

TSKS10 Signaler, information & Kommunikation

Föreläsning 7

Kanalkodning: Exempel på explicita koder

Kanalkodningssatsen

Mikael Olofsson

Institutionen för Systemteknik (ISY)

Ämnesområdet Kommunikationssystem

Enkel felrättande kod – Repetitionskod

Allmänt: För BSC med felsannolikhet $p < \frac{1}{2}$, så ska man avkoda till närmaste kodord.
Det minimerar resulterande felsannolikhet.

Repetitionskod

Info		Kodord
0	$\mapsto$	00 ... 00
1	$\mapsto$	11 ... 11

Repetitionskoder
avkodas med
majoritetsbeslut.

Vid udda längd N :
Avkodningsfel om
vi har minst $\frac{N+1}{2}$ fel.

Exempel, $N = 5$: {00000,11111}

Mottaget		Avkodat
01001	$\mapsto$	0
11100	$\mapsto$	1

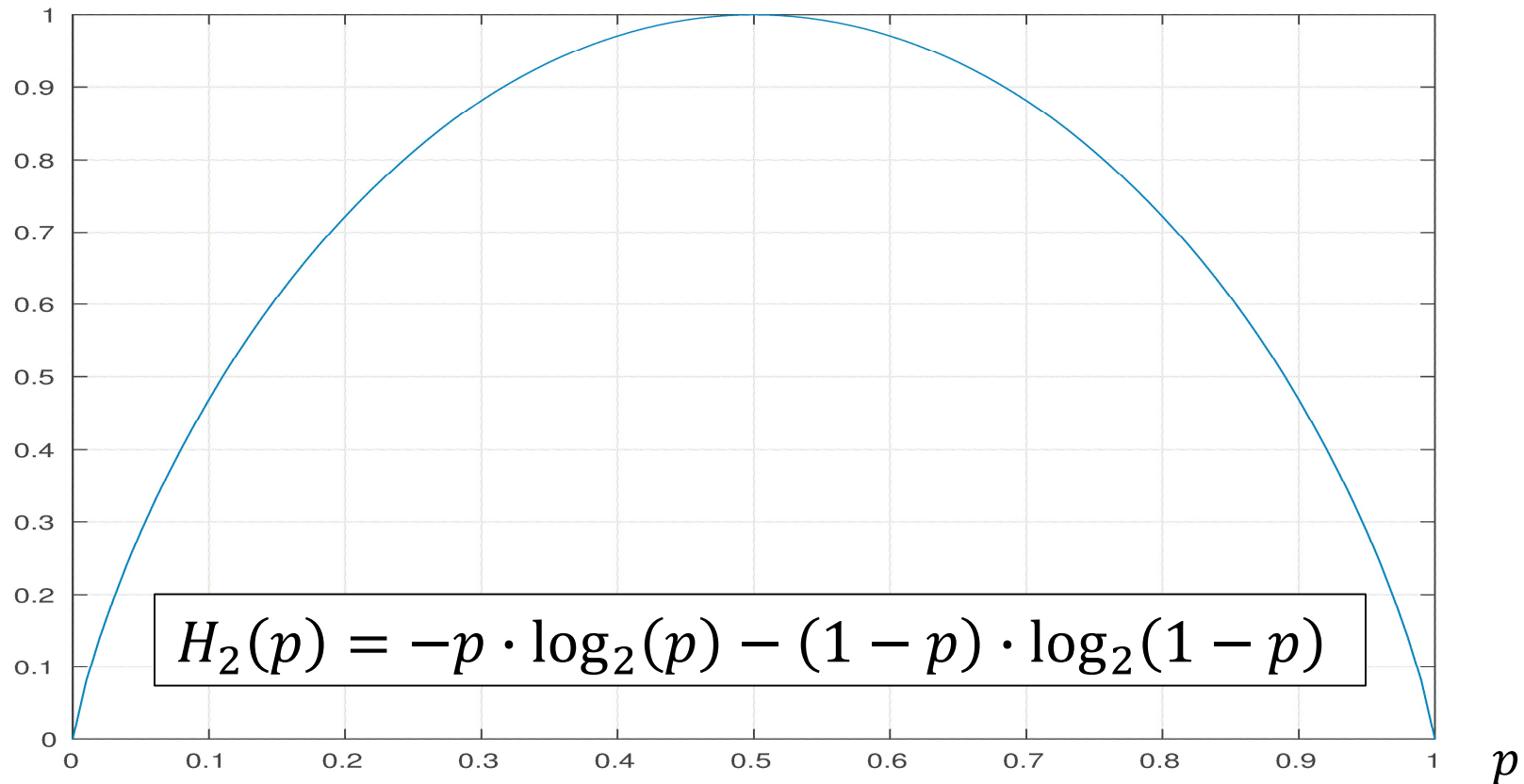
Sannolikhet för avkodningsfel i exemplet:

$$\begin{aligned} P_e &= P\{3,4 \text{ eller } 5 \text{ fel bland } 5 \text{ bitar}\} \\ &= \binom{5}{3} p^3 (1-p)^2 + \binom{5}{4} p^4 (1-p) + \binom{5}{5} p^5 \\ &= 10p^3 - 15p^4 + 6p^5 \end{aligned}$$

Dominerande term

Binära entropifunktionen (Fö 5, slide 8)

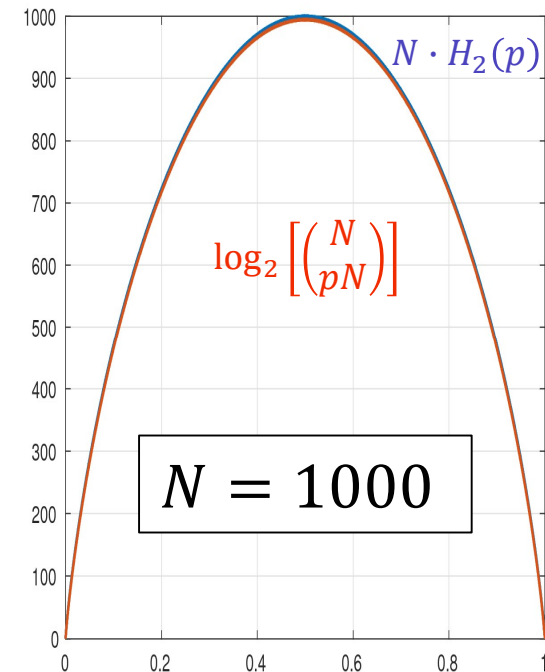
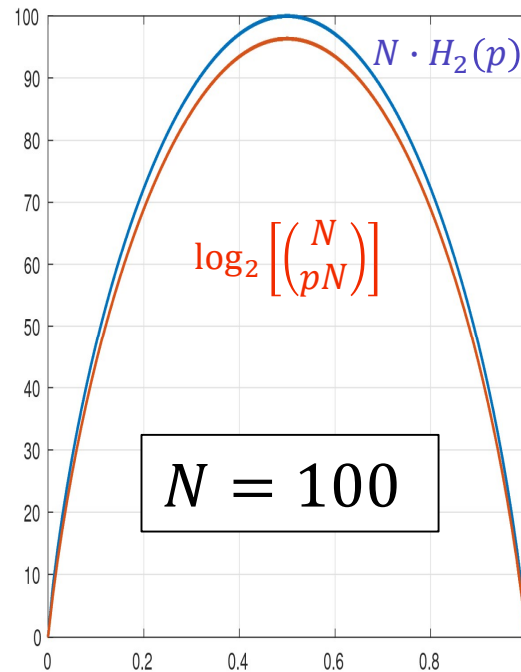
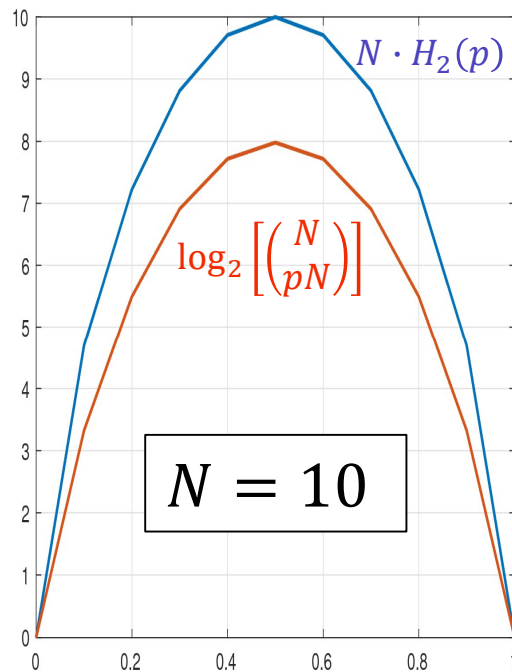
$H_2(p)$



Motsvarar figur 5.2 i kursboken

Användbar approximation (Fö 5, slide 9)

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



Repetitionskoder igen

$$P_e \stackrel{\text{N udda}}{=} \sum_{i=\frac{N+1}{2}}^N \binom{N}{i} p^i (1-p)^{N-i} \stackrel{\text{dominerande term}}{\approx} \binom{N}{(N+1)/2} p^{\frac{N+1}{2}} (1-p)^{\frac{N-1}{2}}$$

$$\stackrel{\text{Approx. slide 4}}{\approx} 2^{NH_2(\frac{N+1}{2N})} p^{\frac{N+1}{2}} (1-p)^{\frac{N-1}{2}} \stackrel{\text{N stort}}{\approx} 2^{NH_2(\frac{1}{2})} p^{\frac{N}{2}} (1-p)^{\frac{N}{2}}$$

$$H_2\left(\frac{1}{2}\right) = 1$$

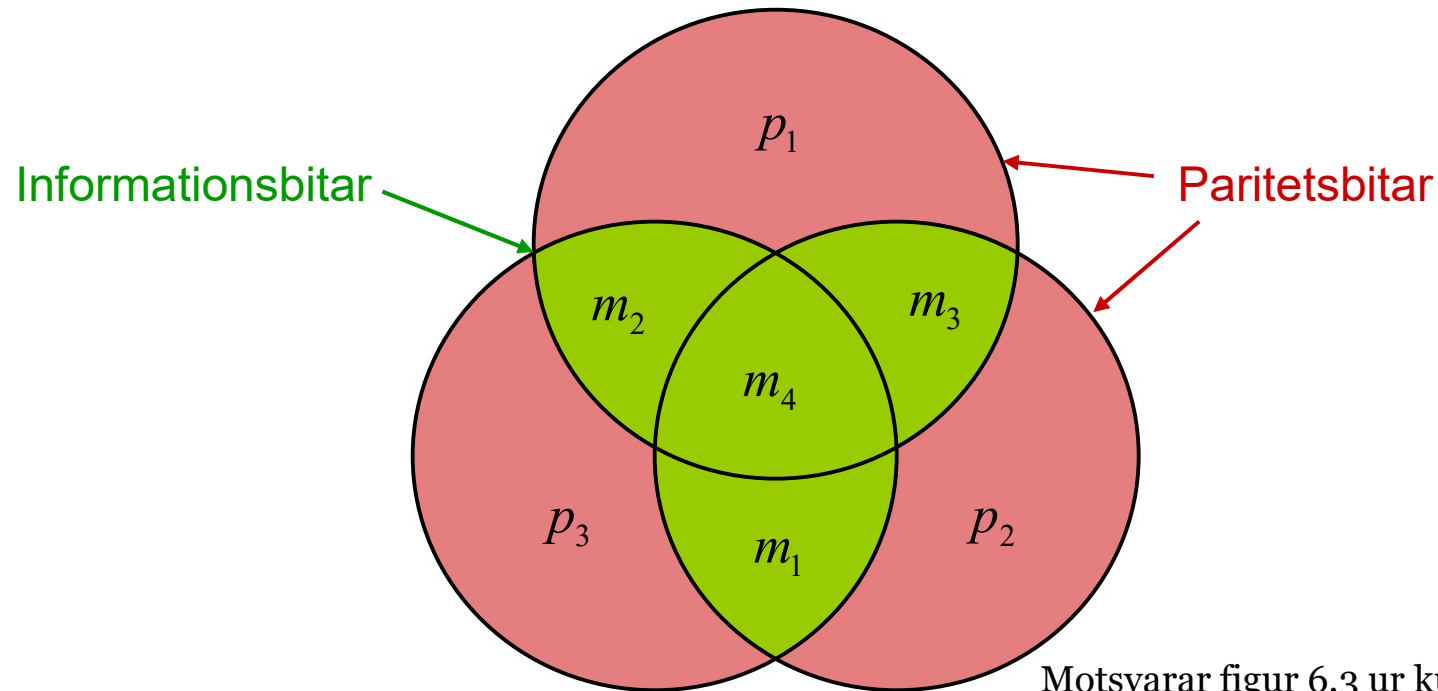
$$= \left(2\sqrt{p(1-p)}\right)^N$$

Alltså storleksordning $p^{N/2}$ (p litet)

Problem: P_e litet kräver N stort. Dåligt kanalutnyttjande.
Kodens takt är $1/N$ informationsbitar per kanalanvändning.

Allmänt K/N informationsbitar per kanalanvändning,
där K är antalet informationsbitar.

Hamming-[7,4]-koden



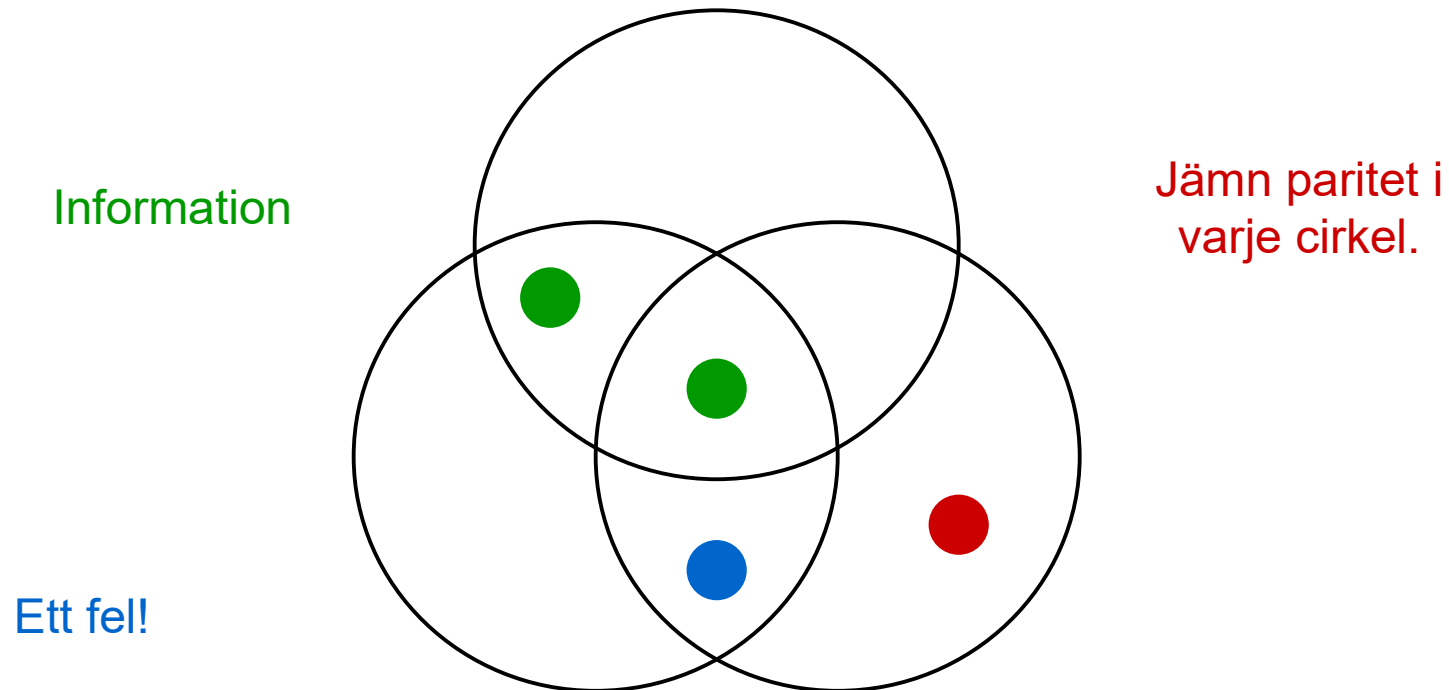
Motsvarar figur 6.3 ur kursboken

Jämn paritet i varje cirkel.

$\Rightarrow$

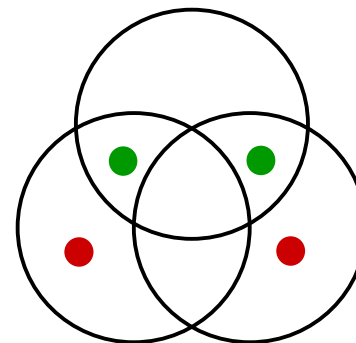
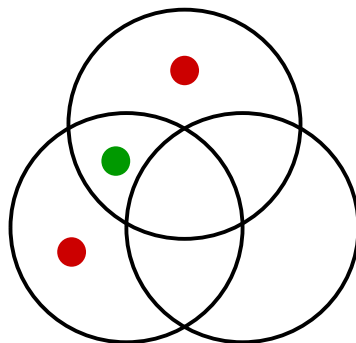
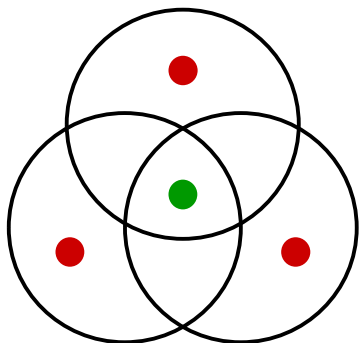
$$\begin{cases} p_1 = m_2 + m_3 + m_4 \pmod{2} \\ p_2 = m_1 + m_3 + m_4 \pmod{2} \\ p_3 = m_1 + m_2 + m_4 \pmod{2} \end{cases}$$

Hamming-[7,4]-koden – Exempel



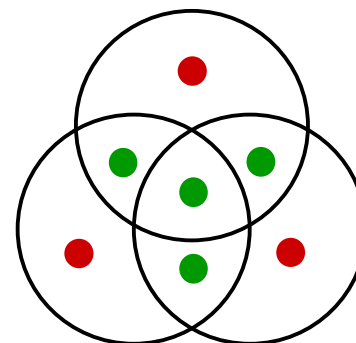
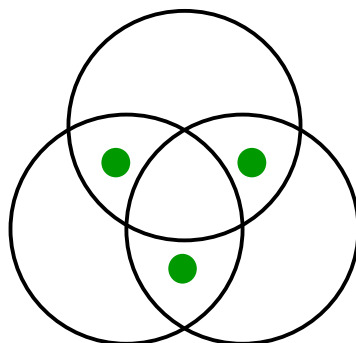
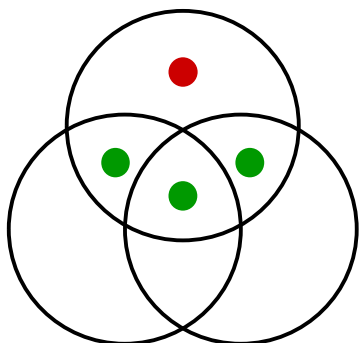
Resultat: Jämn paritet i den övre cirkeln, udda paritet i de andra två cirkelarna. Endast en position kan förklara det – det faktiska felet.

Hamming-[7,4]-koden – Fler exempel



Information

Jämn paritet i varje cirkel.



Förmåga att rätta och detektera fel

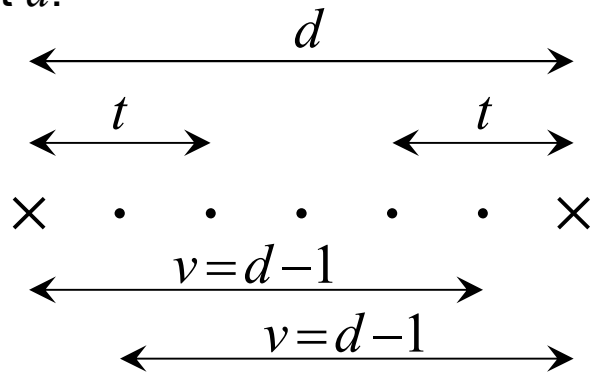
Felrättningsförmåga: $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

Feldetekteringsförmåga: $v = d - 1$

Koden kan rätta varje w -bitars fel om $w \leq t$.

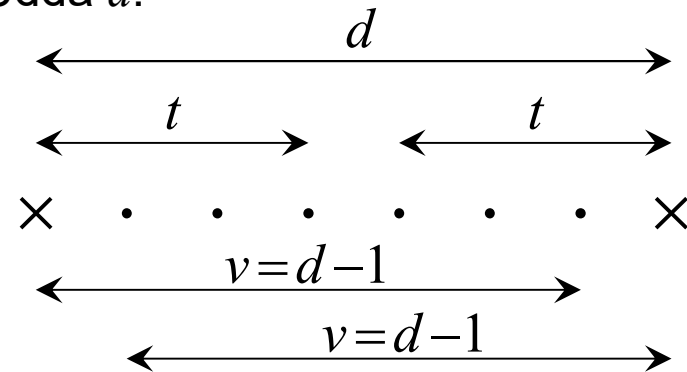
Koden kan detektera varje w -bitars fel om $w \leq v$.

Jämnt d :



$$t = \frac{d-2}{2}$$

Udda d :



$$t = \frac{d-1}{2}$$

Kodparametrar

Längd (# bitar i ett kodord):	N
Dimension (# informationsbitar):	K
Storlek (# kodord):	$M = 2^K$
Minavstånd (minsta avstånd i koden):	d
Takt (informationsbit per kodordsbit):	$R = K/N$

Kan visas: $P_e \sim p^{\lfloor d/2 \rfloor}$

Vi vill därför ha stort d .

Kan också visas: $N - K \geq d - 1$

Behöver stort N .

Fixerad takt kräver stort K .

Därmed väldigt stort M .

Jämförelse Hammingkod vs repetitionskod

Hamming-(7,4):

$$d = 3 \qquad P_e \sim p^{\lceil d/2 \rceil} = p^2 \qquad R = 4/7 \approx 0,57$$

Använder 7 bitar för att representera 4 informationsbitar.

Repetitionskod med samma minavstånd (motsvarande P_e):

$$N = d = 3 \qquad P_e \sim p^{\lceil d/2 \rceil} = p^2 \qquad R = 1/3 \approx 0,33$$

Använder $4 \cdot 3 = 12$ bitar för att representera 4 informationsbitar.

Exempel på en kod – Takt $R = \log_2(M)/N$

$$\begin{array}{l}
 M \\
 \text{(number of} \\
 \text{codewords)}
 \end{array}
 \left\{ \begin{array}{ll}
 000000000000000000000000000000 \dots 00000 & (X_1) \\
 000000000000000000000000000000 \dots 00100 & (X_2) \\
 000000000000000000000000000000 \dots 01001 & (X_3) \\
 \vdots & \vdots \\
 00010010010000100000000011 \dots 00101 & \\
 0001111000000001011110010 \dots 01000 & \\
 111111001111110011111100 \dots 11001 & (X_M)
 \end{array} \right.$$

$\underbrace{\hspace{15em}}$
 N (number of binary digits per codeword)

Figur 6.2 ur kursboken

Kanalkodningssatsen (för diskreta kanaler)

– slarvig formulering

För varje diskret kanal finns det ett C , $0 \leq C$, sådan att det går att kommunicera med godtyckligt låg felsannolikhet med någon kod med takt R för varje $R < C$. C kallas kanalens kapacitet.

Man kan också visa:

Om vi försöker kommunicera med takt $R > C$, så är vi garanterade att få en nollskild felsannolikhet. Det går också att ge en explicit undre gräns för denna felsannolikhet.

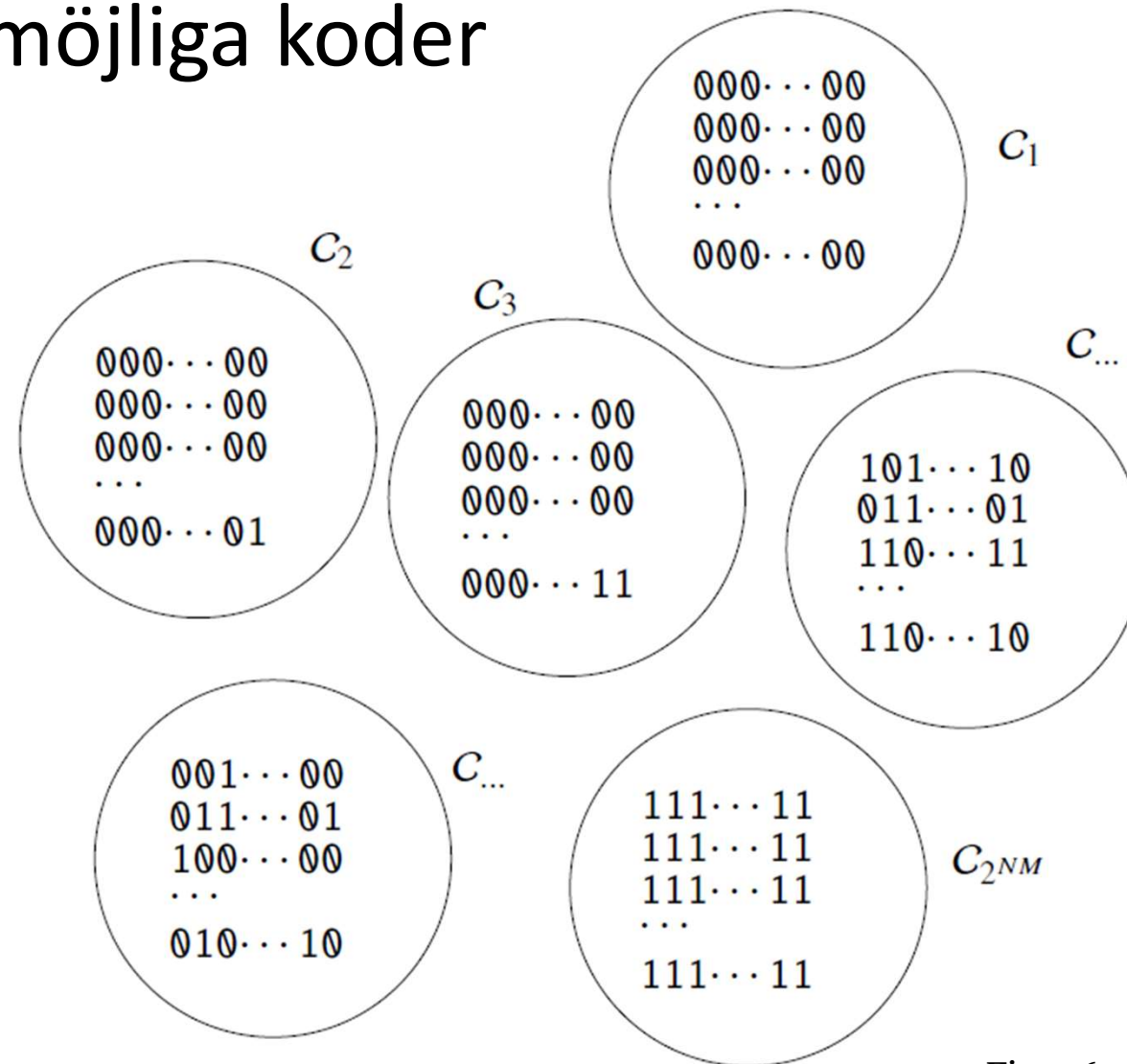
Eksempel på en kod – Takt $R = \log_2(M)/N$

$$M \begin{cases} 000000000000000000000000000000\ldots & 000000 & (X_1) \\ 000000000000000000000000000000\ldots & 00100 & (X_2) \\ 000000000000000000000000000000100\ldots & 01001 & (X_3) \\ \vdots & \vdots & \\ 00010010010000100000000011\ldots & 00101 & \\ 000111100000001011110010\ldots & 01000 & \\ 111111001111110011111100\ldots & 11001 & (X_M) \end{cases}$$

N (antal bitar per kodord)

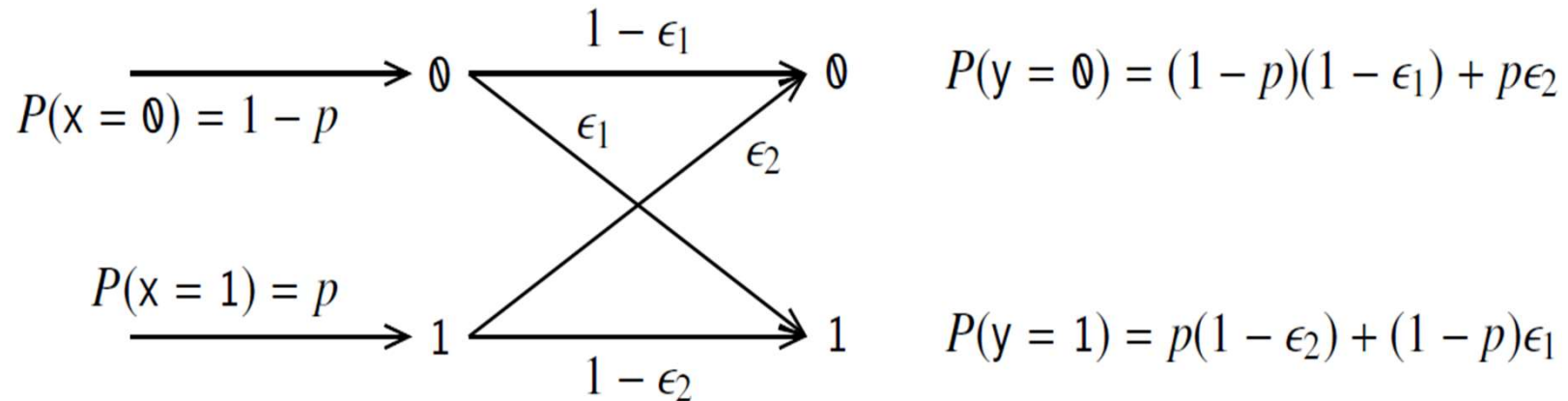
Motsvarar figur 6.2 ur kursboken

Alla möjliga koder



Figur 6.15 ur kursboken

Binär källa och binär kanal



Figur 6.5 ur kursboken

Antal typiska insignaler:

$$\binom{N}{pN} \approx 2^{N \cdot H_2(p)} = 2^{N \cdot H(x)}$$

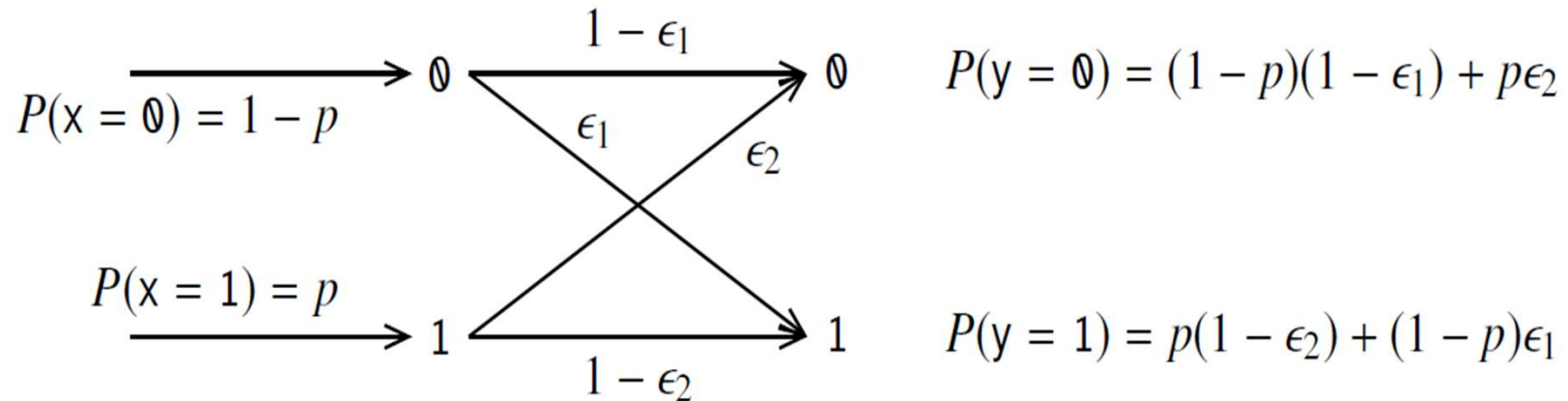
Antal typiska utsignaler för de bitar där insignalen är 0:

$$\binom{(1-p)N}{\epsilon_1(1-p)N} \approx 2^{(1-p)N \cdot H_2(\epsilon_1)}$$

Antal typiska utsignaler för de bitar där insignalen är 1:

$$\binom{pN}{\epsilon_2 pN} \approx 2^{pN \cdot H_2(\epsilon_2)}$$

Binär källa och binär kanal



Figur 6.5 ur kursboken

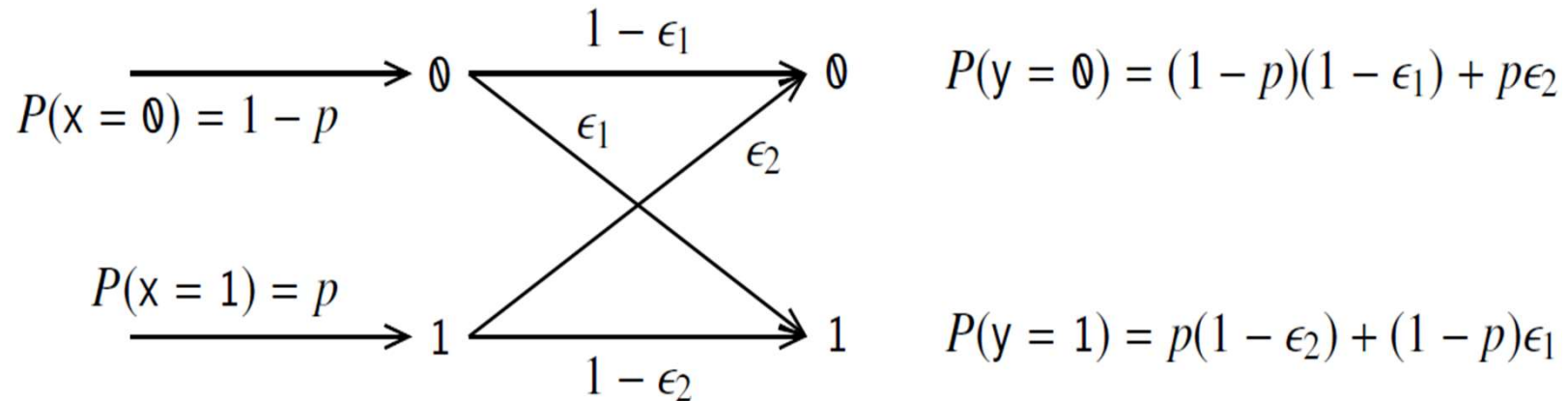
Typiska för insignal 0: $\binom{(1-p)N}{\epsilon_1(1-p)N} \approx 2^{(1-p)N \cdot H_2(\epsilon_1)}$

Typiska för insignal 1: $\binom{pN}{\epsilon_2 pN} \approx 2^{pN \cdot H_2(\epsilon_2)}$

Antal typiska utsignaler för en typisk insignal:

$$\binom{(1-p)N}{\epsilon_1(1-p)N} \binom{pN}{\epsilon_2 pN} \approx 2^{N \cdot ((1-p)H_2(\epsilon_1) + p \cdot H_2(\epsilon_2))}$$

Betingad entropi



Figur 6.5 ur kursboken

Entropi, betingad på ett utfall:

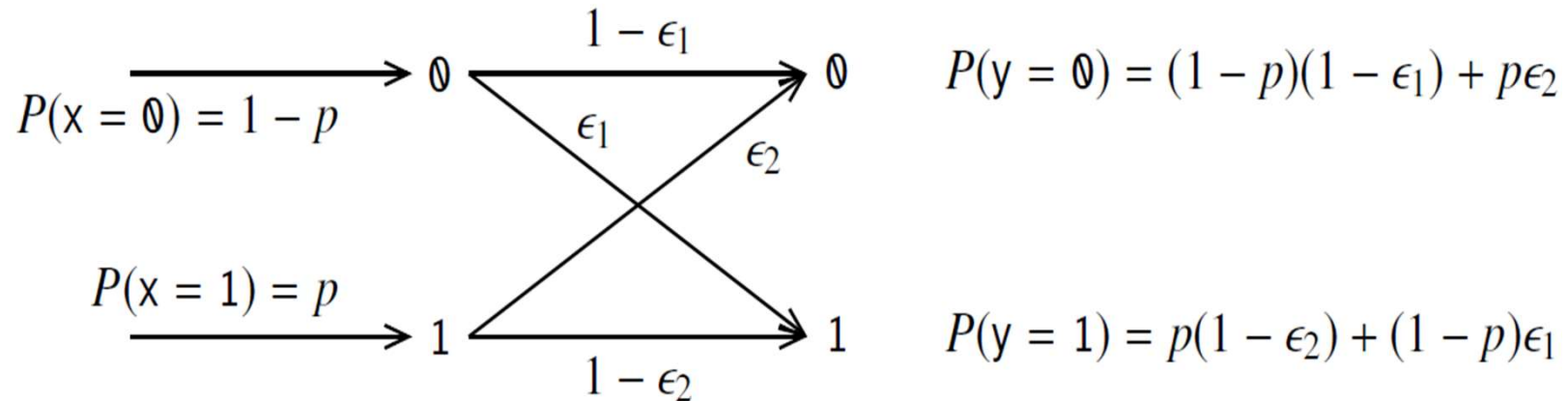
$$H(y|x = 0) = - \sum_{b=0}^1 P(y = b|x = 0) \log_2(P(y = b|x = 0)) = H_2(\epsilon_1)$$

$$H(y|x = 1) = - \sum_{b=0}^1 P(y = b|x = 1) \log_2(P(y = b|x = 1)) = H_2(\epsilon_2)$$

Betingad entropi, medelvärde av dessa map. x :

$$H(y|x) = \sum_{b=0}^1 P(x = b) H(y|x = b) = (1 - p)H_2(\epsilon_1) + p \cdot H_2(\epsilon_2)$$

Binär källa och binär kanal



Figur 6.5 ur kursboken

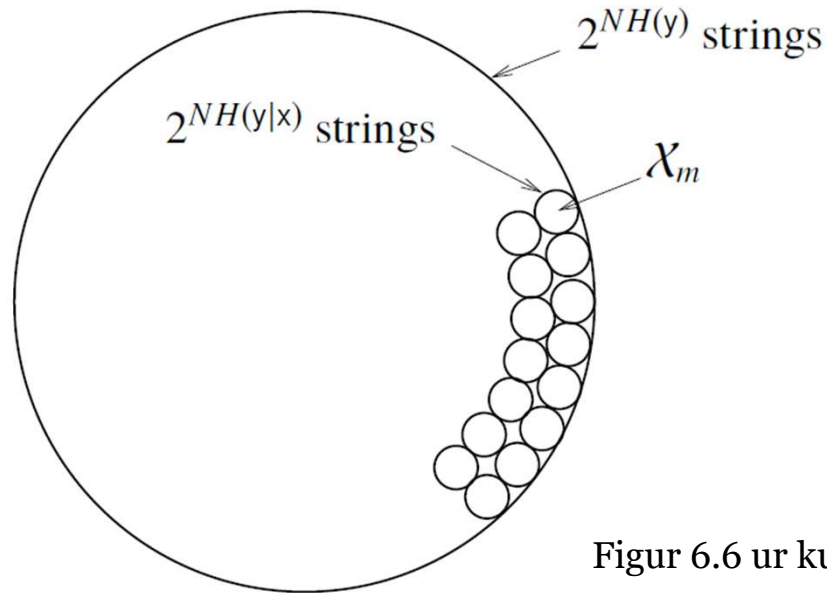
Antal typiska utsignaler för en typisk insignal:

$$\binom{(1-p)N}{\epsilon_1(1-p)N} \binom{pN}{\epsilon_2 p N} \approx 2^{N \cdot H(y|x)}$$

Totalt antal typiska utsignaler:

$$\binom{N}{((1 - \epsilon_2)p + \epsilon_1(1 - p))N} \approx 2^{N \cdot H(y)}$$

Packa mängder av typiska utsekvenser



Figur 6.6 ur kursboken

Ömsesidig information: $I(y; x) = H(y) - H(y|x)$

Vi har plats för
$$\frac{2^{N \cdot H(y)}}{2^{N \cdot H(y|x)}} = 2^{N \cdot I(y; x)}$$

disjunkta mängder
av storlek

$$2^{N \cdot H(y|x)}$$

bland dessa

$$2^{N \cdot H(y)}$$

typiska utsekvenser.

Tänkbar kod: Välj $2^{N \cdot I(y; x)}$ typiska insekvenser som kodord, så att motsvarande mängder av typiska utsekvenser väsentligen inte överlappar. Koden har $N \cdot I(y; x)$ info-bitar, och därmed takt $R = \frac{N \cdot I(y; x)}{N} = I(y; x)$.

Kanalkodningssatsen (för diskreta kanaler)

Ömsesidig information:

$$\begin{aligned} I(y; x) &= H(y) - H(y|x) \\ &= H_2((1 - \epsilon_2)p + \epsilon_1(1 - p)) - (1 - p)H_2(\epsilon_1) - pH_2(\epsilon_2) \end{aligned}$$

Kanalens kapacitet:

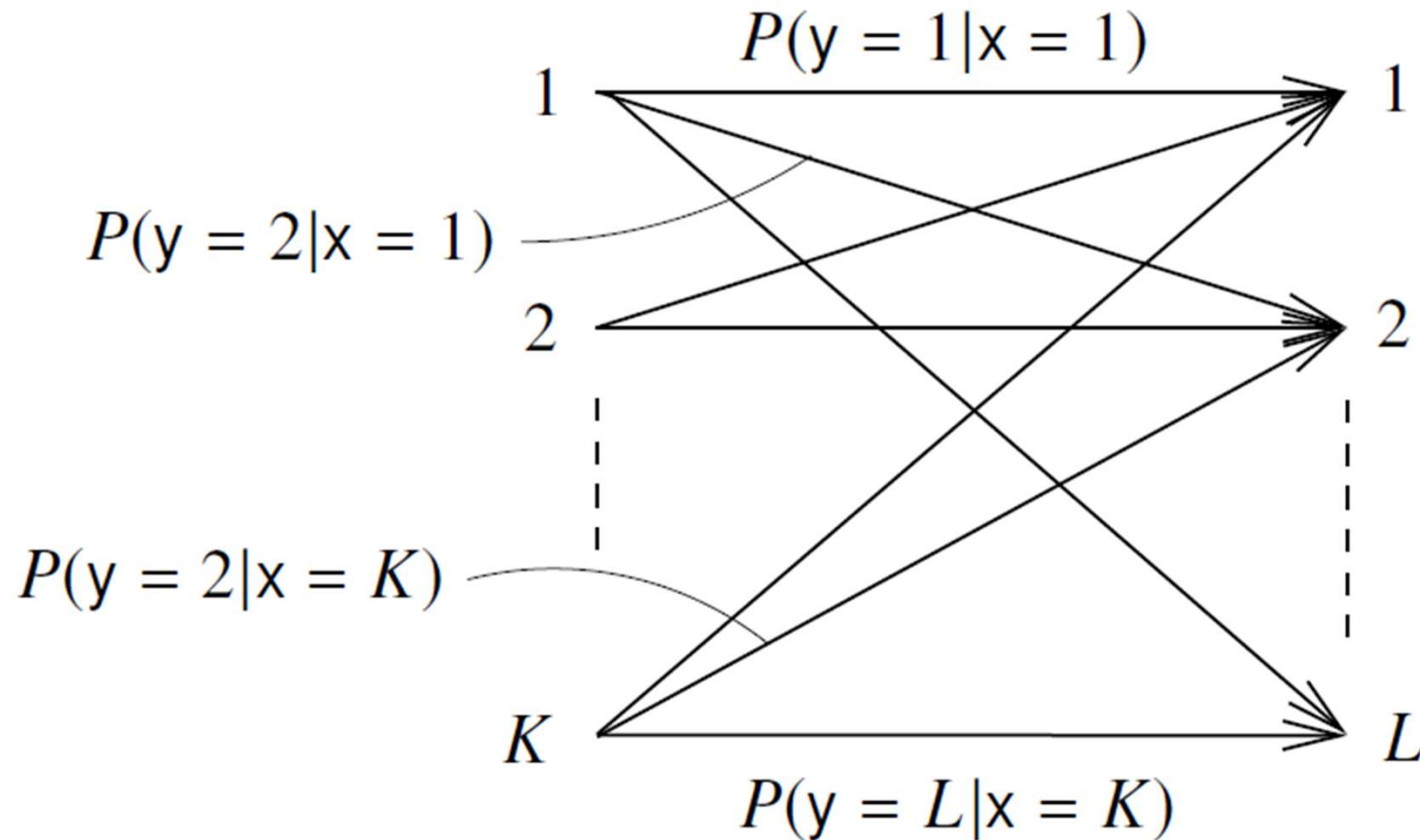
$$C = \max_p I(y; x)$$

Kanalkodningssatsen:

För en diskret kanal och för givna konstanter $\delta > 0$ och $\gamma > 0$ så finns det en kodordslängd N och en kod med kodord av längd N som har takt $C - \delta$, och som gör det möjligt att kommunicera med felsannolikhet $P_e < \gamma$.

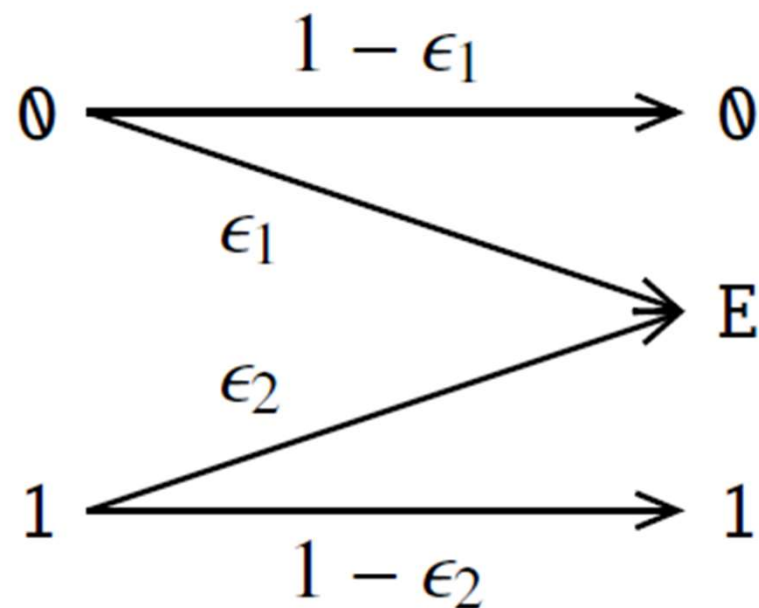
Men! Satsen säger ingenting om hur en sådan kod kan se ut.

Diskret minnesfri kanal



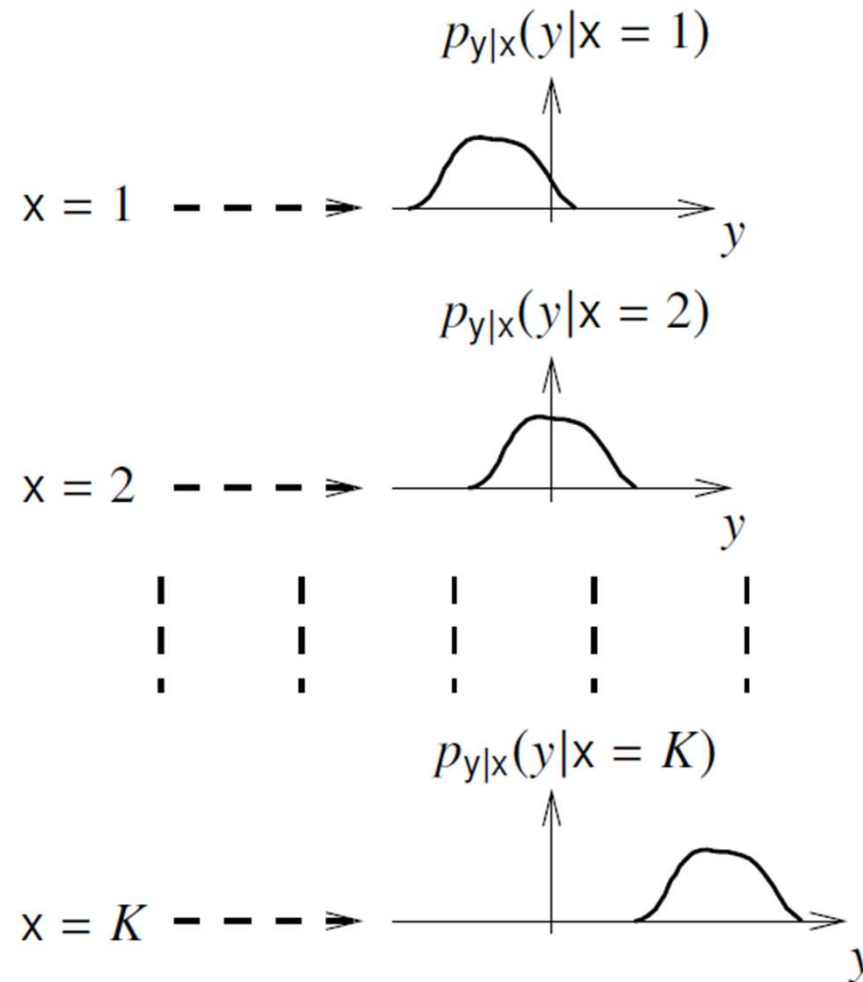
Figur 6.9 ur kursboken

Binär suddningskanal



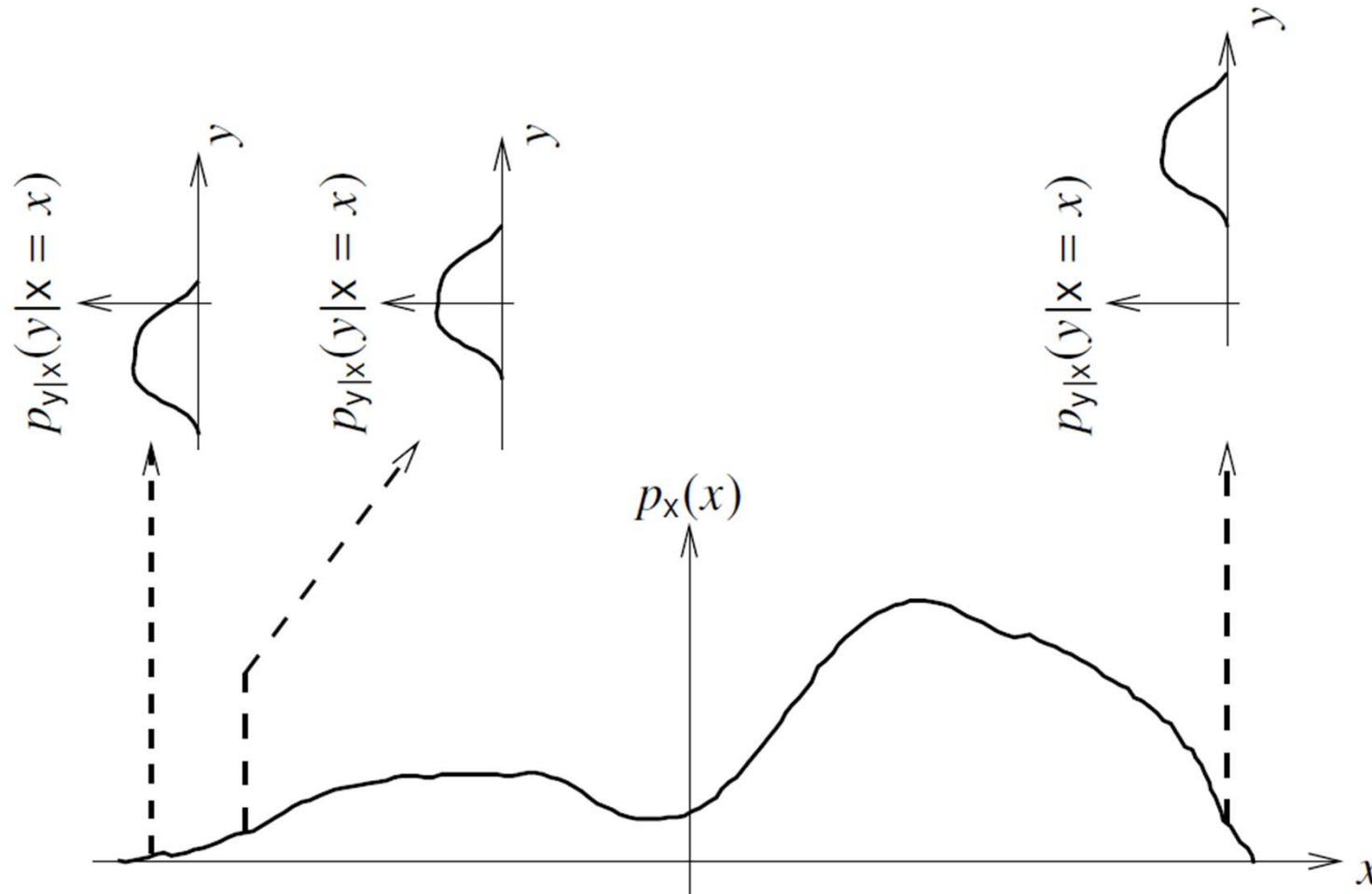
Figur 6.10 ur kursboken

Kanal som är diskret in och kontinuerlig ut



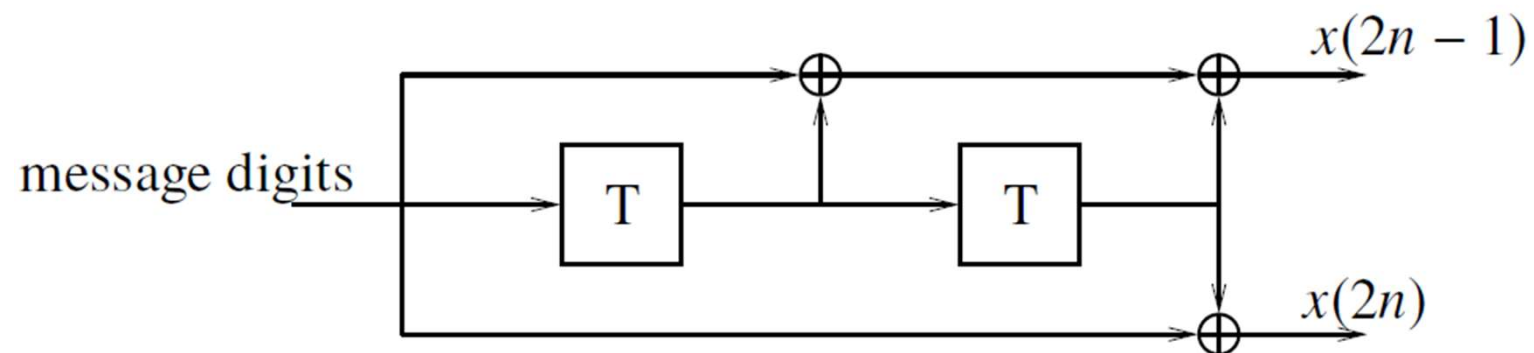
Figur 7.11 ur kursboken

Kanal som är kontinuerlig in och kontinuerlig ut



Figur 7.12 ur kursboken

En enkel faltningskod



Figur 7.7 ur kursboken

Mikael Olofsson
ISY/CommSys

www.liu.se