# Praktinis darbas

## Kodavimo teorija, 2013/14 m.m. rudens sem.

|  |  |
| --- | --- |
| **Atliko:** | Jonas Inčius |
| **Pradėtas:** | 2012-09-10 |
| **Baigtas:** | 2012-09-15 |
| **Sugaišta:** | 16 h |

## Uždavinio formulavimas

B1. Duotas tiesinis kodas C[n,k] virš Fq. Apskaičiuoti jo svorių skirstinį:

* Tiesioginio perrinkimo būdu,
* apskaičiuoti dualaus kodo svorių skirstinį tiesioginio perrinkimo būdu ir panaudoti MacWilliams tapatybę.

## Programa

Programa pateikiama faile Coding.exe. Ji reikalauja vieno komandinės eilutės parametro, kuriuo nurodomas duomenų failas. Paleidimo pavyzdys: Coding.exe input.txt

Papildomai pridėtas komandinis failas uzd.bat, kuris paleidžia programą su iš anksto nustatytu duomenų failu input.txt.

Rezultatas (svorių skirstinys) išvedamas ekrane.

## Duomenų failo struktūra

Duomenų failo pirmą eilutę sudaro keturi skaičiai atskirti tarpais:

* Skaičiavimo būdas. 0 – tiesioginio perrinkimo, 1 – skaičiuoti dualaus kodo skirstinį tiesioginio perrinkimo būdu ir panaudoti MacWilliams tapatybę.
* Baigtinio kūno elementų skaičius q.
* Tiesinio kodo ilgis n.
* Tiesinio kodo dimensija k.

Sekančiose eilutėse išdėstoma generuojanti matrica. Generuojančios matricos elementus skiria kableliai. Kiekviena matricos eilutė užrašoma į naują failo eilutę. Jeigu q nėra pirminis, tada baigtinio kūno elementai užrašomi polinomais, kurie atvaizduojami išvardinant koeficientus juos atskiriant tarpais. Atskyrimas tarpais reikalingas, nes koeficientai gali viršyti 10.

Pvz: 1 + 2x^2 + 2x^2 duomenų faile bus užrašomas: 1 0 2 2.

Pastaba. Nenurodžius generuojančios matricos, arba ją nurodžius neteisingai, ji bus sugeneruota atsitiktinai.

## Duomenų failo pavyzdys

1 5 12 5

1,0,0,0,2,3,0,1,4,3,0,1

0,1,0,0,1,3,0,1,3,1,4,4

0,0,1,0,1,2,0,1,2,0,2,0

0,0,0,1,1,1,0,0,0,1,1,3

0,0,0,0,0,0,1,1,1,1,1,1

Paaiškinimas:

Programa vykdoma MacWilliams būdu, nes pirmasis skaičius 1. Baigtinį kūną sudaro 5 elementai. Kodo ilgis 12, dimensija 5.

## Programiniai sprendimai

Polinomai modeliuojami std::vector<int> pagalba. Vektoriuje saugomi koeficientai. Indeksas vektoriuje atitinka prie kokio laipsnio kintamojo yra koeficientas.

Baigtinio kūno elementai modeliuojami polinomais. Net ir pirminių kūnų, šitaip tas pats kodas veikia visais variantais.

Baigtinių laukų polinomai paimti iš čia <http://uosis.mif.vu.lt/~skersys/doc/ktkt/prim_pol.pdf>. Įkoduoti tiesiai į programą. Sudaroma maišos lentelė std::map<std::pair<int, int>, Polynomial >, kur pagal baigtinio kūno elementų skaičių randamas jį atitinkantis polinomas. Programa gali veikti su bet kuriuo polinomu, tačiau kode apibrėžti tik polinomai iš pateikto sąrašo.

Baigtiniai kūnai gali turėti tiek pirminius, tiek nepirminius pagrindus. Programa abiem atvejais dirba vienodai. Ji pasiima pagrindą ir jį išskaito į jo pirminę dalį ir laipsnį, kuriuo ši pakelta. Esant pirminiam pagrindui tas laipsnis tiesiog vienetas.

Atsitiktinai sudarant generuojančią matricą, ji iškart sudaroma laiptuotų pavidalu, kad nereikėtų rūpintis ar ji tiesiškai nepriklausoma.

## Testavimo aprašymas:

**Duomenys**

0 8 20 5

1 0 0,0 0 0,0 0 0,0 0 0,0 0 0,0 1 1,0 0 1,1 0 0,0 1 1,0 0 0,0 0 1,0 1 0,1 1 1,1 0 0,1 0 0,1 0 1,0 0 1,1 1 1,0 1 1,0 1 1

0 0 0,1 0 0,0 0 0,0 0 0,0 0 0,0 1 0,0 0 1,0 1 1,0 0 0,0 1 1,1 0 1,1 1 0,1 1 1,1 0 0,0 0 1,1 1 0,0 1 1,1 0 1,1 1 0,0 0 1

0 0 0,0 0 0,1 0 0,0 0 0,0 0 0,0 1 0,0 1 0,0 0 0,1 1 0,0 1 0,1 0 0,1 1 0,1 1 1,0 0 1,1 0 1,0 0 1,1 1 0,0 0 1,0 1 0,1 1 1

0 0 0,0 0 0,0 0 0,1 0 0,0 0 0,1 0 0,0 0 0,1 1 0,1 0 0,0 1 0,1 0 0,1 1 0,0 1 1,1 0 1,1 0 0,0 1 0,1 1 1,1 1 0,1 0 1,0 1 0

0 0 0,0 0 0,0 0 0,0 0 0,1 0 0,0 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0,1 0 0

**Rezultatai**

Tiesinis perrinkimas. Baigtinis kūnas iš 8 elementų. Kodo ilgis 20, dimensija 5

w[0] = 1 w[1] = 0 w[2] = 0 w[3] = 0 w[4] = 0 w[5] = 0 w[6] = 0

w[7] = 0 w[8] = 0 w[9] = 0 w[10] = 0 w[11] = 0 w[12] = 35 w[13] = 147

w[14] = 910 w[15] = 2086 w[16] = 4536 w[17] = 7511 w[18] = 8764 w[19] = 6496 w[20] = 2282

**Duomenys**

1 5 12 5

1,0,0,0,2,3,0,1,4,3,0,1

0,1,0,0,1,3,0,1,3,1,4,4

0,0,1,0,1,2,0,1,2,0,2,0

0,0,0,1,1,1,0,0,0,1,1,3

0,0,0,0,0,0,1,1,1,1,1,1

**Rezultatai**

MacWilliams tapatybė. Baigtinis kūnas iš 5 elementų. Kodo ilgis 12, dimensija 5

w[0] = 1 w[1] = 0 w[2] = 0 w[3] = 0 w[4] = 0 w[5] = 0 w[6] = 20

w[7] = 244 w[8] = 460 w[9] = 600 w[10] = 884 w[11] = 740 w[12] = 176

**Duomenys**

0 2 38 12

1,1,1,1,0,0,1,0,1,0,0,0,0,1,1,1,1,1,0,1,1,0,1,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0

0,0,0,1,1,0,1,1,1,0,0,1,1,0,1,1,0,0,1,1,0,1,1,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0

1,1,0,1,0,1,1,1,1,1,0,1,1,0,0,0,1,1,0,0,0,0,0,1,1,1,0,0,1,0,0,0,0,0,0,0,0,0

0,1,0,1,1,0,0,1,1,1,1,1,0,1,0,0,1,0,1,1,1,0,1,0,1,0,0,0,0,1,0,0,0,0,0,0,0,0

0,0,1,0,1,1,0,0,1,1,1,1,0,0,0,1,1,1,0,1,1,1,0,1,0,1,0,0,0,0,1,0,0,0,0,0,0,0

1,0,1,1,0,1,0,0,0,0,1,1,1,1,1,0,1,0,1,1,0,1,0,0,1,1,0,0,0,0,0,1,0,0,0,0,0,0

1,0,0,0,1,0,0,1,0,1,0,1,1,0,0,0,0,1,1,1,0,0,1,1,1,0,0,0,0,0,0,0,1,0,0,0,0,0

0,0,1,0,1,1,1,1,0,1,1,0,1,1,0,0,1,0,1,1,1,1,0,1,1,0,0,0,0,0,0,0,0,1,0,0,0,0

0,1,1,1,1,1,0,1,0,0,0,1,0,0,0,0,1,0,0,0,1,1,0,0,1,1,0,0,0,0,0,0,0,0,1,0,0,0

1,0,0,1,0,0,0,1,1,1,1,1,1,1,0,1,1,1,0,1,0,1,1,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0

0,1,1,0,1,0,0,0,1,0,0,0,1,1,1,0,0,1,1,0,0,0,1,1,0,1,0,0,0,0,0,0,0,0,0,0,1,0

1,0,1,0,1,0,1,0,0,1,0,1,1,0,1,1,1,0,0,1,1,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,0,1

**Rezultatai**

Tiesinis perrinkimas. Baigtinis kūnas iš 2 elementų. Kodo ilgis 38, dimensija 12

w[0] = 1 w[1] = 0 w[2] = 0 w[3] = 0 w[4] = 0 w[5] = 0 w[6] = 0

w[7] = 0 w[8] = 0 w[9] = 0 w[10] = 0 w[11] = 0 w[12] = 0 w[13] = 112

w[14] = 244 w[15] = 320 w[16] = 302 w[17] = 224 w[18] = 480 w[19] = 640 w[20] = 480

w[21] = 384 w[22] = 296 w[23] = 320 w[24] = 240 w[25] = 32 w[26] = 0 w[27] = 0

w[28] = 0 w[29] = 16 w[30] = 4 w[31] = 0 w[32] = 1 w[33] = 0 w[34] = 0

w[35] = 0 w[36] = 0 w[37] = 0 w[38] = 0

## Kodo failai

Coding\FiniteField.h  
Coding\FiniteField.cpp – Modeliuoja baigtinį kūną. Apibrėžia veiksmus tarp kūno elementų.

Coding\LinearCode.h  
Coding\LinearCode.cpp – Modeliuoja tiesinį kodą. Iš generuojančios matricos leidžia sukonstruoti kodą, bei svorių skirstinį dviem skirtingais būdais.

Coding\Polynomial.h  
Coding\Polynomial.cpp – Modeliuoja polinomą. Iš tiesų tėra std::vector<int> ‚wrapperis‘. Apibrėžia veiksmus tarp polinomų.

Coding\Util.h  
Coding\Util.cpp – Įgyvendintos kelios matematinės ir eilučių operacijos.

Coding\WordMatrix.h  
Coding\WordMatrix.cpp – Modeliuoja matricą sudarytą iš baigtinio kūno elementų. Apibrėžia veiksmus reikalingus matricos privedimui iki standartinio pavidalo.

Coding\main.cpp – Pagrindinis programos failas, kuriame atliekami pradiniai veiksmai, nuskaitomi duomenys, bei išvedami rezultatai.

# Literatūros sąrašas

<http://en.wikipedia.org/wiki/Linear_code>

<http://en.wikipedia.org/wiki/Finite_field>

<http://www.mathi.uni-heidelberg.de/~yves/Matritzen/Codes/CodeMatIndex.html>

<http://www.maths.manchester.ac.uk/~pas/code/notes/part6.pdf>

[V. Stakėnas. Kodai ir šifrai. Vilnius, 2007.](http://www.mif.vu.lt/lmd/kodai_sifrai.pdf)