Daugianarių kodai

2010 m. ruduo

Žodžiai ir daugianariai

$\mathbb{F}_q$ žymėsime kūną iš $q = p^m$ elementų, čia p – pirminis skaičius (dažnai imsime tiesiog $q = p$). Daugianarių tiesinės erdvės

$$\begin{aligned} \mathbb{F}_q[x] &= \{a_0 + a_1x + \ldots + a_mx^m : a_i \in \mathbb{F}_q, a_m \neq 0\}, \\ \mathbb{F}_{q,n}[x] &= \{f \in \mathbb{F}_q[x] : \deg(f) < n\}. \end{aligned}$$

Tiesinės erdvės $\mathbb{F}_q^n$ ir $\mathbb{F}_{q,n}[x]$ yra izomorfiškos:

$$\mathbf{a} \in \mathbb{F}_q^n,\ \mathbf{a} = a_0a_1\ldots a_{n-1} \mapsto a_0 + a_1x + \ldots + a_{n-1}x^{n-1} \in \mathbb{F}_{q,n}[x].$$

2 / 33

Daugianario svoris

Apibrėžimas. Daugianario $g(x) \in \mathbb{F}_q[x]$ svoriu vadinsime jo nenulinių koeficientų skaičių. Svorį žymėsime $w(g)$.

Jeigu apsiribojame tik sudėties bei daugybos iš kūno elementų veiksmais, tai visai tas pats, ar juos taikome žodžiams, ar daugianariams. Tačiau daugianarius dar galime ir dauginti!

3 / 33

Daugianarių kodas

Apibrėžimas. Tegu $g(x) = g_0 + g_1x + \ldots + g_kx^k$ yra daugianaris iš $\mathbb{F}_q[x],\ 0 \leq k < n,\ g_k \neq 0$. Aibę

$$\mathbb{C}_{g,n} = \{a(x)g(x) : a(x) \in \mathbb{F}_{q,n-k}[x]\} \subset \mathbb{F}_{q,n}[x]$$

vadinsime daugianarių kodu, generuotu $g(x)$.

Daugianario $g(x)$ generuotas kodas – šio daugianario kartotinių, kurių laipsnis ne didesnis kaip n, aibė. Dydį n galime pasirinkti, taigi su tuo pačiu daugianariu galime generuoti įvairius kodus.

4 / 33

Daugianarių kodas

Teorema. Daugianarių kodas $\mathbb{C}_{g,n}$, kurį generuoja k-ojo laipsnio daugianaris g, yra tiesinis kodas. Daugianariai

$$g(x),\ xg(x),\ \ldots,\ x^{n-k-1}g(x)$$

sudaro šio kodo bazę.

Išvada. *Daugianario* $g,\ \deg(g) = k$, *generuoto kodo* $\mathbb{C}_{g,n}$ *parametrai yra* $[n, n-k]$.

Generuojanti matrica

Interpretuodami kodo $\mathbb{C}_{g,n}$ elementus kaip žodžius, sudarytus iš daugianarių koeficientų, galime pagal bazę sudaryti generuojančią kodo matricą:

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_k & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_k & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & g_0 & \ldots & g_k \end{pmatrix}.$$

Sisteminis kodavimas

Teorema. Tegu g yra k-ojo laipsnio daugianaris, o $r_j(x)$ yra daugianario x^j dalybos iš $g(x)$ liekana. Tada daugianariai

$$x^k - r_k(x),\ x^{k+1} - r_{k+1}(x), \ldots, x^{n-1} - r_{n-1}(x)$$

sudaro $g(x)$ generuoto kodo $\mathbb{C}_{g,n}$ bazę.

Golay kodas

Prisiminkime, kaip sudarėme generuojančią Golay kodo $\mathbf{G}_{23}$ matricą: į pirmąją eilutę surašėme žodžio

$$\mathbb{C}_1 = 11000111010100000000000$$

simbolius, o į kitas – žodžius, gautus iš $\mathbb{C}_0$ cikliškais postūmiais. Tokią pačią generuojančią matricą turi daugianario

$$g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$$

generuotas 23 bitų ilgio žodžių kodas. Taigi Golay kodas $\mathbf{G}_{23}$ yra daugianarių kodas.

8 / 33

Tiesiniai kodai ir daugianarių kodai - ne tas pats

Nagrinėkime tiesinį kodą $\mathbb{L} = \{000, 010, 101, 111\}$. Pakeitę žodžius daugianariais, gautume $\mathbb{L} = \{0, x, 1 + x^2, 1 + x + x^2\} \subset \mathbb{F}_{2,3}[x]$.
Yra tik vienas daugianaris, kuris dalija visus $\mathbb{L}$ daugianarius: $g(x) = 1$.
Tačiau $\mathbb{C}_{g,3} \neq \mathbb{L}$.

9 / 33

Kodavimas ir dekodavimas

Kodavimas daugianario kodo žodžiais yra daugianarių daugyba. Iš tiesų:

$$a_0 a_1 \ldots a_{n-k-1} \mapsto a_0 + a_1 x + \ldots + a_{n-k-1} x^{n-k-1} = a(x)$$
$$a(x) \mapsto a(x) g(x) \in \mathbb{C}_{g,n}.$$

O dekodavimas – galbūt daugianarių dalyba?

10 / 33

Daugianarių sluoksniai

Kiekvienam daugianariui $a(x) \in \mathbb{F}_{q,n}[x]$ galime sudaryti jo „sluoksnį“:

$$\mathbb{L}_a = \{a(x) + c(x) : c(x) \in \mathbb{C}_{g,n}\}.$$

Kiekvienas sluoksnis turi po q^{n-k} elementų. Skirtingus daugianarius $a(x), b(x)$ atitinkantys sluoksniai arba sutampa, arba nesikerta. Taigi visą daugianarių erdvę $\mathbb{F}_{q,n}[x]$ galima išskaidyti į nesikertančių sluoksnių

$$\mathbb{L}_1,\ \mathbb{L}_2,\ \ldots,\ \mathbb{L}_{q^k},\ \mathbb{L}_1 = \mathbb{C}_{g,n},$$

sąjungą.

Dekodavimas

Vieno sluoksnio atstovų dalybos iš $g(x)$ liekanos sutampa. Vadinasi, pagal gautojo iš kanalo iškraipyto žodžio

$$d(x) = c(x) + e(x),\ c(x) \in \mathbb{C}_{g,n},$$

dalybos iš $g(x)$ liekaną galime nustatyti, į kurią klasę žodis pateko. Ši dalybos liekana daugianario kodo atveju atlieka sindromo vaidmenį. Suradę šios klasės lyderį $e(x)$ – mažiausią svorį turintį jos elementą – gautąjį žodį dekoduojame taip:

$$d(x) \mapsto d(x) - e(x).$$

Minimalus atstumas

Teorema. Jei daugianaris $g(x) \in \mathbb{F}_2[x]$ su nenuliniu laisvuoju nariu nedalija jokio daugianario $x^k + 1$, kur $k < n$, tai $g(x)$ generuoto kodo iš n ilgio žodžių minimalus atstumas ne mažesnis už 3.

Pavyzdys

Tegu $g(x) = 1 + x + x^3 \in \mathbb{F}_2[x]$.
Pasirėmę akivaizdžiomis lygybėmis (jos teisingos tik kūne $\mathbb{F}_2$!):

$$x^4 + 1 = (x+1)^4, \quad x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1),$$

matome, kad $g(x) = 1 + x + x^3$ nedalija nei $x^4 + 1$, nei $x^5 + 1$. Taigi $g(x)$ generuoja $[6, 3]$ kodą, visada ištaisantį vieną klaidą.

14 / 33

Daugianarių žiedai ir idealai

15 / 33

Daugianarių daugyba

Pasirinkime kokį nors n-ojo laipsnio daugianarį

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad a_i \in \mathbb{F}_q.$$

Dalydami kitus daugianarius $g \in \mathbb{F}_q[x]$ iš f, gausime liekanas. Šių liekanų aibė sutampa su nedidesnio kaip $n-1$-ojo laipsnio daugianarių aibe $\mathbb{F}_{q,n}[x]$.

16 / 33

Daugianarių žiedas

Jeigu sudėsime dvi dalybos iš f liekanas – vėl gausime liekaną, t. y. $\mathbb{F}_{q,n}[x]$ elementą. Jeigu liekanas dauginsime – sandauga nebūtinai bus liekana.
Tačiau, kaip ir dalybos iš skaičių liekanų atveju, daugianarių daugybos apibrėžimą galime pakeisti:

jei $g, h \in \mathbb{F}_{q,n}[x]$, tai $g \times_f h \; = \; g \cdot h$ dalybos iš f liekana.

Naujosios liekanų daugybos rezultatas – vėl tos pačios aibės elementas, t. y. dalybos iš f liekana.
Teorema. Tegu f yra n-ojo laipsnio daugianaris. Daugianarių aibė $\mathbb{F}_{q,n}[x]$ su sudėties ir daugybos veiksmais $+, \times_f$ sudaro žiedą.

17 / 33

Daugianarių žiedas

Jeigu $f \in \mathbb{F}_q[x]$ yra n-ojo laipsnio daugianaris, tai daugianarių erdvė $\mathbb{F}_{q,n}[x]$ su sudėties ir daugybos operacijomis $+, \times_f$ sudaro žiedą. Šį žiedą žymėsime $\mathbb{F}_q[x]/f$.

Jame galime ieškoti mažesnių žiedų, kitaip sakant, požiedžių.

18 / 33

Požiedžiai

Apibrėžimas. Žiedo R su sudėties ir daugybos operacijomis $+, \cdot$ netuščią poaibį $R' \subset R$ vadiname požiedžiu, jeigu su visais $x, y \in R'$ teisingi sąryšiai $x + y, x \cdot y \in R'$.

19 / 33

Idealas

Ieškosime ne bet kokių, bet „gerų“ žiedo $\mathbb{F}_q[x]/f$ požiedžių.
Apibrėžimas. Žiedo $\mathbb{F}_q[x]/f$ požiedį I vadinsime idealu, jeigu kiekvienam $b(x) \in I$ teisingas sąryšis $x \times_f b(x) \in I$.

Išvada. *Jeigu I yra žiedo $\mathbb{F}_q[x]/f$ idealas, tai su visais $a(x) \in \mathbb{F}_q[x]/f$, $b(x) \in I$, teisingas sąryšis $a(x) \times_f b(x) \in I$.*

Jeigu daugianaris priklauso idealui, tai ir visi jo „kartotiniai“ sandaugos $\times_f$ prasme yra šio idealo elementai.

20 / 33

Pagrindiniai idealai

Apibrėžimas. Tegu $g(x) \in \mathbb{F}_q[x]/f, \deg(g) < n$. Idealą

$$\langle g \rangle = \{a(x) \times_f g(x) : a(x) \in \mathbb{F}_q[x]/f\}$$

vadinsime pagrindiniu idealu. Daugianarį $g(x)$ vadinsime šio idealo generatoriumi.

Teorema. Jeigu I yra žiedo $\mathbb{F}_q[x]/f$ idealas, tai $I = \langle g \rangle$, čia g yra mažiausio laipsnio nenulinis daugianaris, priklausantis I.

21 / 33

Pagrindiniai idealai

Mums svarbiausi – mažiausio laipsnio daugianariai generuojantys idealą. Kiek jų yra? Jeigu

$$g(x) = g_0 + g_1 x + \ldots + g_k x^k$$

yra vienas iš jų, tai daugianariai $\alpha g(x),\ \alpha \in \mathbb{F}_q, \alpha \neq 0$, irgi yra to paties laipsnio ir generuoja tą patį idealą. Dažniausiai patogu pasirinkti tą daugianarį iš šio būrio, kurio vyriausiasis koeficientas lygus 1.

22 / 33

Cikliniai kodai

Daugianarių žiedas

Šiame skyrelyje nagrinėsime tik daugianarių žiedą $\mathbb{F}_q[x]/f$ su

$$f(x) = x^n - 1.$$

Jeigu

$$a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]/f,$$

tai

$$\begin{aligned}
&x \times_f a(x) = a_{n-1} + a_0 x + \ldots + a_{n-2}x^{n-1},\\
&x^2 \times_f a(x) = a_{n-2} + a_{n-1} x + \ldots + a_{n-3}x^{n-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x^m \times_f a(x) = a_{n-m} + a_{n-1} x + \ldots + a_{n-m-1}x^{n-1}.
\end{aligned}$$

Ciklinis kodas

Apibrėžimas. Tiesinį kodą $\mathbb{C} \subset \mathbb{F}_q^n$ vadinsime cikliniu, jeigu

kiekvienam $\mathbb{C} = c_0 c_1 \ldots c_{n-1} \in \mathbb{C} \quad c_{n-1} c_0 \ldots c_{n-2} \in \mathbb{C}.$

Atlikę ciklinio kodo žodžių simbolių postūmį, vėl gauname to paties kodo žodį. Akivaizdu, kad, cikliškai pastūmę simbolius per bet kiek pozicijų, vėl gausime kodo žodžius.

Cikliniai kodai ir idealai

Interpretuokime kiekvieną ciklinio kodo žodį $\mathbb{C} = c_0c_1 \ldots c_{n-1}$ kaip žiedo elementą

$$c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}.$$

Kodas $\mathbb{C}$ yra $\mathbb{F}_q[x]/f$ poaibis. Kadangi $\mathbb{C}$ yra ciklinis kodas, tai

$$x \times_f c(x) = c_{n-1} + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1} \in \mathbb{C}.$$

Nebesudėtinga padaryti išvadą, kad $\mathbb{C}$ yra žiedo $\mathbb{F}_q[x]/f$ idealas!
Teisingas ir atvirkštinis teiginys: kiekvienas žiedo $\mathbb{F}_q[x]/f$ idealas yra ciklinis kodas.
Teorema. Žiedo $\mathbb{F}_q[x]/f$ idealų ir erdvės $\mathbb{F}_{q,n}[x]$ ciklinių kodų aibės sutampa.

Cikliniai kodai

Teorema. Ciklinis kodas $\mathbb{C} \subset \mathbb{F}_q[x]/f$ yra daugianarių kodas, kurį generuoja mažiausio laipsnio nenulinis $\mathbb{C}$ daugianaris $g(x)$, t. y. $\mathbb{C} = \mathbb{C}_{g,n}$.
Šis daugianaris yra $f(x) = x^n - 1$ daliklis.
Jei daugianaris $h(x)$ dalija $f(x)$, tai jo generuotas daugianarių kodas $\mathbb{C}_{h,n} \subset \mathbb{F}_q[x]/f$ yra ciklinis.

Cikliniai kodai

Daugianarių kodo generatorius – tai daugianaris $g(x)$, su kuriuo sudaroma kodo bazė

$$g(x), xg(x), \ldots, x^{n-k-1}g(x).$$

Taigi visi daugianarių kodo žodžiai dalijasi iš $g(x)$. Ciklinis kodas yra idealas; idealas turi ne vieną generatorių; ne visus juos, bet tik mažiausio laipsnio daugianarius vadiname kodo generatoriais!

Ciklinio kodo dekodavimas

Tegu $g(x)$ yra ciklinio kodo generatorius, t. y. daugianaris, dalijantis $f(x) = x^n - 1$. Kadangi ciklinis kodas yra daugianarių kodas, tai gautojo iš kanalo (tikriausiai iškraipyto) žodžio $d(x)$ sindromu galime laikyti dalybos iš $g(x)$ liekaną:

$$d(x) = k(x)g(x) + r(x), \quad \deg(r) < \deg(g).$$

Tegu $x^n - 1 = g(x)h(x)$. Padauginę lygybės puses iš $h(x)$, gausime:

$$\begin{aligned} d(x)h(x) &= k(x)g(x)h(x) + r(x)h(x) \\ &= k(x)f(x) + r(x)h(x), \\ & \quad d(x) \times_f h(x) = r(x)h(x). \end{aligned}$$

29 / 33

Ciklinio kodo dekodavimas

Jei dviejų žodžių $d_1(x), d_2(x)$, gautų iš kanalo, dalybos iš $g(x)$ liekanos $r_1(x), r_2(x)$ yra skirtingos, tai ir sandaugos $d_1(x) \times_f h(x), d_2(x) \times_f h(x)$ bus skirtingos. Kai kodas ciklinis, tai žodžio $d(x)$ sindromo vaidmenį atlieka sandauga $d(x) \times_f h(x)$, o daugianariui $h(x)$ tinka kontrolinio daugianario vardas.

30 / 33

Pavyzdžiai

Daugianaris $x^9 - 1$ virš kūno $\mathbb{F}_2$ skaidomas neskaidžiais daugikliais tokiu būdu:

$$x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1).$$

Taigi iš $\mathbb{F}_2^9$ elementų galima sudaryti 8 ciklinius kodus. Pavyzdžiui, generuojantį daugianarį $g(x) = (x - 1)(x^6 + x^3 + 1)$ atitinka ciklinis kodas, kurio generuojanti matrica

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

31 / 33

Pavyzdžiai

Daugianaris $x^{23}-1$ virš kūno $\mathbb{F}_2$:

$$x^{23}-1=(x+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)\times$$
$$\times(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1).$$

Jau įsitikinome, kad daugianaris

$$g(x)=x^{11}+x^9+x^7+x^6+x^5+x+1$$

generuoja Golay kodą $\mathbb{G}_{23}$. Galima įrodyti, kad ciklinis kodas, kurio generuojantis daugianaris yra

$$g(x)=x^{11}+x^{10}+x^6+x^5+x^4+x^2+1,$$

ekvivalentus $\mathbb{G}_{23}$.

32 / 33

Ciklinis kodas

Daugianario $x^{11}-1$ skaidinys virš kūno $\mathbb{F}_3$ yra toks:

$$x^{11}-1=(x-1)(x^5+x^4-x^3+x^2-1)(x^5-x^3+x^2-x-1).$$

Ciklinis kodas, kurį generuoja daugianaris

$$g(x)=x^5+x^4-x^3+x^2-1,$$

vadinamas trinarės abėcėlės Golay kodu $\mathbb{G}_{11}$. Šio kodo iš abėcėlės $\mathbb{F}_3$ žodžių parametrai tokie: $[11,6,5]$. Nesudėtinga įsitikinti, kad tai tobulas kodas.

33 / 33