z

Def: Låt vikten $w(z)$ hos ett ord z vara antalet ettor i z. Med andra ord $w(z) = \partial(z, 0)$.

Vi har att (linjär kod)

$$\partial(x, y) = \partial(x-y, y-y) = \partial(x-y, 0) = w(x-y).$$

Alltså får vi

δ = minsta vikten =
minsta antalet ettor hos
ett ord $\neq 0$.

Ex: C_2 $\quad 000, \underset{w=2}{110}, \underset{w=2}{011}, \underset{w=2}{101}$

$\delta_{C_2} = 2$

Ex: DNA koden är uppbyggd av A, C, G, T och orden har längd 3. Det finns 20 aminosyror så vi behöver 20 kodord. Hur många fel rättar koden?

Lösn: Totalt finns det $64 = 4^3$ möjliga ord. Antalet ord vi kan få genom att ändra i r positioner är $\binom{3}{r}3^r$. Vi får så

$$64 \geq 20 \cdot \left(1 + \binom{3}{1}3 + \ldots + \binom{3}{e}3^e\right)$$

men det ger $e = 0$.

($e=1$ tex ger $64 \geq 20 \cdot (1+9) = 200$)

Koden rättar alltså noll fel.

Konstruktion av linjära koder

Antag att $\overset{x_1}{(a},\overset{x_2}{b},\overset{x_3}{c},\overset{x_4}{d)} \in V^4$ är

en lösning till ekvationssystemet

$$\begin{cases} 1 \cdot x_1 + 0 \cdot x_2 + 1 \cdot x_3 + 0 \cdot x_4 = 0 \\ 0 \cdot x_1 + 1 \cdot x_2 + 1 \cdot x_3 + 1 \cdot x_4 = 0 \end{cases}$$

och att (a', b', c', d') är

en annan lösning

Då är även $(a,b,c,d)+(a',b',c',d')$ $=(a+a',b+b',c+c',d+d')$

en lösning. Vi har att

$$* \quad 1\cdot(a+a')+1\cdot(c+c')=(a+c)+(a'+c')=$$
$$=0+0=0$$

$$* \quad (b+b')+(c+c')+(d+d')=(b+c+d)+(b'+c'+d')=$$
$$=0+0=0$$

vilket visar att $(a+a',b+b',c+c',d+d')$

är en lösning.

Givet ett ekvationssystem kan vi bilda koden av ord som är lösningar till ekvationssystemet. Koden blir en linjär.

paritets matris

$$\begin{cases} 1\cdot x_1 + 0\cdot x_2 + 1\, x_3 + 0\cdot x_4 = 0 \\ 0\cdot x_1 + 1\cdot x_2 + 1\cdot x_3 + 1\cdot x_4 = 0 \end{cases} \qquad \underbrace{\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}}_{H} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}}_{x} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$C = \{ x \in V^4 ; Hx = 0 \}$$

Ex: Med paritetsmatrisen

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \text{ får vi:}$$

$$\begin{cases} x_1 = x_3 \\ x_2 = x_3 + x_4 \end{cases}$$

så x_3, x_4 kan väljas godtyckligt och det ger sedan x_1, x_2.

$$C = \{\overset{x_1 x_2 x_3 x_4}{00\underline{00}},\ \overset{x_1}{0}1\underset{}{\overset{x_3}{\underline{0}}}\underline{1},\ 11\underline{10},\ 10\underline{11}\}$$

C's dimension = antalet möjliga val av x_3, x_4.

Ex 2: Skapa en linjär kod med dimension 8 och längd 5.

Lösn: Vi gör som i förra exemplet

$$\begin{cases} x_1 = x_3 + x_4 \\ x_2 = x_3 + x_5 \end{cases}$$

$$\left(\begin{array}{cc:ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right)$$

Här kan x_3, x_4 och x_5 väljas godtyckligt så vi får $2^3 = 8$ kodord.

$C = \{00\underline{000}, 01\underline{001}, 10\underline{010}, 11\underline{011},$
$11\underline{100}, 10\underline{101}, 01\underline{110}, 00\underline{111}\}$

$x_1 = x_3 + x_4$, $x_2 = x_3 + x_5$

Ex 3 Vad ger matrisen

$$
\begin{array}{l}
1\cdot x_1 + 1\cdot x_4 \leftarrow \\
1\cdot x_2 + 1\cdot x_4 + 1\cdot x_5 \leftarrow \\
1\cdot x_3 + 1\cdot x_5 \leftarrow
\end{array}
\begin{pmatrix} 1 & 0 & 0 & \vdots & 1 & 0 \\ 0 & 1 & 0 & \vdots & 1 & 1 \\ 0 & 0 & 1 & \vdots & 0 & 1 \end{pmatrix}
$$

för kod?

$x_1 = x_4$
$x_2 = x_4 + x_5$
$x_3 = x_5$

$C = \{000\underline{00}, \overset{w=3}{011\underline{01}}, \underset{w=3}{110\underline{10}}, \underset{w=4}{101\underline{11}}\}$

$3 = w_{min} = \delta \geq 2e + 1$
$\Rightarrow e \leq 1.$

Vad händer om vi stoppar in ett felaktigt ord i systemet?

Tex ordet 00101

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

Eftersom $\partial(01101, 00101) = 1$ så ska ordet rättas till 01101. Felet är därmed i den andra biten.

Tittar vi i paritetsmatrisen

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

kan vi konstatera att $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ är den andra kolumnen. Det här sambandet är inte någon slump. Att ändra ett kodord x i position r svarar mot att byta x mot $x + \underbrace{00\ldots010\ldots0}_{\text{pos } r}$

Eftersom $Hx = 0$ så blir

$$H(x + 0 \ldots 0\underset{\text{pos } r}{1}0 \ldots 0) = Hx + H(0 \ldots 0\underset{\text{pos } r}{1}0 \ldots 0)$$

$$= 0 + H(0 \ldots 0\underset{\text{pos } r}{1}0 \ldots 0)$$

och $H(0 \ldots 0\underset{\text{pos } r}{1}0 \ldots 0)$ ser precis ut som r:te kolumnen i H.

För att det här ska fungera är det viktigt att alla kolumnerna i H är olika.

Ex 4: Om vi i exempel 2 ändrar 2:a biten i kodordet 01001 får vi 00001 och

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

men både kolumn 2 och 5 i H är $\begin{pmatrix}0\\1\end{pmatrix}$. Vi kan därför inte avgöra vilken position

som ska ändras. Vi ser
ju också att 00001 nycket
riktigt även kan fås genom
att ändra position 5 i ordet
00000.
Ett annat problem uppstår om en
av kolumnerna är 0 eftersom
$Hx=0$. (Att ändra motsvarande bit
ger således nya kodord)

Från det här resonemanget ser vi att för att få så många kodord som möjligt vill vi ha så många kolumner som möjligt men om vi ska kunna rätta måste alla kolumner vara olika och ingen 0.
De bästa paritetsmatriserna fås därför om man låter kolumnerna i H vara alla möjliga binära ord utom 0.

Ex 5: I exempel 3 var kolumnerna olika men alla kombinationer fanns inte. Låt oss lägga till de kolumner som saknades

$$H = \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right) \qquad \begin{aligned} x_1 &= x_4 + x_6 + x_7 \\ x_2 &= x_4 + x_5 + x_7 \\ x_3 &= x_5 + x_6 + x_7 \end{aligned}$$

Kodordens längd: $2^3 - 1 = 7$

Antalet kodord: $2^4 = 16 = 2^{2^3-1-3}$

$\{0000000, 1110001, 1010010, 0100011, 0110100, 1000101, 1100110, 0010111, 1101000, 0011001, 0111010, 1001011, 1011100, 0101101, 0001110, 1111111\}$

$\delta = w_{min} = 3. \geq 2 \cdot 1 + 1$ rättar ett fel

(Kallas Hamming kod)

Antal ord som kan fås från ett kodord genom att göra högst ett fel är $7 + 1 = 8$ st. Vi får så $|C| \cdot 8 \leq 2^7$ men $|C| = 2^4$ så vi har faktiskt $|C| \cdot 8 = 2^7$.

En sådan kod kallas perfekt.

Övn 17.4.4: Visa att det inte kan finnas någon perfekt kod med a) $n=5$, $e=1$, b) $n=10$, $e=2$.

Lösn: a) $|C|(1+5)=6\cdot|C|\neq 2^5$ för det finns inget k så att $6\cdot 2^k=2^5$.

b) $$|C|\Big(\underbrace{1+10+\tbinom{10}{2}}_{56}\Big)\neq 2^{10}$$