BCH kodų dekodavimas

2010

BCH kodas

$\mathbb{L} \subset \mathbb{F}_p^n$ yra BCH kodas su numatytuoju atstumu $r = 2t + 1$. Naudodamiesi šiuo kodu garantuotai galime ištaisyti t klaidų.

Šis kodas yra Reedo-Solomono kodo iš abėcėlės $\mathbb{F}_q (q = p^m, q - 1$ dalijasi iš $n)$ žodžių poaibis.

Kodo generatorius yra daugianaris

$$g(x) = (x - \beta)(x - \beta^2) \cdots (x - \beta^{2t}),$$

čia $\beta \in \mathbb{F}_q$ yra n-osios eilės elementas.

2 / 19

Klaidų daugianaris

Kiekvienam kodo $\mathbb{L}$ žodžiui, interpretuojant jį kaip daugianarį

$$c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1},$$

teisingos lygybės

$$c(\beta) = c(\beta^2) = \ldots = c(\beta^{2t}) = 0.$$

3 / 19

Klaidų daugianaris

Tarkime, siunčiant kodo žodį $c(x)$ kanalu įvyko klaidos ir gautasis žodis yra

$$d(x) = c(x) + e(x), \quad e(x) = e_0 + e_1 x + \ldots + e_{n-1} x^{n-1}.$$

Jeigu surastume klaidų daugianarį $e(x)$, galėtume ištaisyti įvykusias klaidas.

Tai įmanoma, jeigu klaidų skaičius nedidesnis už t, taigi – daugianario $e(x)$ svoris turi būti nedidesnis už t.

4 / 19

Klaidų daugianaris

Kadangi daugianarį $d(x)$ žinome, tai galime suskaičiuoti dydžius

$$s_j = d(\beta^j) = c(\beta^j) + e(\beta^j) = e(\beta^j), \quad j = 1, 2, \ldots, 2t.$$

Sindromas, lokatorius ir identifikatorius

Apibrėžimas. Tegu

$$\begin{aligned} s(x) &= s_1 + s_2 x + \ldots + s_{2t} x^{2t-1}, \\ \lambda(x) &= \prod_{\substack{j=0,\ldots,n-1 \\ e_j \neq 0}} \left(1 - \beta^j x\right), \\ \omega(x) &= s(x) \times_f \lambda(x) \quad (f(x) = x^{2t}). \end{aligned}$$

Daugianarį $s(x)$ vadinsime gautojo žodžio sindromu, $\lambda(x)$ – klaidų lokatorium, $\omega(x)$ – klaidų identifikatorium.

Jei sužinotume lokatorių...

Jeigu lokatorių sužinotume, galėtume suskaičiuoti elementus

$$\lambda(\beta^{-0}), \quad \lambda(\beta^{-1}), \quad \ldots, \lambda(\beta^{-m}), \quad \ldots, \lambda(\beta^{-n+1});$$

nuliai šioje elementų eilėje parodytų klaidų vietą, taigi lokalizuotų klaidas.

Svarbus sąryšis

Teorema. Teisinga lygybė

$$\omega(x) = \sum_{i=0}^{n-1} e_i \beta^i \prod_{\substack{j \neq i \\ e_j \neq 0}} \left(1 - \beta^j x\right).$$

Klaidų taisymas

Klaidų identifikatorius yra nedidesnio kaip $t-1$ laipsnio daugianaris. Jeigu žinotome, kad $e_k \neq 0$ ir apskaičiuotume $\omega(\beta^{-k})$ gautume,

$$\omega(\beta^{-k}) = e_k \beta^k \prod_{\substack{j \neq k \\ e_j \neq 0}} \left(1 - \beta^j \beta^{-k}\right).$$

9 / 19

Klaidų taisymas

O šį reiškinį galima užrašyti dar paprasčiau – pasinaudojus formaliomis daugianarių išvestinėmis (jas skaičiuojame pagal tas pačias realiųjų skaičių funkcijoms įrodytas taisykles):

$$\omega(\beta^{-k}) = -e_k \lambda'(\beta^{-k}).$$

Naudojantis $\omega(x)$ galime surasti klaidų daugianario koeficientus:

$$\text{jei } \lambda(\beta^{-k}) \neq 0, \quad \text{tai} \quad e_k = -\frac{\omega(\beta^{-k})}{\lambda'(\beta^{-k})}.$$

10 / 19

Klaidų identifikatoriaus savybė

Klaidų identifikatoriaus apibrėžimo lygybė:

$$\omega(x) = s(x) \times_f \lambda(x) \quad (f(x) = x^{2t}).$$

Ji reiškia, kad egzistuoja daugianaris $m(x) \in \mathbb{F}_q[x]$, kad

$$m(x)x^{2t} + \lambda(x)s(x) = \omega(x), \quad \deg(\omega) < t.$$

Taigi iš $\omega(x)$ dalijasi bendrasis didžiausias žinomų daugianarių x^{2t} ir $s(x)$ daliklis.

11 / 19

Euklido algoritmas

Klaidų taisymui reikalingus daugianarius naudojantis Euklido algoritmu galime surasti šitaip : pažymėkime $f_0(x) = x^{2t}, f_1(x) = s(x)$ ir atlikime Euklido algoritmo žingsnius, kol gausime pirmąją liekaną, kurios laipsnis mažesnis už t :

$$\begin{aligned} f_0(x) &= m_1(x)f_1(x) + f_2(x), \quad t \le \deg(f_2) < \deg(f_1), \\ f_1(x) &= m_2(x)f_2(x) + f_3(x), \quad t \le \deg(f_3) < \deg(f_2), \\ \ldots & \quad \ldots \\ f_{k-2}(x) &= m_{k-1}(x)f_{k-1}(x) + f_k(x), \quad t \le \deg(f_k), \\ f_{k-1}(x) &= m_k(x)f_k(x) + f_{k+1}(x), \quad 0 \le \deg(f_{k+1}) < t. \end{aligned}$$

12 / 19

Euklido algoritmas

Daugianaris $f_{k+1}(x)$ yra jau beveik klaidų identifikatorius. Pradėję nuo paskutinės lygybės ir kopdami į viršų suraskime išraišką

$$f_{k+1}(x) = m_*(x)x^{2t} + \lambda_*(x)s(x).$$

13 / 19

Euklido algoritmas

Prisiminkime, kad klaidų lokatoriaus laisvasis narys turi būti lygus $1.$ Padauginę gautąją lygybę iš $\delta = \lambda_*(0)^{-1}$ gausime

$$\begin{aligned} \delta f_{k+1}(x) &= (\delta m_*(x))x^{2t} + (\delta\lambda_*(x))s(x), \\ \omega(x) &= \delta f_{k+1}(x), \ \lambda(x) = \delta\lambda_*(x). \end{aligned}$$

14 / 19

Skaitinis pavyzdys

Sudarykime $n = 5$ simbolių ilgio BCH kodą iš aibės $\mathbb{F}_{11}$ žodžių, kuris taisytų vieną klaidą, t.y. $t = 1$. Tada numatytasis atstumas turi būti $r = 3$.

Kokiame plėtinyje yra $n-$osios eilės elementas? Kadangi $p - 1 = 10$ dalijasi iš n, tai reikiamą elementą rasime jau kūne $\mathbb{F}_{11}$.

Šiuo atveju BCH kodas sutaps su Reedo-Solomono kodu, sudarytu iš abėcėlės $\mathbb{F}_{11}$ žodžių. $\gamma = 2$ yra generuojantis šio kūno elementas, tada $\beta = \gamma^2 = 4$ bus reikalingas kodo konstrukcijai elementas.

Skaitinis pavyzdys

Generuojantis daugianaris:

$$g(x) = (x - \beta)(x - \beta^2) = (x - 4)(x - 5) = x^2 + 2x + 9.$$

Kodo dimensija $k = 3$.

Skaitinis pavyzdys

Sudarykime kokį nors kodo žodį, pavyzdžiui,

$$c(x) = (x^2 + 7)g(x) = x^4 + 2x^3 + 5x^2 + 3x + 8.$$

Tarkime, siunčiant kanalu šis žodis pavirto į $d(x) = x^4 + 5x^2 + 3x + 8$.

Pabandykime vien tik naudodamiesi juo surasti klaidų žodį. Sudarykime sindromą:

$$s_1 = d(\beta) = d(4) = 4, \ s_2 = d(\beta^2) = d(5) = 3, \quad s(x) = 4 + 3x.$$

Skaitinis pavyzdys

Užtenka vieno Euklido algoritmo žingsnio:

$$x^{2t} = x^2 = (4x+2)s(x) + 3,\ 3 = x^2 + (7x+9)s(x),$$
$$4 = 5x^2 + (2x+1)s(x),\ \lambda(x) = 2x+1, \omega(x) = 4.$$

Skaičiuodami pasinaudojome tuo, kad $9^{-1} \equiv 5 \pmod{11}$. Taigi $\omega(x) = 4$ ir $\lambda(x) = 2x+1$. Iš karto randame lygties $\lambda(x) = 0$ šaknį:

$$x = -2^{-1} = 5 = \beta^2 = \beta^{2-5} = \beta^{-3}.$$

18 / 19

Skaitinis pavyzdys

Klaidų lokatorius rodo, kad neteisingai perduotas koeficientas prie x^3. Raskime atitinkamą klaidos žodžio koeficientą: $\lambda'(x) = 2$

$$e_3 = -\omega(\beta^{-3})\lambda(\beta^{-3})^{-1} = -4 \cdot 2^{-1} = 7 \cdot 6 = 9.$$

Taigi $e(x) = 9x^3$ ir $c(x) = d(x) - e(x) = x^4 + 2x^3 + 5x^2 + 3x + 8.$

19 / 19