Kļūdu korekcija IV

Iepriekšējā lekcijā tika izstāstīts par Rīda-Solomona kodiem vienkāršotā formā. Dati tiek pārveidoti par skaitļu virkni, kas tiek sadalīti k skaitļus garos blokos. Pieņemsim, ka $a_0, a_1, ..., a_{k-1}$ ir viens šāds bloks. Tad mēs ņemam polinomu

$$f(x) = a_{k-1}x^{k-1} + ... + a_1x + a_0$$

un pārraidām polinoma vērtības f(0), ..., f(s-1). Tad ir iespējams atjaunot sākotnējo polinomu f(x) (un līdz ar to arī $a_0, a_1, ..., a_{k-1}$), ja pārraidot datus ir bijis līdz (s-k)/2 kļūdām.

Diemžēl polinoma vērtības f(i) var būt daudz lielākas par sākotnējiem skaitļiem $a_0, a_1, ..., a_{k-1}$. Tāpēc pārraidāmās informācijas apjoms var kļūt pārāk liels. To var labot izmantojot aritmētiku pār galīgiem laukiem.

1. Ievads par galīgiem laukiem

Definīcija. Lauks ir kopa L, kurā definētas operācijas + un * ar šādām īpašībām:

- Visurdefinētība: priekš jebkura a un b ir definēts gan a + b, gan a * b.
- Komutativitāte: a + b = b + a, a * b = b * a.
- Asociativitāte: (a + b) + c = a + (b + c), (a * b) * c = a * (b * c).
- Distributivitāte: a * (b + c) = a * b + a * c.
- 0 elements: eksistē elements 0 ar īpašību, ka 0 + a = a jebkuram a.
- 1 elements: eksistē elements 1 ar īpašību, ka 1 * a = a jebkuram a.
- Apgriezto elementu eksistence: katram a eksistē tāds –a, ka a + (-a) = 0 un, ja $a \neq 0$, tad eksistē arī elements a^{-1}, kuram $a * a^{-1} = 1$.

Piemēram, visu reālo skaitļu kopa **R** ir lauks. Eksistē arī citi lauki. Ja mums ir lauks, tad mēs varam ieviest atņemšanu un dalīšanu (definējot a – b = a + (-b) un a / b = a * b^{-1}). Priekš daudziem bieži lietotiem faktiem no algebras, ko parasti pierāda priekš polinomiem ar reāliem koeficientiem, pietiek ar to, ka koeficienti ir ņemti no kaut kāda lauka. Piemēram, ar to pietiek priekš algebras pamatteorēmas, kas ir pamatā Rīda-Solomona kodiem.

Galīgs lauks ir galīga kopa, kas ir lauks.

1. piemērs. Mēs varam ņemt kopu {0, 1, 2} un definēt a + b kā saskaitīšanu pēc moduļa 3: a + b = (a + b) mod 3 un a * b kā reizināšanu pēc moduļa 3: a * b = (a * b) mod 3. Tad mēs iegūstam šādas saskaitīšanas un reizināšanas tabulas:

+	0	1	2
0	0	1	2
1	1	2	0

2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

0 un 1 elementi ir vienkārši 0 un 1. Apgrieztie elementi tiek definēti šādi:
$(-1) = 2$, $(-2) = 1$, $1^{-1} = 1$, $2^{-1} = 2$.

2. piemērs. Ja p ir pirmskaitlis, tad kopa {0, 1, ..., p-1} ar operācijām a + b = (a + b) mod p un a * b = (a * b) mod p ir lauks. Atkal, 0 un 1 elementi ir 0 un 1. Apgrieztais elements priekš saskaitīšanas tiek definēts šādi: (-0) = 0, un ja a≠0, tad (-a) = p-a. Lai pierādītu, ka eksistē apgrieztais elements priekš reizināšanas, jāpierāda, ka kongruencei

$$a * x \equiv 1 \pmod p$$

eksistē atrisinājums priekš jebkura a ≠ 0. To pierāda skaitļu teorijas kursā.

3. piemērs. Ja p ir pirmskaitlis un m ≥ 1 ir vesels skaitlis, tad var uzkonstruēt galīgu lauku $GF(p^m)$ ar p^m elementiem. Šī lauka konstrukcija šajā kursā aplūkota netiks.

2. Pielietojums Rīda – Solomona kodiem

Izvēlamies galīgu lauku GF(q). Datus pārveidojam par šī lauka elementu virkni. Virknes elementus sadalām blokos $a_0, a_1, ..., a_{k-1}$ (kur k < q). Tad ņemam to pašu polinomu

$$f(x) = a_{k-1}x^{k-1} + ... + a_1x + a_0$$

un izrēķinam vērtības f(0), f(1), ..., f(s-1) priekš galīgā lauka elementiem 0, 1, ..., s-1, visām operācijām izmantojot + un *, kas definēts galīgajā laukā.

Atkodēšanas algoritms un kļūdu skaits, ko spēj koriģēt Rīda-Solomona kods nemainās (jo atkodēšanā un pierādījumā par kļūdu korekcijas spējām netika izmantots nekas tāds, kas neizpildītos patvaļīgam laukam), bet mēs esam izvairījušies no operācijām ar lieliem skaitļiem.

Piemērs.
Tiek izmantots galīgs lauks {0, 1, 2, 3, 4}, aritmētiskās operācijas veicot pēc moduļa 5. Informācija tiek kodēta ar 2 pakāpes polinomu

$$f(x) = a\,x^2 + b\,x + c,$$

ņemot 5 polinoma vērtības: f(0), f(1), f(2), f(3) un f(4).

1. uzdevums. Nokodēt 3, 2, 1.
Risinājums. Ņemam polinomu

$$f(x) = 3\,x^2 + 2\,x + 1.$$

Izrēķinam vērtības

$$f(0) = 3 \blacktriangledown 0^2 + 2 \blacktriangledown 0 + 1 = 1,$$
$$f(1) = (3 \blacktriangledown 1^2 + 2 \blacktriangledown 1 + 1) \bmod 5 = 6 \bmod 5 = 1,$$
$$f(2) = (3 \blacktriangledown 2^2 + 2 \blacktriangledown 2 + 1) \bmod 5 = 17 \bmod 5 = 2,$$
$$f(3) = (3 \blacktriangledown 3^2 + 2 \blacktriangledown 3 + 1) \bmod 5 = 34 \bmod 5 = 4,$$
$$f(4) = (3 \blacktriangledown 4^2 + 2 \blacktriangledown 4 + 1) \bmod 5 = 57 \bmod 5 = 2.$$

Tātad, tiek pārraidītas vērtības 1, 1, 2, 4, 2.

2. uzdevums. Atkodēt 1, 1, *, 4, *.

Risinājums. Sastādām vienādojumu sistēmu (pēc mod 5):

$$0^2 a + 0\, b + c = 1 \pmod 5,$$
$$1^2 a + 1\, b + c = 1 \pmod 5,$$
$$3^2 a + 3\, b + c = 4 \pmod 5.$$

Tā kā $3^2 = 9 = 4 \pmod 5$, tad šo sistēmu var pārrakstīt kā

$$c = 1 \pmod 5,$$
$$a + b + c = 1 \pmod 5,$$
$$4\, a + 3\, b + c = 4 \pmod 5.$$

Ievietojot c=1 otrajā un trešajā vienādojumā, iegūstam

$$a + b = 1 - 1 = 0 \pmod 5,$$
$$4\, a + 3\, b = 4 - 1 = 3 \pmod 5.$$

Tagad atrisinām šo divu vienādojumu sistēmu ar izslēgšanas metodi. Pareizinot pirmo vienādojumu ar 3 un atņemot no otrā vienādojuma iegūst

$$(4a+3b) - 3\,(a+b) = a = 3 - 3 \blacktriangledown 0 = 3 \pmod 5.$$

No vienādojuma $a + b = 0 \pmod 5$ iegūstam, ka

$$b = 0 - 3 = -3 = 2 \pmod 5.$$

Tātad polinoms bija

$$f(x) = 3\, x^2 + 2\, x + 1.$$

2. uzdevums. Atkodēt 2, 3, *, *, 2, kur * - pazaudēta vērtība. (Saņemtās vērtības ir pareizas.)

Risinājums. Sastādām vienādojumu sistēmu (pēc mod 5):

$$0^2 a + 0\, b + c = 2 \pmod 5,$$
$$1^2 a + 1\, b + c = 3 \pmod 5,$$
$$4^2 a + 4\, b + c = 2 \pmod 5.$$

Tā kā $4^2 = 16 = 1 \pmod 5$, tad šo sistēmu var pārrakstīt kā

$$c = 2 \pmod 5,$$
$$a + b + c = 3 \pmod 5,$$
$$a + 4\, b + c = 2 \pmod 5.$$

Ievietojot c=2 otrajā un trešajā vienādojumā, iegūstam

$$a + b = 3 - 2 = 1 \pmod 5,$$
$$a + 4\, b = 2 - 2 = 0 \pmod 5.$$

Tagad atrisinām šo divu vienādojumu sistēmu ar izslēgšanas metodi. Atņemot pirmo vienādojumu no otrā iegūst

$$(a+4b) - (a+b) = 3\, b = 0 - 1 = 4 \pmod 5$$

Tagad mums jāatrisina $3\, b = 4 \pmod 5$.

[Lūdzu, ievērot, ka atrisinājums nebūs daļskaitlis 4/3, jo tas nav lauka elements!]

Pārbaudot b = 0, 1, 2, 3, 4, secinām, ka $3 \blacktriangledown 3 = 9 = 4 \pmod 5$. Tātad $b = 3 \pmod 5$.

[Ir algoritmi, kā atrast b, neizmantojot pilno pārlasi un tos var apgūt skaitļu teorijas kursā (vai „Datu drošībā un kriptogrāfijā"). Bet priekš mod 5, iespējamo b ir tik maz, ka pārlase ir ātrāka.]

No vienādojuma a + b = 1 (mod 5) iegūstam, ka

$$a = 1 - 3 = -2 = 3 \pmod 5.$$

Tātad polinoms bija

$$f(x) = 3x^2 + 3x + 2.$$

3. Atkodēšana ar interpolāciju

Otrs veids, kā veikt atkodēšanu ir interpolācija (labi strādā pie neliela polinomu skaita un pakāpēm). Ja zinām, ka

$$f(x_1) = r_1;\ f(x_2) = r_2;\ \ldots\ f(x_k) = r_k,$$

tad varam aprēķināt

$$f_i(x) = \frac{(x - r_1)\ldots(x - r_{i-1})(x - r_{i+1})\ldots(x - r_k)}{(r_i - r_1)\ldots(r_i - r_{i-1})(r_i - r_{i+1})\ldots(r_i - r_k)}$$

Šim polinomam ir laba īpašība:

1) Ja $x = r_i$, tad $f_i(x) = 1$
2) Ja $x = r_j$, $(i \neq j)$ tad $f_i(x) = 0$, jo kaut kur polinomā ir reizinātājs $(x - r_j) = 0$, kas visu reizinājumu padara par 0.

Meklētais polinoms ir:

$$f(x) = r_1 * f_1(x) + r_2 * f_2(x) + \ldots + r_k * f_k(x).$$

Kāpēc šis polinoms dod pareizu rezultātu?
Ja x vietā ievietojam r_i, tad visi $f_j(x)$ $(i \neq j)$ būs vienādi ar 0, un vienīgais $f_i(x)$ dos rezultātu 1. Tātad

$$f(x) = r_i * f_i(x) = r_i$$

Ja vienīgais kļūdu veids ir dažu vērtību pazušana, tad pietiek ar šo pieeju.

Ja ir kļūdas, kurās vienas vērtības vietā ir saņemta cita, tad ir grūtāk:

k : sākotnējie skaitļi
s : pārraidītās vērtības (f(0), f(1) ... f(s-1))
$c \leq (s - k) / 2$: maksimālais pieļaujamais kļūdu skaits
vismaz s - c vērtības ir pareizas
Rezultātā ir pietiekami daudz pareizo vērtību, lai atrastu kļūdas, taču nezinām tieši kuras ir pareizas, lai tās varētu izmantot kļūdu meklēšanā.

4. Berlekampa – Velča algoritms

Šī ir atkodēšanas metode, ko lieto tad, ja iespējama ne tikai datu pazušana, bet arī nepareizu datu saņemšana pareizo datu vietā.
Pieņemsim, ka

Kļūdas ir $x_1, x_2, \ldots x_c$
Sākotnējais polinoms p(x)
$p(x_i)$ vietā saņemts r_i
Pārējie saņemtie dati, atskaitot c vērtības ir pareizi.

Definējam kļūdu lokatoru:

$Y(x) = (x-x_1)(x-x_2) \ldots (x-x_c)$
$Y(x_i) = 0$ deg $Y(x) \leq c$

Šis polinoms ir 0 pie tām argumenta vērtībām x_i, kurām saņemta nepareiza p(x) vērtība.

Definējam polinomu Z(x), kas ir kļūdu lokatora un sākotnējā polinoma reizinājums:

$$Z(x) = Y(x) * p(x)$$

$$\deg Z(x) \le \deg Y(x) + \deg p(x) \le c + (k - 1) = k + c - 1$$

Iedomājamies, ka mēs protam atrast Y un Z, tad izdalot abas vienādības puses ar Y iegūstam vienādību

$$p(x) = Z(x) / Y(x)$$

Tātad, lai atrastu p(x), pietiek izrēķināt Z(x) un Y(x).
Ja r ir vērtība, kas saņemta kā p(x), tad

$$Z(x) = Y(x)*r$$

Šāda vienādība ir spēkā, jo

1) Ja $r = p(x)$, tad $Z(x) = Y(x) * p(x)$ - ir saņemta pareiza vērtība
2) Ja $r \neq p(x)$, tad $Y(x) = 0$; $Z(x) = 0$

Tātad $Z(x) = Y(x)*r$ ir spēkā.

Pieņemsim, ka

$Y(x) = b_c x^c + b_{c-1}x^{c-1} + ... + b_0$ - polinoms ar pakāpi c

Tā kā p(x) – polinoms ar pakāpi k-1, tad

$Z(x) = a_{k+c-1}x^{k+c-1} + a_{k+c-2}x^{k+c-2} + ...+ a_0$ - polinoms ar pakāpi k+c-1

Katra saņemtā vērtība dod pa vienam nosacījumam:

$Z(0) = Y(0)\, r_0$
$Z(1) = Y(1)\, r_1$
...
$Z(s-1) = Y(s-1)\, r_{s-1}$

Katrā nosacījumā ievietojot i un r_i, iegūst vienādojumu, kura nezināmie ir $a_0, ... a_{k+c-1}, b_0, ... b_c$

$Z(i) = Y(i) * r_i$ - s vienādojumu sistēma ar k+2*c +1 nezināmajiem.

Atrisinām šo vienādojumu sistēmu un no nezināmajiem iegūstam Z(x) un Y(x). Tad izmantojot p(x) = Z(x) / Y(x) aprēķinām p(x).

Jautājumi:

1. Vai vienādojumu sistēmai ir atrisinājums?
2. Vai vienādojumu sistēmai nav vairāki atrisinājumi?
3. Vai varam atrast algoritmisku metodi, kā atrisināt vienādojumu sistēmu?

Atbildes:

1. Jā, atrisinājums vienmēr būs pareizais (meklējamais) Y(x) un Z(x) polinomu pāris, jo tas apmierina visus nosacījumus.
2. Nav garantijas, ka nav vairāki atrisinājumi (Y(x), Z(x)) un (Y'(x), Z'(x)) un

$$Z(x) / Y(x) \neq Z'(x) / Y'(x)$$

Kā tikt ar to galā?
Ja tiek pārraidītas pietiekami daudz vērtības, tad atrisinājums ir viennozīmīgi noteikts. (Y(x), Z(x))
<u>Apgalvojums:</u> Ja Y un Z ir tādi, ka:

1) $\deg Y \le c$
2) $\deg Z \le k + c - 1$
3) $Y \neq 0$

Un visiem i $Z(i) = Y(i) * r_i$, un Y', Z' ir tādas pašas īpašības, tad
$Z(x) / Y(x) = Z'(x) / Y'(x)$

<u>Pierādījums:</u>

$Z(i) = Y(i) * r_i$ - r_i – saņemtā vērtība priekš p(i)
$Z'(i) = Y'(i) * r_i$

Sareizinām krustiski un iegūstam

$$Z(i) * Y'(i) * r_i = Z'(i) * Y(i) * r_i$$

Noīsinām r_i un iegūstam

$$Z(i) * Y'(i) = Z'(i) * Y(i)$$

$Z'(i) * Y(i)$ kopā pakāpe ir $k + 2c + 1$

i var būt 0, 1, ... s-1

$Z(i) * Y'(i)$ un $Z'(i) * Y(i)$ sakrīt pie s dažādiem x.

Algebras pamatteorēma:

Ja divi polinomi ir dažādi, tad maksimālais vietu skaits, kurās viņi sakrīt ir pakāpe.

Tas nozīmē, ka, ja $k+c-1<s$, tad $Z(i) * Y'(i) = Z'(i) * Y(i)$

Izdalām abas puses ar $Y(x)$ un $Y'(x)$ un iegūstam

$$Z(x) / Y(x) = Z'(x) / Y'(x)$$

3. Nosacījumos $Z(i) = Y(i) * r_i$ ievietojot i un r_i, iegūst lineārus vienādojumus ar nezināmajiem a_i, b_i, kuriem ir koeficienti y_i un z_i:

$$y_{11}a_{k+c-1} + ... + y_{1k+c}a_0 = z_{11}b_c + ... + z_{1c+1}b_0$$

Ja lineārai vienādojumu sistēmai ir atrisinājums, tad izslēdzot pa vienam mainīgajam (ar apzīmēšanas palīdzību) ir iespējams atrast atrisinājumu.