Kodavimo teorija

Vilius Stakėnas

2010 metų ruduo

Golay kodas

1948 metais Richardas Hammingas paskelbė kodą, kuris garantuotai taiso vieną klaidą.

Šveicarų matematikas
Marcelis Golay 1949 metais sugalvojo net tris klaidas taisantį kodą. Šis kodas yra didelis ir geras – tiesiog tobulas.

Dvylika žodžių

$$\mathbf{c}_1 = 11000111010100000000000.$$

Cikliškai perstūmę žodžio simbolius sudarykime dar vienuolika žodžių:

$$\begin{aligned}
\mathbf{c}_2 &= 01100011101010000000000,\\
\mathbf{c}_3 &= 00110001110101000000000,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\mathbf{c}_{12} &= 00000000000110001110101.
\end{aligned}$$

Apibrėžimas

Visi šie žodžiai yra tiesiškai nepriklausomi. Taigi galime šią žodžių sistemą panaudoti kaip tiesinio kodo bazę.

Apibrėžimas. Kodą, kurį generuoja žodžiai $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{12}$ vadinsime dvejetainiu Golay kodu $\mathbb{G}_{23}$.

$\mathbb{G}_{24}$

Pailginkime visus žodžius $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{12}$ prirašydami kiekvieno žodžio gale simbolį 1. Gausime erdvės $\mathbf{F}_2^{24}$ žodžius; juos žymėkime $\mathbf{c}_1^*, \mathbf{c}_2^*, \ldots, \mathbf{c}_{12}^*$.

Apibrėžimas. Kodą, kurį generuoja žodžiai $\mathbf{c}_1^*, \mathbf{c}_2^*, \ldots, \mathbf{c}_{12}^*$ vadinsime dvejetainiu Golay kodu $\mathbb{G}_{24}$.

6 / 36

Savidualumas

Surašę žodžių $\mathbf{c}_i^*$ simbolius į eilutes, gautume kodo $\mathbf{G}_{24}$ generuojančią matricą. Patikrinę įsitikintume, kad visos šios matricos eilutės poromis yra ortogonalios.

Teorema. Kodas $\mathbb{G}_{24}$ yra savidualus.

7 / 36

Didelė matrica

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

8 / 36

Matricos A sudarymas

A^* yra matrica, gauta iš A, nubraukus pirmą eilutę ir pirmą stulpelį:

$$A^* = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Matricos A sudarymas

A^* stulpelius numeruokime $0, 1, \ldots, 10$. Pirmos A^* eilutės sudarymas:

$$\begin{array}{rccccccccccc} i = & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ i^2 \pmod{11} = & 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \end{array}$$

i^2 reikšmės rodo, kuriose pirmos eilutės vietose įrašyti 1.

Kitos eilutės gaunamos postūmiais.

Standartinio pavidalo generuojanti matrica

Teorema. Matrica $G = (I_{12}, A)$, yra kodo $\mathbb{G}_{24}$ generuojanti matrica.

Universalios matricos

Turėdami standartinio pavidalo generuojančią matricą galime sudaryti kontrolinę matricą:

$$H = (-A^\top, I_{12}) = (A, I_{12}), \quad \text{nes } -A^\top = A^\top = A.$$

Tačiau kodas $\mathbb{G}_{24}$ yra savidualus, todėl abi matricos

$$G = (I_{12}, A),\ H = (A, I_{12})$$

yra ir generuojančios, ir kontrolinės.

12 / 36

Parametrai

Teorema. Kodo $\mathbb{G}_{24}$ parametrai yra $[24, 12, 8]$ o kodo $\mathbb{G}_{23}$ – $[23, 12, 7]$.

13 / 36

Įrodymas

Įrodymas. Pakanka nustatyti, kad kodo $\mathbb{G}_{24}$ minimalus atstumas yra 8. Kodo $\mathbb{G}_{23}$ minimalus atstumas gali būti mažesnis ne daugiau kaip vienetu. Tačiau šis kodas turi daug žodžių, kurių svoriai lygūs 7, pavyzdžiui, žodžiai $\mathbf{c}_i$. Taigi jei kodo $\mathbb{G}_{24}$ minimalus atstumas yra 8, tai kodo $\mathbb{G}_{23}$ – 7. Pirmiausia įsitikinsime, kad visų kodo $\mathbb{G}_{24}$ žodžių svoriai dalijasi iš 4.

14 / 36

Įrodymas

Tegu $\mathbf{x} = x_1x_2\ldots x_{24}, y = y_1y_2\ldots y_{24}$ yra du kodo žodžiai. Nesunku įsitikinti, jog svoriams galioja tokia lygybės:

$$w(\mathbf{x}+\mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2S, \quad S = x_1y_1 + x_2y_2 + \ldots + x_{24}y_{24}.$$

Tačiau kodas $\mathbb{G}_{24}$ yra savidualus, todėl skaičius S yra lyginis,

$$w(\mathbf{x}+\mathbf{y}) \equiv w(\mathbf{x}) + w(\mathbf{y}) \pmod 4.$$

15 / 36

Įrodymas

Jeigu $\mathbf{x}$ ir $\mathbf{y}$ yra žodžiai sudaryti iš dviejų matricos G eilučių elementų (du kodo bazės žodžiai), tai $w(\mathbf{x}) = w(\mathbf{y}) = 8$.

$$w(\mathbf{x}+\mathbf{y}) \equiv w(\mathbf{x}) + w(\mathbf{y}) \pmod 4.$$

Iš lygybės gauname, kad žodžio $\mathbf{x}+\mathbf{y}$ svoris dalijasi iš 4.
Taigi bet kurio žodžio, sudaryto iš dviejų bazės žodžių, svoris dalijasi iš 4.

16 / 36

Įrodymas

Tegu $\mathbf{a}$ yra dviejų kodo bazės žodžių suma, taigi jo svoris dalijasi iš 4. Jei $\mathbf{y}$ – bazės žodis (matricos G eilutė), tai pasinaudoję

$$w(\mathbf{a}+\mathbf{y}) \equiv w(\mathbf{a}) + w(\mathbf{y}) \pmod 4.$$

gauname, kad kodo žodžių, kurie yra trijų bazės žodžių tiesinės kombinacijos, svoriai taip pat dalijasi iš 4.
Kaip tęsti samprotavimus tikriausiai aišku.

17 / 36

Įrodymas

Liko įrodyti, kad nėra nei vieno kodo $\mathbb{G}_{24}$ žodžio, kurio svoris būtų lygus 4. Samprotaudami naudosimės tuo, kad matricos G ir H yra generuojančios kodo $\mathbb{G}_{24}$ matricos.

Tarkime, kad egzistuoja kodo $\mathbb{G}_{24}$ žodis $\mathbf{x}$, kad $w(\mathbf{x}) = 4$. Kadangi abi matricos G, H generuoja tą patį kodą $\mathbb{G}_{24}$, tai $\mathbf{x}$ galime nagrinėti kaip matricos G arba H eilučių tiesinę kombinaciją.
Pažymėję $\mathbf{l}, \mathbf{r}$ atitinkamai kairiąją ir dešiniąją žodžio $\mathbf{x}$ puses (sudarytas iš 12 simbolių), gausime

$$w(\mathbf{x}) = w(\mathbf{l}) + w(\mathbf{r}).$$

18 / 36

Įrodymas

Atvejis $w(\mathbf{l}) = 0$ arba $w(\mathbf{r}) = 0$ yra negalimas.

Jei $w(\mathbf{l}) = 1$, tai $w(\mathbf{r}) = 3$; $\mathbf{x}$ turi būti viena iš matricos G eilučių, bet eilutės su dešinės pusės svoriu, lygiu 3, nėra.

Analogiškai gauname, jog atvejis $w(\mathbf{l}) = 3$, $w(\mathbf{r}) = 1$ taip pat neįmanomas.

19 / 36

Įrodymas

Lieka atvejis $w(\mathbf{l}) = w(\mathbf{r}) = 2$.
Bet tokiu atveju $\mathbf{x}$ yra dviejų skirtingų matricos G eilučių suma. Tiesiogiai tikrinant, galime nustatyti, jog $w(\mathbf{u} + \mathbf{v}) \neq 4$ jokioms dviem skirtingoms G eilutėms $\mathbf{u}, \mathbf{v}$.

20 / 36

Golay kodas yra tobulas

Patikrinę įsitikintume, kad kodo $\mathbb{G}_{23}$ parametrai tenkina tobulumo sąlygas.

Išvada. *Kodas $\mathbb{G}_{23}$ yra tobulas.*

21 / 36

Dekodavimas

Naudojantis šiuo kodu galime ištaisyti nedaugiau kaip 3 klaidas. Jeigu siunčiant kodo žodį $\mathbf{c}$ įvyko iškraipymas $\mathbf{e}$ (šį žodį sudaro nuliai tose pozicijose, kurios perduotos teisingai, ir vienetai ten, kur įvyko perdavimo klaidos), tai gautasis žodis yra $\mathbf{x} = \mathbf{c} + \mathbf{e}$.

Nagrinėsime metodą, kuris leidžia teisingai nustatyti nežinomą $\mathbf{e}$, kai $w(\mathbf{e}) \leq 3$. Radę $\mathbf{e}$, gautą žodį $\mathbf{x}$ dekoduosime kodo žodžiu $\mathbf{c} = \mathbf{x} - \mathbf{e}$.

22 / 36

Dekodavimas

Dekoduodami iš anksto nežinome, ar $w(\mathbf{e}) \le 3$. Jeigu metodas „neveikia“, tai ši sąlyga nėra patenkinta ir įvykusių klaidų skaičius yra didesnis nei kodas gali ištaisyti!

23 / 36

Dekodavimas

Kairiąją iškraipymo $\mathbf{e}$ dalį, sudarytą iš 12 pirmųjų simbolių, pažymėję $\mathbf{e}_1$, o dešiniąją – $\mathbf{e}_2$, gauname

$$\mathbf{e} = \mathbf{e}_1\mathbf{e}_2, \quad w(\mathbf{e}) = w(\mathbf{e}_1) + w(\mathbf{e}_2) \le 3.$$

Galimi atvejai:

1. $w(\mathbf{e}_1) = 0;$
2. $w(\mathbf{e}_2) = 0;$
3. $w(\mathbf{e}_1) > 0,\ w(\mathbf{e}_2) > 0.$

24 / 36

Atvejų atskyrimas

Iš pradžių ištirsime, kaip pagal gautą žodį nustatyti, kuris iš 1), 2), 3) atvejų įvyko.

Kadangi abi generuojančios matricos $G = (I_{12}, A), H = (A, I_{12})$ yra kartu ir kontrolinės, tai galime nagrinėti du gauto žodžio $\mathbf{x}$ sindromus:

$$\begin{aligned} \mathbf{s}_1 &= (\mathbf{c}+\mathbf{e})G^\top = \mathbf{e}G^\top = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} I_{12} \\ A \end{pmatrix} = \mathbf{e}_1 + \mathbf{e}_2 A, \\ \mathbf{s}_2 &= (\mathbf{c}+\mathbf{e})H^\top = \mathbf{e}H^\top = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} A \\ I_{12} \end{pmatrix} = \mathbf{e}_1 A + \mathbf{e}_2. \end{aligned}$$

25 / 36

Pirmas atvejis

Jeigu $w(\mathbf{e}_1) = 0$, tai iš

$$\begin{aligned}
\mathbf{s}_1 &= (\mathbf{c}+\mathbf{e})G^\top = \mathbf{e}G^\top = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} I_{12} \\ A \end{pmatrix} = \mathbf{e}_1 + \mathbf{e}_2 A, \\
\mathbf{s}_2 &= (\mathbf{c}+\mathbf{e})H^\top = \mathbf{e}H^\top = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} A \\ I_{12} \end{pmatrix} = \mathbf{e}_1 A + \mathbf{e}_2.
\end{aligned}$$

gauname $\mathbf{s}_1 = \mathbf{e}_2 A, \mathbf{s}_2 = \mathbf{e}_2$. Taigi $w(\mathbf{e}) = w(\mathbf{e}_2) = w(\mathbf{s}_2) \leq 3$.

Kita vertus s_1 yra dešinioji kodo žodžio $\mathbf{c} = \mathbf{e}_2(I_{12}, A)$ pusė. Kadangi $w(\mathbf{c}) \geq 8$, o kairioji pusė sveria ne daugiau kaip 3, tai $w(\mathbf{s}_1) = w(\mathbf{c}) - w(\mathbf{e}_2) \geq 8 - 3 = 5$.

26 / 36

Antras atvejis

Jeigu $w(\mathbf{e}_2) = 0$, tai analogiškai iš

$$\begin{aligned}
\mathbf{s}_1 &= (\mathbf{c}+\mathbf{e})G^\top = \mathbf{e}G^\top = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} I_{12} \\ A \end{pmatrix} = \mathbf{e}_1 + \mathbf{e}_2 A, \\
\mathbf{s}_2 &= (\mathbf{c}+\mathbf{e})H^\top = \mathbf{e}H^\top = \mathbf{e}_1\mathbf{e}_2\begin{pmatrix} A \\ I_{12} \end{pmatrix} = \mathbf{e}_1 A + \mathbf{e}_2.
\end{aligned}$$

gauname $w(\mathbf{e}) = w(\mathbf{e}_1) = w(\mathbf{s}_1) \leq 3, w(\mathbf{s}_2) \geq 5$.

27 / 36

Trečias atvejis

Jei $w(\mathbf{e}_1) > 0,\ w(\mathbf{e}_2) > 0$, tai $w(\mathbf{s}_1) \geq 5,\ w(\mathbf{s}_2) \geq 5$. Pavyzdžiui, jei $w(\mathbf{e}_1) = 1, w(\mathbf{e}_1) = 2$, tai

$$w(\mathbf{s}_1) = w(\mathbf{e}_1 + \mathbf{e}_2 A) \geq w(\mathbf{e}_2 A) - w(\mathbf{e}_1) \geq (8-2) - 1 = 5.$$

Taigi pagal sindromų svorius $w(\mathbf{s}_1), w(\mathbf{s}_2)$ galima nustatyti, kuris iš 1), 2), 3) atvejų įvyko.

28 / 36

Dekodavimas pirmasiais atvejais

Jei $w(\mathbf{s}_1) \leq 3$, tai $w(\mathbf{e}_2) = 0$, ir $\mathbf{e} = \mathbf{e}_1\mathbf{o} = \mathbf{s}_1\mathbf{o}$; čia $\mathbf{o}$ yra žodis, sudarytas iš 12 nulių.

Analogiškai, jei $w(\mathbf{s}_2) \leq 3$, tai $\mathbf{e} = \mathbf{o}\mathbf{s}_2$.

Lieka ištirti dekodavimą tuo atveju, kai $w(\mathbf{s}_1) \geq 5,\ w(\mathbf{s}_2) \geq 5$, t. y. 3) atveju. Jį suskaidysime į dvi galimybes:

1. $w(\mathbf{e}_1) = 1,\ w(\mathbf{e}_2) = 1$ arba 2;
2. $w(\mathbf{e}_1) = 2,\ w(\mathbf{e}_2) = 1.$

Pastebėsime, jog 1) atveju pakanka rasti $\mathbf{e}_1$. Išties, suradę šią dalį, galime manyti, jog gautasis žodis yra $\mathbf{x}' = \mathbf{x} - \mathbf{e}_1\mathbf{o}$ ir dekoduoti jau aptartu būdu. Analogiška pastaba teisinga ir 2) atvejui.

Dvylika sindromų

Pakaks išnagrinėti 1) atvejį. Tegu iškraipymas įvyko j-ojoje pozicijoje, $1 \leq j \leq 12$. Tada $\mathbf{e}_1 = \varepsilon_j$; čia ε_j žymime žodį iš 12 simbolių, kurių tik j-asis yra vienetas, kiti – nuliai. Sudarykime 12 naujų žodžių

$$\mathbf{x} + \varepsilon_1\mathbf{o}, \ldots, \mathbf{x} + \varepsilon_{12}\mathbf{o}$$

ir 12 juos atitinkančių sindromų

$$\begin{aligned} \mathbf{s}_i &= (\mathbf{x} + \varepsilon_i\mathbf{o})\begin{pmatrix} A \\ I_{12} \end{pmatrix} = (\mathbf{e} + \varepsilon_i\mathbf{o})\begin{pmatrix} A \\ I_{12} \end{pmatrix} \\ &= (\varepsilon_j\mathbf{e}_2 + \varepsilon_i\mathbf{o})\begin{pmatrix} A \\ I_{12} \end{pmatrix} = \varepsilon_j A + \mathbf{e}_2 + \varepsilon_i A. \end{aligned}$$

Sindromų svoriai

Jeigu $i \neq j$, tai
$$w(\mathbf{s}_i) \geq w(\varepsilon_j A + \varepsilon_i A) - w(\mathbf{e}_2).$$

Žodis $\varepsilon_j A + \varepsilon_i A = (\varepsilon_j + \varepsilon_i)A$ yra kodo žodžio $(\varepsilon_j + \varepsilon_i)(I_{12}, A)$ dešinioji pusė; kadangi visas žodis sveria nemažiau kaip 8, kairioji – lygiai 2, tai $w((\varepsilon_j + \varepsilon_i)A) \geq 8 - 2 = 6$. Tada

$$w(\mathbf{s}_i) \geq 6 - 2 = 4.$$

Klaidos radimas

Taigi peržiūrėję sindromų svorius, pamatysime, kad visi jie, išskyrus vieną, yra ne mažesni už 4. Imdami tą j, kuriam $w(\mathbf{s}_j) \leq 2$, rasime $\mathbf{e}_1 = \varepsilon_j$.

Klaidos radimas

Jeigu svorių seka kitokia, tai susidūrėme su 2) atveju. Tenka ieškoti $\mathbf{e}_2 = \varepsilon_j$. Dabar teks peržiūrėti sindromus

$$\mathbf{s}'_i = (\mathbf{x} + \mathbf{o}\varepsilon_i)\begin{pmatrix} I_{12} \\ A \end{pmatrix}.$$

Radę j, kuriam $w(\mathbf{s}'_j) \leq 2$, gausime $\mathbf{e}_2 = \varepsilon_j$.

Kodo $\mathbb{G}_{24} svoriai$

$\mathbb{G}_{24}$ yra savidualus, todėl jo žodžius galima „pasverti“ naudojant MacWilliams tapatybę:
$w_{\mathbb{G}_{24}}(1, y) = \frac{1}{|\mathbb{G}_{24}|} \cdot w_{\mathbb{G}_{24}}(1 + y, 1 - y)$.
Svorio funkcijos koeficientai:

$$A_0 = 1, \quad A_8 = 759, \quad A_{12} = 2576, \quad A_{16} = 759, \quad A_{20} = 0, \quad A_{24} = 1.$$