TSKS21 Signaler, information & bilder

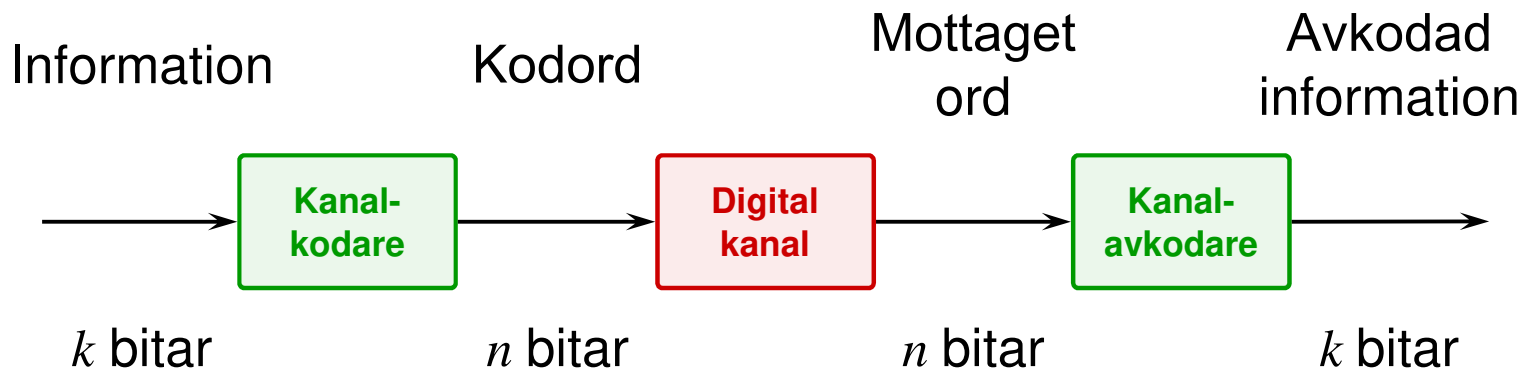
Föreläsning 12

Informationsteori – kanalkodning 2

Mikael Olofsson
Institutionen för Systemteknik (ISY)
Ämnesområdet Kommunikationssystem

LINKÖPINGS UNIVERSITET

Block-koder – Gränser

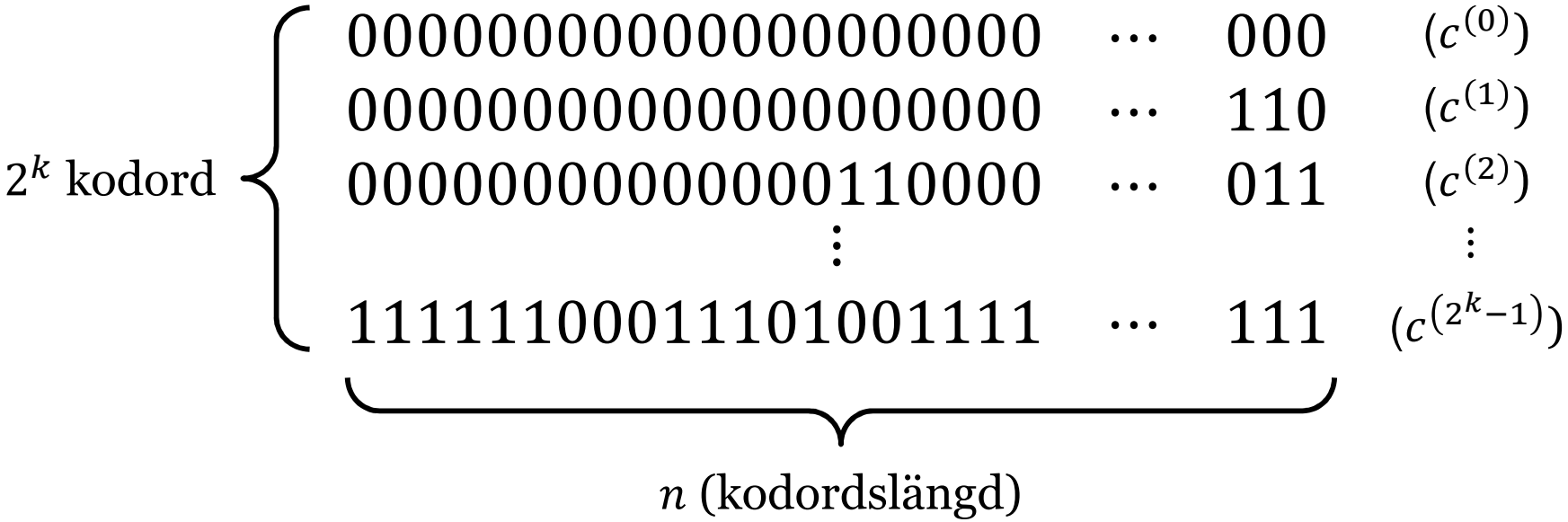


Kanalkodningssatsen (slarvig formulering):

För varje kanal finns det ett C, som vi kallar kanalens kapacitet, och om vi kommunicerar med en takt R så går det att kommunicera med godtyckligt låg resulterande felsannolikhet så länge vi har $R < C$.

Takt: $R = \frac{k}{n}$

Kod med takt $R = k/n$ bpcu



Alla koder med takt $R = k/n$ bpcu

C_0:

000	⋯	000
000	⋯	000
000	⋯	000
	⋮	
000	⋯	000

C_1:

000	⋯	000
000	⋯	000
000	⋯	000
	⋮	
000	⋯	001

C_2:

000	⋯	000
000	⋯	000
000	⋯	000
	⋮	
000	⋯	010

C_3:

000	⋯	000
000	⋯	000
000	⋯	000
	⋮	
000	⋯	011

• • •

C_i:

000	⋯	000
000	⋯	110
000	⋯	011
	⋮	
111	⋯	111

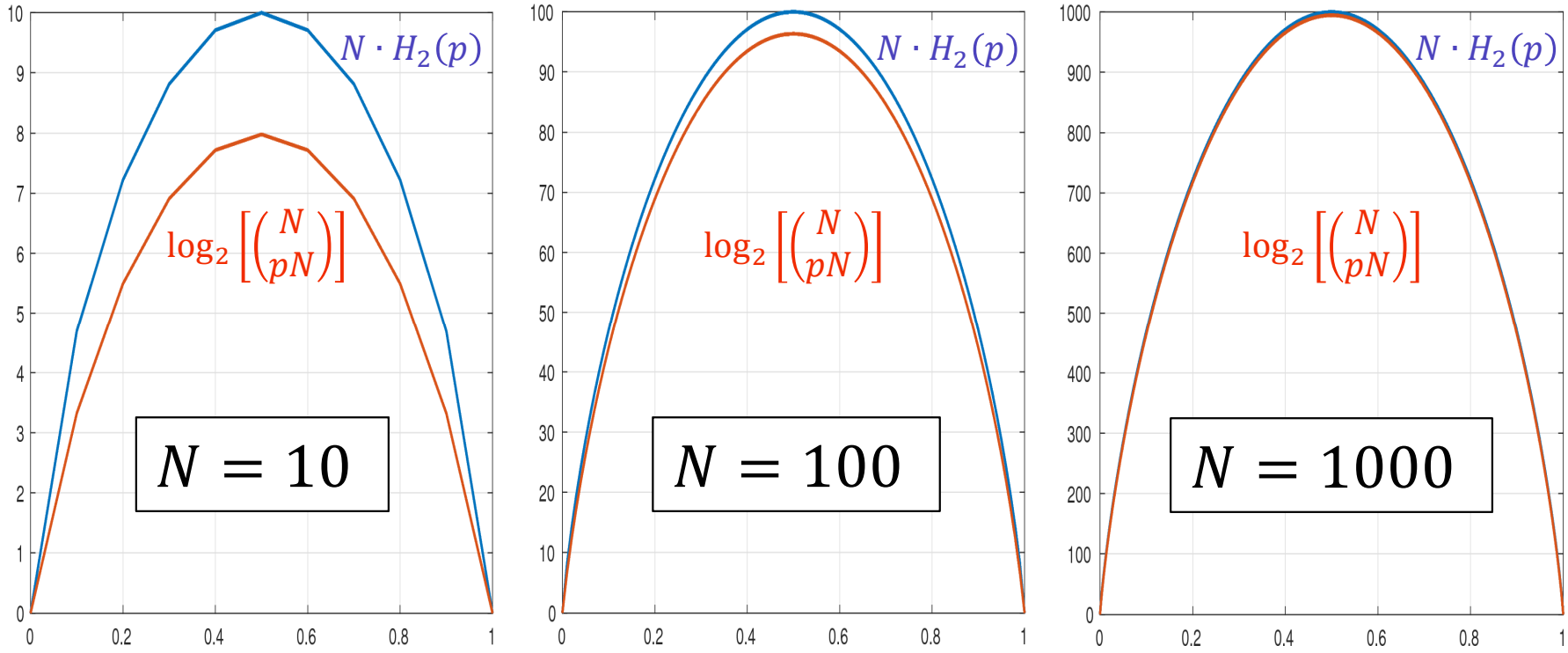
• • •

$C_{2^{kn}-1}$:

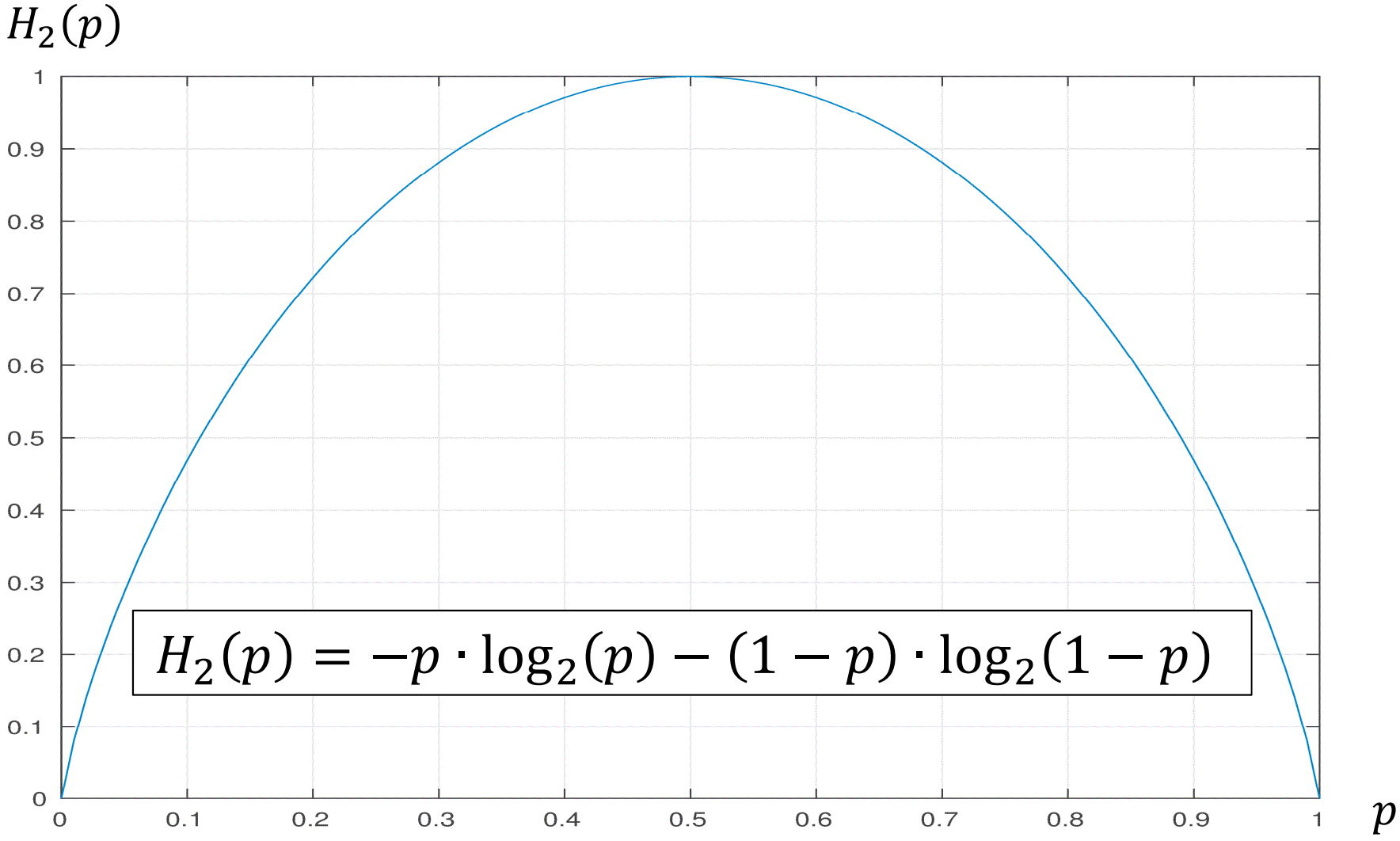
111	⋯	111
111	⋯	111
111	⋯	111
	⋮	
111	⋯	111

Användbar approximation

$$\log_2 \left[\binom{N}{pN} \right] \approx N \cdot H_2(p)$$



Binära entropifunktionen



Kanalkodningssatsen

För en kanal och givna konstanter $\delta > 0$ och $\gamma > 0$, så finns det en kodordslängd n och en kod av denna längd som har takt $R = C - \delta$ och som gör det möjligt att kommunicera med en resulterande felsannolikhet $P_e < \gamma$, där C är kanalens kapacitet.

Den binära kroppen, GF(2)

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Heltalsaritmetik reducerat modulo 2.

Associativa lagen: $(a+b)+c=a+(b+c) \quad \forall\, a,b,c \in \mathrm{GF}(2)$

$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\, a,b,c \in \mathrm{GF}(2)$

Commutativa lagen: $a+b=b+a \quad \forall\, a,b \in \mathrm{GF}(2)$

$a \cdot b = b \cdot a \quad \forall\, a,b \in \mathrm{GF}(2)$

Enhetselement: $\exists\, 0 \in \mathrm{GF}(2): \quad a+0=a \quad \forall\, a \in \mathrm{GF}(2)$

$\exists\, 1 \in \mathrm{GF}(2): \quad a \cdot 1 = a \quad \forall\, a \in \mathrm{GF}(2)$

Inverser: $\exists\, -a \in \mathrm{GF}(2): \quad a+(-a)=0 \quad \forall\, a \in \mathrm{GF}(2)$

$\exists\, a^{-1} \in \mathrm{GF}(2): \quad a \cdot a^{-1} = 1 \quad \forall\, a \in \mathrm{GF}(2), a \neq 0$

Distributiva lagen: $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall\, a,b,c \in \mathrm{GF}(2)$

Binära linjära koder

Definition:
En binär linjär kod är ett linjärt underrum till vektorrummet $\mathrm{GF}(2)^n$.

Ekvivalent definition:
Den binära koden $\mathscr{C}$ kallas linjär om $\bar{c}_1 + \bar{c}_2 \in \mathscr{C}$ gäller för alla $\bar{c}_1, \bar{c}_2 \in \mathscr{C}$.

Generatormatris G:

$$\mathscr{C} = \left\{ \bar{m}G \;\forall\; \bar{m} \in \mathrm{GF}(2)^k \right\}$$

Generatormatris, $k \times n$

Informationsvektor, k bitar

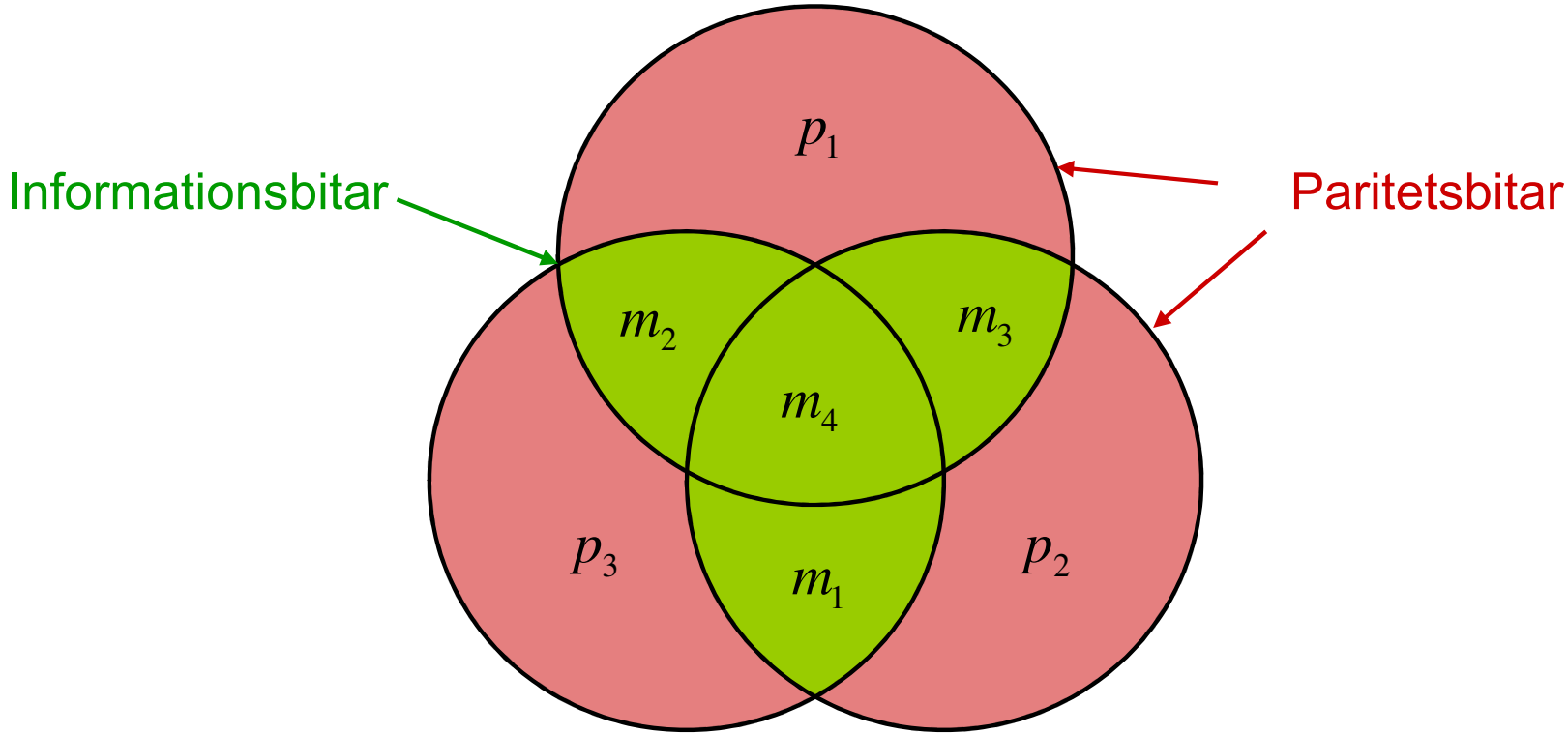
Exempel:

$$G = \begin{pmatrix} 1100 \\ 0111 \end{pmatrix}$$

$\bar{m}$	$\bar{c} = \bar{m}G$
00	0000
01	0111
10	1100
11	1011

Vi kan använda allt från linjär algebra!!

Hamming-[7,4]-koden



Jämn paritet i varje cirkel. $\Rightarrow$

$$\begin{cases} p_1 + m_2 + m_3 + m_4 = 0 \pmod 2 \\ p_2 + m_1 + m_3 + m_4 = 0 \pmod 2 \\ p_3 + m_1 + m_2 + m_4 = 0 \pmod 2 \end{cases}$$

Hamming-[7,4]-koden – Generatormatris

$$\begin{cases} p_1+m_2+m_3+m_4=0 \pmod 2 \\ p_2+m_1+m_3+m_4=0 \pmod 2 \\ p_3+m_1+m_2+m_4=0 \pmod 2 \end{cases} \Rightarrow \begin{cases} p_1=m_2+m_3+m_4 \pmod 2 \\ p_2=m_1+m_3+m_4 \pmod 2 \\ p_3=m_1+m_2+m_4 \pmod 2 \end{cases}$$

Kodord:

$$\bar{c}=(m_1,m_2,m_3,m_4,p_1,p_2,p_3)=(m_1,m_2,m_3,m_4)\left(\begin{array}{cccc:ccc} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{array}\right)$$

Generatormatris, G, på systematisk form

$$G=(I_k,P) \text{ med } P=\begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix}$$

Kod:

$$\mathscr{C}=\left\{\bar{c}=\bar{m}G \;\forall\, \bar{m}\in \mathrm{GF}(2)^4\right\}$$

Dimension:
k = # rader i G. Här 4.

Längd:
n = # kolumner i G. Här 7.

Nollrum och paritetsmatriser

Ett vektorrum (en kod) uttryckt i en bas:

$$\mathscr{C} = \left\{ \overline{m}G \;\forall\; \overline{m} \in \mathrm{GF}(2)^k \right\}$$

Generatormatris ($k \times n$), linjärt oberoende rader.

Ett vektorrum (en kod) uttryckt som nollrummet av en matris:

$$\mathscr{C} = \left\{ \overline{c} \in \mathrm{GF}(2)^n : H\overline{c}^{\mathrm{T}} = \overline{0} \right\}$$

Paritetsmatris ($(n-k) \times n$), linjärt oberoende rader.

Egenskap: $HG^{\mathrm{T}} = 0$

Hamming-[7,4]-koden– Paritetsmatris

$$\begin{cases} m_2+m_3+m_4+p_1=0 \\ m_1+m_3+m_4+p_2=0 \\ m_1+m_2+m_4+p_3=0 \end{cases} \Rightarrow \left(\begin{array}{cccc:ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ p_1 \\ p_2 \\ p_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Paritetsmatris, H, på systematisk form

Jämför med generatormatrisen:

$$G = \left(\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) = (I_4, P)$$

$$H = (P^{\mathrm{T}}, I_3)$$

Allmänt för systematisk form:

$$\begin{cases} G = (I_k, P) \\ H = (P^{\mathrm{T}}, I_{n-k}) \end{cases} \quad \text{eller} \quad \begin{cases} G = (P, I_k) \\ H = (I_{n-k}, P^{\mathrm{T}}) \end{cases}$$

Koder kan ha icke-systematiska generator- och/eller paritetsmatriser.

Vikter och avstånd

Hammingvikt: $w_{\mathrm{H}}(\bar{a})$ # positioner där $\bar{a}$ är 1 (nollskilt).

Hammingavstånd: $d_{\mathrm{H}}(\bar{a},\bar{b})$ # positioner där $\bar{a}$ och $\bar{b}$ är olika.

Samband: $d_{\mathrm{H}}(\bar{a},\bar{b}) = w_{\mathrm{H}}(\bar{a}+\bar{b})$

Minavstånd:

$$d \overset{\text{Definition}}{=} \min_{i\neq j} d_{\mathrm{H}}(\bar{c}_i,\bar{c}_j) = \min_{i\neq j} w_{\mathrm{H}}(\bar{c}_i+\bar{c}_j) \overset{\text{Linjär kod}}{=} \min_{\substack{\bar{c}\in\mathscr{C}\\ \bar{c}\neq\bar{0}}} w_{\mathrm{H}}(\bar{c})$$

Vidare, d är det minsta antal linjärt beroende kolumner in H. (eftersom $H\bar{c}^{\mathrm{T}} = \bar{0}$)

Exempel Hamming-[7,4]:

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

Inga kolumner $= \bar{0} \Rightarrow d > 1$

Inga 2 kolumner är lika

$\bar{h}_1 + \bar{h}_6 + \bar{h}_7 = \bar{0}$

$\Rightarrow d > 2 \Rightarrow d = 3$

Mikael Olofsson

ISY/KS

www.liu.se

LINKÖPINGS UNIVERSITET