Insinöörimatematiikka: Lineaarialgebra

Mika Hirvensalo
mikhirve@utu.fi

Matematiikan ja tilastotieteen laitos
Turun yliopisto

2024

Avaruuden $\mathbb{R}^3$ tasot

Määritelmä

Olkoon $V \leq \mathbb{R}^n$ aliavaruus ja $\boldsymbol{r} \in \mathbb{R}^n$ jokin vektori. Tällöin sanotaan, että joukko

$$\boldsymbol{r} + V = \{\boldsymbol{r} + \boldsymbol{v} \mid \boldsymbol{v} \in V\}$$

on aliavaruuden V *sivuluokka*.

Lause

$$\boldsymbol{r_1} + V = \boldsymbol{r_2} + V \Leftrightarrow \boldsymbol{r}_1 - \boldsymbol{r}_2 \in V.$$

Määritelmä

Avaruuden $\mathbb{R}^3$ taso on kaksiulotteisen aliavaruuden V sivuluokka.

Avaruuden $\mathbb{R}^3$ tasot

Parametriesitys

$$T = \boldsymbol{r} + L(\boldsymbol{s}_1, \boldsymbol{s}_2) = \{\boldsymbol{r} + c_1\boldsymbol{s}_1 + c_2\boldsymbol{s}_2 \mid c_1, c_2 \in \mathbb{R}\}$$

- Jos vektorit $\boldsymbol{s}_1$ ja $\boldsymbol{s}_2$ *eivät* ole lineaarisesti riippumattomia, ei aliavaruus $L(\boldsymbol{s}_1, \boldsymbol{s}_2)$ ole kaksiulotteinen eikä tällöin kyseessä ole taso.
- Vektoreita $\boldsymbol{s}_1$ ja $\boldsymbol{s}_2$ sanotaan tason T suuntavektoreiksi ja vektoria $\boldsymbol{r}$ tason T paikkavektoriksi.
- Käyttökelpoinen tason T pisteiden generoimiseksi.
- Parametrimuodosta hankala selvittää, onko $\boldsymbol{x} \in T$.
- Hankala selvittää, ovatko kaksi tasoa samat.

Avaruuden $\mathbb{R}^3$ tasot

Normaalimuoto

$$T = \{\boldsymbol{r} + \boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{R}^3, \boldsymbol{n} \cdot \boldsymbol{x} = 0\} = \{\boldsymbol{x} \in \mathbb{R}^3 \mid (\boldsymbol{x} - \boldsymbol{r}) \cdot \boldsymbol{n} = 0\}$$

Vektoria $\boldsymbol{n}$ kutsutaan tason T normaalivektoriksi.

Koordinaattimuoto

Merkitsemällä $\boldsymbol{n} = (a, b, c)$, $\boldsymbol{x} = (x, y, z)$ ja $\boldsymbol{r} = (r_1, r_2, r_3)$ saadaan yhtälö $(\boldsymbol{x} - \boldsymbol{r}) \cdot \boldsymbol{n} = 0$ muotoon
$a(x - r_1) + b(y - r_2) + c(z - r_3) = 0$, ja edelleen

$$ax + by + cz = d,$$

missä $d = ar_1 + br_2 + cr_3$.

- Käyttökelpoinen kysymyksen $\boldsymbol{x} \in T$? ratkaisemiseksi
- Hankala tason pisteiden generoimiseksi.

Avaruuden $\mathbb{R}^3$ tasot

Kolme pistettä

Jos avaruuden $\mathbb{R}^3$ pisteet $\boldsymbol{p}_1$, $\boldsymbol{p}_2$ ja $\boldsymbol{p}_3$ eivät ole samalla suoralla, ne määrittävät tason T yksikäsitteisesti.

Huomautus

Pisteet $\boldsymbol{p}_1$, $\boldsymbol{p}_2$ ja $\boldsymbol{p}_3$ ovat samalla suoralla tarkalleen silloin kun $\boldsymbol{p}_3 - \boldsymbol{p}_1$ ja $\boldsymbol{p}_2 - \boldsymbol{p}_1$ ovat lineaarisesti riippuvat.

Määritelmä

Tasojen T_1 ja T_2 välisellä kulmalla tarkoitetaan niiden normaalivektorien välistä kulmaa.

Avaruuden $\mathbb{R}^3$ suorat

Määritelmä

Avaruuden $\mathbb{R}^3$ suora on yksiulotteisen avaruuden sivuluokka.

Parametrimuoto

$$L = \boldsymbol{r} + L(\boldsymbol{s}) = \{\boldsymbol{r} + c\boldsymbol{s} \mid c \in \mathbb{R}\}$$

- Vektoria $\boldsymbol{r}$ kutsutaan suoran L paikkavektoriksi ja vektoria $\boldsymbol{s}$ sen suuntavektoriksi.
- Käyttökelpoinen suoran pisteiden generoimiseksi.
- Hankala kysymyksen $\boldsymbol{x} \in L$ ratkaisemiseksi.

Avaruuden $\mathbb{R}^3$ suorat

Merkintä

$\boldsymbol{r} = (x_0, y_0, z_0)$ ja $\boldsymbol{s} = (a, b, c)$, jolloin

$$L = \{(x_0, y_0, z_0) + t(a, b, c) \mid t \in \mathbb{R}\},$$

jolloin suoran pisteet ovat muotoa
$(x, y, z) = (x_0 + ta, y_0 + tb, z_0 + tc)$, josta $t = \frac{x-x_0}{a} = \frac{y-y_0}{b} = \frac{z-z_0}{c}$

Koordinaattimuoto

$$\frac{x - x_0}{a} = \frac{y - y_0}{b} = \frac{z - z_0}{c}$$

Virheet tiedonsiirrossa

Esimerkki

- ”Pysäyttäkää auto JBN–372”
- ”Pysäyttäkää auto IPM–372”
- JBN $\rightarrow$ ”Jaakko – Bertta – Niilo”
- IPM $\rightarrow$ ”Ilmari – Pekka – Mika”
- Redundantti informaatio parantaa luotettavuutta

Tiedonsiirto

- Sähkömagneettinen säteily
- Ääniaallot
- Analoginen $\leftrightarrow$ digitaalinen
- Digitaalisessa muodossa informaation suojaaminen virheiltä on helpompaa.

Digitaalinen informaatio

Audio CD-standardi

- Kaksi äänikanavaa, 44100 Hz, 16 bitin näytteet.
- $2^{16} = 65536$
- $2 \cdot 44100 \cdot 16 = 1411200$ bit/s $= 172{,}266$ KB/s
- 5 minuuttia vaatii $5 \cdot 60 \cdot 172,266$ KB ≈ 50 MB
- 74 minuuttia vaatii $74 \cdot 60 \cdot 172,266$ KB ≈ 746 MB

4K kuvaformaatti

- $3840 \times 2160 = 8294400$ pikseliä
- Joka pikseliä varten RGB-komponentit vaativat $3 \cdot 8 = 24$ bittiä.
- Yhteensä $24 \cdot 8294400$ bit ≈ 23 MB
- 25 kuvaa sekunnissa vaatii n. 593 MB/s

Digitaalinen

Digitaalisuus

Digitaalisesti esitettävä informatio merkitsee sitä, että ainoastaan äärellinen määrä erilaisia symboleita on käytettävissä.
Minimalistisessa tapauksessa jolloin symboleja on vain kaksi, sanotaan informaation olevan binääristä. Binäärisen informaation perusyksikkö on *bitti*, jolla voi olla arvo 0 tai 1.
Laajempia symbolijoukkoja voidaan esittää bittijonoilla.
Esimerkiksi kahden bitin jonoilla voidaan esittää neljä erilaista symbolia: 00, 01, 10, ja 11.

Digitaalinen tiedonsiirto

Monenlaiset häiriötekijät voivat aiheuttaa virheitä tiedonsiirtoon, jolloin digitaalinen viesti 1110100111010111 voi muuntua esim. muotoon 1110100111010101. Virheellinen viesti pitäisi voida tunnistaa ja siitä pitäisi voida päätellä alkuperäinen.

Virheitä korjaavat koodit

Esimerkki: Pariteettibitti

Lisätään 7-pituisten bittijonojen perään 0 tai 1 siten, että ykkösten määrä tulee olemaan parillinen. Esimerkiksi $0010100 \mapsto 00101000$ ja $0101100 \mapsto 01011001$. Jos näin saaduissa jonoissa yksi bitti vaihtuu, voidaan todeta virhe mutta ei palauttaa alkuperäistä.

Esimerkki: Toistokoodi

$0 \to 000$, $1 \to 111$, jolloin esimerkiksi

$$01001 \mapsto 000111000000111.$$

Tällöin yksi virhe muuntaa viestin esim. muotoon

$$000111000000101,$$

joka voidaan dekoodata viestiksi $000111000000111 \to 01001$.

Virheitä korjaavat koodit

Toistokoodi

$0 \to 000$, $1 \to 111$. Hintana kolminkertainen lähetysaika,1 virhe korjattavissa / 3-pituinen lohko

Esimerkki

Koodaus $00 \mapsto 00000$ $01 \mapsto 00111$, $10 \mapsto 11100$, $11 \mapsto 11011$. hintana $2,5$-kertainen lähetysaika, 1 virhe korjattavissa / 5-pituinen lohko.

Määritelmä

- $\mathbb{F}_2 = \{0, 1\}$ on kahden alkion kunta
- Esim. $0 + 1 = 1$, $1 + 1 = 0$.
- n-ulotteinen vektoriavaruus $\mathbb{F}_2^n$ yli kunnan $\mathbb{F}_2$ koostuu n-pituisista järjestetyistä kunnan $\mathbb{F}_2$ jonoista (bittijonoista): $\mathbb{F}_2^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{F}_2\}$, jossa yhteenlasku ja skalaarikertolasku on määritelty kuten reaalisessa vektoriavaruudessa.

Määritelmä

Vektoreiden $\boldsymbol{x} = (x_1, \ldots, x_n)$ ja $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$
Hamming-etäisyys on

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = |\{i \mid x_i \neq y_i\}|$$

Vektorin $\boldsymbol{x}$ Hamming-paino määritellään $w_H(\boldsymbol{x}) = d_H(\boldsymbol{x}, \boldsymbol{0})$.

Esimerkki

$$d_H(00000, 00111) = 3, d_H(00000, 11100) = 3,$$
$$d_H(00111, 11100) = 4, d_H(11100, 11011) = 3$$
$$d_H(00111, 11011) = 3 \text{ ja } d_H(00000, 11011) = 4$$

Virheitä korjaavat koodit

Huomautus

- Hamming-etäisyys toteuttaa metriikan aksioomat
- $\boldsymbol{e}_i = (0, \ldots, 1, \ldots, 0)$
- Jos $d_H(\boldsymbol{x}, \boldsymbol{y}) \geq 3$ on $\boldsymbol{x}' = \boldsymbol{x} + \boldsymbol{e}_i$ edelleen lähempänä vektoria $\boldsymbol{x}$ kuin vektoria $\boldsymbol{y}$, joten virhe $\boldsymbol{x} \mapsto \boldsymbol{x}' = \boldsymbol{x} + \boldsymbol{e}_i$ voidaan korjata dekoodaamalla $\boldsymbol{x}'$ vektoriksi $\boldsymbol{x}$.
- Yleistys: Jos $d_H(\boldsymbol{x}, \boldsymbol{y}) \geq 2t + 1$, voidaan t:n virheen jälkeen saatu $\boldsymbol{x}'$ palauttaa vektoriksi $\boldsymbol{x}$, sillä $\boldsymbol{y}$ on silti vielä kauempana.

Virheitä korjaavat koodit

Määritelmä

$C \subset \mathbb{F}_2^n$ on t virhettä korjaava koodi, jos $d_h(\boldsymbol{x}, \boldsymbol{y}) \geq 2t + 1$ aina kun $\boldsymbol{x} \neq \boldsymbol{y} \in C$.

Periaate

Viestit $\boldsymbol{x} \in \mathbb{F}_2^m$ (pituus m) koodataan *koodisanoiksi* (pituus $n > m$), jotka ovat etäällä toisistaan. Mikäli tiedonsiirtokanava aiheuttaa virheitä koodisanoissa, on toivottavaa että muuttuneet viestit yhä muistuttaisivat eniten lähetettyjä koodisanoja ja voitaisiin täten dekoodata.

Määritelmä

Koodia C sanotaan (n, M, d)-koodiksi, jos koodisanojen pituus on n, $|C| = M$, ja erisuurten koodisanojen Hamming-etäisyys on vähintään d.

Periaate

Kuvataan lyhyemmät jonot (pituus m) bijektiivisesti pidemmiksi jonoiksi (pituus n),

$$\mathbb{F}_2^m \to C \subset \mathbb{F}_2^n$$

siten että kaikkien $\boldsymbol{x} \neq \boldsymbol{y} \in C$ Hamming-etäisyys on ainakin $2t + 1$. Mikäli kuvavektorin lähetys tiedonsiirtokanavassa $\boldsymbol{x} \mapsto \boldsymbol{x}' \notin C$ tuottaa korkeintaan t virhettä, voidaan alkuperäinen vektori $\boldsymbol{x}$ saada yksikäsitteisesti lähimpänä Hamming-etäisyyden vektorina jolle $\boldsymbol{x} \in C$.

Ongelmia

- Miten valita *koodisanojen* joukko $C \subseteq \mathbb{F}_2^n$ siten että $d_H(\boldsymbol{x}, \boldsymbol{y})$ olisi suuri aina kun $\boldsymbol{x} \neq \boldsymbol{y} \in \mathbb{F}_2^m$.
- Miten laskea koodaus $\mathbb{F}_2^m \to C$ tehokkaasti?
- Miten laskea dekoodaus $\mathbb{F}_2^n \to C$ tehokkaasti?
- Miten laskea kuvaus $C \to \mathbb{F}_2^m$ tehokkaasti?

Ongelmia

- Monissa sovelluksissa dekoodaus $\mathbb{F}_2^n \to C$ on hankalinta toteuttaa tehokkaasti.
- Osoittautuu, että informaatiosuhde paranee lohkon pituutta kasvatettaessa, mutta laskennalliset ongelmat kasvavat myös.

Virheitä korjaavat koodit

Esimerkki: Taulukointi

Koodi: $\{00000, 00111, 11100, 11011\}$, dekoodaus

$$
\begin{aligned}
00000 &\to 00000 \\
00001 &\to 00000 \\
00010 &\to 00000 \\
00011 &\to 00111 \\
&\dots \\
01001 &\to 00000 \text{ tai } 11011 \\
&\dots \\
11110 &\to 11100 \\
11111 &\to 11011
\end{aligned}
$$

Bittijonon pituuden ollessa $n \geq 30$ on taulukoinnin mahdollisuus suljettu käytännössä pois: $2^{30} = 1\,073\,741\,824$

Määritelmä

Koodi $C \in \mathbb{F}_2^n$ on *lineaarinen*, jos $C \subseteq \mathbb{F}_2^n$ on aliavaruus. Tällöin $\alpha \boldsymbol{x} + \beta \boldsymbol{y} \in \mathbb{C}$ aina, kun $\boldsymbol{x}$, $\boldsymbol{y} \in C$ ja α, $\beta \in \mathbb{F}_2 = \{0, 1\}$.

Huomautus

Jos C on avaruuden $\mathbb{F}_2^n$ m-ulotteinen aliavaruus ($m < n$), on sillä kanta $\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m\} \subset \mathbb{F}_2^n$ ja jokainen $\boldsymbol{c} \in C$ voidaan esittää yksikäsitteisesti muodossa

$$\boldsymbol{c} = x_1 \boldsymbol{c}_1 + \ldots x_m \boldsymbol{c}_m = (x_1, \ldots, x_m) \begin{pmatrix} \boldsymbol{c}_1 \\ \ldots \\ \boldsymbol{c}_m \end{pmatrix} = (x_1, \ldots, x_m) G.$$

Matriisia $G = \begin{pmatrix} \boldsymbol{c}_1 \\ \ldots \\ \boldsymbol{c}_m \end{pmatrix}$ kutsutaan koodin *generoijamatriisiksi*.

Huomautus

Lineaarisen koodin *koodausfunktio* $\mathbb{F}_2^m \to \mathbb{F}_2^n$ voidaan esittää matriisikertolaskuna

$$\boldsymbol{c} = \boldsymbol{x}G,$$

missä $\boldsymbol{x} \in \mathbb{F}_2^m$ on lähetettävä viesti (esitetään rivivektorina), G on $m \times n$-matriisi yli kunnan $\mathbb{F}_2$, ja $\boldsymbol{c} \in C \subset \mathbb{F}_2^n$ on koodattu viesti. Tällöin kyseessä on $(n, 2^m, d)$-koodi, jossa minimietäisyys d riippuu generoijamatriisin ominaisuuksista.

Määritelmä

Lineaarikoodia, jonka pituus on n ja dimensio m ja minimietäisyys d, sanotaan $[n, m, d]$-koodiksi. Jos minimietäisyyttä ei ilmoiteta, sanotaan koodia $[n, m]$-koodiksi.

Lause

Jos $C \subseteq \mathbb{F}_2^n$, on $[n, m]$-koodi, on olemassa sellainen $(n - m) \times n$-matriisi H, että

$$C = \{\boldsymbol{x} \in \mathbb{F}_2^n \mid H\boldsymbol{x}^T = 0\}.$$

Matriisia H kutsutaan koodin C tarkistusmatriisiksi. Jos G on koodin generoijamatriisi, on $GH^T = O$ nollamatriisi.

Huomautus

Tarkistusmatriisi voidaan muodostaa generoijamatriisista ja päinvastoin.

Virheen havaitseminen

- Jos $\boldsymbol{x} \in \mathbb{F}_2^n$ toteuttaa $H\boldsymbol{x}^T = \boldsymbol{0}$, on $\boldsymbol{x} \in C$ koodisana, eikä virhettä tulkita tapahtuneen.
- $H\boldsymbol{x}^T \neq \boldsymbol{0}$, tulkitaan virhe tapahtuneeksi.

Syndromit

Jos $\boldsymbol{c} \in C$ ja $\boldsymbol{x} = \boldsymbol{c} + \boldsymbol{e}$ on "virheellinen", on kuitenkin $H\boldsymbol{x}^T = H(\boldsymbol{c} + \boldsymbol{e})^T = H\boldsymbol{c}^T + H\boldsymbol{e}^T = H\boldsymbol{e}^T$. Virheenkorjaus perustuu vektoreihin $H\boldsymbol{e}^T$. Näitä kutsutaan *syndromeiksi*. Ns. Syndromipankki muodostetaan tallentamalla muistiin Hamming-painon suhteen kaikkein kevyimmät syndromin tuottavat vektorit $\boldsymbol{x} \in \mathbb{F}_2^n$. Dekoodaus perustuu näihin, *johtajiksi* kutsuttuihin vektoreihin.

Dekoodaus

- Vastaanotettaessa (mahdollisesti) virheellinen vektori $\boldsymbol{x} \in \mathbb{F}_2^n$, lasketaan $\boldsymbol{e} = H\boldsymbol{x}^T$ ja valitaan syndromipankista vektori $\boldsymbol{s}$ joka toteuttaa ehdon $H\boldsymbol{s}^T = \boldsymbol{e}$.
- Dekoodataan vektori $\boldsymbol{x}$ vektoriksi $\boldsymbol{x} - \boldsymbol{s}$.

Esimerkki: Hammingin $[7,4]$-koodi

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

on $[7,4]$-koodin tarkistusmatriisi (Huomioi että H:n sarakkeet ovat lukujen 1–7 binääriesitykset). Generoijamatriisi voidaan muodostaa ehdon $GH^T = O$ perusteella, mutta dekoodaus edellyttää syndromipankin luomista. Voidaan valita

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

Syndromit

$$
\begin{aligned}
H(0000000)^T &= (000)^T \\
H(0000001)^T &= (001)^T \\
H(0000010)^T &= (010)^T \\
&\dots \\
H(1000000)^T &= (110)^T
\end{aligned}
$$

Esimerkki: Hammingin koodi

$$(1,0,1,1)\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (1,0,1,1,0,1,0).$$

Virhe lähetyksessä

$(1,0,1,1,0,1,0) \mapsto (1,0,1,1,0,0,0)$

Dekoodaus

Esimerkki

$$H(1,0,1,1,0,0,0)^T = (0,1,0),$$

jota vastaava syndromipankin alkio on $(0,0,0,0,0,1,0)$.
Dekoodattu vektori on siis $(1,0,1,1,0,1,0)$.

Lineaariset koodit

Hammingin koodi

- $[7, 4, 3]$-koodi
- Hintana $7/4 = 1.75$-kertainen lähetysaika
- 1 virhe korjattavissa / 7- pituinen lohko

Hammingin koodit

Jokaista $r \geq 1$ kohti on olemassa $[2^r - 1, 2^r - r - 1, 3]$-koodi, jonka tarkistusmatriisi muodostetaan kaikista r-bittisten lukujen $\neq 0$ binääriesityksistä.

Huomautus

Hammingin koodit korjaavat lähtökohtaisesti vain yhden virheen, mutta osoittavat, että informaatiosuhde voidaan saada korkeaksi: Hintana $(2^r - 1)/(2^r - r - 1)$-pituinen lähetysaika

Ongelmia

- Useampien kuin yhden virheen korjaus.
- Informaatiosuhdetta voidaan parantaa lohkon pituutta kasvattamalla, mutta tällöin myös laskennalliset ongelmat suurenevat.
- Informaatiosuhteen parantaminen teoreettisesti.
- Maksimaalisen informaatiosuhteen etsiminen.
- Generoija- tai tarkistusmatriisin esittäminen kompaktisti.

Lineaariset koodit

Ratkaisuja

- BCH-koodit
- Reed-Solomon -koodit
- Reed-Muller -koodit
- Hadamardin koodit