Diskret matematik 2018-05-03 #16

Def^n Låt $\mathcal{C} \subseteq \{0,1\}^n$ vara en kod. Ett binärt ord x sägs rättas till kodordet $c \in \mathcal{C}$ enligt närmaste-granne-principen (NGP) om c är det unika ordet i $\mathcal{C}$ som ligger närmast x, dvs om
$$d(x,c') > d(x,c) \text{ för alla andra } c' \in \mathcal{C}$$

Om det finns mer än ett kodord $c \in \mathcal{C}$ som ligger närmast x säger vi att rättningen misslyckades.

Def^n En kod $\mathcal{C} \subseteq \{0,1\}^n$ sägs vara E-felsrättande om det för varje kodord $c \in \mathcal{C}$ och varje godtyckligt binärt ord $x \in \{0,1\}^n$ som kan fås från c genom att flippa $\leq E$ bitar, dvs med $d(x,c) \leq E$, gäller att x rättas till c under NGP.

Ex
1. Koden $\mathcal{C}_1 = \{00, 01, 10, 11\}$ är INTE 1-felsrättande.
2. Koden $\mathcal{C}_2 = \{000, 110, 011, 101\}$ är INTE 1-felsrättande.

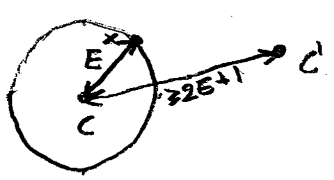
Varför?
1. t.ex. om vi tar $c = 00$ och flippar sista biten $\Rightarrow x = 01$, då rättar NGP x till x, inte c.
2. t.ex. om $c = 000$ och $x = 010$ (så $d(x,c) \leq 1$), då misslyckas NGP-rättningen.

Ex Koden $\mathcal{C}_3 = \{000000, 111000, 001110, 110011\}$ är 1-felsrättande

$4_{\text{kodord}} \cdot 6_{\text{bitar}} = 24$ NGP-rättningar att kolla.

Sats En kod $\mathcal{C} \subseteq \{0,1\}^n$ med minimidistans δ är E-felsrättande så länge $\delta \geq 2E+1$

Hur många beräkningar för att bestämma δ?
För $\mathcal{C}_3$: $\binom{|\mathcal{C}_3|}{2} = \binom{4}{2} = \frac{4 \cdot 3}{2} = 6$



$\Rightarrow d(x,c') \geq (2E+1) - E \geq E+1$
för $c' \in \mathcal{C}$, $c' \neq c$

Linjära koder

Vill:

(1) ha korta kodord
(2) kunna rätta ord snabbt
(3) ha stor minimidistans, så att många fel går att rätta.
(4) ha många kodord → ett "rikt språk".

Vi använder linjär algebra "över $\mathbb{Z}_2$", dvs med skalärerna 0, 1 modulo 2. $(\mathbb{Z}_2\ +)$

$0+0=0 \quad 1+0=1=0+1 \quad 1+1=0 \quad \boxed{\text{OBS}}\ -1=1$

$\mathbb{R}^3 \ni (0,2,5)$

$\mathbb{Z}_2^3 \ni (0,1,0)$

Så $\{0,1\}^n$ identifierar vi med $\mathbb{Z}_2^n$ och vi gör operationen $+$ på $\mathbb{Z}_2^n$ i varje komponent.

$$\begin{array}{r} (0,0,1,1,0) \\ +(1,0,1,0,1) \\ \hline =(1,0,0,1,1) \end{array}$$

<u>Def$^{\underline{n}}$</u> En (icke-tom) mängd $\mathcal{C} \subseteq \mathbb{Z}_2^n$ sägs vara en linjär kod av längd n om $\mathcal{C}$ är en delgrupp till $(\mathbb{Z}_2^n, +)$, dvs om $x+y \in \mathcal{C}$ för alla $x, y \in \mathcal{C}$

<u>Ex</u> $\mathcal{C}_2 = \{000, 110, 011, 101\} \subseteq \mathbb{Z}_2^3$ är en linjär kod.

<u>Ex</u> $\mathcal{C}_3 = \{000000, 111000, 001110, 110011\}$ är INTE linjär
$\quad 111000 + 001110 = 110110 \notin \mathcal{C}_3$

Enligt Lagrange så måste storleken $|\mathcal{C}|$ av en linjär kod av längd n dela $|\mathbb{Z}_2^n| = 2^n$,
dvs $|\mathcal{C}| \mid 2^n$

Alltså är $|\mathcal{C}| = 2^k$ för något k, enligt aritmetikens fundamentalsats.

<u>Def$^{\underline{n}}$</u> Om $\mathcal{C}$ är en linjär kod och $|\mathcal{C}| = 2^k$ säger vi att koden har dimension k.

<u>Sats</u> Låt $\mathcal{C} \subseteq \mathbb{Z}_2^n$ vara en linjär kod. Då ges minimidistansen δ av
$$\delta = \min\{d(x, \underbrace{00\ldots0}_{\underline{0}}) : x \in \mathcal{C},\ x \neq \underline{0}\}$$

$=$ det minsta antalet 1:or bland de nollskilda orden.

<u>Bevis</u> $\quad d(x,y) = d(x-y,\underline{0})$ i $\mathbb{Z}_2^n$

(för $d(x,y)=d(x+t,y+t)$ för alla $t\in\mathbb{Z}_2^n$) och $x-y\in\mathcal{C}$ eftersom $\mathcal{C}$ är en delgrupp (så är sluten). ∎

<u>Ex.</u> Låt H vara matrisen

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

Då är

$\mathcal{C}=\{x\in\mathbb{Z}_2^5 : Hx=\underline{0}\}$, dvs nollrummet till H, en linjär kod.

För: Denna mängd är sluten under $+$.
Varför? Om $x,y\in\mathcal{C}$, då ligger $x+y\in\mathcal{C}$
Varför? För
$$H(x+y)=Hx+Hy=\underline{0}+\underline{0}=\underline{0}$$

Om vi vill skriva ned orden i $\mathcal{C}$: vi löser systemet

$$\begin{pmatrix}1&0&0&1&1\\0&1&0&1&0\\0&0&1&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\x_5\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$$

fria variabler

$$\begin{aligned}x_1+x_4+x_5&=0\\x_2+x_4&=0\\x_3+x_5&=0\end{aligned}$$

$$\begin{array}{c}x_1\\x_2\\x_3\\x_4\\x_5\end{array}\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\\0\\1\end{pmatrix},\begin{pmatrix}0\\1\\1\\1\\1\end{pmatrix}$$

<u>Sats & def^n</u>

Låt H vara en binär matris med n kolonner. Då är

$\mathcal{C}=\{x\in\mathbb{Z}_2^n : Hx=\underline{0}\}$

en linjär kod av längd n. H kallas en kontrollmatris/parity-check matris för $\mathcal{C}$.

Säg att vi har skapat en kod $\mathcal{C}\subseteq\mathbb{Z}_2^n$ från en kontrollmatris H.

Vi tar emot ett ord $x\in\mathbb{Z}_2^n$.

→ Hur kollar vi om $x\in\mathcal{C}$?
- Kolla om $Hx=\underline{0}$, enligt def^n

→ Om $Hx\neq\underline{0}$, hur rättar vi ordet?

<u>Sats</u> Om vi har en matris där
- ingen kolonn består enbart av 0:or, <u>OCH</u>
- inga två kolonner är lika,

då är koden $\mathcal{C}$ som har H som kontrollmatris 1-felsrättande.

Bevis Visa att minimidistansen i $\mathcal{C}$ är ≥ 3.
(Om $\delta \geq 2E+1$, då E-felsrättande. Så, $E=1$ ger $\delta \geq 3 \Rightarrow$ 1-felsrätt)

För linj. koder är δ = minsta antalet 1:or i ett nollskilt ord.
Så visa att alla nollskilda ord i $\mathcal{C}$ har ≥ 3 st. 1:or. ∎

Metod (Rätta fel)

Låt $\mathcal{C}$ ha kontrollmatris H och vara 1-felsrättande. Låt oss säga att vi tar emot ordet x.

1) Om $Hx = 0$, då är $x \in \mathcal{C}$ och x rättas till sig självt under NGP.

2) Om $Hx \neq 0$, kolla om det finns någon kolonn h_j i H så att $Hx = h_j$.

Om det finns, ändra på bit nummer j i ordet x.
Detta ger det rättade ordet

Ex Låt H vara matrisen

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

Koden $\mathcal{C}$ från H är 1-felsrättande enligt sats. Vi tar emot $x = 11101$.
Vad rättas detta till?

$$Hx = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$ vilket är kolonn nr 2 i H

Ändra alltså bit nr 2 i x: får ordet 10101

Sats (Egenskaper hos $\mathcal{C}$ från H)

Om H är en kontrollmatris för en kod $\mathcal{C}$, med n kolonner, då

- är kodens längd n och
- dimensionen av $\mathcal{C}$ är n-rang där
  rang = matrisens rang = största antalet linjärt oberoende kolonner eller rader.

$|\mathcal{C}| = 2^{n-\text{rang}}$