą su pradinio pranešimo vektoriumi, kur kiekvienas rezultato elementas yra apskaičiuojamas kaip reikšmių suma mod 2.

6.3. Vektorių siuntimas kanalu

Tekstas yra verčiamas į bitų seką ir siunčiamas kanalu, kur kiekvienam elementui taikoma klaidos tikimybė p_e . Kanalas tikrina kiekvieną bitą sugeneruojant atsitiktinę reikšmę iš intervalo $[0, 1]$. Jei ši reikšmė yra mažesnė už p , bitas yra iškraipomas - 1 pakeičiamas į 0 arba 0 į 1. Jei atsitiktinė reikšmė didesnė arba lygi p , bitas išlieka nepakitęs. Pranešimo vektorius siunčiamas elementas po elemento, kiekvieną iš jų atskirai tikrinant ir prireikus modifikuojant, o modifikuotas vektorius grąžinamas kaip kanalo išvestis.

6.4. Dekodavimas

Dekodavimas – gavus pranešimą iš kanalo, kiekvienas jo elementas paverčiamas į signalinę reikšmę: 0 pakeičiamas į -1, o 1 paliekamas nepakitęs. Naudojant Rydo-Miulerio kodo Hadamardo matricą, iteratyviai atliekama greitoji Hadamardo transformacija, kuri apskaičiuoja galimus pranešimo rekonstrukcijos koeficientus. Transformacijos rezultatas analizuojamas siekiant nustatyti didžiausios absoliučios reikšmės poziciją. Ši pozicija atitinka užkoduotą pradinį pranešimą, kuris paverčiamas į dvejetainę reikšmę, atkuriant pradinę žinutę. Jei didžiausios reikšmės pozicijos reikšmė teigiama, pridedamas papildomas bitas 1, jei neigiama – bitas 0.

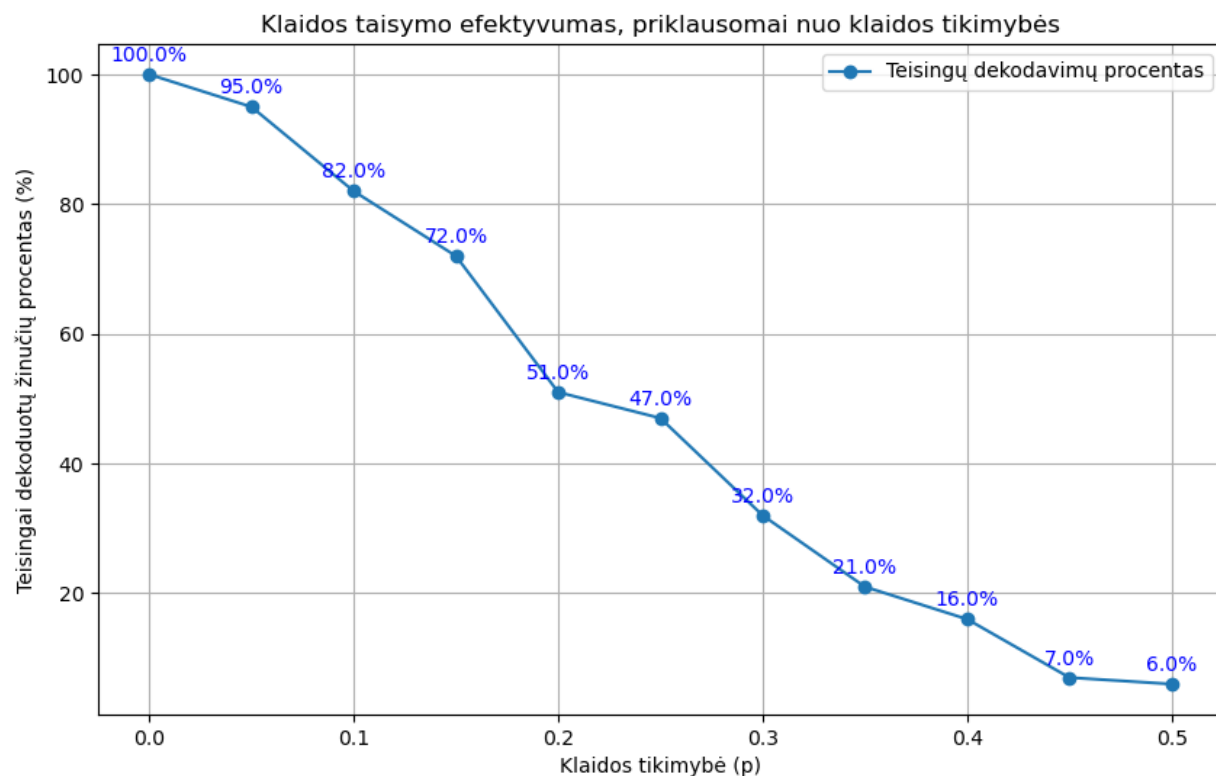
7. Eksperimentai

Buvo atliktas pirmasis eksperimentas siekiant įvertinti kaip klaidos tikimybė p siunčiant užkoduotą pranešimą per kanalą veikia Rydo-Miulerio kodo $RM(1, m)$ klaidų taisymo efektyvumą. Nustatyta kiek pranešimų sėkmingai dekoduojami be klaidų esant skirtingos klaidos tikimybėms.

- Eksperimento metu buvo naudojamas $RM(1, 3)$ kodas, o vektorius buvo $2^m = 8$ bitų, pradinė žinutė 4 bitus ($m+1$).
- Klaidos tikimybė p buvo imama nuo 0 iki 0.5 su 0.05 žingsniu, o kiekvienai klaidos tikimybei atlikta 50 bandymų.

Kiekvienos iteracijos metu atsitiktinai buvo generuota pradinė pranešimo žinutė, ji užkoduota kodu RM(1,3), siųsta kanalu su klaidos tikimybe kur kiekvienas bitas iškraipomas jei atsitiktinis skaičius mažesnis už p . Galiausiai, žinutė buvo dekoduoja naudojant greitąją Hadamardo transformaciją ir lyginome dekoduoatą žinutę su pradine. Jei jos sutampa, dekodavimas buvo laikomas teisingu. Galiausiai, kiekvienai klaidos tikimybei buvo skaičiuojama teisingai dekoduoatų pranešimų kiekis ir jų procentali dalis.

Klaidos tikimybė p	Teisingų dekodavimų skaičius
0.0	50
0.05	47
0.1	41
0.15	36
0.2	25
0,25	23
0.3	16
0.35	10
0.4	8
0.45	4
0.5	3



Žvelgiant į lentelės ir grafiko rezultatus, galime matyti, mažėjant p nuo 0.05 iki 0.5 klaidų taisymo efektyvumas palaipsniui mažėja iki kol teisingai dekoduojamų žinučių procentas jau tampa mažesnis nei 10% kai p yra 0.45 ir 0.5.

Antrajame eksperimente buvo analizuojama kaip dekodavimo laikas priklauso nuo RM kodo parametro m . Eksperimentas imituoja duomenų užkodavimą, jų siuntimą per klaidų turintį kanalą (klaidos tikimybė $p=0.25$) ir vėlesnį dekodavimą. Pagrindinis tikslas – įvertinti vidutinį dekodavimo laiką skirtingoms m reikšmėms ir atvaizduoti rezultatus grafike. Iteracijoms pasirinkta buvo m reikšmės nuo 2 iki 12, o vidutinis dekodavimo laikas buvo apskaičiuotas bandant imituoti dekodavimą 5 kartus su tuo pačiu m .

<i>m</i>	Vidutinis dekodavimo laikas (s)
2	0.0018
3	0.0025
4	0.0047
5	0.0118
6	0.0422
7	0.0767
8	0.2243
9	0.7662
10	3.3178
11	13.7999
12	58.8082



Tiek iš lentelės ir grafiko duomenų galima matyti, kad mažoms m reikšmėms tarp 2 ir 6 imtinai, vidutinis dekodavimo laikas yra mažas ir beveik pastovus, tačiau nuo $m = 8$, pradeda ryškiai augti.

Eksperimentas parodo, kad RM kodo dekodavimo laikas stipriai priklauso nuo parametro m , o skirtumas labiausiai pasimato imant didesnes reikšmes m .

8. Literatūra

- D.G.Hoffman, D.A.Leonard, C.C.Lindner, K.T.Phelps, C.A.Rodger, J.R.Wall. Coding Theory: The Essentials. Dekker, New York, 1991.
(<https://klevas.mif.vu.lt/~skersys/doc/ktkt/literatura13.pdf>)